Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine

CiscoWorks WLSE and WLSE Express, Release 2.13

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-8377-01

Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine

Preface 5

Audience 5

Conventions 5

Product Documentation 6

Obtaining Documentation 7

Cisco.com 7

Product Documentation DVD 7

Ordering Documentation 8

Documentation Feedback 8

Cisco Product Security Overview 8

Reporting Security Problems in Cisco Products 9

Obtaining Technical Assistance 9

Cisco Technical Support & Documentation Website 9

Submitting a Service Request 10

Definitions of Service Request Severity 10

Obtaining Additional Publications and Information 10

CHAPTER 1 **Introduction** 1-1

CHAPTER 2 **Configuring Access Points for Network Management** 2-1

Introduction 2-1

Using the AP CLI for Network Management Setup 2-2

Using the AP Web Interface for Network Management Set Up 2-4

Using WLSE Configuration Templates for Network Management Set Up 2-5

Using the Deployment Wizard for Network Management Set Up 2-5

CHAPTER 3 **Configuring Devices for Radio Management** 3-1

Understanding WDS 3-3

What is WDS and Why Do I Need It? 3-3

How To Use WDS Devices 3-7

Radio Management Setup Quick Reference 3-9

Configuring WDS Access Points (AP-WDS) 3-11

Using the Web Interface to Configure WDS APs 3-11

Using the CLI Interface to Configure WDS APs 3-12

Using a WLSE Configuration Template to Configure WDS APs 3-12

Configuring WLSM Access Points (AP-WLSM) 3-16

Configuring Infrastructure APs 3-17

Using the Web Interface to Configure Infrastructure APs 3-18

Using the CLI to Configure Infrastructure APs 3-18

Using a WLSE Configuration Job to Configure Infrastructure APs 3-18

Configuring Scanning APs 3-19

Configuring the WLSE 3-21

Configuring Authentication 3-21

Confirming the Configuration 3-22

Using the Web Interface to Validate the Configuration 3-23

Using the Command-Line Interface to Validate the Configuration 3-23

CHAPTER 4 **Configuring Routers and Switches** 4-1

CHAPTER 5 **Configuring AAA Servers** 5-1

Setting Up an ACS Server 5-1

INDEX

Preface

This guide provides procedures for configuring devices to be managed by the CiscoWorks Wireless LAN Solution Engine. This guide consists of the following chapters:

- Introduction
- Configuring Access Points for Network Management
- Configuring Devices for Radio Management
- Configuring Routers and Switches
- Configuring AAA Servers

Audience

This document is for system administrators and network administrators who are responsible for managing a wireless network and are familiar with the concepts and terminology of Ethernet and wireless local area networking.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** `font`
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item in paragraphs	**Option > Network Preferences**
Selecting a menu item in tables	Option > Network Preferences

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Product Documentation

Note We sometimes update the printed and electronic documentation after initial publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation for WLSE 2.13.

Table 1 Product Documentation

Document Title	Available Formats
Release Notes for the CiscoWorks Wireless LAN Solution Engine	On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_release_notes_list.html
Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine	On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_installation_and_configuration_guides_list.html
Installation and Configuration Guide for the 1130-19CiscoWorks Wireless LAN Solution Engine	• Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html
Installation and Configuration Guide for the 1030CiscoWorks Wireless LAN Solution Engine Express	• Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/products/ps6379/prod_installation_guides_list.html
Regulatory Compliance and Safety Information for the 1130-19 CiscoWorks Wireless LAN Solution Engine	• Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html
Regulatory Compliance and Safety Information for the 1030 CiscoWorks Wireless LAN Solution Engine Express	• Printed document included with the product. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/products/ps6379/prod_installation_guides_list.html

Table 1 Product Documentation (continued)

Document Title	Available Formats
User Guide for the CiscoWorks Wireless LAN Solution Engine	• From the WLSE online help. • PDF on the WLSE Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html
Upgrading CiscoWorks Wireless LAN Solution Engine Software	• From the WLSE online help. • On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_installation_guides_list.html
Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine	On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_device_support_tables_list.html
Context-sensitive online help	Select an option from the WLSE navigation tree, then click **Help**.
FAQ and Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine	• From the WLSE online help. • On Cisco.com: http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_troubleshooting_guides_list.html

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Instructions for ordering documentation using the Ordering tool are at this URL:

  http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output.

Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Introduction

You must set up devices before the WLSE can discover and manage them and before you can use the following WLSE features: monitoring, reporting, configuration, firmware upgrade. In addition, IOS access points must be configured for radio management.

Note If you are using Wireless Domain Services (WDS), you can use the WLSE's Deployment Wizard to set up your IOS access points and WDS devices. For information on the Deployment Wizard, see the WLSE online help or the WLSE user guide on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html.

Note After access points are being managed by the WLSE, you should avoid making direct modifications to them (by using the command-line interface or Web interface). Instead, you should use WLSE configuration templates to make changes. If configuration changes are made directly and not through the WLSE, the WLSE will not detect them immediately. This can cause inconsistencies in WLSE operations, especially in radio management.

Table 1 provides a high-level view of device setup tasks.

Table 1 Device Setup Quick Reference

Task	Reference
Set up IOS access points for basic network management.	Chapter 2, "Configuring Access Points for Network Management"
Set up IOS access points and other devices for radio management.	Chapter 3, "Configuring Devices for Radio Management"
Set up routers and switches for network management.	Chapter 4, "Configuring Routers and Switches"
Set up a Wireless LAN Services Module (WLSM)	Chapter 3, "Configuring Devices for Radio Management"
Set up external AAA servers for monitoring.	Chapter 5, "Configuring AAA Servers"

Configuring Access Points for Network Management

This chapter provides procedures for preparing IOS access points for basic network management by the WLSE.

Note If you are using Wireless Domain Services (WDS), you can use the WLSE's Deployment Wizard to set up your IOS access points and WDS devices for both network management and radio management. For a brief description of the Wizard, see Using the Deployment Wizard for Network Management Set Up, page 5. For detailed information on using the Wizard, see the WLSE online help or the WLSE user guide on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html.

Preparing IOS access points and the WLSE for participation in the Cisco Structured Wireless-Aware Network (SWAN), is covered in Chapter 3, "Configuring Devices for Radio Management."

This chapter contains the following topics:

- Introduction, page 1
- Using the AP CLI for Network Management Setup, page 2
- Using the AP Web Interface for Network Management Set Up, page 4
- Using WLSE Configuration Templates for Network Management Set Up, page 5
- Using the Deployment Wizard for Network Management Set Up, page 5

Introduction

Use one of the following methods to set up IOS access points and bridges:

- Log into each device by using Telnet or SSH and use the device's CLI commands—See Using the AP CLI for Network Management Setup, page 2.
- Log into each device's Web interface—See Using the AP Web Interface for Network Management Set Up, page 4.
- Use the WLSE's automatic configuration option for first-time device configuration and applying a configuration template to a number of access points—See Using WLSE Configuration Templates for Network Management Set Up, page 5.

After you set up a device, all of its MIB variables can be accessed and the device can be discovered by the WLSE.

After discovering and managing devices, you should use WLSE configuration templates for configuration changes—See the information on IOS templates in the WLSE online help or the WLSE user guide on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html.

Access points that function as AAA servers can be monitored by the WLSE. However, if you are registering an AP 1100 or AP 1210 as an AAA server with the WLSE, that access point can no longer be managed by the WLSE as an access point that provides wireless services.

Note VLAN information for IOS access points might not be collected by the WLSE if WEP keys are not configured in each VLAN. This affects VLAN reports, grouping, and faults. VLAN information becomes accessible through SNMP as soon as WEP keys are configured.

Using the AP CLI for Network Management Setup

To configure IOS devices by using the device CLI:

Procedure

Step 1 Access the device CLI via Telnet, SSH, or the console.

Step 2 Enter configuration mode.

Step 3 Enable Cisco Discovery Protocol (CDP) by entering the following commands for each interface that will participate in CDP. Do not enable CDP on radio interfaces.

```
configure terminal
interface interface
cdp run
```

where *interface* is the name of the interface; for example FastEthernet0.

Note You can find out whether CDP has been enabled by using the **show cdp** command in enable mode.

Note If you do not want to use CDP, you can add all access points as seeds or import devices. For more information, see the device discovery information in the WLSE online help or the WLSE user guide on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html.

Step 4 To configure SNMP, enter the following commands in the sequence shown. The first command includes the ISO view in the AP's configuration. The read-only SNMP community string enables discovery, fault monitoring, and reporting. The read/write community string enables firmware updating, configuration management, and all radio management features (such as client walkabout and radio scanning).

Note The community strings must also be entered on the WLSE. See the information on entering device credentials in the WLSE online help or the WLSE user guide on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html.

a. Include the ISO view:

```
snmp-server view iso iso included
```

Note IOS access points that do not have an ISO view will be placed in the Misconfigured Devices system group after discovery and a fault will be generated. The fault refers to a "dot 11 MIB" problem.

b. Configure the read-only community:

```
snmp-server community community_string view iso ro
```

c. Configure the read/write community:

```
snmp-server community community_string view iso rw
```

Caution Do not configure an IOS access point with an iee802dot11 view. An access point configured with such a view will not be discovered by the WLSE.

Step 5 (Optional) It is useful to set the system name, contact, and location SNMP variables to make the device more manageable and take advantage of system-defined device grouping. Use the following commands:

```
configuration terminal
hostname access_point
snmp-server location AP_location
snmp-server contact AP_contact
```

where *access_point* is the access point's host name, *AP_location* is its location, and *AP_contact* is the name of the contact person.

Step 6 You can use either Telnet or SSH to push configuration templates to IOS access points. To use templates to configure IOS access points, you must configure either Telnet or SSH or both, as follows.

- To enable and configure SSH, enter the following commands. In these commands, *hostname* is the hostname of the access point, and *domain_name* is your network's domain name (for example, cisco.com). At the prompt for the number of bits in the modulus, press **Return** to accept the default or enter a value.

  ```
  hostname hostname
  ip domain-name domain_name
  crypto key generate rsa
  How many bits in the modulus [512]:
  ```

  The following commands are recommended, but optional:

  ```
  ip ssh time-out 120
  ip ssh authentication-retries 3
  ```

- To configure Telnet, enter the following commands:

  ```
  line 0 4
  no access-class 111 in
  ```

  The following commands are recommended, but optional:

  ```
  width 80
  length 24
  ```

Step 7 Exit global configuration mode, then enter the following command:

```
write memory
```

Using the AP Web Interface for Network Management Set Up

To configure IOS devices by using the device Web interface:

Procedure

Step 1 Log into the Web interface of the access point.

Step 2 To enable CDP, select **SERVICES** from the menu, then click **CDP**:

a. After Cisco Discovery Protocol (CDP), select **Enabled**.

b. Click **Apply**.

Note If you do not wish to use CDP, you can add all access points as seeds or import devices. For more information, see the device discovery information in the WLSE online help or in the WLSE user guide on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html.

Step 3 You can use either Telnet or SSH (secure shell protocol) to push configuration templates to IOS access points. To use templates to configure IOS access points, you must configure either Telnet or SSH or both.

- To enable and configure SSH (secure shell protocol), enter the following:
  1. Select **SERVICES > Telnet/SSH**.
  2. Enable **Secure Shell**.
  3. Enter a System Name.
  4. Enter a Domain Name (for example, cisco.com).
  5. (Optional) Enter the RSA key size.
  6. (Optional) Enter the Authentication Timeout.
  7. (Optional) Enter Authentication Retries.
  8. Click **Apply**.
- To enable and configure Telnet:
  1. Select **SERVICES > Telnet/SSH**.
  2. Enable **Telnet**.
  3. (Optional) Enable **Teletype**.
  4. Enter the number of Columns.
  5. Enter the number of Lines.
  6. Click **Apply**.

Step 4 To enable SNMP:

a. Select **Services > SNMP**.

b. After Simple Network Management Protocol (SNMP), select **Enabled**.

c. Enter the System Name (sysName), System Location (sysLocation), and System Contact (sysContact).

d. Click **Apply**.

Step 5 In the SNMP Request Communities section, enter a read-only community string and configure an ISO view. This community string is required for discovery and to enable the fault and report features of the WLSE. Community strings are also required for radio management.

a. Enter the community string in the SNMP Community field.

b. Enter `iso` in the Object Identifier field.

Note IOS access points that do not have an ISO view will be placed in the Misconfigured Devices system group after discovery, and a fault will be generated. The fault message refers to a "dot11 MIB problem."

c. Select **Read-Only.**

d. Click **Apply**.

Note Do not configure an IOS access point with an iee802dot11 view. An access point configured with such a view will not be discovered by the WLSE.

Step 6 In the SNMP Request Communities section, enter a read/write community string to enable firmware and configuration updates on the access point.

a. Enter the community string in the SNMP Community field.

b. Select **Read-Write**.

c. Enter `iso` in the Object Identifier field.

d. Click **Apply**.

Step 7 The community strings created in Steps 5 and 6 must be entered on the WLSE before the device can be discovered and other WLSE features can be used. For more information, see the information on entering device credentials in the WLSE online help or the WLSE user guide on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html.

Using WLSE Configuration Templates for Network Management Set Up

You can perform initial configuration by using the WLSE's startup template feature. For more information on startup templates, see the information on managing device configuration in the WLSE online help or the WLSE user guide on Cisco.com at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html.

Note Do not configure an IOS access point with an iee802dot11 view. An access point configured with such a view will not be discovered by the WLSE.

Using the Deployment Wizard for Network Management Set Up

The Deployment Wizard appears in a separate window when you log in to the Web interface of the WLSE. The Wizard assists with the deployment and planning of WDS devices and IOS access points. For more information, see the WLSE online help or the WLSE user guide at http://www.cisco.com/en/US/products/sw/cscowork/ps3915/products_user_guide_list.html.

Configuring Devices for Radio Management

This chapter provides procedures for preparing IOS access points, Wireless LAN Services Modules (WLSMs), and the WLSE for participation in the Cisco Structured Wireless-Aware Network (SWAN).

Note Alternative methods of device configuration are described in this document. However, after access points are being managed by the WLSE, you should avoid making direct modifications to them (by using the command-line interface or Web interface). Instead, use the WLSE configuration templates to make changes. If configuration changes are made directly and not through the WLSE, the WLSE will not detect them immediately. This can cause inconsistencies in WLSE operations, especially in Radio Management.

There are two basic methods you can use to configure your network for Radio Management:

- You can use the WLSE Deployment Wizard

  If you are configuring APs or WLSM modules as WDS devices, you can use the Deployment Wizard. The Deployment Wizard replaces many of the manual configuration procedures that are normally required to configure infrastructure access points and WDS devices and to configure the WLSE to discover and manage those devices.

Note Although you can use the Deployment Wizard to set up most APs, you must use the manual procedures to configure an external ACS server for AP-WDS-WLSE authentication.

For more information about using the Deployment Wizard, see the WLSE online help or the "Deployment Wizard" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

For more information about WDS, see What is WDS and Why Do I Need It?, page 3-3.

- You can perform the configuration tasks manually.

  Setting up access points for Radio Management involves configuring all access points to register with Wireless Domain Services (WDS). The following sections describe this process:

  - Understanding WDS, page 3-3
  - Radio Management Setup Quick Reference, page 3-9
  - Configuring WDS Access Points (AP-WDS), page 3-11
  - Configuring WLSM Access Points (AP-WLSM), page 3-16
  - Configuring Infrastructure APs, page 3-17
  - Configuring Scanning APs, page 3-19
  - Configuring the WLSE, page 3-21
  - Configuring Authentication, page 3-21
  - Confirming the Configuration, page 3-22

Understanding WDS

Setting up access points for Radio Management involves configuring all access points to register with Wireless Domain Services (WDS). WDS provides wireless client roaming and Radio Management aggregation.

The following topics describe how WDS relates to managing your radio network:

- What is WDS and Why Do I Need It?, page 3-3
- How To Use WDS Devices, page 3-7

What is WDS and Why Do I Need It?

The critical software component in the network is a set of IOS features called the Wireless Domain Services (WDS). The following types of devices can supply the WDS:

- An access point configured for WDS

  Each WDS access point supports one AP subnet. You can add additional WDS access points for redundancy. The priorities you set on the WDS access points determine which one is the active and which ones are backups.

- A Wireless LAN Services Module (WLSM)

  WLSM is a CAT6K blade that provides WDS services and allows L3 seamless roaming among APs. Each WLSM can support multiple AP subnets, as long as all of the subnets are served by the switch on which the WLSM is installed.

The following topics describe these devices types:

- Understanding WDS Access Points, page 3-4
- Understanding WDS WLSM Devices, page 3-5

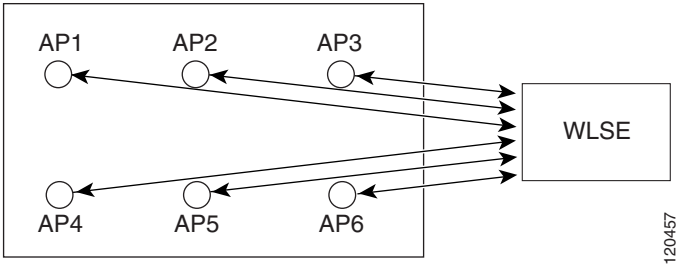
Understanding WDS Access Points

The WDS provides control path technologies that must be active on an AP in each AP subnet; a backup WDS can also be defined in each AP subnet. The WDS provides:

- Fast, secure layer-2 wireless client roaming—The WDS acts as an 802.1x authenticator for wireless clients within the layer-2 network.
- Radio Management (RM) data aggregation—The WLSE provides intelligent processing of aggregated data collected by the WDS access points from other wireless clients in the network. The WLSE can manage multiple subnets, so it can receive radio data from many APs running WDS.

There is no RM data aggregation without a WDS. Without a WDS, the communication between the access points and WLSE looks like this:

Figure 3-1 Basic Network Management Communications



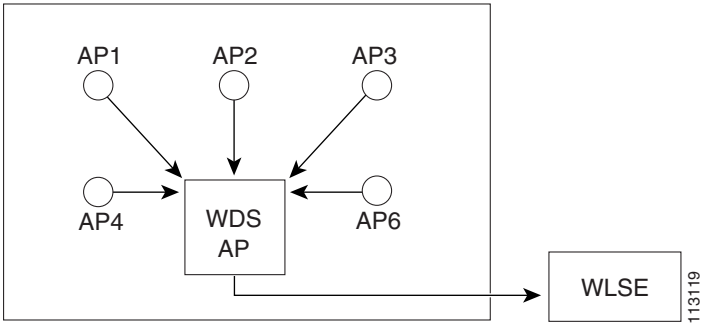
Using this approach, the WLSE can communicate with the APs using only these two methods:

- Primary: SNMP
- Secondary: CLI over telnet or SSH

Caution The WLSE must register with the WDS in each managed AP subnet to receive Radio Manager data. If the WLSE is not registered, *none of the Radio Manager functions will work*.

After you configure the network for Radio Management tasks, the WLSE communicates all Radio Management activities with one or more WDS APs instead of all APs in the network. Each WDS AP collects data from other wireless clients in the network and sends this aggregated data to the WLSE.

Figure 3-2 Additional Radio Management Communications



Understanding WDS WLSM Devices

A Wireless LAN Services Module (WLSM) device is a module for the Catalyst 6000 switch that provides WDS to the wireless network. Each WLSM supports multiple AP subnets, as long as all of the subnets are served by the switch on which the WLSM is installed.

You can add a second WLSM to serve as a standby. The WLSE authenticates with both the HSRP active and HSRP standby WLSM devices (WLSM uses HSRP to handle redundancies). In the reports, both WLSM devices (HSRP active and HSRP standby) will appear as active WDSs.

If the HSRP active WLSM goes down, the HSRP standby WLSM will communicate with the AP subnets (see Figure 3-3).

Figure 3-3 WLSE-WLSM Communications

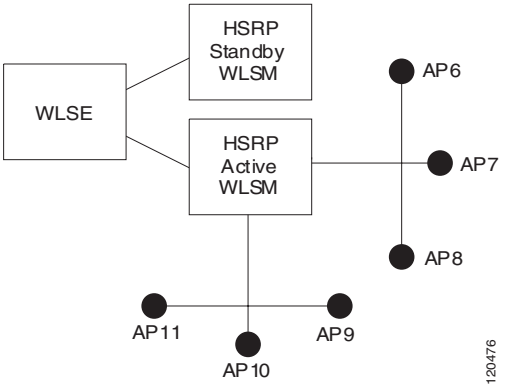
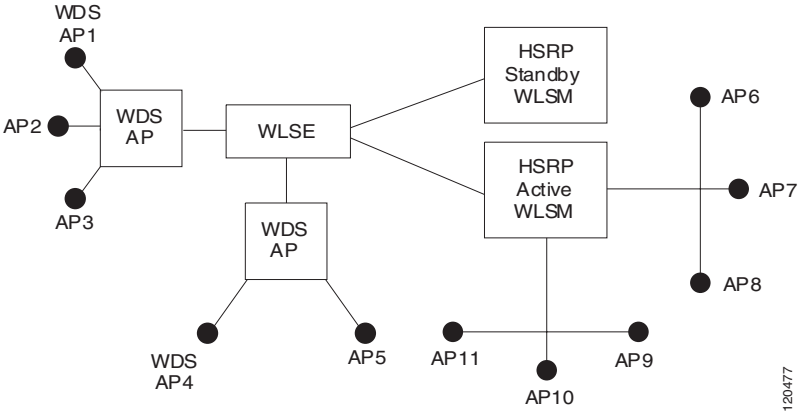


Figure 3-4 illustrates a network that uses both AP and WLSM WDS devices to manage the access points in the network. In this example, additional access points have been identified as backup AP-WDS devices (AP1 and AP4), and an additional HSRP-based WLSM-WDS device has been added to as a standby for the active WLSM-WDS.

Figure 3-4 Sample Network Using AP-WDS and WLSM-WDS Devices



How To Use WDS Devices

To use WDS devices:

- One access point or one WLSM must be designated as the *WDS*. The WDS is the only device that speaks to the authentication server.
  - For AP-WDS devices, WDS must be active on an access point in each subnet in which APs are placed; backup WDS access points can also be defined in each AP subnet.
  - For WLSM-WDS devices, each WLSM can support multiple AP subnets, as long as all of the subnets are served by the switch on which the WLSM is installed.
- The WDS device establishes a relationship with the *authentication server* (either an external RADIUS server or the local RADIUS server feature in the WDS access point itself) by authenticating to it using a WDS user name and password.
- Other access points, called *infrastructure access points*, communicate with the WDS device. Infrastructure access points must authenticate themselves to the WDS before they are registered. This *infrastructure authentication* is defined by an *infrastructure server group* on the WDS device.

  Communication between the WDS and the infrastructure access points happens over *Wireless LAN Context Control Protocol (WLCCP)*. For an AP-WDS, WDS multicast messages are used for WDS discovery by the infrastructure access points. Therefore, an AP-WDS device and its associated infrastructure access points must be in the same IP subnet and on the same LAN segment.

  Between the WDS and the WLSE, WLCCP uses TCP and User Datagram Protocol (UDP) on port 2887. When the WDS and WLSE are on different subnets, the packets cannot be translated with a protocol like Network Address Translation (NAT).
- *Client authentication* is defined by one or more *client server groups* on the WDS devices.

When a client attempts to associate to an infrastructure access point:

1. The infrastructure access point passes the user's credentials to the WDS device for evaluation. If it is the first time that the WDS has seen a given user's credentials, it uses the authentication server to validate the credentials.

2. The WDS device then caches the user's credentials so it does not have to return to the authentication server when that user attempts authentication again (for example, reauthentication for rekeying, for roaming, or for when the user starts up the client device).

Any RADIUS-based EAP authentication protocol can be tunneled through WDS (for example, Lightweight EAP [LEAP], Protected EAP [PEAP], EAP-Transport Layer Security [EAP-TLS], or EAP-Flexible Authentication via Secure Tunneling [EAP-FAST]).

Radio Management Setup Quick Reference

Note Before you can configure your network for Radio Management, you must configure all access points for basic network management (see Chapter 2, "Configuring Access Points for Network Management"). If your network is not properly configured, *none of the Radio Manager, Location Manager, or Intrusion Detection System functions will work.*

Table 3-1 lists the general setup tasks for WDS devices:

Table 3-1 Radio Management Setup Tasks

Task	Description	Notes
1.	Configure WDS devices	Configuring WDS devices involves: • Defining the AAA servers and server groups that the WDS will use to LEAP authenticate infrastructure access points and the WLSE. • Enabling WDS and setting WDS priorities. • Entering the WNM IP address. These sections describe how to configure WDS devices: • Configuring WDS Access Points (AP-WDS), page 3-11 • Configuring WLSM Access Points (AP-WLSM), page 3-16
2.	Configure infrastructure access points to authenticate to a WDS device	The infrastructure access points are the APs with which the clients associate. The infrastructure access points ask the WDS to perform authentication for them. (See Configuring Infrastructure APs, page 3-17).

Table 3-1 Radio Management Setup Tasks

Task	Description	Notes
3.	Configure access points to be scanning-only APs	Scanning APs can detect and report clients associated to unauthorized access points. Scanning APs do not accept client associations. (See Configuring Scanning APs, page 3-19). **Note** Radio scanning requires a read/write SNMP community string on APs. For more information, see Understanding WDS, page 3-3,
4.	Configure the WLSE with WLCCP credentials	WLCCP credentials are entered on the WLSE for each WDS device. The Deployment Wizard can do this for WDS-AP and WDS-WLSM devices. (See Configuring the WLSE, page 3-21).
5.	Define authentication methods	Both the infrastructure APs and the WLSE must use LEAP to authenticate to the WDS devices. (See Configuring Authentication, page 3-21).
6.	Confirm the configuration	The configuration steps are performed on the *active* WDS devices. (See Confirming the Configuration, page 3-22).

Related Topics

- What is WDS and Why Do I Need It?, page 3-3
- How To Use WDS Devices, page 3-7

Configuring WDS Access Points (AP-WDS)

Note Before making changes to device configuration, back up the current configuration and test the new configuration on non-production devices.

Note Only Cisco Aironet 1100 and 1200 series access points support WDS. For information about the supported access points and IOS firmware versions, see the *Supported Devices Table for WLSE 2.12* on cisco.com.

There are several ways to configure WDS access points:

- Using the Web Interface to Configure WDS APs, page 3-11
- Using the CLI Interface to Configure WDS APs, page 3-12
- Using a WLSE Configuration Template to Configure WDS APs, page 3-12

Note For a sample WDS configuration, see the document titled **Wireless Domain Services Configuration** on Cisco.com. To locate this document, use the following navigation path from the Cisco.com home page: **Products and Services > Wireless > Cisco Aironet 1200 Series Access Point> Technical Documentation > Configuration Examples**.

Using the Web Interface to Configure WDS APs

Procedure

Step 1 See the "Designate an Access Point as WDS" section in the tech tip at http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801c951f.shtml.

Step 2 Go to the next step, Configuring Infrastructure APs, page 3-17. Or, to configure WLSM access points, go to Configuring WLSM Access Points (AP-WLSM), page 3-16.

Using the CLI Interface to Configure WDS APs

Procedure

Step 1 See the "Designate an Access Point as WDS" section in the tech tip at http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801c951f.shtml.

Tip Consult the IOS and access point documentation for details on the subtleties of IOS commands.

Step 2 Go to the next step, Configuring Infrastructure APs, page 3-17. Or, to configure WLSM access points, go to Configuring WLSM Access Points (AP-WLSM), page 3-16.

Using a WLSE Configuration Template to Configure WDS APs

You can use the WLSE to configure one or more WDS access points.

The major configuration steps are:

- Creating a configuration template to set up AAA servers and the WDS.
- Applying the configuration template to the appropriate access points by running a configuration job.

Before You Begin

- Back up the current configuration and test the new configuration on non-production devices.
- Configure all access points for basic network management (see Chapter 2, "Configuring Access Points for Network Management").

Procedure

Step 1 Log in to the WLSE web interface.

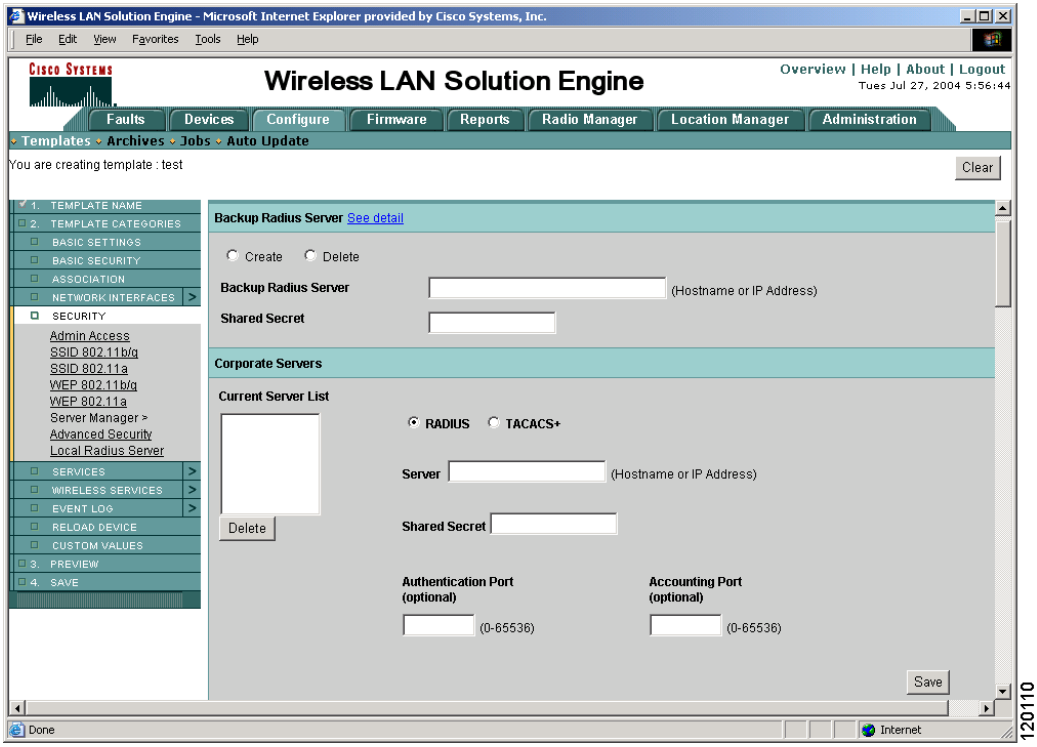
Step 2 Select **Configure > Templates.**

a. Enter a template name, selecting IOS as the template type.

b. Click **Create New**.

Step 3 Enter the AAA servers that will be used to LEAP authenticate the infrastructure access points and the WLSE to the WDS, and the AAA servers that will be used to authenticate wireless client devices:

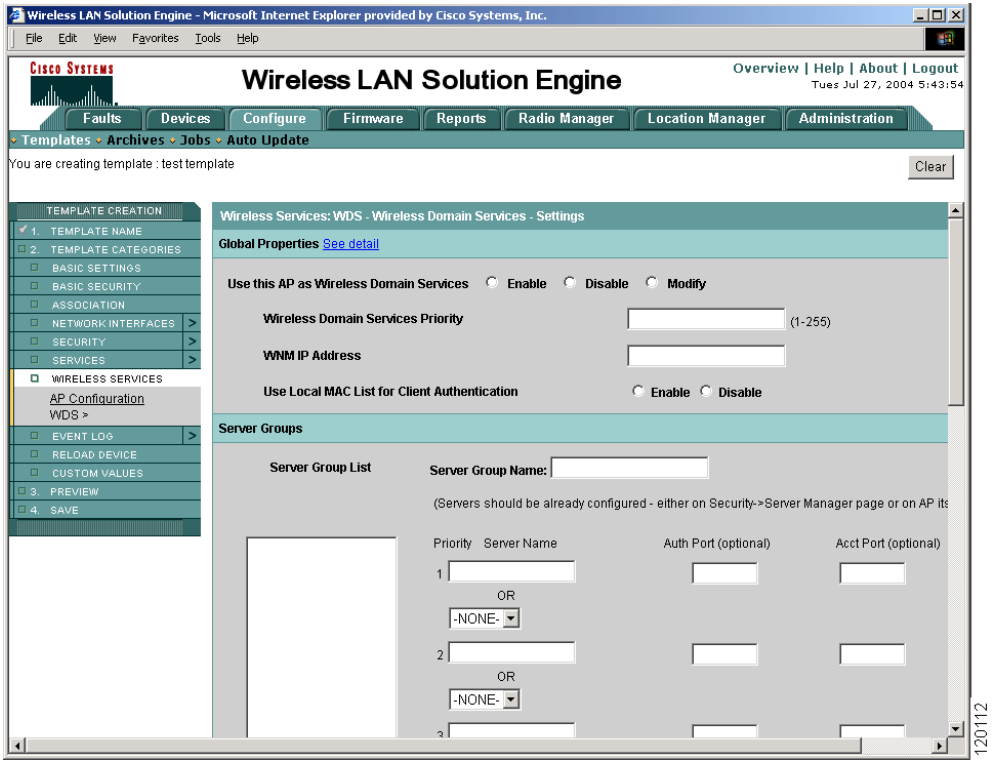
a. From the menu on the left, select **Security > Server Manager**.



b. In the Corporate Servers section, for each server, enter the IP address, select RADIUS, and enter the shared secret.

c. Click **Save**.

Step 4 From the menu on the left, select **Wireless Services > WDS** to configure the WDS parameters.



In the Global Properties section:

a. Select **Enable**.

b. Enter the Wireless Domain Services priority. This value determines which access point will serve as the active WDS when multiple access points are configured to run WDS on the same subnet. Valid priority values are 1-255, with 255 being the highest.

c. Enter the WLSE's IP address in the WNM IP Address field.

Step 5 Configure a server group for authenticating the SWAN infrastructure components.

In the Server Groups section:

a. Enter one or more server names or server IP addresses.

b. Under Use Group For, select **Infrastructure Authentication**.

c. Click **Save**.

Step 6 The WDS access point must also register and authenticate itself to the WDS to participate in the SWAN hierarchy, so the WDS AP is also an infrastructure AP. To authenticate and register the WDS AP as an infrastructure AP:

a. Select **Wireless Services > AP Configuration**.

b. Select **Enable** as the Wireless Services option.

c. Enter a username and password that can be LEAP authenticated by the AAA servers in the infrastructure server group.

Step 7 (Optional) From the menu on the left, select **Preview** to see a preview of the configuration template.

Step 8 From the menu on the left, select **Save**, then click the **Save** button.

Step 9 Select **Yes** to apply the template immediately or select **No** to save the template. For information on configuration jobs, see Chapter 7, Managing Device Configuration, in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

Step 10 Go to the next step, Configuring Infrastructure APs, page 3-17. Or, to configure WLSM access points, go to Configuring WLSM Access Points (AP-WLSM), page 3-16.

Configuring WLSM Access Points (AP-WLSM)

WLSM configuration details are explained in the *Cisco Catalyst 6550 Series Wireless LAN Services Module (WLSM) Deployment Guide* on Cisco.com. The following procedure provides a brief description of the required configuration steps for WDS and for discovery and management by the WLSE.

Guidelines for Using WLSM Access Points

- WLSM does not implement CDP, so the only way to discover a WLSM device is through WLCCP. The following procedure shows you how to configure the WLSM for WDS and add the WNM IP address (`wlccp wnm ip address ip_address`) at the WLSM.
- The SNMP credentials for the WLSM and the WLSE must match before the WLSE can get certain MIB objects during discovery and inventory.

Note Because the WLSM does not support CDP, it cannot be discovered by using the regular discovery job mechanism that is used to discover other devices. If you run a regular discovery job on the WLSM, a "device is not supported" appears in the discovery log.

Before You Begin

- Back up the current configuration and test the new configuration on non-production devices.
- Configure all access points for basic network management (see Chapter 2, "Configuring Access Points for Network Management").

Procedure

Step 1 Select **Devices > Discover > Device Credentials > WLCCP Credentials** and enter the WLSE WLCCP credentials.

This is the LEAP username and password that the WLSE will pass to the WDS.

Step 2 Configure the community strings on the WLSM as described the *Cisco Catalyst 6550 Series Wireless LAN Services Module (WLSM) Deployment Guide*.

Step 3 Enter the WLSM's community strings on the **WLSE under Devices > Discover > Device Credentials > SNMP Communities**.

Step 4 Use the following command to configure the WLSM with the address of the WLSE:

```
wlccp wnm ip address WLSE_IP_address
```

After this command is entered on the WLSM, the WLSE will automatically discover it.

Step 5 Go to the next step, Configuring Infrastructure APs, page 3-17.

Configuring Infrastructure APs

The infrastructure access points are the APs with which the clients associate. The infrastructure access points ask the WDS to perform authentication for them. There are several ways to configure infrastructure access points to register with a WDS device:

- Using the Web Interface to Configure Infrastructure APs, page 3-18
- Using the CLI to Configure Infrastructure APs, page 3-18
- Using a WLSE Configuration Job to Configure Infrastructure APs, page 3-18

Using the Web Interface to Configure Infrastructure APs

Procedure

Step 1 See the "Designate an Access Point as Infrastructure" section in the tech tip at http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801c951f.shtml.

Step 2 Go to the next step, Configuring Scanning APs, page 3-19.

Using the CLI to Configure Infrastructure APs

Procedure

Step 1 See the "Designate an Access Point as Infrastructure" section in the tech tip at http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801c951f.shtml.

Step 2 Go to the next step, Configuring Scanning APs, page 3-19.

Using a WLSE Configuration Job to Configure Infrastructure APs

When you use a WLSE configuration template, you can configure multiple infrastructure APs in a single job. Use the template creation wizard to create a configuration template, then apply the template in a configuration job.

For more information about using the template creation wizard and the configuration job interface, see WLSE online help or the "Using IOS Templates" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

Procedure

Step 1 Log in to the WLSE web interface.

Step 2 Select **Configure > Templates**.

a. Enter a template name, selecting IOS as the template type.

b. Click **Create New**.

Step 3 Select **Wireless Services > AP Configuration**.

Step 4 Select **Enable**.

Step 5 Select the mechanism that should be used to discover the WDS device:

- For access points that will register with an AP-WDS, select **Auto Discovery**.
- For access points that will register with a WLSM-WDS, select **Specified Discovery** and enter the IP address of the WLSM-WDS.

Step 6 Enter the username and password for LEAP authenticating infrastructure APs to the WDS.

Step 7 (Optional) Select **Preview** to see a preview of the configuration template.

Step 8 Select **Save**, then click the **Save** button.

Step 9 Select **Yes** to apply the template immediately or select **No** to save the template.

Step 10 Create a configuration job to apply the template to the appropriate devices.

For information about configuration jobs, see the online help or the "Managing Device Configuration" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

Step 11 Go to the next step, Configuring Scanning APs, page 3-19.

Configuring Scanning APs

This section describes how to configure an AP as a scanning-only AP. After you have performed the basic network management configuration and Radio Management configuration described in this chapter, perform the additional configuration described in this section to make the AP into a scanning-only AP. Scanning APs can detect and report clients associated to unauthorized access points. Scanning-only APs do not accept client associations.

Note Radio scanning requires a read/write SNMP community string on the APs.

For more information about scanning APs and other requirements for using scanning APs with a WLSE, see the "Radio Management" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

Before You Begin

- Configure scanning APs for basic network management (see Chapter 2, "Configuring Access Points for Network Management").

Note *Do not* configure a scanning AP as a WDS device.

- Configure scanning APs for Radio Management (see Configuring Infrastructure APs, page 3-17).

Procedure

Step 1 To configure a scanning AP using a WLSE configuration template:

a. Select **Configuration > Templates > IOS > Basic Settings,** then select **Scanner Access Point**.

b. Select **Configuration > Templates > IOS > Network Interfaces**. Select a radio and select **Scanner Access Point**.

Step 2 To configure a scanning AP using the AP CLI, enter:

```
config t
int dot11 0 (for interface 0)
station-role scanner
```

Step 3 To run inventory so the WLSE can update the role of the AP, select **Administration > Devices > Discover > Inventory**. The scanning APs will be listed in the WLSE's Scanning AP system group.

For more information, see the online help or the "Managing Devices" chapter of the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*

Step 4 To enable Client Registration Scanning to detect clients associated to unauthorized access points, select **Radio Management > Radio Monitoring**.

For more information, see the online help or the "Radio Management" chapter of the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

Step 5 Go to the next step, Configuring the WLSE, page 3-21.

Configuring the WLSE

The WLSE is the Wireless Network Manager (WNM) component of SWAN. The WLSE polls and aggregates Radio Management data from WDS devices and processes this data.

For more information about configuring the WLSE, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

Procedure

Step 1 Enter the WLCCP username and password in the WLSE.

SWAN components communicate via a Cisco proprietary technology called WLCCP. This username and password is used to LEAP authenticate the WLSE to the WDS devices in the network.

Step 2 Enter the SNMP read-only and read/write communities for all managed IOS access points.

Step 3 Enter Telnet/SSH credentials for IOS access points.

Step 4 Go to the next step, Configuring Authentication, page 3-21.

Configuring Authentication

Both the infrastructure APs and the WLSE must use LEAP to authenticate to the WDS devices.You can use:

- Local authentication (on an AP-WDS device only)—see Configuring WDS Access Points (AP-WDS), page 3-11.
- AAA servers that you have already configured, or you can configure servers as described in the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

Note *Do not set a session timeout on the ACS server that is less than 600 seconds*. A session timeout of less than 600 seconds can disrupt Radio Management operations.

Procedure

Step 1 Create server groups on the WDS devices for infrastructure authentication (see Configuring WDS Access Points (AP-WDS), page 3-11).

Step 2 Create server groups on the WDS devices for client authentication (see the "Define Client Authentication Method" section in the tech tip at http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801c951f.shtml).

Step 3 Go to the next step, Confirming the Configuration, page 3-22.

Confirming the Configuration

After the configuration is complete, you should confirm that configuration is correct and that the SWAN components are communicating properly. The configuration steps are performed on the *active* WDS devices.

To determine which WLSEs are actively providing WDS services, you can display the WDS Summary Report. For more information about this report, see the Reports chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

For AP WDS devices, there are two ways to confirm configuration:

- Using the Web interface (see Using the Web Interface to Validate the Configuration, page 3-23).
- Using the command-line interface (see Using the Command-Line Interface to Validate the Configuration, page 3-23).

For WLSM WDS devices, use the command-line interface to confirm the configuration (see Using the Command-Line Interface to Validate the Configuration, page 3-23).

Using the Web Interface to Validate the Configuration

Use this procedure to use the web interface (on WDS APs only) to confirm the configurations.

Procedure

Step 1 Log in to the web interface on each active WDS AP.

Step 2 Select **Wireless Services > WDS > WDS Status**.

Check for the following:

- The WDS Information section should display the device WDS state as ACTIVE.
- The WDS Registration and AP Information sections should show the correct number of APs (all of the infrastructure APs and the WDS AP).
- The Mobile Node Information section should display the wireless clients participating in SWAN.
- The Wireless Network Manager section should contain the WLSE IP address. If the WLSE authentication status is SECURITY KEYS SETUP, the WLSE is properly registered.

Using the Command-Line Interface to Validate the Configuration

Use this procedure to confirm the configurations on AP or WLSM WDS devices.

Procedure

Step 1 Log in to the CLI on each active WDS device.

Step 2 To validate the WDS configuration, enter:

```
# show wlccp wds ap
MAC-ADDR IP-ADDR STATE LIFETIME
000c.ce12.92ce 172.16.99.212 REGISTERED 62
000c.85a8.8bdd 172.16.99.213 REGISTERED 391
```

This command lists all of the infrastructure APs and the WDS.

Step 3 To verify that the WLSE is correctly registered, enter:

```
# show wlccp wnm status
WNM IP Address : 172.16.100.81 Status : SECURITY KEYS SETUP
```

This command should display the WLSE IP address. If the WLSE authentication status is SECURITY KEYS SETUP, the WLSE is properly registered.

CHAPTER 4

Configuring Routers and Switches

This chapter provides procedures for preparing routers and switches for management by the WLSE.

Note Only routers and switches that have properly configured access points or bridges attached to them will be discovered.

Procedure

Configure each router and switch as follows.

Step 1 Enable CDP and verify that access points and bridges are visible from the router or switch.

CDP is required for the WLSE to discover the router or switch.

a. In enable mode, verify that CDP is running on the device by using one of the following commands:
   - On IOS-based devices—**show cdp run**.
   - On Hybrid OS-based Catalyst switches—**show cdp**.

b. If CDP is not running, in global configuration mode, enter **cdp run** to enable CDP.

c. To verify that access points or bridges are visible in the device's CDP table, enter **show cdp neighbors**.

Step 2 Enable SNMP and set up community strings.

SNMP is required for the WLSE to discover and manage the device.

- On IOS-based devices, enter configuration mode and use the **snmp-server community** *community_string* **ro** command.
- On Hybrid OS-based Catalyst devices, enter enable mode and use the **set snmp community read-only** *community_string* command.

Step 3 (Optional) Set system name, contact, and location variables.

These variables make the device more manageable. The system name, system contact, and location will appear in the device detail displays.

- On IOS-based devices, enter configuration mode and use the following commands to set the system name, system contact, and system location:
  - **hostname** *name*
  - **snmp-server contact** *contact*
  - **snmp-server location** *location*

- On Hybrid OS-based Catalyst switches, enter enable mode and use the following commands to set the system name, system contact, and system location:
  - **set system name** *name* command
  - **set system contact** *contact*
  - **set system location** *location*

Configuring AAA Servers

The WLSE can monitor the performance of AAA (Authentication, Authorization, and Accounting) services provided by CiscoSecure ACS. The services supported are LEAP, RADIUS, EAP-MD5, PEAP (EAP-GTC only), and EAP-FAST.

This chapter covers setting up an ACS server:

- To set up a CAR server, see the CAR documentation on Cisco.com.
- To set up an access point as an AAA server, see the access point documentation on Cisco.com.
- To set up the WLSE's internal AAA server, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*. The internal AAA server is available only on the WLSE Express (WLSE 1030).

Setting Up an ACS Server

Note For PEAP, besides the procedure in this section, you must set up a certificate and private key on the ACS server and then enable PEAP. For more information, see the CiscoSecure ACS documentation.

To enable monitoring of an ACS server, you must:

- Configure CiscoSecure ACS server to recognize the WLSE as a client. Follow the procedure in this section on each server.
- Configure the WLSE to add information about AAA servers. For more information, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.13*.

In addition, you can use an AAA server to authenticate to Wireless Domain Services (WDS) devices. To enable this authentication, make sure an AAA server is configured as described in this section.

Procedure

Step 1 Log into the CiscoSecure ACS Server that will provide authentication services to the wireless network.

Note You will need the IP address or name of the system on which CiscoSecure ACS Server is running when you configure the WLSE.

Step 2 Click **User Setup** on the left side of the initial page.

Step 3 Enter a username for the user the WLSE will use for synthetic transactions and click **Add/Edit**.

Step 4 Enter a password in the first set of Password and Confirm Password fields. Click **Submit**.

Note You will need this name and password when configuring the WLSE.

Step 5 Click **Network Configuration** on the left side of the page.

Step 6 Click **Add Entry**. In the Add AAA Client area, enter the WLSE information in the following text boxes:

- Client Hostname—enter the WLSE hostname (or IP address)
- Client IP—enter the WLSE IP address
- Key—enter a secret key

Note You will need this key when configuring the WLSE.

Step 7 Select RADIUS (Cisco Aironet) from the Authenticate Using list.

Step 8 If you are using this server for Wireless Domain Services (WDS) authentication, configure the server for simultaneous login sessions. See the ACS documentation for details.

Step 9 If you are setting the session timeout, do not set it to less than 600 seconds.

Caution A session timeout of less than 600 seconds can disrupt Radio Manager operations.

Step 10 Click **Submit** or **Submit+Restart**. A restart is required for the changes to take effect.

A

AAA servers, external
  setting up 5-1
access point
  network management, configuring for 2-1
    IOS 3-1
  scanning AP, configuring 3-19
  using AP 1100 or AP 1210 as an AAA server 2-2
AP 1100, using as AAA server 2-2
AP 1210, using as as AAA server 2-2
AP radio scans, SNMP requirement for 2-2
APs, setting up
  network management 2-1
audience for this document 5
authentication
  clients 3-22
  server groups 3-22
  WDS 3-11, 3-17

B

bridge
  setting up 1-1
bug-lighted clients, detecting 3-19

C

cautions
  significance of 6
CDP, enabling
  on access points 2-2, 2-4
  on routers and switches 4-2
Cisco Access Registrar (CAR) 4-2, 5-1
Cisco Discovery Protocol (CDP)
  enabling
    on access points 2-2, 2-4
    on routers and switches 4-1
CiscoSecure ACS Server, configuring 5-1
client
  authenticating 3-22
  bug-lighted clients, detecting 3-19
community strings
  configuring on access points 2-2, 2-5
  configuring on routers and switches 4-1

D

discovery
  CDP
    enabling on routers and switches 4-1
documentation 6
  audience for this 5
  locating on Cisco.com 6
  typographical conventions in 5
dot11 mib fault
  configuring APs to prevent 2-2
  Misconfigured group, devices in 2-3

I

iee802dot11 view 2-3
ISO view
  configuring on access points 2-2

S

scanning AP, configuring 3-19
server groups, for WDS authentication 3-22
servers, AAA
  setting up 4-2, 5-1
SNMP
  enabling
    access points 2-4
    on routers and switches 4-1
SSH
  credentials for access points 2-3, 2-4

T

Telnet/SSH
  credentials for access points 2-4
typographical conventions
  in this document 5

W

WDS
  and radio manager 3-3
  configuration, confirming 3-22
  configuring authentication for 3-11, 3-17
  WLSM, using as WDS device 3-17
Wireless LAN Services Module (WLSM), using as a WDS device 3-17