Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine Express

Release 2.8

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-5843-01

Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine Express

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 External AAA Servers, page 6-1

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 option for first-time device configuration. You can apply a configuration template to a number of access points—See the online help or the "Managing Device Configurations" chapter in the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.

After discovering and managing devices, you can use WLSE configuration templates for configuration changes—See the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.

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, add all APs as seed devices or import devices. See the online help or the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.
2. Enable SNMP. **Note** 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. **Note** 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. You must also enter all community strings on the WLSE. See the online help or the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*. The username is the AP read/write community.[2]
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 Wireless LAN Solution Engine Express, Release 2.8*.

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. **Note** 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 Wireless LAN Solution Engine Express, Release 2.8*.

Configuring IOS Access Points for Network Management

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

To prepare IOS access points and the WLSE for participation in the Cisco Structured Wireless-Aware Network (SWAN), see 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 the online help or the "Managing Device Configuration" chapter in the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.

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 can use WLSE configuration templates for configuration changes—See the "Using IOS Templates" chapter in the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.

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 Wireless LAN Solution Engine Express, Release 2.8*.

Step 4 To configure SNMP, enter the following commands in the sequence shown. The first command includes the ISO view. The second command sets the read-only SNMP community string, which enables discovery and the fault and report features on the WLSE. The third command sets the read/write community string, which enables firmware, configuration upload, and radio scanning. The community strings are also required for radio management.

a. Configure the SNMP read-only community. The minimal command set is:

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

b. Configure the SNMP read/write community. The minimal command is:

```
snmp-server community community_string rw
```

Note The community strings must also be entered on the WLSE. See the online help or the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.

Caution 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.

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 Wireless LAN Solution Engine Express, Release 2.8*.

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**.

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 Wireless LAN Solution Engine Express, Release 2.8*.

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 Wireless LAN Solution Engine Express, Release 2.8*.

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).

For procedures for preparing IOS access points for basic network management, see Chapter 3, "Configuring IOS Access Points for Network 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.

This chapter contains the following major topics:

- Introduction, page 4-2
- About WDS Devices, page 4-2
- Radio Management Setup Quick Reference, page 4-3
- Configuring Authentication, page 4-3
- Configuring WDS Access Points, page 4-4
- Configuring WDS on a Wireless LAN Services Module (WLSM), page 4-9

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.

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 2.8* on cisco.com.

About WDS Devices

WDS devices supply the services to other access points, which are called *infrastructure* access points in this document. 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 primary, and which ones are backups

- A Wireless LAN Services Module (WLSM)

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

Radio Management Setup Quick Reference

Table 4-1 lists the high-level setup tasks and sections in this document where you can find the detailed instructions:

Table 4-1 Radio Management Setup Tasks

Task	References
Configure WDS devices	Configuring WDS Access Points, page 4-4 Configuring WDS on a Wireless LAN Services Module (WLSM), page 4-9
Configure infrastructure access points to authenticate to a WDS device	Configuring Infrastructure Access Points to Register with WDS Access Points, page 4-10 Configuring Infrastructure Access Points to Register with a Wireless LAN Services Module, page 4-12
Configure access points to be scanning-only APs	Configuring Scanning APs, page 4-12
Configure the WLSE with WLCCP credentials	Configuring the WLSE, page 4-14
Define authentication servers	Configuring Authentication, page 4-3
Confirm the configuration	Confirming the Configuration, page 4-15

Configuring Authentication

To use WDS, both the infrastructure APs and the WLSE must use LEAP to authenticate to the WDS devices. For this purpose, you can use:

- Local authentication on a WDS device. See Configuring WDS Access Points, page 4-4.
- AAA servers that you have already configured, or configure servers as described in the online help or the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.

In addition, server groups must be created on the WDS access points for:

- Infrastructure authentication

For information on creating server groups for infrastructure authentication, see Configuring WDS Access Points, page 4-4.

- Client authentication

  For information on creating server groups for client authentication, see the access point documentation.

Configuring WDS Access Points

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

Note For an example 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**.

WDS must be active on an access point in each subnet in which APs are placed; backup WDS access point(s) can also be defined in each AP subnet.

Configuring WDS involves the following. See the rest of this section for detailed instructions.

- Define the AAA servers and server groups that the WDS will use to LEAP authenticate infrastructure access points and the WLSE.
- Enable WDS and set WDS priorities.
- Enter the WNM IP address.

There are three ways to configure WDS access points:

- Using the access point web interface—See Using the Web Interface to Configure WDS Access Points, page 4-5.
- Using the access point CLI interface—See Using the CLI Interface to Configure WDS Access Points, page 4-6.

- Using a WLSE configuration template—Using a WLSE Configuration Template to Configure WDS Access Points, page 4-8.

Using the Web Interface to Configure WDS Access Points

To configure WDS access points by using the web interface:

Step 1 Log in to an AP that will serve as a WDS device.

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

Step 3 Select the General Set-Up tab.

Step 4 To enable WDS, select **Use this AP as Wireless Domain Services**.

Step 5 Enter a value between 1 and 255 in the **Wireless Domain Services** priority field.

The priority value is used to determine which AP will be the active WDS AP when multiple APs are configured to run WDS. The highest priority is 255.

Step 6 Configure the Wireless Network Manager (WNM) options:

a. Select **Configure Wireless Network Manager.**

b. Enter the IP address of your WLSE in the **Wireless Network Manager IP Address** field.

c. Click **Apply**.

Step 7 Define the AAA server group(s) that will be used to LEAP authenticate infrastructure access points participating in SWAN and the WLSE:

a. Select the Server Groups tab.

b. Enter a server group name.

c. From the **Priority** lists, select the appropriate AAA servers.

If no AAA servers have been entered into the AP, click **Define Servers** to add the servers, then select the appropriate servers. Consult the AP online help for assistance in entering AAA servers into the AP.

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

Step 8 Configure the WDS AP to authenticate itself to the WDS so that it can participate in the SWAN hierarchy:

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

b. Select **Enable**.

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

Step 9 To commit the configuration, click **Apply**.

Note To configure authentication for wireless clients, see the relevant access point documentation.

Using the CLI Interface to Configure WDS Access Points

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

The key steps in configuring the WDS are:

- Configure AAA servers to authenticate SWAN infrastructure access points and the WLSE.
- Configure WDS.
- Configure the WNM.

To configure the WDS access points using the IOS command line interface:

Step 1 Log in to an access point that will be a WDS device.

Step 2 Turn on AAA services:

```
aaa new-model
```

Step 3 Define the RADIUS servers that you will use for infrastructure authentication and/or client authentication. Consult your RADIUS server documentation for the correct port numbers. CiscoSecure ACS uses port 1645 for authorization and port 1646 for accounting.

```
radius-server host [ ip_address | hostname ] auth-port port
acct-port port key shared_secret_key
```

Step 4 Define a server group for infrastructure authentication:

```
aaa group server radius server_group_name
    server radius_server
```

Step 5 Define at least one additional server group for wireless client authentication.

Step 6 Configure the AP to run WDS:

```
wlccp wds priority priority interface BVI1
```

where *priority* is a value from 1 to 255. Priority determines which AP will be the active WDS AP when multiple APs are configured to run WDS. The highest priority is 255.

Step 7 Configure the Wireless Network Manager (WNM) component:

```
wlccp wnm ip address wlse_ip_address
```

where *wlse_ip_address* is the address of the WLSE.

Step 8 Configure the server group the WDS will use to LEAP authenticate SWAN infrastructure access points. Use the server group name that you created in Step 4.

```
aaa authentication login named_authentication_list group
server_group_name

wlccp authentication-server infrastructure named_authentication_list
```

Step 9 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. Configure the WDS access point as an infrastructure access point:

```
wlccp ap username username password password
```

Note To configure authentication for wireless clients, see the relevant access point documentation.

Using a WLSE Configuration Template to Configure WDS Access Points

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

The major configuration steps are:

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

To configure WDS access points by using a WLSE configuration template:

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. 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 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 **Enabled** 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) 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. For information on configuration jobs, see Chapter 7, Managing Device Configuration, in the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.

Configuring WDS on a Wireless LAN Services Module (WLSM)

If you are using a WLSM to provide WDS, instead of using APs for WDS, follow the procedures in the WLSM documentation to configure it for WDS.

Also, 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.

Configuring Infrastructure Access Points to Register with WDS Access Points

The infrastructure access points initiate participation in SWAN by registering and LEAP authenticating with the WDS.

The only required configuration for infrastructure access points is the username and password used to register with the WDS.

There are three ways to configure infrastructure access points to register with WDS access points:

- Using the access point web interface—See Using the Web Interface to Configure Infrastructure APs, page 4-10.
- Using the access point CLI interface—See Using the Command Line Interface to Configure Infrastructure APs, page 4-11.
- Using a WLSE configuration template—See Using a WLSE Configuration Job to Configure Infrastructure APs, page 4-11.

Using the Web Interface to Configure Infrastructure APs

To use the web-based interface to configure infrastructure APs:

Step 1 Log in to the AP's web interface.

Step 2 Select **Wireless Services > AP**.

Step 3 Select **Enabled**.

Step 4 Enter the username and password for authenticating the infrastructure AP to the WDS.

Step 5 Click **Apply**.

Using the Command Line Interface to Configure Infrastructure APs

To use the command line interface to configure infrastructure APs:

Step 1 Log in to the AP's CLI.

Step 2 Enter the following command:

```
wlccp ap username username password password
```

where *username* and *password* are the credentials for authenticating the infrastructure access point to the WDS.

Using a WLSE Configuration Job to Configure Infrastructure APs

The WLSE can configure multiple infrastructure APs in a single job. To configure infrastructure APs using the WLSE, create a configuration template using the template creation wizard, 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 Wireless LAN Solution Engine Express, Release 2.8*.

To configure the username and password used to authenticate the AP to the WDS:

Step 1 Log in to the WLSE web interface.

Step 2 Select **Configure > Templates**.

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

Step 4 Select **Enabled**.

Step 5 Enter the username and password for LEAP authenticating infrastructure APs to the WDS.

Step 6 Create a configuration job to apply the template to the appropriate devices. For information on configuration jobs, see the online help or the "Managing Device Configuration" chapter in the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.

Configuring Infrastructure Access Points to Register with a Wireless LAN Services Module

To configure infrastructure access points to register with a WLSM, see the access point documentation on Cisco.com.

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 AP. Scanning APs can detect and report "bug-lighted" clients (clients associated to unauthorized access points). Scanning APs do not accept client associations. For more information on scanning APs and other requirements for using scanning APs with a WLSE, see the "Radio Management" chapter in the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.

Table 4-2 on page 4-12 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

Task	References
1. 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" Configuring Infrastructure Access Points to Register with WDS Access Points, page 4-10

Table 4-2 Scanning AP Setup Tasks (continued) (continued)

Task	References
2. Configure specific scanning AP parameters.	Configure a Scanning AP—Using the AP CLI, page 4-13 Configure a Scanning AP—Using a WLSE Configuration Template, page 4-13
3. Run inventory on WLSE.	Run Inventory, page 4-14
4. Enable client registration scanning on WLSE.	Enable Client Registration Scanning, page 4-14

Configure a Scanning AP—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
```

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**.

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 Wireless LAN Solution Engine Express, Release 2.8*

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 Wireless LAN Solution Engine Express, Release 2.8*.

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 APs in the network. See the online help or the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.
- 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 Wireless LAN Solution Engine Express, Release 2.8*.
- Enter Telnet/SSH credentials for IOS access points. See the online help or the *User Guide for the Wireless LAN Solution Engine Express, Release 2.8*.

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 access points. There are two ways to confirm configuration:

- Using the Web interface—See Using the Web Interface to Validate the Configuration, page 4-15.
- Using the command-line interface—See Using the Command-Line Interface to Validate the Configuration, page 4-16.

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 Wireless LAN Solution Engine Express, Release 2.8*.

Using the Web Interface to Validate the Configuration

To confirm the configurations using the web interface on WDS APs:

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

To use the CLI on the WDS APs to validate the configuration:

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

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 AP.

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.

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. **Note** R	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.

CHAPTER 6

Configuring External AAA Servers

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

This chapter covers setting up an ACS server. To set up a CAR server, see the CAR 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 Wireless LAN Solution Engine Express, Release 2.8*.

In addition to monitoring AAA servers, you can use an AAA server to authenticate to Wireless Domain Services (WDS) access points. 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