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.
- The 1240AG series access point uses externally connected antennas for each band instead of built-in antennas.
- The 1300 series outdoor access point/bridge uses an integrated antenna and can be configured to use external, dual-diversity antennas.

This chapter provides information on the following topics:

- Features, page 1-2
- Management Options, page 1-9
- Roaming Client Devices, page 1-9
- Network Configuration Examples, page 1-10
- How to Log-in to an Access Point, page 1-13

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

Table 1-1 lists the new features in Cisco IOS Release 12.3(8)JA and the supported platforms.

Table 1-1 New Cisco IOS Software Features

Feature	Cisco Aironet 1100 Series Access Point	Cisco Aironet 1130AG Series Access Point	Cisco Aironet 1200 Series Access Point	Cisco Aironet 1230AG Series Access Point	Cisco Aironet 1240AG Series Access Point	Cisco Aironet 1300 Series Access Point/Bridge	Cisco Aironet 1400 Series Wireless Bridge
Wireless IDS Management Frame Protection (32 Mb platforms only)	–	x	–	–	x	–	–
IBNS 802.1X Supplicant (EAP-FAST, EAP-TLS) (32 Mb platforms only)	–	x	–	–	x	x	x
Packet of Disconnect	x	x	x	x	x	x	–
Wi-Fi Multimedia TSPEC Call Admission Control (CAC)	x	x	x	x	x	x	–
Gratuitous Probe Response for Dual-Mode Phones	–	x	x	x	x	–	–
Unscheduled Automatic Power Save Delivery (U-APSD)	x	x	x	x	x	x	–
VoIP Packet Handling	x	x	x	x	x	x	–
VoWLAN Metrics	x	x	x	x	x	x	–
FIPS 140-2 Level 2 Certification	x	x	x	x	x	x	–
Manual Configuration of Channels on W52/W53 for Dynamic Frequency Selection (DFS)	–	x	–	x	x	–	–
New features for Cisco WLSM Software Release Image Version 2.1, a deployment release supporting the Cisco Catalyst® 6500 Series Wireless LAN Services Module (WLSM)	x	x	x	x	x	x	–

WLSM Support for Access Points and Workgroup Bridges Repeater Mode

Cisco Aironet access points, including the 1300 series access point/bridge in access point mode, support the following features in WLSM Version 2.1 Release:

- Increased Access Point Scalability—Memory and software improvements increase scalability of Cisco Catalyst 6500 series WLSM from 300 to 600 access points per WLSM.
- RADIUS-Based Mobility Group Assignment—This feature provides the ability to assign wireless users to different mobility groups based on user credentials stored in the RADIUS server.
- Resilient Tunnel Recovery—Automatic recovery of mobility tunnels after WLSM failure with zero client interruption.
- Active and Standby WLSMs Per Chassis—Active and standby WLSMs in a common Cisco Catalyst 6500 series chassis provide the ability for administrators to deploy a second WLSM in a given chassis for failover support. One WSLM serves in an active role, the other WLSM serves in a standby role at any given time.
- IGMP Snooping-Based Multicast—This feature provides the ability to deliver multicast traffic to wireless clients across the Native VLAN of an access point without requiring the need for trunking or multiple multicast enabled networks on the first hop layer 3 router. With this feature, the access point is able to deliver multicast to wireless clients with dynamically assigned mobility groups.

  Note No configuration is required. By default, IGMP snooping is enabled on an access point. As long as you don't disable IGMP snooping, this feature works.

  Note If there is no multicast router for processing IGMP query and response from the host, it is mandatory that **no ip igmp snooping** be configured on the access point. When IGMP snooping is enabled, all multicast group traffic must send IGMP query and response. If an IGMP query or response is not detected, all multicast traffic for that group is dropped.

- Support for 240 Mobility Groups—This feature increases the number of mobility groups that may be assigned per WLSM. Mobility groups may be dynamically assigned based upon user authentication or posture validation. With 240 mobility groups supported per WLSM, each mobility domain may be smaller, thus reducing the subnet size required for each mobility group.
- Enhanced Cisco Catalyst WLSM MIB Support—MIB support (CISCO-WDS-INFO-MIB) introduces the capability of querying the Cisco Catalyst 6500 series WLSM for client, access point, and WLSM configuration and statistics. This information may be used to query the WLSM for client association, roaming, and performance data via the CiscoWorks Wireless LAN Solution Engine (WLSE) or custom Simple Network Management Protocol (SNMP) applications.

Wireless IDS Management Frame Protection (32 MB platforms only)

Typically, wireless LANs use unprotected management frames that are not authenticated, encrypted, or signed. To protect the integrity of IEEE 802.11 management frames, the management frame protection feature lets you insert a signature into these frames. This signature allows network devices like client systems and access points to determine that the frames came from an authorized source. For more information about protecting management frames, refer to the "Configuring Management Frame Protection" section on page 12-25.

IBNS 802.1x Supplicant (EAP-FAST and EAP-TLS)

802.1x is a standardized framework defined by the IEEE to provide port-based network access. 802.1x authenticates network clients using information unique to the client and with credentials known only to the client. This service is called *port-level authentication* because, for security reasons, it is offered to a single endpoint for a given physical port. 802.1x now supports both EAP-TLS and EAP-FAST.

The supplicant refers to the client software that supports the 802.1x and EAP protocols. As access points are being placed in public places, they are susceptible to being unplugged and their network connection being used by an outsider. In addition, access point repeaters need to authenticate to the root access point exactly the same way clients do. The 802.1x supplicant provides a secure method for accomplishing this authentication.

The supplicant is not supported on 350, 1100, and 1200 series access points

Unscheduled Automatic Power Save Delivery

U-APSD is a new QoS facility defined in IEEE 802.11e that extends battery life of mobile clients. In addition to extending battery life, the feature reduces the latency of traffic flow delivered over the wireless media.

Because APSD does not require the client station to poll each individual packet buffered at the access point, U-APSD allows delivery of multiple downlink packets by sending a single uplink trigger packet.

Unscheduled Automatic Power Save Delivery (UPSD) is enabled when Wi-Fi Multimedia (WMM) is enabled on the radio interface.

Note In Cisco IOS Software Release 12.3(8)JA, UPSD supports only the access point role. Repeaters, bridges, and workgroup bridge roles are not supported.

Wi-Fi Multimedia TSPEC Call Admission Control

This quality of service (QoS) feature helps ensure predictable voice quality. Call Admission Control (CAC) keeps the number of active voice calls from exceeding the configured limits of an access point. This helps ensure that the voice quality of existing calls is maintained. Special *roaming reserve* ensures a good user experience as a phone roams from one access point to another. For more information about configuring CAC, refer to the "Configuring Call Admission Control" section on page 15-13.

Gratuitous Probe Response for Dual-Mode Phones

Dual-mode phones that support cellular and WLAN modes of operation consume significant battery power in order to detect the presence of a WLAN. The high battery consumption is related to the amount of time the phone must wait while passively listening for beacons on each channel. Since beacon intervals are typically on the order of hundreds of milliseconds, these scans require the phone's receiver to be enabled for at least a typical beacon interval on each channel. The Gratuitious Probe Response (GPR) feature aids in conserving the phone's battery power by providing a high rate packet on the order of tens of milliseconds. The GPR packet is transmitted from the access point at a predefined time interval.

VoIP Packet Handling

This feature improves the quality of VoIP packet handling on access points by enhancing 802.11 MAC behavior for lower latency. It provides enhanced retry and rate shifting algorithms that reduce congestion on wireless networks.

VoWLAN Metrics

This feature provides diagnostic information pertinent to VoIP performance on the WLAN and aids in determining whether problems are being introduced by the WLAN or the wired network. The metrics provides measurements of jitter and packet loss on a location, access point, or client basis. It also provides metrics on client roaming and roam latency. The access point will report, or be polled, on a configurable and periodic basis. Reports generated by the access point are sent to the WLSE or a system logger.

FIPS 140-2 Level 2 Certification

The Federal Information Processing Standards (FIPS) stipulate the security requirements for cryptographic modules. FIPS 140-2, issued in May 2001, is recognized by the United States and Canadian governments. This release provides level 2 FIPS certification for Cisco Aironet 1100, 1130, and 1200 Series Access Points and the Cisco Aironet 1300 Series Outdoor Access Point/Bridge.

FIPS requires no configuration. The access point performs a FIPS power on self test (POST) at the beginning of the boot process. If any part of the test fails, the access point stops the POST and displays a failure message. The radio interfaces on the access point are shut down.

Packet of Disconnect

Packet of Disconnect (PoD) provides the ability to terminate a user session from a RADIUS server. The PoD protocol is already supported within Cisco IOS and has been implemented on voice and dial access servers, as well as for GPRS. This feature allows the PoD protocol to be used to terminate 802.11 sessions connected to an access point.

Manual Configuration of Channels on W52/W53 for DFS

In Japan, you can now manually select a channel for DFS-enabled 5-GHz radios if a radar has not been detected on it for the previous 30 minutes.

Existing Features

- 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 DFS—This feature allows Cisco Aironet access points configured at the factory for use in Europe, Singapore, and Japan 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.
- 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.
- 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 introduced support for the Cisco Aironet 1200 series access point IEEE 802.11a radio part numbers AIR-RM21A and AIR-RM22A. These 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.
- Support for the Cisco Aironet 1240AG Series Access Point—This release fully supports the Cisco Aironet 1240AG Series Access Point.
- Access Point Link Role Flexibility—This feature provides bridge mode functionality support for access points having dual-band capability (1200, 1230, and 1240AG series).

Note The Access Point Link Role Flexibility is not supported on 350, 1100, and 1130AG series access points.

- QoS Basic Service Set (QBSS) support—This feature aligns Cisco QBSS implementation with the evolving 892.11e standard.
- AAA Authentication/Authorization Cache and Profile—This feature reduces the authentication load on RADIUS/TACACS servers caused when loading GUI pages by caching the authentication locally on the access point so only one authentication with the RADIUS/TACACS server is performed. The feature is supported only for administrative authentication on the access point. Other uses of this feature are not recommended and not supported.
- Secure Shell version 2 (SSHv2) support.
- Network Admission Control (NAC) L2 IEEE 802.1x extends NAC support to layer 2 switches and wireless access points. Combining it with 802.1x provides a unified authentication and posture validation mechanism at the layer 2 network edge. This helps protect the network from attack by machines with insufficient antivirus posture. Performing posture validation at the edge maximizes the portion of the network which is protected and allows posture validation to be performed with a VLAN.

  If the access point is configured to support EAP authentication of clients and VLAN override is configured on the RADIUS server, no additional configuration of the access point is required to support NAC.

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 3, "Using the Command-Line Interface," provides a detailed description of the CLI.
- A web-browser interface, which you use through a Web browser. Chapter 2, "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 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.

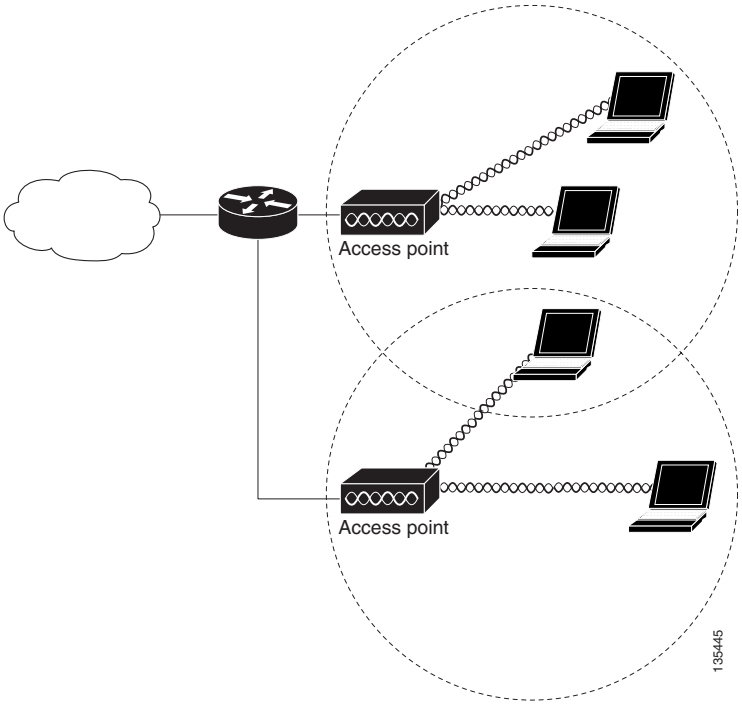
Network Configuration Examples

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. Access points can also be configured as repeater access points, bridges, and workgroup bridges. These roles require specific configurations.

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 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



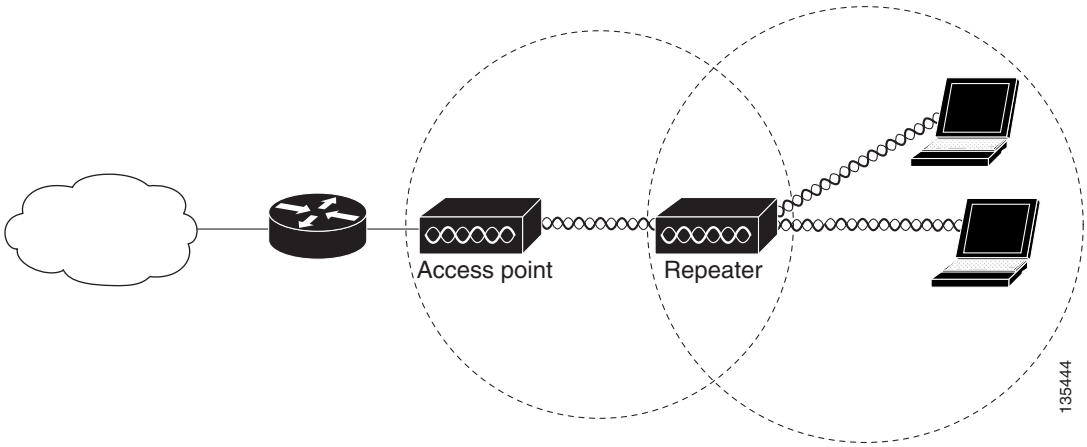
Repeater Access Point

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



Bridges

The 1200 and 1240AG access points can be configured as root or non-root bridges. In this role, an access point establishes a wireless link with a non-root bridge. Traffic is passed over the link to the wired LAN. Access points in root and non-root bridge roles can be configured to accept associations from clients. Figure 1-3 shows an access point configured as a root bridge with clients. Figure 1-4 shows two access points configured as a root and non-root bridge, both accepting client associations. Consult the "Configuring the Role in Radio Network" section on page 6-2 for instructions on setting up a 1200 or 1240AG series access point as a bridge.

Figure 1-3 Access Point as a Root Bridge with Clients

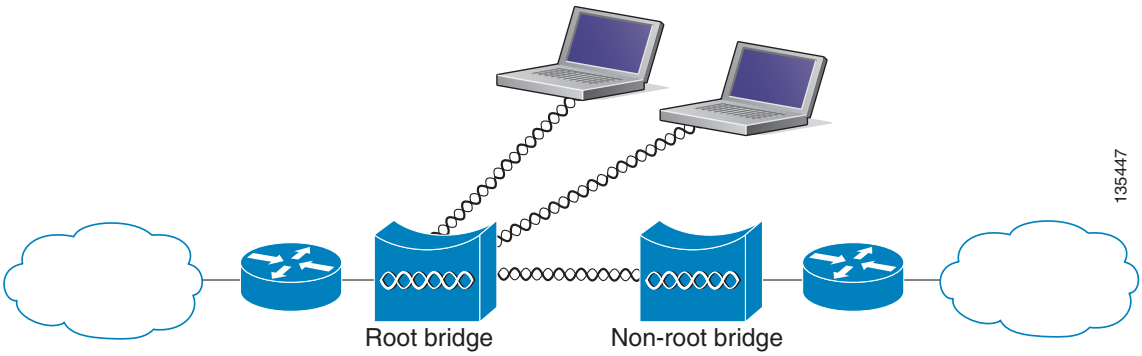
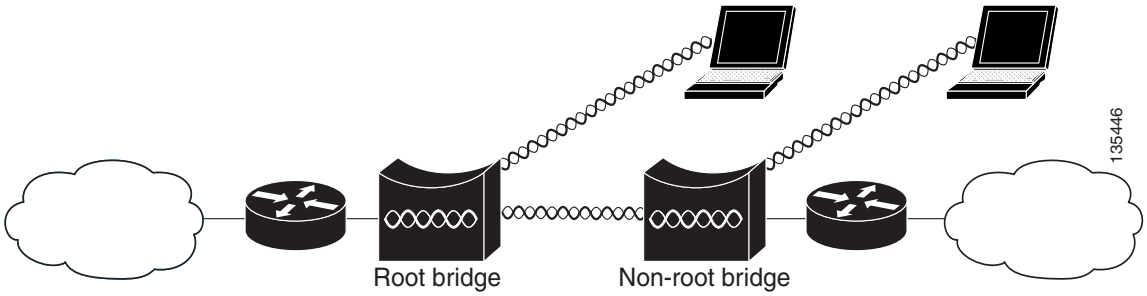


Figure 1-4 Access Points as Root and Non-root Bridges with Clients



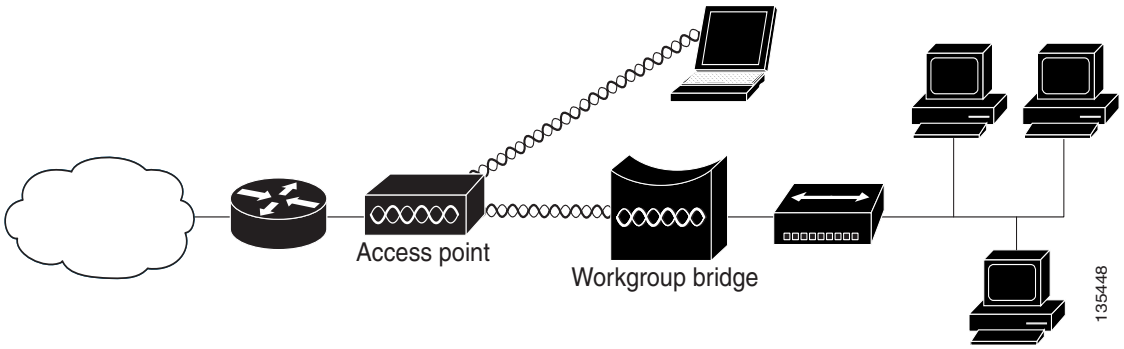
Workgroup Bridge

You can configure access points as workgroup bridges. In workgroup bridge mode, the unit associates to another access point as a client and provides a network connection for the devices connected to its Ethernet port. For example, if you need to provide wireless connectivity for a group of network printers, you can connect the printers to a hub or to a switch, connect the hub or switch to the access point Ethernet port, and configure the access point as a workgroup bridge. The workgroup bridge associates to an access point on your network.

If your access point has two radios, either the 2.4-GHz radio or the 5-GHz radio can function in workgroup bridge mode. When you configure one radio interface as a workgroup bridge, the other radio interface is automatically disabled.

Figure 1-5 shows an access point configured as a workgroup bridge. Consult the "Understanding Workgroup Bridge Mode" section on page 19-12 and the "Configuring Workgroup Bridge Mode" section on page 19-14 for information on configuring your access point as a workgroup bridge.

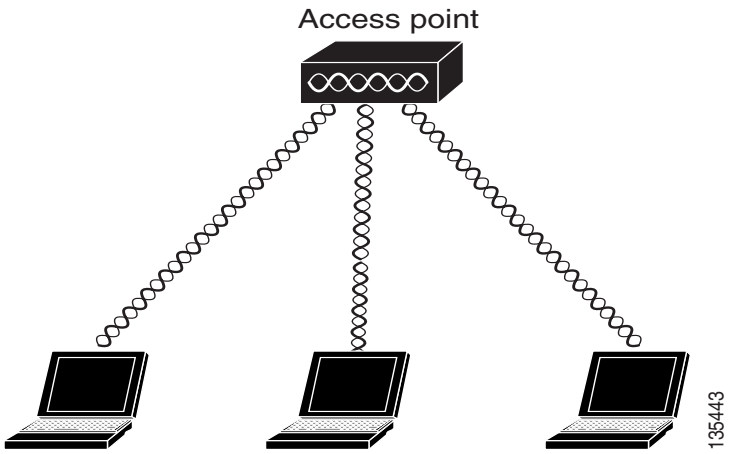
Figure 1-5 Access Point as a Workgroup Bridge



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

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



How to Log-in to an Access Point

You can log-in to an access point by using one of these methods:

- Using the local console port—see the "Using the Local Console Port" section on page 1-13.
- Using a browser—see the "Using a Browser" section on page 1-14.
- Using Telnet—see the "Using Telnet" section on page 1-16.

Using the Local Console Port

The 1130, 1200, 1240, and 1250 series access points have a console port that can be used to log-in to the access point locally.

Note The 1100 and 1300 series access points do not have a console port. On the 1130 access point, you must open the access point cover to access the console port.

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its console port using a DB-9 to RJ-45 serial cable. The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. To order a serial cable, browse to http://www.cisco.com/go/marketplace.

Follow these steps to open the console port and the access point CLI:

Step 1 Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on your PC.

Step 2 Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Note If no flow control does not work, try Xon/Xoff flow control.

Step 3 Connect power to the access point. The access point displays the power up configuration sequence.

Step 4 When the power up sequence ends, press **Enter** and the access point CLI command prompt displays, such as AP>.

Step 5 When prompted, enter the username and password for the access point.

Note The access point default username is Cisco and the default password is Cisco.

You can now use the access point CLI to configure or revise the access point settings. For additional information on using the access point CLI, See the "Using the Command-Line Interface" section on page 3-1.

Note When your configuration changes are completed, you must remove the serial cable from the access point.

Using a Browser

You can use a Web browser and a Category 5 Ethernet cable to log-in to your access point locally or remotely. To connect to an access point locally, you use the Ethernet port on the access point. On the 1300 series access point, the Ethernet port is located on the power injector.

Note You do not need a special crossover cable to connect your PC to the access point; you can use either a straight-through cable or a crossover cable.

For local access to the 1100 series access point, if it is configured with default values and it does not receive an IP address from a DHCP server, it defaults to IP address 10.0.0.1 for five minutes. During that five minutes, you can browse to that IP address to configure the unit. If after five minutes the unit has not been reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from the DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the five-minute window for browsing to the access point at 10.0.0.1, you can power-cycle the access point to repeat the process.

Follow these steps to connect to the access point using your browser:

Step 1 For local access, follow these steps:

a. Make sure that the PC is configured with an IP address within the same subnet as the access point, such as 10.0.0.2 to 10.0.0.10 for an access point with an IP address of 10.0.0.1.

b. Connect a Category 5 Ethernet cable from your PC to the access point.

Note On the 1300 series access point, the Ethernet port is located on the power injector. On the 1130 series access point, you need to open the access point cover to access the Ethernet connector.

Step 2 For remote network access, follow these steps:

a. Make sure that your PC is configured to receive an IP address from a DHCP server.

b. Connect a Category 5 Ethernet cable from your PC to the network.

Step 3 PC Power up the access point.

Step 4 Turn on your PC and activate the Web browser.

Step 5 Enter the access point's IP address in the browser Location field (Netscape Communicator) or Address field (Internet Explorer) and press **Enter**.

Step 6 When prompted, enter the username and password for the access point and click **OK** .

Note The access point default username is Cisco and the default password is Cisco.

The Summary Status page appears to enable you to configure or revise the access point settings.

Step 7 After configuring the access point using the local Ethernet port, remove your Ethernet cable from the access point or power injector and connect the access point to your wired LAN.

Note When you connect your PC to the access point or reconnect your PC to the wired LAN, you might need to release and renew the IP address on the PC. On most PCs, you can perform a release and renew by rebooting your PC or by entering **ipconfig /release** and **ipconfig /renew** commands in a command prompt window. Consult your PC operating instructions for detailed instructions.

Note On the 1300 series access point, communication takes place between the power injector and the access point using Ethernet Port 0. Do not change any of the Ethernet Port 0 settings.

For additional information, see the Using the "Using the Web-Browser Interface" section on page 2-1.

Using Telnet

To use Telnet to log-on to an access point connected to the wired LAN, follow these instructions:

Step 1 Make sure that your PC is configured to receive an IP address from a DHCP server and is connected to the wired LAN.

Step 2 Click **Start** > **Run** > **Telnet** and click ***OK*** .

Step 3 In the Telnet window, type **open** and the IP address of the access point, for example, open 10.0.0.1. Press **Enter.**

Step 4 When prompted, enter the username for the access point and press **Enter**.

Note The access point default username is Cisco.

Step 5 When prompted, enter the password for the access point and press **Enter**. The access point CLI prompt appears, such as AP>.

Note The access point default password is Cisco.

You can now use CLI commands to configure or revise the access point settings.

For additional information, see the "Using the Command-Line Interface" section on page 3-1.