



CHAPTER 1

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 access points are Wi-Fi certified, 802.11a-compliant, 802.11b-compliant, and 802.11g-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 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 1130 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 1230 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 1240 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 1-4](#)
- [Roaming Client Devices, page 1-4](#)
- [Network Configuration Examples, page 1-4](#)

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.



Note

Cisco IOS Release 12.3(8)JEB is a maintenance release only. No new features are included in this release.

Features Introduced in This Release

Table 1-1 lists the new features in Cisco IOS Release 12.4(3g)JA and the supported platforms.

Table 1-1 New Cisco IOS Software Features for Cisco IOS Release 12.4(3g)JA

Feature	Cisco Aironet 1240 Series Access Points	Cisco Aironet 1300 Series Outdoor Access Point/Bridge	Cisco Aironet 1400 Series Wireless Bridge
Japan upgrade utility ¹	x	x	x
Multiple VLAN and rate limiting support for point-to-multipoint bridging	x	x	—
Universal workgroup bridge	x	x	—
Client MFP support	x	x	—
Regulatory changes for Taiwan	x	x	x

1. The utility also operates on 1130 series access points and 1200 series access points with RM21 and RM22A radios.

Japan Upgrade Utility

The Japanese government has changed their 5-GHz radio spectrum regulations to allow a field upgrade of 802.11a radios. Japan allows three different frequency sets organized into regulatory domains as shown in Table 1-2.

Table 1-2 Japan Frequency Sets

Frequency Set	Channel (Freq)	Channel (Freq)	Channel (Freq)	Channel (Freq)
J52	34 (5170 MHz)	38 (5190 MHz)	42 (5210 MHz)	46 (5230 MHz)
W52	36 (5180 MHz)	40 (5200 MHz)	44 (5220 MHz)	48 (5240 MHz)
W53	52 (5260 MHz)	56 (5280 MHz)	60 (5300 MHz)	64 (5320 MHz)

These frequency sets have 3 legal combinations in which Cisco has organized into regulatory domains:

- J regulatory domain = J52
- P regulatory domain = W52+W53

- U regulatory domain = W52

The upgrade utility allows users to migrate their 802.11a radios from J52 to W52. The utility operates on the following devices:

- 1130 series access points
- 1200 series access points with RM21 and RM22A radios
- 1240 series access points

Users must migrate all 802.11a radios in their wireless network from J52 to W52. There cannot be a mix of radios in the network operating in the J52 and W52 bands because of overlap.

See the [“Migrating to Japan W52 Domain” section on page 5-37](#) for more information about this utility.

Multiple VLAN and Rate Limiting Support for Point-to-Multipoint Bridging

This feature modifies the way point-to-multipoint bridging can be configured to operate on multiple VLANs with the ability to control traffic rates on each VLAN. The feature is available on 32 Mb access points configured as bridges (1240 series) and the 1300 series access point/bridge. The feature is not available on 16 Mb access points (1100, 1200, and 350 series)

In a typical scenario, multiple VLAN support permits users to set up point-to-multipoint bridge links with remote sites, with each remote site on a separate VLAN. This configuration provides the user to separate and control traffic to each site. Rate limiting ensures that no remote site consumes more than a specified amount of the entire link band width. Only uplink traffic can be controlled by the FastEthernet ingress ports of non-root bridges.

See the [“Configuring Multiple VLAN and Rate Limiting for Point-to-Multipoint Bridging” section on page 5-39](#) for more information on this feature.

Client MFP Support

Client MFP encrypts class 3 management frames sent between access points and CCXv5-capable client stations, so that both access point and client can take preventative action by dropping spoofed class 3 management frames (management frames passed between an access point and a client that are authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect class 3 Unicast management frames. The unicast cipher suite negotiated by the station in the (re)association request's Robust Security Network Information Element (RSNIE) is used to protect both unicast data and class 3 management frames. access points in workgroup bridge, repeater, and non-root bridge modes must negotiate either TKIP or AES-CCMP in order to use Client MFP.

See the [“Management Frame Protection” section on page 12-25](#) for more information on Client MFP support.

Regulatory Changes for Taiwan

In June 2006, the FCC finalized rules governing the use of frequencies in the 5.250 – 5.725 GHz range. Products using these frequencies must employ Dynamic Frequency Selection (DFS). With Cisco IOS Release 12.3(8)JA, FCC DFC compliance was enabled in the North American domain for 1130, 1200, and 1240 series access points.

Taiwan's regulatory agencies have elected to adhere to the United State's FCC regulations regarding DFS. This release supports DFS for the Taiwan (-T) regulatory domain. This also enables the use of additional channels in the 5.250 – 5.725 GHz band.

See the [“Dynamic Frequency Selection” section on page 6-17](#) for more information on DFS.

Universal Workgroup Bridge

This feature provides the means for Cisco access points configured as workgroup bridges (WGBs) to associate with non-Cisco access points. In addition, the feature provides the WGB with the ability to be continuously in World Mode.

See the “[Configuring the Role in Radio Network](#)” section on page 6-2 for more information on universal workgroup bridge configuration.

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 1, “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.

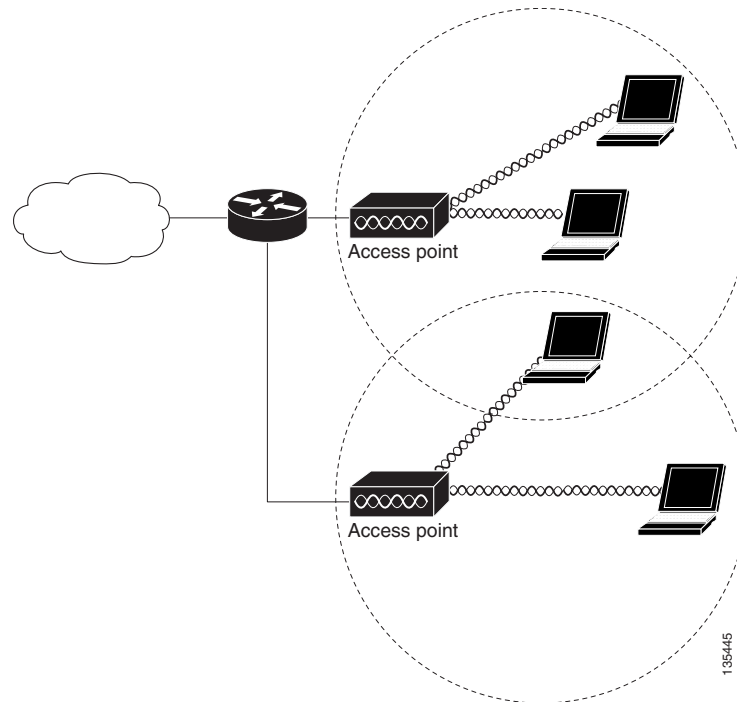
Network Configuration Examples

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



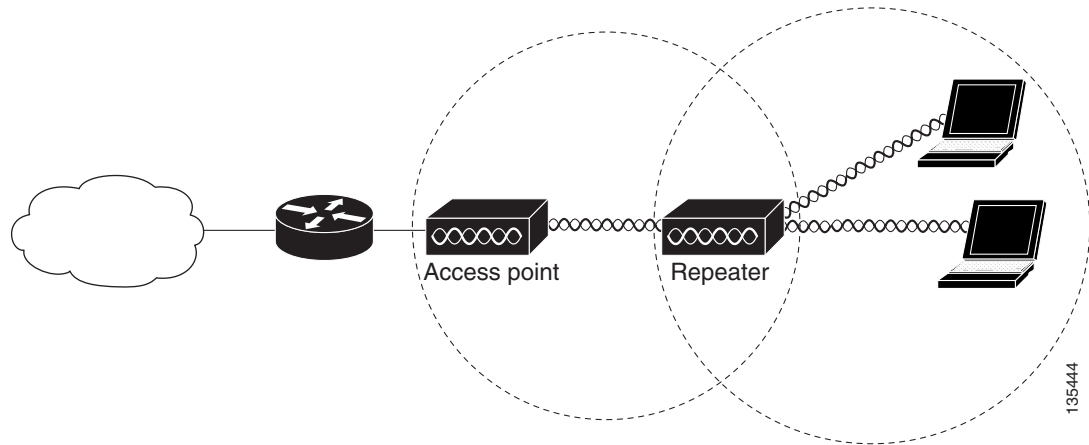
Repeater Access Point

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 1240 access points and the 1300 access point/bridge 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 an access point as a bridge.

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

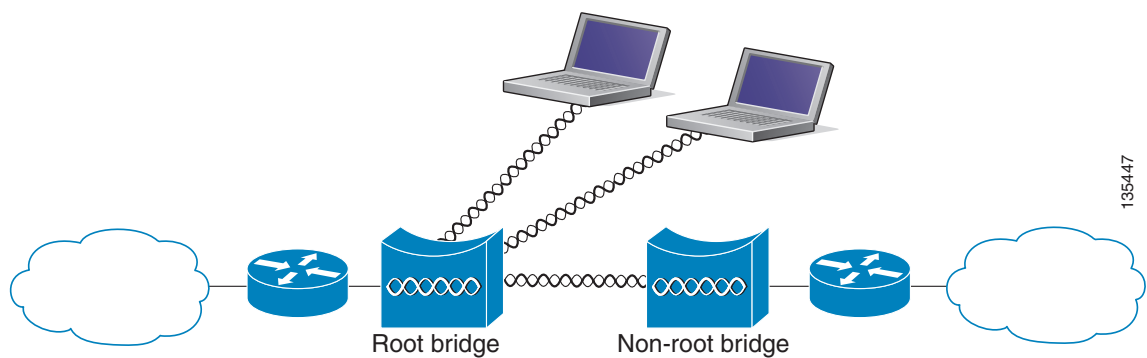
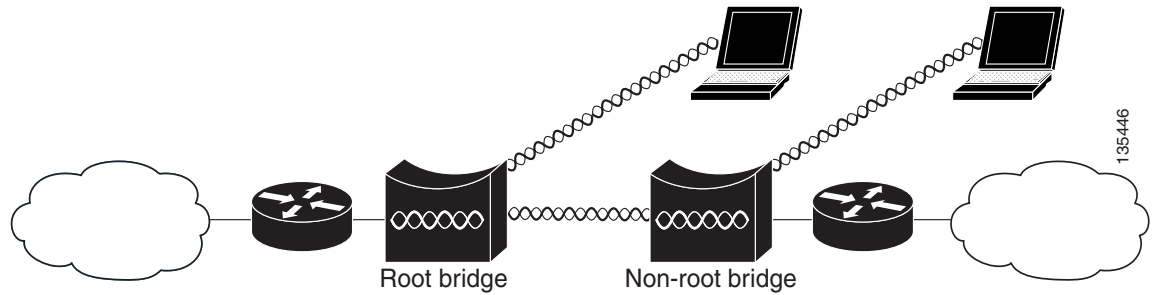


Figure 1-4 Access Points as Root and Non-root Bridges with Clients



When wireless bridges are used in a point-to-multipoint configuration the throughput is reduced depending on the number of non-root bridges that associate with the root bridge. The maximum throughput is about 25 Mbps in a point to point link. The addition of three bridges to form a point-to-multipoint network reduces the throughput to about 12.5 Mbps.

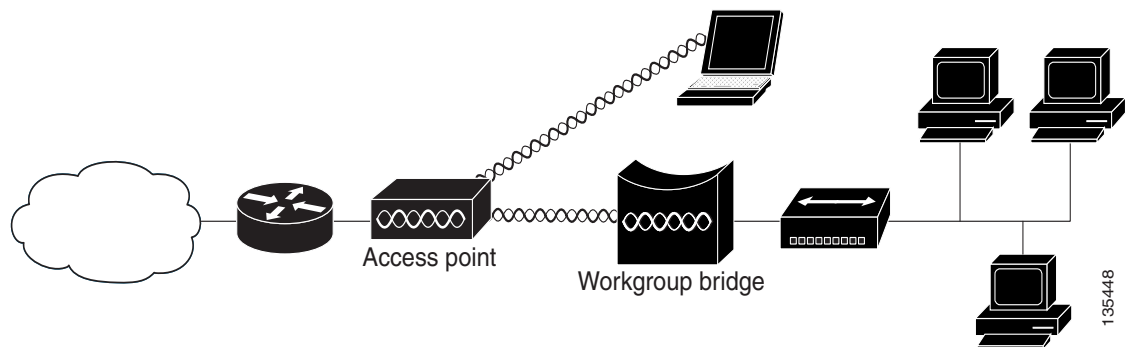
Workgroup Bridge

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 multiple radios, either 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 19-13 and the [“Configuring Workgroup Bridge Mode”](#) section on page 19-16 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

