



Wireless LAN Overview

A wireless LAN (WLAN) is, in some sense, nothing but a radio—with different frequencies and characteristics—acting as a medium for networks. The Cisco 800, 1800, 2800, and 3800 series integrated services routers, hereafter referred to as an access point or AP, serve 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 AP can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

Components of a traditional WLAN network include APs, network interface cards (NICs) or client adapters, bridges, repeaters, and antennae. Additionally, an authentication, authorization, and accounting (AAA) server (specifically a RADIUS server), network management server (NMS), and “wireless aware” switches and routers are considered as part of an enterprise WLAN network.

Module History

This module was first published on December 15, 2005.

Contents

- [Information About Wireless LANs, page 1](#)
- [Additional References, page 5](#)

Information About Wireless LANs

- [Purpose of This Guide, page 2](#)
- [Organization of This Guide, page 2](#)
- [Roaming Wireless Client Devices, page 2](#)
- [Common Wireless Network Configurations, page 3](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Purpose of This Guide

This guide provides the conceptual information, configuration tasks, and examples to help you configure and monitor a “wireless-aware” router using the Cisco IOS CLI, which can be used through a console port or Telnet session. You can also configure and monitor your router using the Security Device Manager (SDM) application or Simple Network Management Protocol (SNMP). SDM comes preinstalled on all new Cisco 850, 870, 1800, 2800, and 3800 series integrated services routers.

Organization of This Guide

This guide is organized into the following modules:

- [“Cisco IOS Wireless LAN Features Roadmap”](#)—Lists the features documented in the Cisco IOS wireless LAN modules and maps the features to the modules in which they appear.
- [“Configuring a Basic Wireless LAN Connection”](#)—Describes how to configure basic wireless settings using the Cisco IOS CLI. Examples of how to configure the AP in bridging and routing mode, and how to set up basic WLAN security, such as encryption and authentication, are provided.
- [“Securing a Wireless LAN”](#)—Describes how to configure security features in a WLAN, such as Wired Equivalent Privacy (WEP) encryption and features to protect WEP keys including Wi-Fi Protected Access (WPA) authenticated key management, Message Integrity Check (MIC), Temporal Key Integrity Protocol (TKIP), and broadcast key rotation. It also describes how to configure various types of AP authentication, such as open, shared key, MAC address, and Extensible Authentication Protocol (EAP), and how to configure multiple Service Set Identifiers (SSIDs).
- [“Configuring RADIUS or a Local Authenticator in a Wireless LAN”](#)—Describes how to enable and configure RADIUS, which provides detailed accounting information and flexible administrative control over the authentication and authorization processes. This module also describes how to configure the AP to act as a local RADIUS server for your WLAN. If a WAN connection to your main RADIUS server fails, the AP acts as a backup server to authenticate wireless devices.
- [“Configuring Wireless VLANs”](#)—Describes how to configure your AP to interoperate with VLANs on your wired LAN.
- [“Implementing Quality of Service in a Wireless LAN”](#)—Describes how to configure your AP to use the quality of service (QoS) features on your wired LAN.
- [“Wireless LAN Error Messages”](#)— Lists the WLAN CLI error and event messages.

Roaming Wireless Client Devices

If you have more than one AP in your WLAN, wireless client devices can roam seamlessly from one AP to another. The roaming functionality is based on signal quality, not proximity. When a client’s signal quality drops, the client device roams to another AP.

WLAN users are sometimes concerned when a client device stays associated to a distant AP instead of roaming to a closer AP. However, if a client’s signal to a distant AP remains strong and the signal quality is high, the client will not roam to a closer AP. Checking constantly for closer APs would be inefficient, and the extra radio traffic would slow throughput on the WLAN.

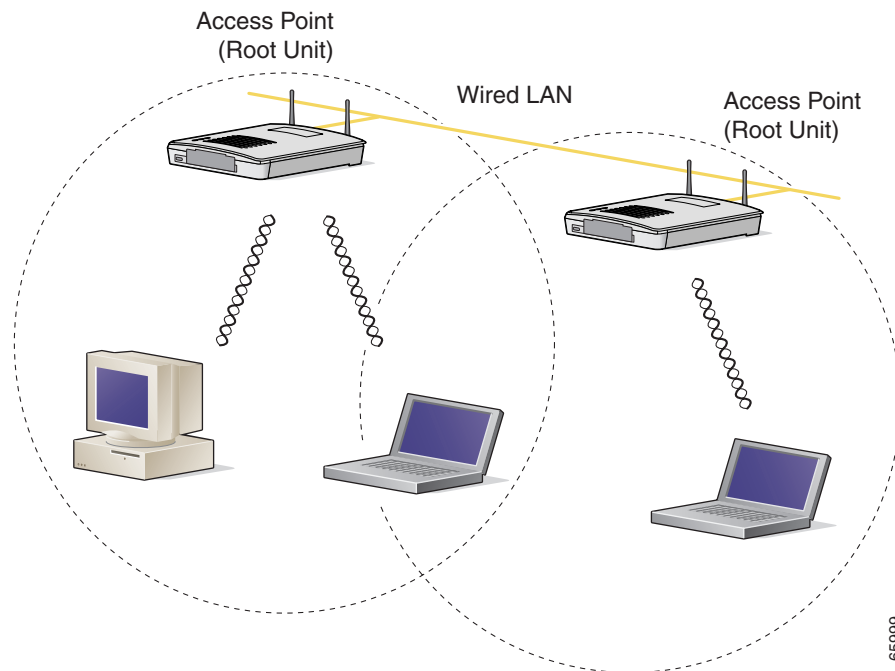
Common Wireless Network Configurations

This section describes the AP's role in three common wireless network configurations. The AP'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 AP connected directly to a wired LAN provides a connection point for wireless users. If more than one AP 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 AP, they automatically associate to the network through another AP. The roaming process is seamless and transparent to the user. [Figure 1](#) shows APs acting as root units on a wired LAN.

Figure 1 Access Points as Root Units on a Wired LAN



65655

Repeater Unit That Extends Wireless Range

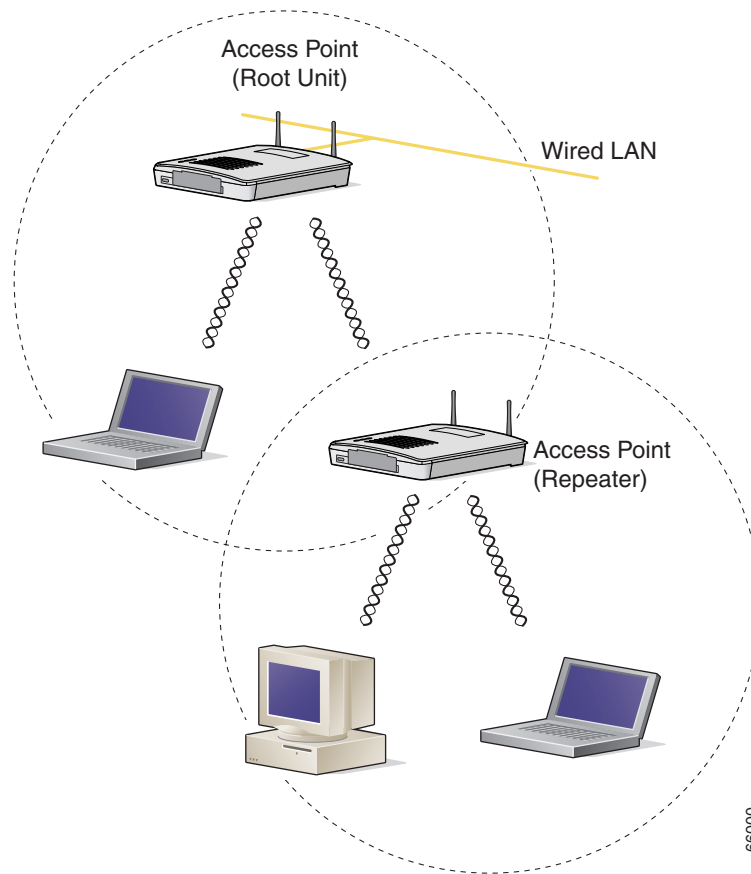
An AP can be configured as a standalone repeater to extend the wireless range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an AP connected to the wired LAN. The data is sent through the route that provides the best performance for the client. [Figure 2](#) shows an AP acting as a repeater.



Note

Non-Cisco client devices might have difficulty communicating with repeater APs.

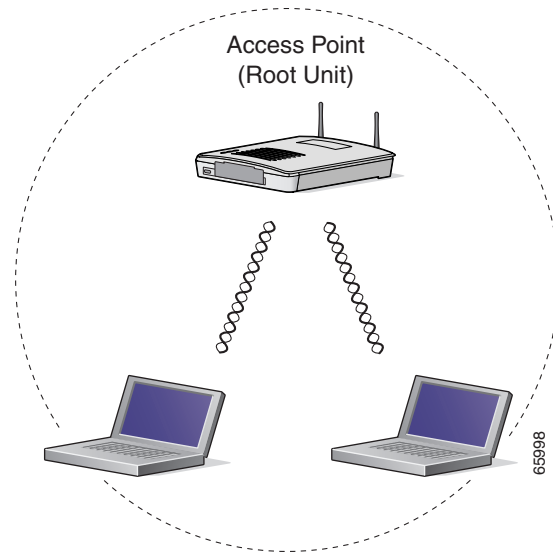
Figure 2 Access Point as a Repeater



Central Unit in an All-Wireless Network

In an all-wireless network, an AP acts as a standalone root unit. The AP is not attached to a wired LAN; it functions as a hub linking all stations. The AP serves as the focal point for communications, increasing the communication range of wireless users. [Figure 3](#) shows an AP in an all-wireless network.

Figure 3 *Access Point as a Central Unit in an All-Wireless Network*



Additional References

The following sections provide references related to configuring and monitoring a WLAN.

Related Documents

Related Topic	Document Title
Cisco IOS wireless LAN commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Wireless LAN Command Reference</i>
Configuration information for the Cisco 850 series and Cisco 870 series access routers	<i>Cisco 850 Series and Cisco 870 Series Access Routers</i> http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/85x87x/index.htm
Configuration information for the Cisco 1800 series integrated services routers (fixed)	<i>Cisco 1800 Series Integrated Services Routers (Fixed)</i> http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1800fix/index.htm
Configuration information for the Cisco 1800 series integrated services routers (modular)	<i>Cisco 1800 Series Integrated Services Routers (Modular)</i> http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1800/index.htm
Configuration information for the Cisco 2800 series integrated services routers	<i>Cisco 2800 Series Integrated Services Routers</i> http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/2800/index.htm
Configuration information for the Cisco 3800 series integrated service routers	<i>Cisco 3800 Series Integrated Services Routers</i> http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/3800/index.htm
Information on SDM	<i>Cisco Router and Security Device Manager</i> http://www.cisco.com/en/US/products/sw/secursw/ps5318/tsd_products_support_series_home.html

Standards

Standard	Title
IEEE 802.11	<i>Part II: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications.</i>
IEEE 802.11a	<i>Higher-Speed Physical Layer Extension in the 5-GHz Band</i>
IEEE 802.11b	<i>Higher-Speed Physical Layer Extension in the 2.4-GHz Band</i>
IEEE 802.11g	<i>Amendment 4: Further Higher Data Rate Extension in the 2.4-GHz Band</i>

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • CISCO-DOT11-ASSOCIATION-MIB • CISCO-DOT11-IF-MIB • CISCO-IETF-DOT11-QOS-EXT-MIB • CISCO-IETF-DOT11-QOS-MIB • CISCO-TBRIDGE-DEV-IF-MIB • CISCO-WLAN-VLAN-MIB 	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Glossary

access point—An AP operates within a specific frequency spectrum and uses an 802.11 standard modulation technique. It also informs the wireless clients of its availability and authenticates and associates wireless clients to the wireless network. An AP also coordinates the wireless clients' use of wired resources. It should be noted that there are several kinds of APs, including single radio and multiple radios, based on different 802.11 technologies.

antenna—An antenna radiates the modulated signal through the air so that wireless clients can receive it. Characteristics of an antenna are defined by propagation pattern (directional versus omnidirectional), gain, transmit power, and so on. Antennas are needed on the APs, bridges, and clients.

client adapter—A PC or workstation uses a client adapter or wireless NIC to connect to the wireless network. The NIC scans the available frequency spectrum for connectivity and associates to the AP or another wireless client. The NIC is coupled to the PC or workstation operating system (OS) using a software driver. Various client adapters are available from Cisco.

EAP—Extensible Authentication Protocol. EAP is a flexible protocol used to carry authentication information. It is defined in RFC 2284.

IEEE—The Institute of Electrical and Electronic Engineers is, among other things, a standards body. IEEE publishes standards for many types of systems, and is well known for its standards on information exchange between computers—from best practices to IT infrastructure to LAN and MAN standards to portable applications standards.

MAC—Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an AP or client adapter.

MIC—Message Integrity Check algorithm.

SSID—Service Set Identifier. A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or with an AP.

TKIP—Temporal Key Integrity Protocol. Developed to fix the problems with WEP. TKIP consists of three protocols: a cryptographic message integrity algorithm, a key mixing algorithm, and an enhancement to the initialization vector (IV).

WEP—Wired Equivalent Privacy. An optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a wired Ethernet.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.