Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine

Release 2.9

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

Text Part Number: OL-5923-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0411R)

Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine
Copyright © 2004 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1

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

Table 1-1 Device Setup Quick Reference

Task	Reference
Set up non-IOS access points for network management.	Chapter 2, "Configuring Non-IOS Access Points"
Set up IOS access points for basic network management.	Chapter 3, "Configuring IOS Access Points for Network Management"
Set up IOS access points for radio management.	Chapter 4, "Configuring IOS Access Points for Radio Management"

Table 1-1 Device Setup Quick Reference (continued)

Task	Reference
Set up routers and switches.	Chapter 5, "Configuring Routers and Switches"
Set up external AAA servers.	Configuring AAA Servers, page 6-1

CHAPTER 2

Configuring Non-IOS Access Points

This chapter provides procedures to prepare non-IOS access points for basic network management by the WLSE.

Configuration Methods

You can perform initial setup of non-IOS access points in two ways:

- By opening a web browser session on each access point—See Setting Up Non-IOS APs and Bridges—Using the Web Interface, page 2-2.
- By using the WLSE startup configuration to apply a configuration template to a number of access points—See Setting Up Non-IOS APs and Bridges—Using a WLSE Startup Template, page 2-4.

After discovering and managing devices, you can use WLSE configuration templates for configuration changes—See the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

Setting Up Non-IOS APs and Bridges—Using the Web Interface

To use this method, you must first configure each access point or bridge for web browsing.

Log in to the Web interface of the AP to be configured and set the following parameters.

Table 2-1 Set Up Procedures for Non-IOS Access Points and Bridges

Tasks	Procedure	Notes
1. Enable Cisco Discovery Protocol (CDP).[1]	1. In the Summary Status page, click **Setup**. 2. Under Services: Cisco Services, click **Cisco Discovery Protocol** and select Enabled. 3. Click **Apply** or **OK**.	Required for the WLSE to use CDP to discover the device. If you are not using CDP, you can add all APs as seed devices or import devices. See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.
2. Enable SNMP. SNMP is supported on version 11.08T and later non-IOS APs.	1. In the Summary Status page, click **Setup**. 2. Under Services, click **SNMP**. 3. Select Enabled. 4. (Optional) Enter a System Name, System Location, and System Contact. 5. Click **Apply** or **OK**.	SNMP is required for the WLSE to discover devices, populate reports, transfer configuration information to devices, and upgrade device firmware. Setting the system name, system contact, and system location ensures that this information is included in device detail displays.

Table 2-1 Set Up Procedures for Non-IOS Access Points and Bridges (continued)

Tasks	Procedure	Notes
3. Set the read/write community string.	1. In the Summary Status page, click **Setup**. 2. Under Services, click **Security**. 3. Click **User Information**; then click **Add New User** or select an existing user. 4. Check all capabilities. Ident privileges are required only for APs that are running a firmware version earlier than 12.01T. 5. Click **Apply** or **OK**.	The community string is required for device discovery, reports, and for configuration and firmware jobs. The username is the AP read/write community.[2] You must also enter all community strings on the WLSE. See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.
4. Add an HTTP user and enable the User Manager.[3] You can use the same user that you created in Task 3, if the user has write, firmware, admin, and ident capabilities.	1. In the Summary Status page, click **Setup**. 2. Click **Security**. 3. Click **User Information**; then click **Add New User** or select an existing user. 4. Enter a username and password and select Firmware; then click **Apply**. 5. Return to the Security Setup page and click **User Manager**. 6. Select **Enabled**; then click **Apply** or **OK**.	Allows configuration uploads from the WLSE to access points. You must also enter HTTP users and passwords on the WLSE. See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

Table 2-1 Set Up Procedures for Non-IOS Access Points and Bridges (continued)

Tasks	Procedure	Notes
5. If you use HTTP to initiate configuration or firmware downloads, select TFTP as the transfer protocol between the WLSE and APs.	1. In the Summary Status page, click **Setup**. 2. Under Services, click **FTP**. 3. Select TFTP as the file transfer protocol. 4. In the Default File Server text box, enter the IP address of the WLSE. 5. Click **Apply** or **OK**.	TFTP is used for transferring configuration and firmware changes to access points. If you use SNMP as the protocol for configuration and firmware update (instead of HTTP), you do not have to select the WLSE as the TFTP server on the access point. The SNMP MIB takes care of this part of the process.

1. Do not run CDP on radio ports.
2. For example, if the AP has a user “lab” with password “cisco”, its SNMP credential is lab::10:1:::lab. Its HTTP username/password is lab/cisco. If the SNMP credential is set incorrectly, jobs on the AP will fail.
3. You can use a non-standard HTTP port. If HTTP browsing is not enabled, you must enable it. Enter the console and navigate to Security > Web Server. Enable Allow Non-Console Browsing.

Setting Up Non-IOS APs and Bridges—Using a WLSE Startup Template

You can perform initial configuration on access points by using the WLSE’s startup template feature.

Startup configuration works in conjunction with a DHCP server. The access points get their IP addresses from the DHCP server. If you prefer static IP addressing, you can either configure the DHCP server like a BOOTP server (using MAC address-to-IP address mapping) or configure the static IP address individually on each access point afterwards.

For information on using a startup template, see the online help or the “Managing Device Configuration” chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

CHAPTER 3

Configuring IOS Access Points for Network Management

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

Preparing IOS access points and the WLSE for participation in the Cisco Structured Wireless-Aware Network (SWAN), is covered in Chapter 4, "Configuring IOS Access Points for Radio Management."

This chapter contains the following topics:

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 3-2.
- Log into each device's Web interface—See Using the AP Web Interface for Network Management Set Up, page 3-5.

- 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 3-7.

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 "Using IOS Templates" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

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 online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

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 online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

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 system 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 online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

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 online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

Using WLSE Configuration Templates for Network Management Set Up

You can perform initial configuration by using the WLSE's startup template feature. For information on using a startup template, see the "Managing Device Configuration" chapter in the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

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.

Configuring IOS Access Points for Radio Management

This chapter provides procedures for preparing IOS access points 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.

This chapter contains the following topics:

Introduction

Note You must first configure all of the access points for basic network management. See Chapter 3, "Configuring IOS Access Points for Network Management."

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.

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). Two 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 4-3
- Understanding WLSM WDS Devices, page 4-5

Understanding WDS Access Points

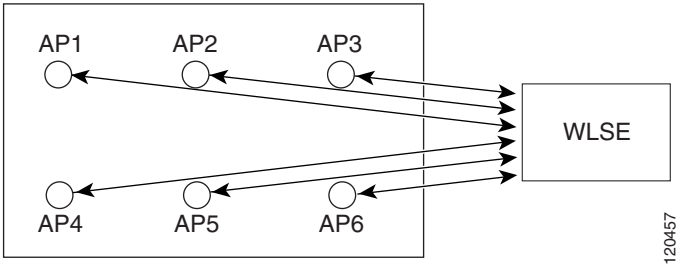
The WDS provides control path technologies that must be active on an AP in each AP subnet; a backup WDS can also be defined in each AP subnet. The WDS provides:

- 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.

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*.

Without a WDS to perform data aggregation, the communication between the access points and WLSE looks like this:

Figure 4-1 WLSE-AP Communications—Without WDS

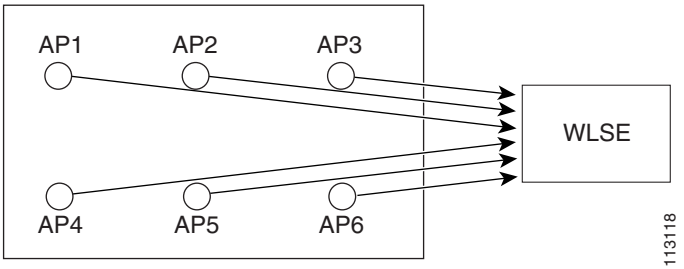


Using this approach, the WLSE can communicate with the APs using only these two methods:

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

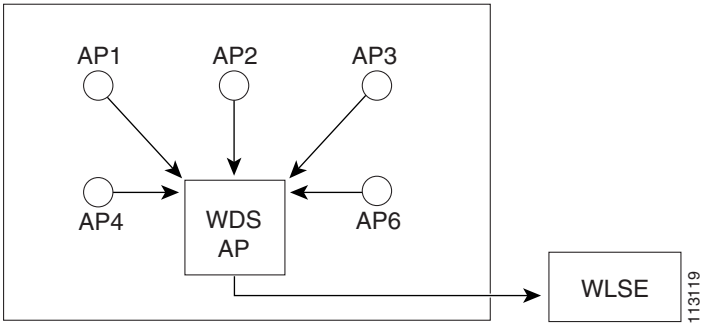
When you set up WLSE to manage the APs (the basic network management configuration), your network looks something like this:

Figure 4-2 AP to WLSE Data Aggregation



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 4-3 WLSE-AP Communications—With WDS



Understanding WLSM WDS 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 4-4).

Figure 4-4 WLSE-WLSM Communications

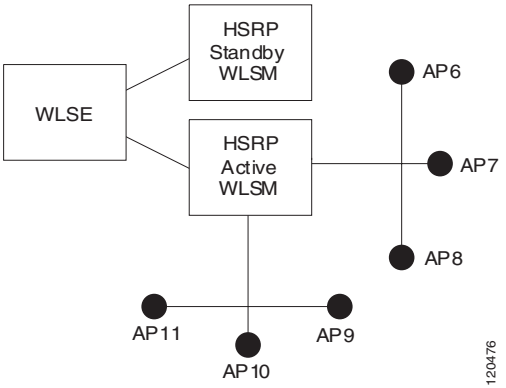
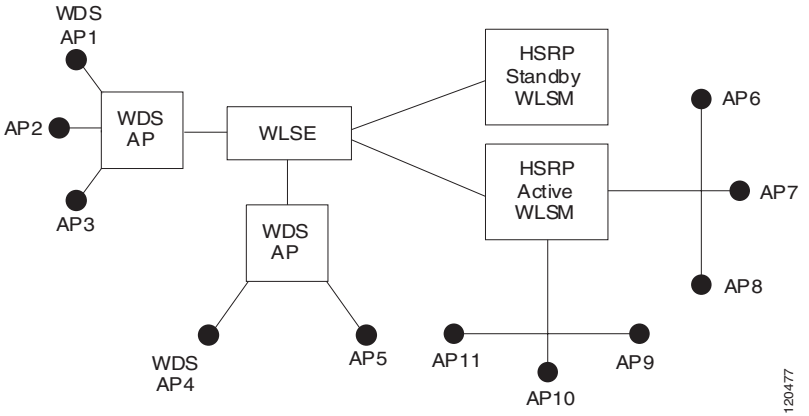


Figure 4-5 illustrates a network that uses both AP and WLSM WDS devices to manage the access points in the network. In this example, additional access points have been identified as backup AP-WDS devices (AP1 and AP4), and an additional HSRP-based WLSM-WDS device has been added to as a standby for the active WLSM-WDS.

Figure 4-5 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.

Note For a WLSM-WDS, the only option is the external RADIUS server; WLSM-WDS devices do not support the local RADIUS server feature.

- 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

Two types of devices can supply the WDS:

- A Wireless LAN Services Module (WLSM)

  Each WLSM supports multiple AP subnets, as long as all of the subnets are served by the switch on which the WLSM is installed.

- 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 primary and which ones are backups.

  Table 4-1 lists the general setup tasks for using these devices to supply the WDS:

Table 4-1 Radio Management Setup Tasks

Task	Description	References
1.	Configure WDS devices	Task 1: Configuring WDS Devices, page 4-9
2.	Configure infrastructure access points to authenticate to a WDS device	Task 2: Configuring Infrastructure APs, page 4-14
3.	Configure access points to be scanning-only APs	Task 3: Configuring Scanning APs, page 4-16
4.	Configure the WLSE with WLCCP credentials	Task 4: Configuring the WLSE, page 4-19
5.	Define authentication methods	Task 5: Configuring Authentication, page 4-19
6.	Confirm the configuration	Task 6: Confirming the Configuration, page 4-20

Task 1: Configuring WDS Devices

Configuring WDS 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.

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

The following sections describe how to configure the types of WDS devices:

- Configuring WDS Access Points (AP-WDS), page 4-9
- Configuring WDS on a Wireless LAN Services Module (WLSM-WDS), page 4-14

Configuring WDS Access Points (AP-WDS)

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 2.9* on cisco.com.

There are several ways to configure WDS access points:

- Using the Web Interface to Configure WDS APs, page 4-10
- Using the CLI Interface to Configure WDS APs, page 4-10
- Using a WLSE Configuration Template to Configure WDS APs, page 4-10

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

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.

Using the CLI Interface to Configure WDS APs

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.

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.

Procedure

Step 1 Log in to the WLSE web interface.

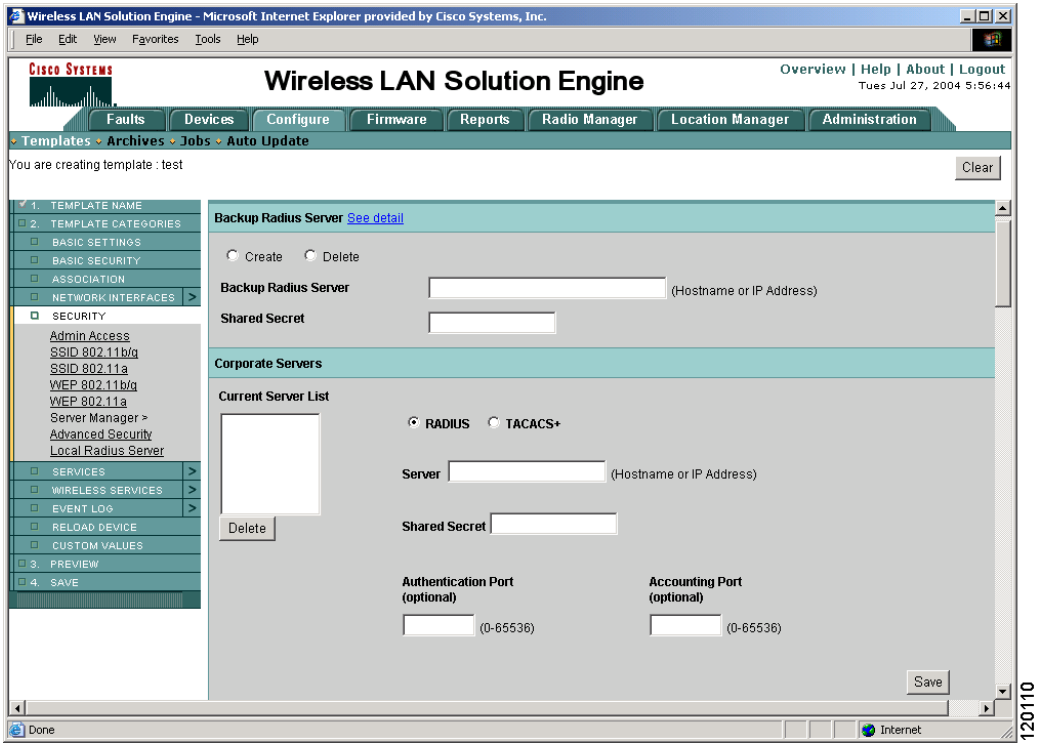
Step 2 Select **Configure > Templates.**

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:

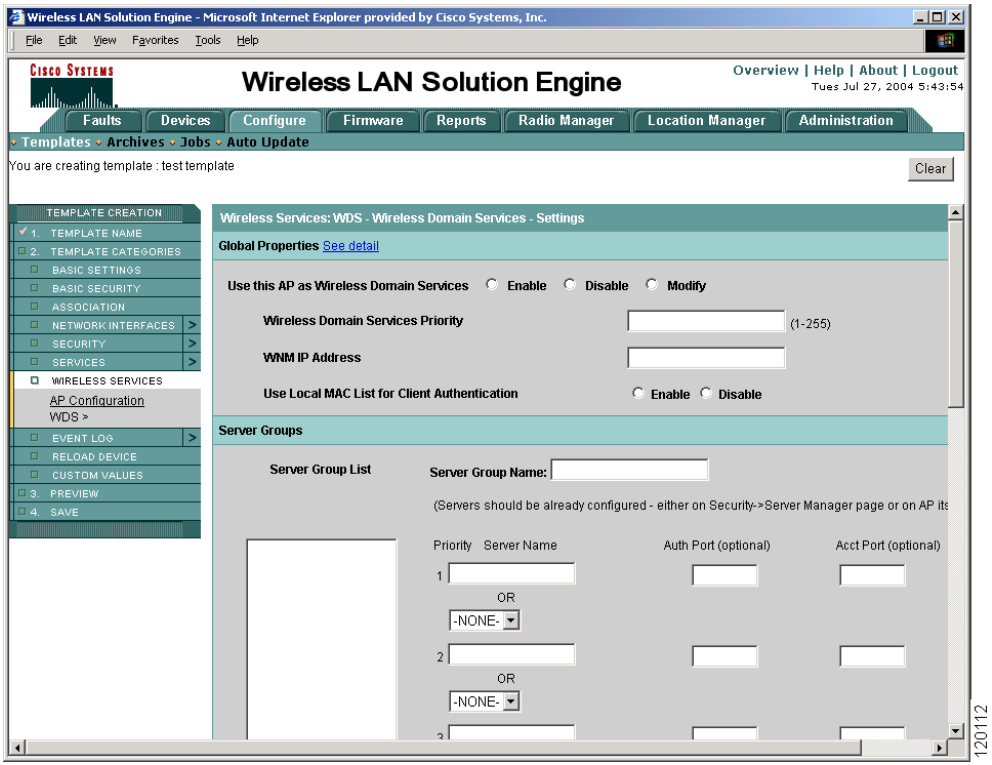
a. From the menu on the left, select **Security > Server Manager**.



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 2.9*.

Configuring WDS on a Wireless LAN Services Module (WLSM-WDS)

To use a WLSM to provide WDS:

Step 1 To configure the WLSM for WDS, follow the procedures in the WLSM documentation. Use the IP address of the WLSE as the WNM IP address.

Step 2 Use the following command to configure the WLSM with the address of the WLSE:

```
wlccp wnm ip address WLSE_IP_address
```

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

Task 2: 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 4-15
- Using the CLI to Configure Infrastructure APs, page 4-15
- Using a WLSE Configuration Job to Configure Infrastructure APs, page 4-15

Using the Web Interface to Configure Infrastructure APs

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.

Using the CLI to Configure Infrastructure APs

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.

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 2.9*.

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 2.9*.

Task 3: 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 "bug-lighted" clients (clients associated to unauthorized access points). Scanning-only APs do not accept client associations.

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 2.9*.

Table 4-2 on page 4-17 lists the high level tasks for setting up scanning APs.

Note Radio scanning requires a read/write SNMP community string on APs. For more information, see Introduction, page 4-2,

Table 4-2 Scanning AP Setup Tasks

Step	Description	References
3a	Configure scanning APs for basic management and radio management. • *Do not* configure VLAN/SSID on a scanning AP. • *Do not* configure a scanning AP as a WDS device.	Chapter 3, "Configuring IOS Access Points for Network Management." Task 2: Configuring Infrastructure APs, page 4-14
3b	Configure specific scanning AP parameters.	Step 3b: Configure a Scanning AP, page 4-18
3c	Run inventory on WLSE.	Step 3c: Run Inventory, page 4-18
3d	Enable client registration scanning on WLSE.	Step 3d: Enable Client Registration Scanning, page 4-18

Step 3a: Configure Scanning APs for Network and Radio Management

To configure scanning APs for basic management and radio management:

1. Configure scanning APs for basic network management.
   - *Do not* configure VLAN/SSID on a scanning AP.
   - *Do not* configure a scanning AP as a WDS device.

   See Chapter 3, "Configuring IOS Access Points for Network Management".
2. Configure scanning APs for radio management.

   See Task 2: Configuring Infrastructure APs, page 4-14.

Step 3b: Configure a Scanning AP

Using a WLSE Configuration Template

To use a WLSE configuration template to configure an access point for scanning only:

1. Select **Configuration > Templates > IOS > Basic Settings,** then select **Scanner Access Point**.
2. Select **Configuration > Templates > IOS > Network Interfaces**. Select a radio and select **Scanner Access Point**.

Using the AP CLI

To use the AP's CLI to configure an access point for scanning only, enter the following commands:

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

Step 3c: Run Inventory

Select **Administration > Devices > Discover > Inventory** and run inventory so the WLSE can update the role of the AP. 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 2.9*

Step 3d: Enable Client Registration Scanning

Select **Radio Management > Radio Monitoring** and enable Client Registration Scanning to detect bug-lighted clients.

For more information, see the online help or the "Radio Management" chapter of the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

Task 4: 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. The following configuration is required on the WLSE for radio management:

- SWAN components communicate via a Cisco proprietary technology called WLCCP. You must enter the WLCCP username and password in the WLSE. This username and password is used to LEAP authenticate the WLSE to the WDS devices in the network. See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.
- Enter the SNMP read-only and read/write communities for all managed IOS access points. See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.
- Enter Telnet/SSH credentials for IOS access points. See the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

Task 5: 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 Task 1: Configuring WDS Devices, page 4-9.
- 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 2.9*.

Create server groups on the WDS devices for:

- Infrastructure authentication—See Task 1: Configuring WDS Devices, page 4-9.
- 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.

Task 6: Confirming the Configuration

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

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 4-20.
- Using the command-line interface—See Using the Command-Line Interface to Validate the Configuration, page 4-21.

For WLSM-WDS devices, use the command-line interface to confirm the configuration.

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 2.9*.

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-WDS 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 5

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.

Configure each router and switch as shown in Table 5-1 on page 5-1.

Table 5-1 Setup Procedures for Routers and Switches

Task	Procedure	Notes
1. Enable CDP and verify that access points and bridges are visible from the router or switch.	1. 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**. 2. If CDP is not running, in global configuration mode, enter **cdp run** to enable CDP. 3. To verify that access points or bridges are visible in the device's CDP table, enter **show cdp neighbors**.	CDP is required for the WLSE to discover the device.

Table 5-1 Setup Procedures for Routers and Switches (continued)

Task	Procedure	Notes
2. Enable SNMP and set up community strings.	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.	SNMP is required for the WLSE to discover and manage the device.
3. (Optional) Set system name, contact, and location variables.	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*	These variables make the device more manageable. The system name, system contact, and location will appear in the device detail displays.

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.

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 servers. For more information, see the online help or the *User Guide for the CiscoWorks Wireless LAN Solution Engine, Release 2.9*.

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

INDEX

A

B

C

D

H

I

N

R

S

T

W