



## Overview

---

Cisco Aironet 1300 Series Outdoor Access Points/Bridges (hereafter called *access points/bridges*) provide campus building-to-building wireless connectivity. Operating in the 2.4-GHz ISM band and conforming to the 802.11g standard, the 1300 series access point/bridge delivers a 54-Mbps data rate. The access point/bridge communicates with any 802.11b or 802.11g clients when in the access point mode and other 1300 series access points/bridges when in the bridging mode.

The access point/bridge is a self-contained unit designed for outdoor installations but can also be used inside with a window mounting option. You can connect external antennas to the access point/bridge to attain various antenna gains and coverage patterns. The access point/bridge supports both point-to-point and point-to-multipoint configurations. Two point-to-point links (three links if 802.11b) can be stacked in order to increase data throughput or provide cold standby redundancy.

You can configure and monitor the access point/bridge 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](#)
- [Network Configuration Examples, page 1-3](#)
- [Troubleshooting, page 1-6](#)

# Features

Access point/bridges running Cisco IOS offer these software features:

- Antenna alignment assistance—Use this feature access an auto configuration and installation mode for quick deployment of point-to-point links without the need to configure the access point/bridge via Telnet, FTP, or Simple Network Management Protocol (SNMP). LEDs show signal strength information used in the installation and antenna alignment process.
- Automatic channel selection—This feature determines and selects the least congested channel to provide the least interference possible.
- Automatic rate scaling—This feature scales down the data rate to maintain connectivity at outlying distances.
- Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2)—Provides access control via per-user, per-session mutual authentication and data privacy via strong dynamic encryption.
- 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.
- World mode—Use this feature to communicate the access point/bridge'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.
- 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
- QoS—Use this feature to support quality of service for prioritizing traffic from the Ethernet to the access point/bridge. The access point/bridge also supports the voice-prioritization schemes used by 802.11b wireless phones such as Spectralink's Netlink™ and Symbol's Netvision™.
- 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.
- RADIUS Accounting—Enable accounting on the access point/bridge 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/bridge.

- Fast Secure Roaming—When configured as an access point the 1300 series allows authenticated client devices to roam securely from one access point to another without any perceptible delay during reassociation.
- Port Aggregation Protocol and Cisco Fast EtherChannel Technology—Bandwidth can be increased between bridged networks through the aggregation of multiple bridges at each site.
- Hot Standby—The access point/bridge supports failover to a standby device.
- Load balancing—The access point/bridge distributes user connections across available access points to optimize aggregate throughput.
- Link distance adjustment—Allows users to tune the Carrier Sense Multiple Access Collision Avoidance (CSMA/CA) parameters for a particular range to maximize performance.
- Wireless packet concatenation—Provides higher overall data throughput by concatenating smaller packets into larger ones.
- Wireless programmable clear-channel assessment—The access point/bridge can be configured to the particular background interference level found in your environment for reduced contention overhead with other wireless systems.
- CiscoWorks Wireless LAN Solution Engine (WLSE)—A component of Cisco Structured Wireless-Aware Network (SWAN), is an available management tool for the access point/bridge. The WSLE has an HTML-based management interface and uses SNMP and Secure Shell (SSH)/Secure Sockets Layer (SSL) for managing Cisco Aironet access points and bridges via a web browser.

## Management Options

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

- The 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 17, “Configuring SNMP,”](#) explains how to configure your access point/bridge for SNMP management.

## Network Configuration Examples

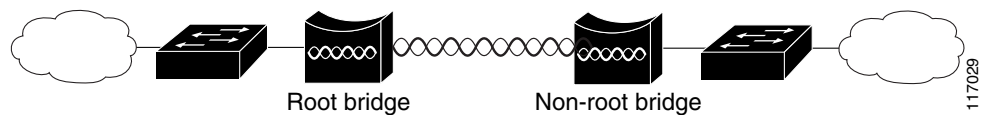
This section describes the access point/bridge’s role in common wireless bridging configurations: point-to-point, point-to-multipoint, redundant bridging, access point mode, and workgroup bridge mode. One bridge in any pair or group of bridges must be a root bridge, and the bridge or bridges associated to the root bridge must be set to non-root.

## Point-to-Point Bridging

In a point-to-point configuration, a non-root bridge associates to a root bridge. In installation mode, the bridge listens for another 1300 series bridge. If it does not recognize another bridge, the bridge becomes a root bridge. If it recognizes another bridge, it becomes a non-root bridge associated to the bridge it recognizes. See [Chapter 2, “Configuring the Access Point/Bridge for the First Time,”](#) for instructions on initial bridge setup.

[Figure 1-1](#) shows bridges in a point-to-point configuration.

**Figure 1-1** Point-to-Point Bridge Configuration

**Note**

If your bridges connect one or more large, flat networks (a network containing more than 256 users on the same subnet) we recommend that you use a router to connect the bridge to the large, flat network.

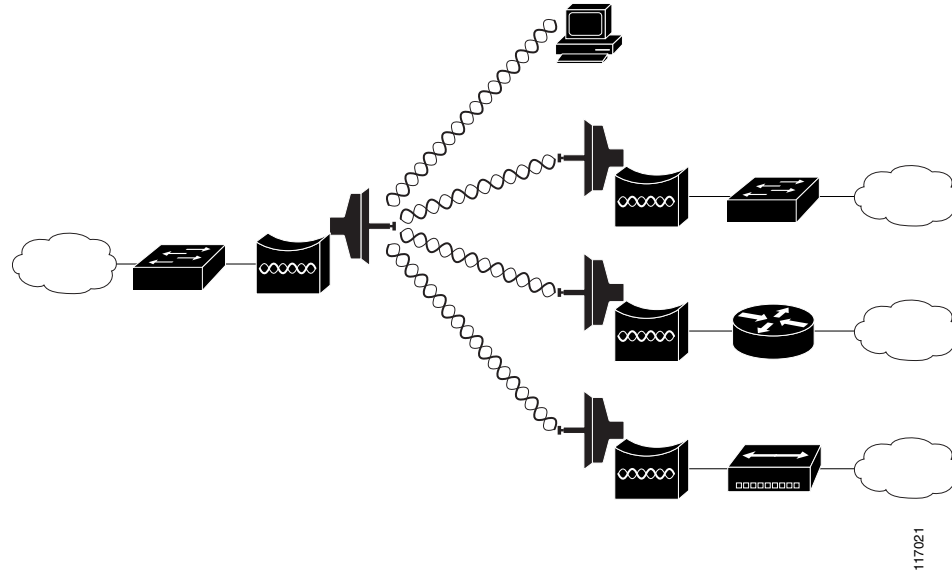
## Point-to-Multipoint Bridging

In a point-to-multipoint configuration, two or more non-root bridges associate to a root bridge. Up to 17 non-root bridges can associate to a root bridge, but the non-root bridges must share the available bandwidth.

See [Chapter 2, “Configuring the Access Point/Bridge for the First Time,”](#) for instructions on initial bridge setup.

[Figure 1-2](#) shows bridges in a point-to-multipoint configuration.

**Figure 1-2** Point-to-Multipoint Bridge Configuration



**Note**

If your bridges connect one or more large, flat networks (a network containing more than 256 users on the same subnet) we recommend that you use a router to connect the bridge to the large, flat network.

## Redundant Bridging

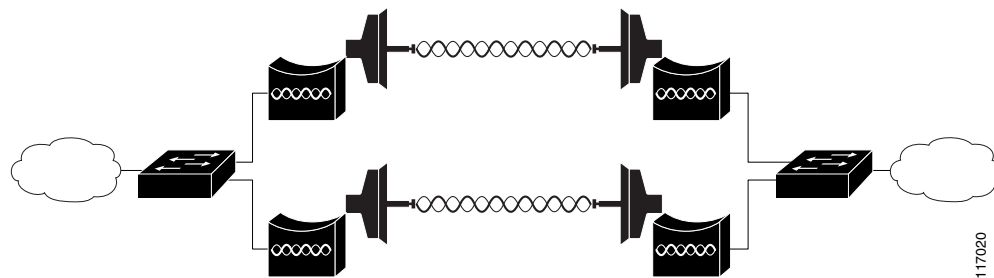
You can set up two pairs of bridges to add redundancy or load balancing to your bridge link. The bridges must use non-adjacent, non-overlapping radio channels to prevent interference, and they must use Spanning Tree Protocol (STP) to prevent bridge loops. See [Chapter 8, “Configuring Spanning Tree Protocol,”](#) for instructions on configuring STP.



**Note** STP is disabled by default.

[Figure 1-3](#) shows two pairs of redundant bridges.

**Figure 1-3** Redundant Bridge Configuration

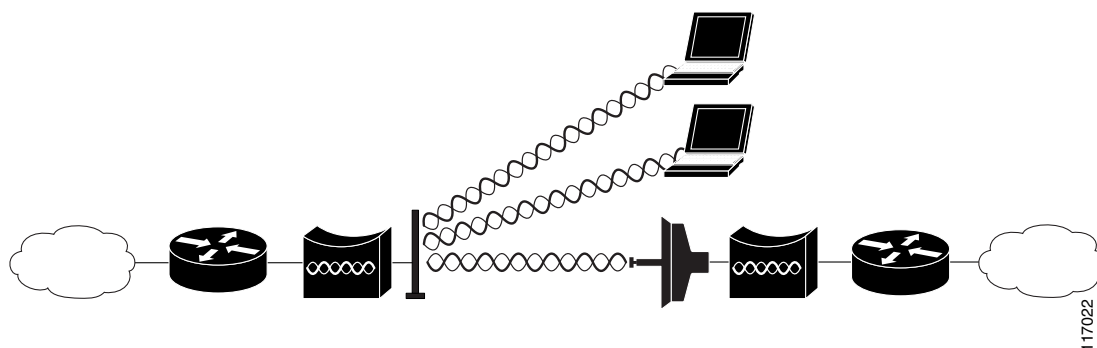


## Access Point Mode

You can configure the access point/bridge to function as an access point. In the access point mode, the access point/bridge emulates a Cisco Aironet 1100 Series Access Point. In the access point mode, the access point/bridge accepts associations from client devices. See [Chapter 20, “Configuring Repeater and Standby Access Points and Workgroup Bridge Mode,”](#) for instructions on configuring the access point/bridge as an access point.

Figure 1-4 Shows a typical scenario where the access point/bridge functions as an access point.

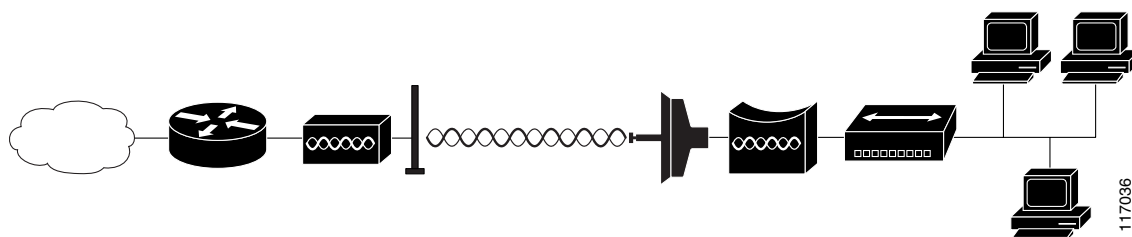
Figure 1-4 Access Point Mode



## Workgroup Bridge Mode

You can configure the access point/bridge to function as a workgroup bridge. In the workgroup bridge mode, the access point/bridge emulates a Cisco Aironet 350 Series Workgroup Bridge; Figure 1-5 shows a typical scenario where the access point/bridge functions as a workgroup bridge. See [Chapter 20, “Configuring Repeater and Standby Access Points and Workgroup Bridge Mode,”](#) for instructions on how to configure the access point/bridge as a workgroup bridge.

Figure 1-5 Workgroup Bridge Mode



## Troubleshooting

For basic troubleshooting procedures, refer to the “Troubleshooting” chapter in the *Cisco Aironet 1300 Series Outdoor Access Point/Bridge Hardware Installation Guide*.

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/tac>. Click **Technology Support**, select **Wireless/Mobility** from the menu on the left, and click **Wireless LAN**.

