Overview

Cisco wireless devices 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 wireless devices are Wi-Fi certified, 802.11b-compliant, 802.11g-compliant, or 802.11a-compliant wireless LAN transceivers.

This document provides information for the following devices:

- Access Point High-speed WAN Interface Card (AP HWIC)
- Cisco 800 Series routers with wireless capabilities
- Cisco 1800 Series routers with wireless capabilities

This chapter provides information on the following topics:

Wireless Device Management

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

- The Cisco IOS command-line interface (CLI), that can be used through a console port or a Telnet session. Use the interface dot11radio configuration command in global mode to place the wireless device into radio configuration mode.
- Simple Network Management Protocol (SNMP).

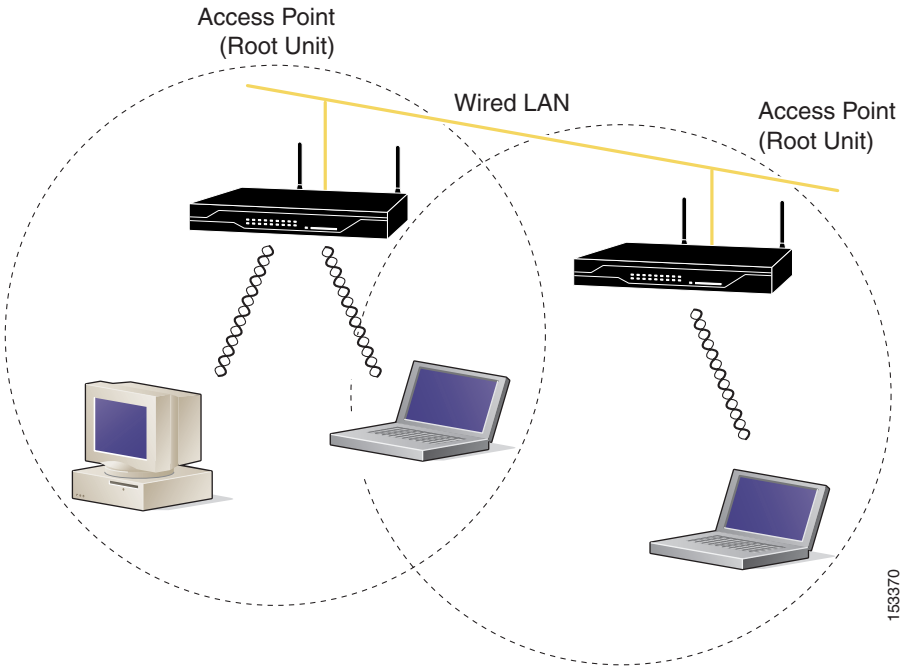
Network Configuration Example

This section describes the wireless device role in common wireless network configurations. The access point default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network.

Root Unit on a Wired LAN

An access point connected directly to a wired LAN provides a connection point for wireless users. 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



Features

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

- Access Point Link Role Flexibility—This feature allows the user to configure root and non-root bridging mode functionality, universal client mode, and support of a WGB client device, in addition to a root access point on the radio interface.

  Note Root/Non-Root bridging mode is supported only on modular ISR platforms, such as Cisco 3800 series , Cisco 2800 and Cisco 1841 series. Fixed ISR platforms, such as the Cisco 800 and Cisco 1800 do not support this feature.

- QoS Basic Service Set (QBSS) support—This feature aligns Cisco QBSS implementation with the evolving 802.11e standard. The QBSS element of the access point's beacon advertises channel load instead of traffic load. A new configuration command, **dot11 phone dot11e** has been added in Release 12.4 that allows the standard QBSS Load element to be sent in the beacon. This command should be used when compatible phones are employed in the network.
- Secure Shell version 2 (SSHv2) support—SSH v2 is a standards-based protocol to provide secure Telnet capability for router configuration and administration.
- 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 access points configured at the factory for use in Europe to detect radar signals such as military and weather sources and switch channels on the access points.
- SNMPv3—This feature enables SNMPv3 support on Cisco wireless devices to provide an additional level of security.
- 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.
- 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

Note Only 10 SSIDs are supported on the Cisco 800 series platforms.

- 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 the Cisco 7920 and Spectralink's Netlink™.
- RADIUS Accounting—Enable accounting on the access point to send accounting data about wireless client devices to a RADIUS server on your network.
- 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.
- 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 number of clients supported varies based on platform, with up to 1000 user accounts supported on the higher end platforms.
- Support for 802.11g radios—Cisco IOS Releases 12.4(2)T or later support the standard 802.11g, 2.4-GHz radio.
- Support for Cisco 802.11a Radios—The 802.11a radios support all access point features introduced in Cisco IOS Release 12.4 and later.
- 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).
- 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 12.4(5)T, 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 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.