Configuring WDS, Fast Secure Roaming, and Radio Management

This chapter describes how to configure your access points for wireless domain services (WDS), fast, secure roaming of client devices, and radio management. This chapter contains these sections:

Understanding WDS

When you configure Wireless Domain Services on your network, access points on your wireless LAN use the WDS device (either an access point or a switch configured as the WDS device) to provide fast, secure roaming for client devices and to participate in radio management. If you use a switch as the WDS device, the switch must be equipped with a Wireless LAN Services Module (WLSM). An access point configured as the WDS device supports up to 60 participating access points. A WLSM-equipped switch supports up to 300 participating access points.

Fast, secure roaming provides rapid reauthentication when a client device roams from one access point to another, preventing delays in voice and other time-sensitive applications.

Access points participating in radio management forward information about the radio environment (such as possible rogue access points and client associations and disassociations) to the WDS device. The WDS device aggregates the information and forwards it to a wireless LAN solution engine (WLSE) device on your network.

Role of the WDS Device

The WDS device performs several tasks on your wireless LAN:

- Advertises its WDS capability and participates in electing the best WDS device for your wireless LAN. When you configure your wireless LAN for WDS, you set up one device as the main WDS candidate and one or more additional devices as backup WDS candidates. If the main WDS device goes off line, one of the backup WDS devices takes its place.
- Authenticates all access points in the subnet and establishes a secure communication channel with each of them.
- Collects radio data from access points in the subnet, aggregates the data, and forwards it to the WLSE device on your network.
- Registers all client devices in the subnet, establishes session keys for them, and caches their security credentials. When a client roams to another access point, the WDS device forwards the client's security credentials to the new access point.

Table 11-1 lists the number of participating access points supported by an acess point configured as the WDS device and by a WLSM-equipped switch configured as the WDS device.

Table 11-1 Participating Access Points Supported by WDS Devices

Unit Configured as WDS Device	Participating Access Points Supported
Access point that also serves client devices	30
Access point with radio interfaces disabled	60
WLSM-equipped switch	300

Role of Access Points Using the WDS Device

The access points on your wireless LAN interact with the WDS device in these activities:

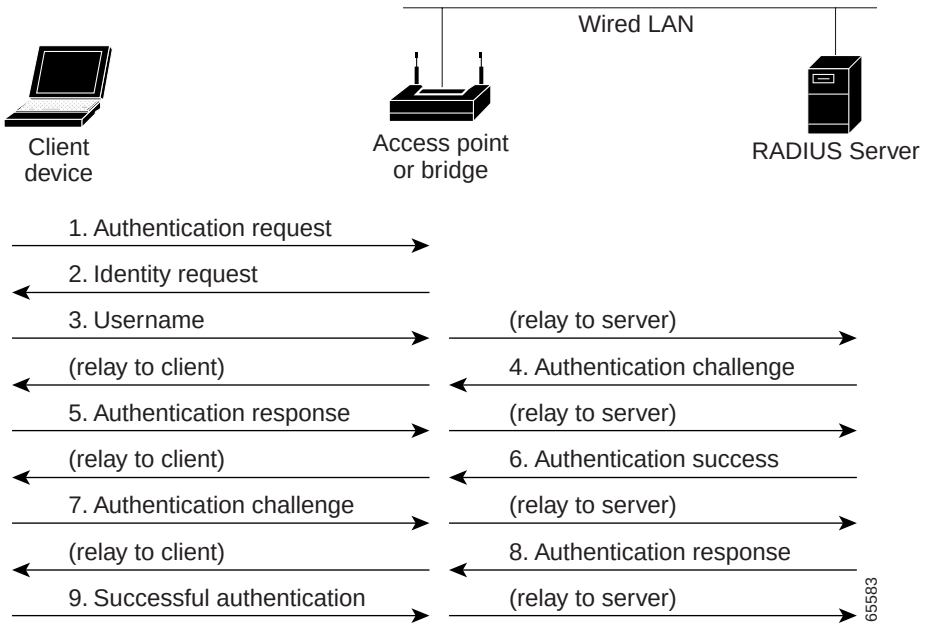
- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.
- Report radio data to the WDS device.

Understanding Fast Secure Roaming

Access points in many wireless LANs serve mobile client devices that roam from access point to access point throughout the installation. Some applications running on client devices require fast reassociation when they roam to a different access point. Voice applications, for example, require seamless roaming to prevent delays and gaps in conversation.

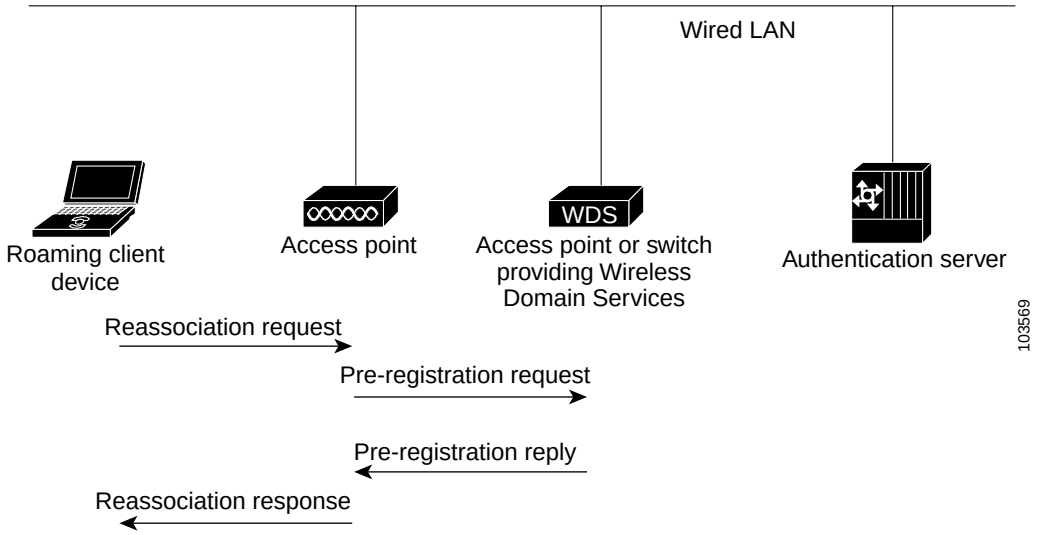
During normal operation, LEAP-enabled client devices mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server, as in Figure 11-1.

Figure 11-1 Client Authentication Using a RADIUS Server



When you configure your wireless LAN for fast, secure roaming, however, LEAP-enabled client devices roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), a device configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client so quickly that there is no perceptible delay in voice or other time-sensitive applications. Figure 11-2 shows client authentication using CCKM.

Figure 11-2 Client Reassociation Using CCKM and a WDS Access Point



The WDS device maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the client sends a reassociation request to the new access point, and the new access point relays the request to the WDS device. The WDS device forwards the client's credentials to the new access point, and the new access point sends the reassociation response to the client. Only two packets pass between the client and the new access point, greatly shortening the reassociation time. The client also uses the reassociation response to generate the unicast key.

Understanding Radio Management

Access points participating in radio management scan the radio environment and send reports to the WDS device on such radio information as potential rogue access points, associated clients, client signal strengths, and the radio signals from other access points. The WDS device forwards the aggregated radio data to the WLSE device on your network. Access points participating in radio management also assist with the self-healing wireless LAN, automatically adjusting settings to provide coverage in case a nearby access point fails. Refer to the "Configuring Radio Management" section on page 11-23 for instructions on configuring radio management.

Understanding Layer 3 Mobility

When you use a WLSM as the WDS device on your network, you can install access points anywhere in a large Layer 3 network without configuring one specific subnet or VLAN throughout the wired switch infrastructure. Client devices use multipoint GRE (mGRE) tunnels to roam to access points that reside on different Layer 3 subnets. The roaming clients stay connected to your network without changing IP addresses.

The access point features that provide mobile clients with fast, secure Layer 3 mobility are IP-Based Wireless Domain Services and Layer 3 Mobility Service Through Fast Secure Roaming Tunnels.

IP-Based Wireless Domain Services

You use IP-based WDS to configure the access point with the IP address of its WDS device. This allows the access point to use a Cisco network infrastructure device running WDS from anywhere in the network.

Layer 3 Mobility Service Through Fast Secure Roaming Tunnels

The access point uses this feature to segregate WLAN clients into different mobility groups. After a client is authenticated according to its mobility group's security policy, all IP traffic from that client is encapsulated using generic routing encapsulation (GRE) and sent to a specific multipoint GRE (mGRE) interface of a Cisco Structured Wireless-Aware Network (SWAN) infrastructure device that supports mobility groups. An access point with Layer 3 Mobility Service provides clients within each mobility group with Layer 3 mobility when used with a Cisco SWAN infrastructure device supporting Layer 3 mobility. Support for Layer 3 roaming is provided for all Wi-Fi certified client devices. Support for fast secure Layer 3 roaming is provided for Cisco or Cisco Compatible wireless LAN client devices using the Cisco Centralized Key Management (CCKM) protocol.

Components Required for Layer 3 Mobility

The Layer 3 mobility wireless LAN solution consists of these hardware and software components:

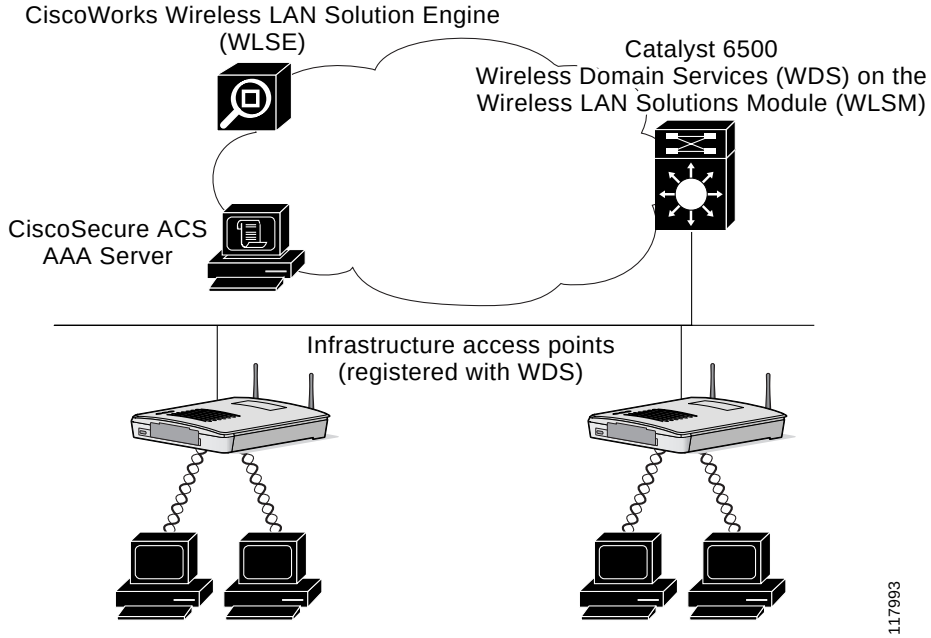
- 1100 or 1200 series access points participating in WDS
- Catalyst 6500 switch with Supervisor Module and WLSM configured as the WDS device

Note You must use a WLSM as your WDS device to properly configure Layer 3 mobility. Layer 3 mobility is not supported when your WDS device is an access point.

- Cisco (or Cisco compatible) client devices

Figure 11-3 shows the components that interact to perform Layer 3 mobility.

Figure 11-3 Required Components for Layer 3 Mobility



Configuring WDS on the WLSM

For instructions on configuring WDS on a switch's Wireless LAN Services Module (WLSM), refer to the *Catalyst 6500 Series Wireless LAN Services Module Installation and Configuration Note*.

Click this link to browse to the information pages for the Cisco Structured Wireless-Aware Network (SWAN):

http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html

Configuring WDS and Fast Secure Roaming

This section describes how to configure WDS on your network and fast, secure roaming on your wireless LAN. This section contains these sections:

Guidelines for WDS

Follow these guidelines when configuring WDS:

- If you use an access point as your WDS device, either disable the radio interfaces on the unit or use an access point that does not serve a large number of client devices. If client devices associate to the WDS access point when it starts up, the clients might wait up to 10 minutes to be authenticated.
- A WDS access point that also serves client devices supports up to 30 participating access points, but a WDS access point with radios disabled supports up to 60 participating access points.
- Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to return (fall back) to repeater mode in case of Ethernet failure.
- You cannot configure a 350 series access point as a WDS access point. However, you can configure 350 series access points to use the WDS access point.

Requirements for WDS and Fast Secure Roaming

To configure WDS, you must have these items on your wireless LAN:

- At least one access point or switch (equipped with a Wireless LAN Services Module) that you can configure as the WDS device
- An authentication server (or an access point configured as a local authenticator)
- Cisco Aironet client devices running Cisco client firmware version 5.20.17 or later

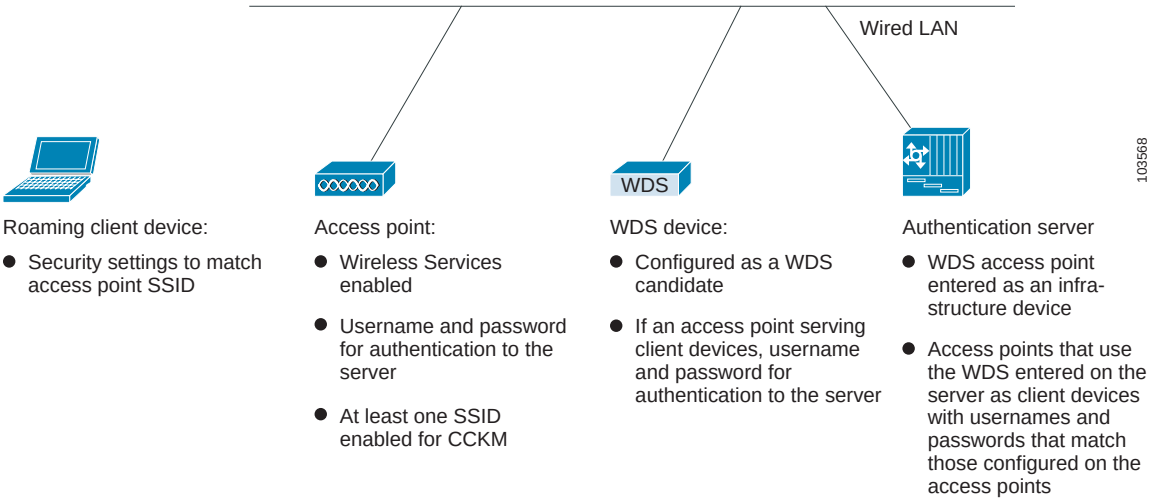
Configuration Overview

You must complete three major steps to set up WDS and fast, secure roaming:

1. Configure access points or switches as potential WDS devices. This chapter provides instructions for configuring an access point as a WDS device. For instructions on configuring a WLSM-equipped switch as a WDS device, refer to the *Catalyst 6500 Series Wireless LAN Services Module Installation and Configuration Note*.
2. Configure the rest of your access points to use the WDS device.
3. Enable access points on the subnet to allow CCKM authenticated key management for at least one SSID. See the "Configuring Authentication Types" section on page 10-10 for complete instructions on enabling CCKM.
4. Configure the authentication server on your network to authenticate the WDS device and the access points that use the WDS device.

Figure 11-4 shows the required configuration for each device that participates in fast, secure roaming.

Figure 11-4 Configurations on Devices Participating in WDS and CCKM



Configuring Access Points as Potential WDS Access Points

Note For the main WDS candidate, configure an access point that does not serve a large number of client devices. If client devices associate to the WDS access point when it starts up, the clients might wait up to 10 minutes to be authenticated.

Note Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in case of Ethernet failure.

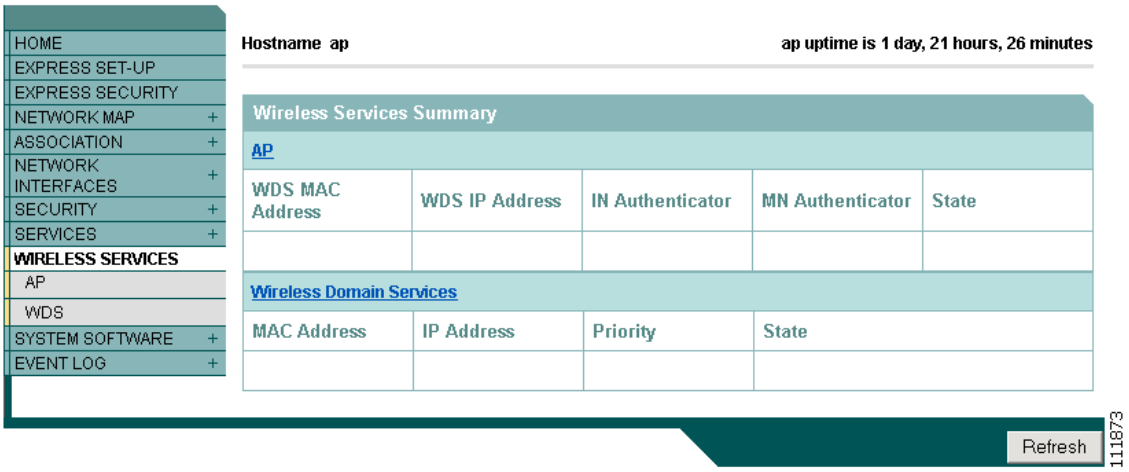
Note When WDS is enabled, the WDS access point performs and tracks all LEAP authentications. Therefore, you must configure EAP security settings on the WDS access point. See Chapter 10, "Configuring Authentication Types," for instructions on configuring EAP on the access point.

Note You cannot configure a 350 series access point as a WDS access point. However, you can configure 350 series access points to participate in WDS through the WDS device on your network.

On the access point that you want to configure as your primary WDS access point, follow these steps to configure the access point as the main WDS candidate:

Step 1 Browse to the Wireless Services Summary page. Figure 11-5 shows the Wireless Services Summary page.

Figure 11-5 Wireless Services Summary Page



Step 2 Click **WDS** to browse to the WDS/WNM Summary page.

Step 3 On the WDS/WNM Summary page, click **General Setup** to browse to the WDS/WNM General Setup page. Figure 11-6 shows the General Setup page.

Figure 11-6 WDS/WNM General Setup Page

Step 4 Check the *Use this AP as Wireless Domain Services* check box.

Step 5 In the Wireless Domain Services Priority field, enter a priority number from 1 to 255 to set the priority of this WDS candidate. The WDS access point candidate with the highest number in the priority field becomes the acting WDS access point. For example, if one WDS candidate is assigned priority 255 and one candidate is assigned priority 100, the candidate with priority 255 becomes the acting WDS access point.

Step 6 (Optional) Select the *Use Local MAC List for Client Authentication* check box to authenticate client devices using MAC addresses in the local list of addresses configured on the WDS device. If you do not select this check box, the WDS device uses the server specified for MAC-address authentication on the Server Groups page to authenticate clients based on MAC addresses.

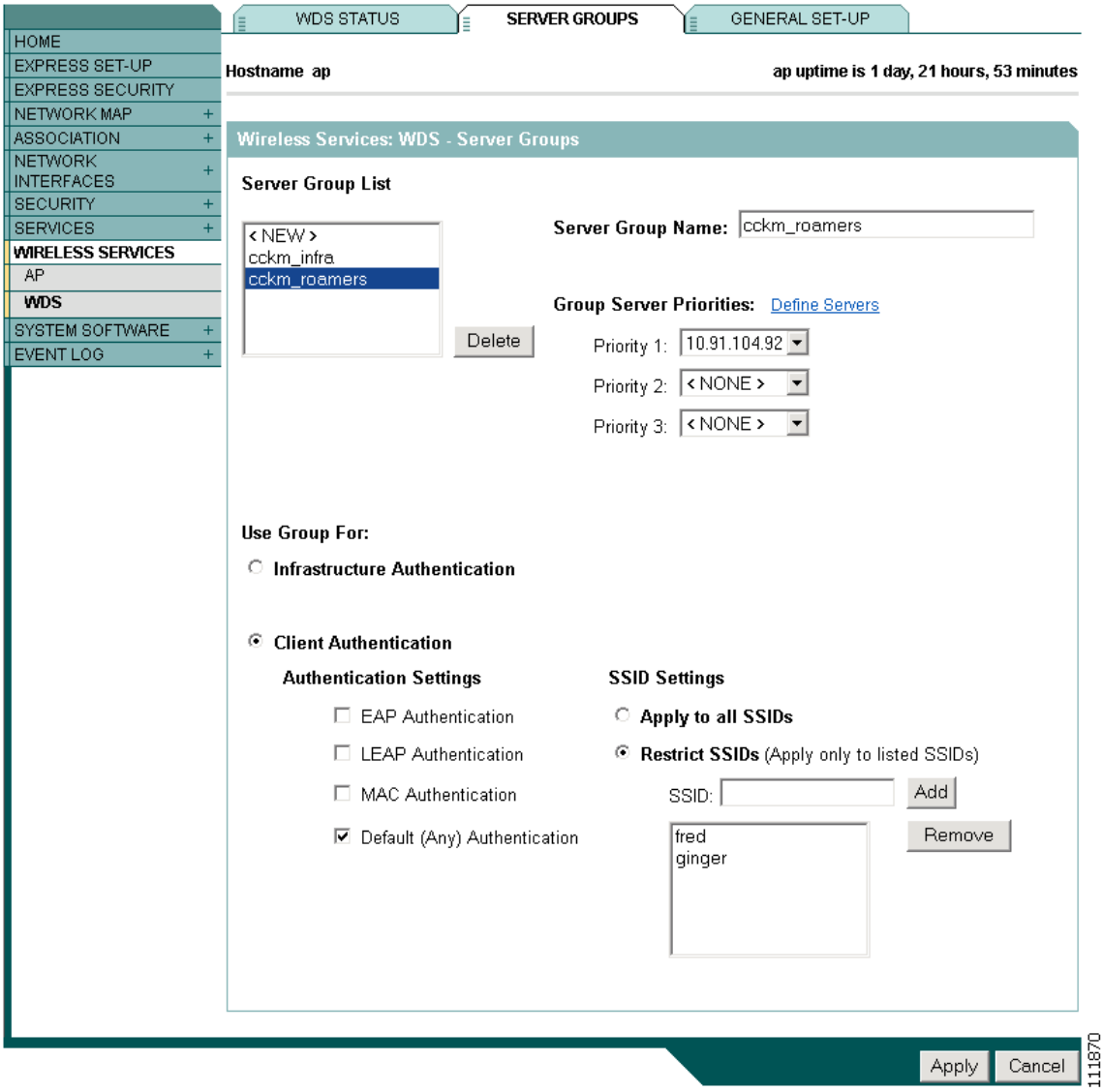
Note Selecting the *Use Local MAC List for Client Authentication* check box does not force client devices to perform MAC-based authentication. It provides a local alternative to server-based MAC-address authentication.

Step 7 (Optional) If you use a Wireless LAN Solutions Engine (WLSE) on your network, check the *Configure Wireless Network Manager* check box and enter the IP address of the WLSE device in the *Wireless Network Manager IP Address* field. The WDS access point collects radio measurement information from access points and client devices and sends the aggregated data to the WLSE device.

Step 8 Click **Apply**.

Step 9 Click **Server Groups** to browse to the WDS Server Groups page. Figure 11-7 shows the WDS Server Groups page.

Figure 11-7 WDS Server Groups Page



Step 10 Create a group of servers to be used for 802.1x authentication for the infrastructure devices (access points) that use the WDS access point. Enter a group name in the Server Group Name field.

Step 11 Select the primary server from the Priority 1 drop-down menu. (If a server that you need to add to the group does not appear in the Priority drop-down menus, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)

Note If you don't have an authentication server on your network, you can configure an access point as a local authentication server. See Chapter 8, "Configuring an Access Point as a Local Authenticator," for configuration instructions.

Step 12 (Optional) Select backup servers from the Priority 2 and 3 drop-down menus.

Step 13 Click **Apply**.

Step 14 Configure the list of servers to be used for 802.1x authentication for CCKM-enabled client devices. You can specify a separate list for clients using a certain type of authentication, such as EAP, LEAP, or MAC-based, or specify a list for client devices using any type of authentication. Enter a group name for the server or servers in the Server Group Name field.

Step 15 Select the primary server from the Priority 1 drop-down menu. (If a server that you need to add to the group does not appear in the Priority drop-down menus, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)

Step 16 (Optional) Select backup servers from the Priority 2 and 3 drop-down menus.

Step 17 (Optional) Select **Restrict SSIDs** to limit use of the server group to client devices using specific SSIDs. Enter an SSID in the SSID field and click **Add**. To remove an SSID, highlight it in the SSID list and click **Remove**.

Step 18 Click **Apply**.

Step 19 Configure the WDS access point for LEAP authentication. See Chapter 10, "Configuring Authentication Types," for instructions on configuring LEAP.

Note If your WDS access point serves client devices, follow the instructions in the "Configuring Access Points to use the WDS Device" section on page 11-13 to configure the WDS access point to use the WDS.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Access Points as Potential WDS Access Points" section on page 11-8:

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bvi1
AP(config)# wlccp authentication-server infrastructure cckm_infra
AP(config)# wlccp authentication-server client any cckm_roamers
AP(config-wlccp-auth)# ssid fred
AP(config-wlccp-auth)# ssid ginger
AP(config)# end
```

In this example, infrastructure devices are authenticated using server group *cckm_infra*; CCKM-enabled client devices using SSIDs *fred* or *ginger* are authenticated using server group *cckm_roamers*.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

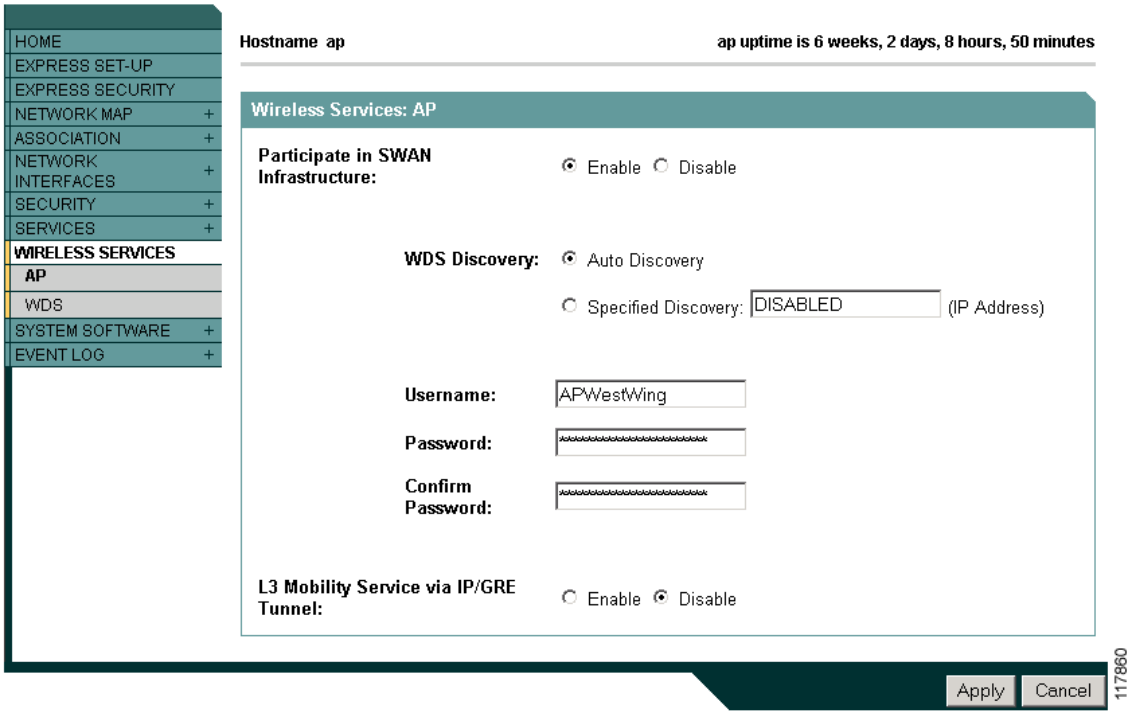
Configuring Access Points to use the WDS Device

Follow these steps to configure an access point to authenticate through the WDS device and participate in CCKM:

Step 1 Browse to the Wireless Services Summary page.

Step 2 Click **AP** to browse to the Wireless Services AP page. Figure 11-8 shows the Wireless Services AP page.

Figure 11-8 Wireless Services AP Page



Step 3 Click **Enable** for the *Participate in SWAN Infrastructure* setting.

Step 4 (Optional) Select **Specified Discovery** and enter the IP address of the WDS device in the entry field. This feature--IP-based WDS--allows the access point to use a Cisco network infrastructure device running WDS from anywhere in the network. When you enable Specified Discovery, the access point immediately authenticates with the WDS device instead of waiting for WDS advertisements. If the WDS device that you specify does not respond, the access point waits for WDS advertisements.

Step 5 In the Username field, enter a username for the access point. This username must match the username that you create for the access point on your authentication server.

Step 6 In the Password field, enter a password for the access point, and enter the password again in the Confirm Password field. This password must match the password that you create for the access point on your authentication server.

Step 7 (Optional) Select **Enable** for the L3 Mobility Service via IP/GRE Tunnel setting to configure the access point to participate in Layer 3 mobility. Your wireless LAN must contain these components to enable Layer 3 mobility:

- 1100 or 1200 series access points participating in WDS
- a Cisco Catalyst 6500 switch equipped with a WLSM configured as the WDS device

Note The **L3 Mobility Service via IP/GRE Tunnel** option does not appear on the Wireless Services AP page on access points running Cisco IOS Release 12.2(15)XR or later. This feature is enabled automatically on access points running Cisco IOS Release 12.2(15)XR or later.

Step 8 Click **Apply**.

The access points that you configure to interact with the WDS automatically perform these steps:

- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Access Points to use the WDS Device" section on page 11-13:

```
AP# configure terminal
AP(config)# wlccp ap wds ip address 10.91.104.92
AP(config)# wlccp ap username APWestWing password 7 wes7win8
AP(config)# end
```

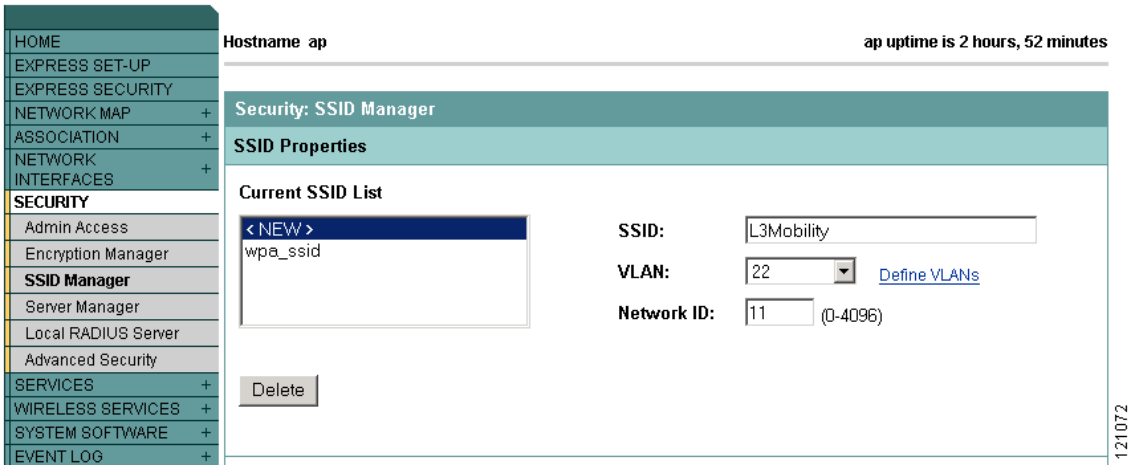
In this example, the access point is enabled to interact with a specific WDS device, and it authenticates to the authentication server using *APWestWing* as its username and *wes7win8* as its password. You must configure the same username and password pair when you set up the access point as a client on your authentication server.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Enabling Layer 3 Mobility on an SSID

Use the Network ID entry field on the SSID Manager page to map an SSID to a specific mobility network ID. Figure 11-9 shows the SSID Manager page.

Figure 11-9 Network ID Entry Field on the SSID Manager Page



CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Enabling Layer 3 Mobility on an SSID" section on page 11-15:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid L3Mobility
AP(config-if-ssid)# mobility network-id 11
AP(config-if-ssid)# end
```

In this example, the SSID *L3Mobility* is mapped to mobility network ID 11.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

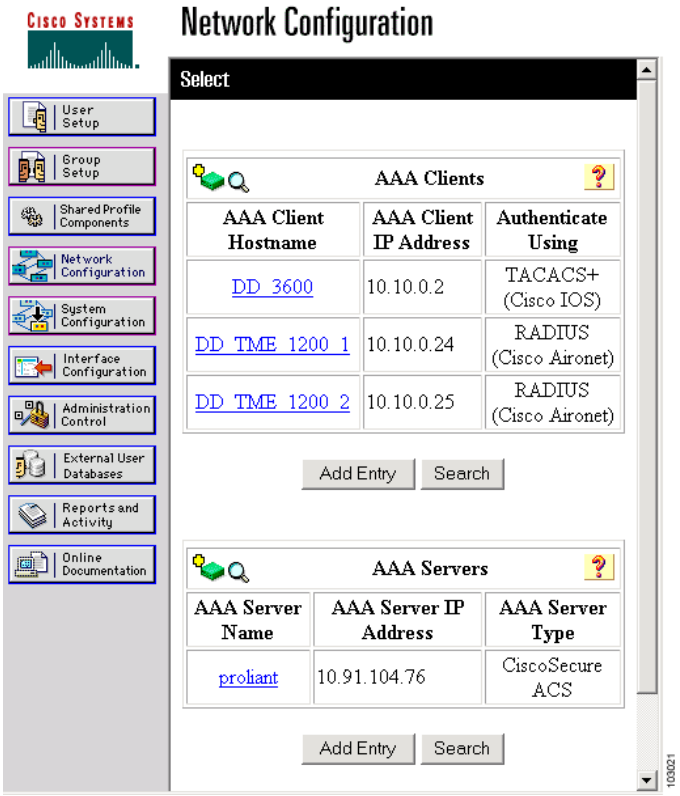
Configuring the Authentication Server to Support Fast Secure Roaming

The WDS device and all access points participating in CCKM must authenticate to your authentication server. On your server, you must configure usernames and passwords for the access points and a username and password for the WDS device.

If your server runs Cisco ACS, follow these steps to configure the access points on your server:

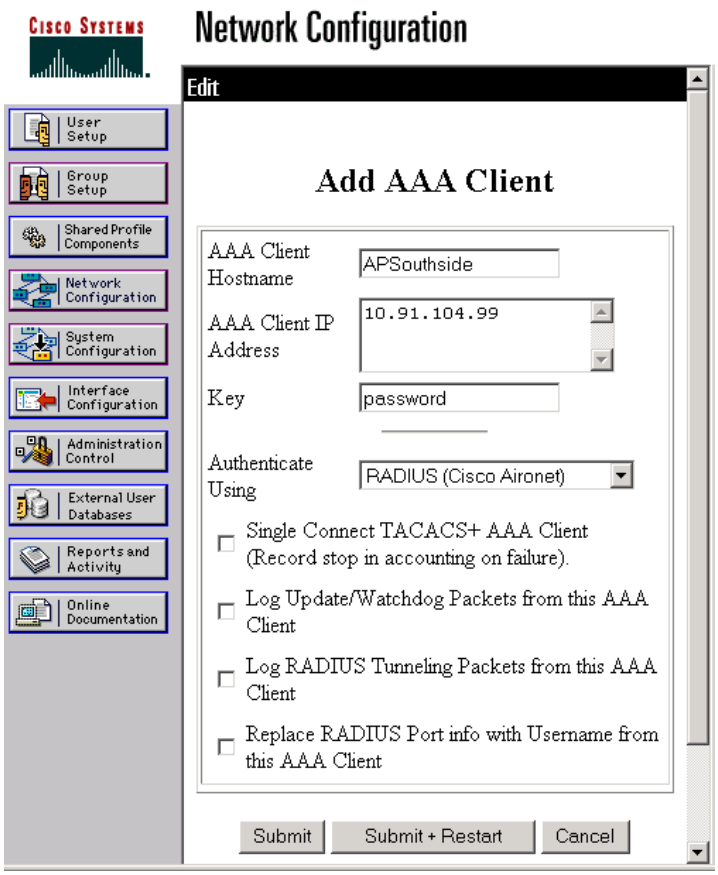
Step 1 Log into Cisco Secure ACS and click **Network Configuration** to browse to the Network Configuration page. You must use the Network Configuration page to create an entry for the WDS device. Figure 11-10 shows the Network Configuration page.

Figure 11-10 Network Configuration Page



Step 2 Click **Add Entry** under the AAA Clients table. The Add AAA Client page appears. Figure 11-11 shows the Add AAA Client page.

Figure 11-11 Add AAA Client Page



Step 3 In the AAA Client Hostname field, enter the name of the WDS device.

Step 4 In the AAA Client IP Address field, enter the IP address of the WDS device.

Step 5 In the Key field, enter exactly the same password that is configured on the WDS device.

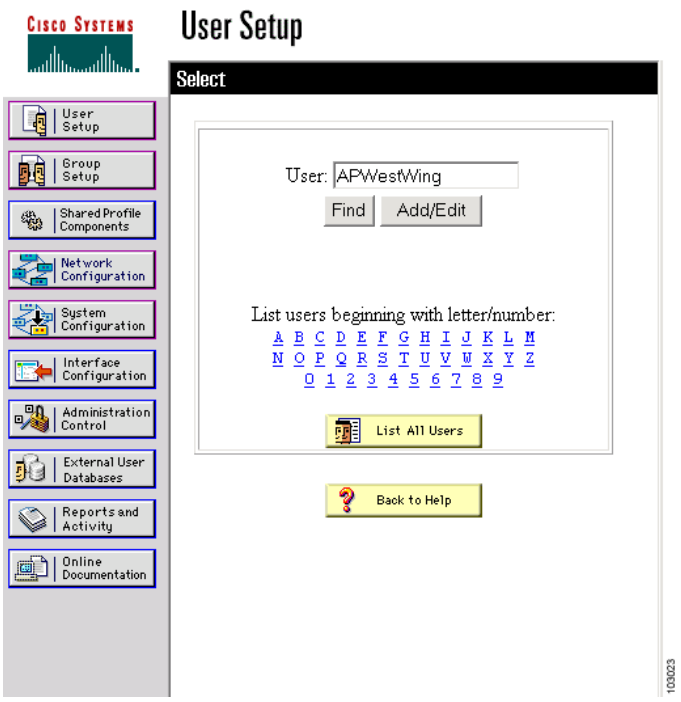
Step 6 From the Authenticate Using drop-down menu, select **RADIUS (Cisco Aironet)**.

Step 7 Click **Submit**.

Step 8 Repeat Step 2 through Step 7 for each WDS device candidate.

Step 9 Click **User Setup** to browse to the User Setup page. You must use the User Setup page to create entries for the access points that use the WDS device. Figure 11-12 shows the User Setup page.

Figure 11-12 User Setup Page

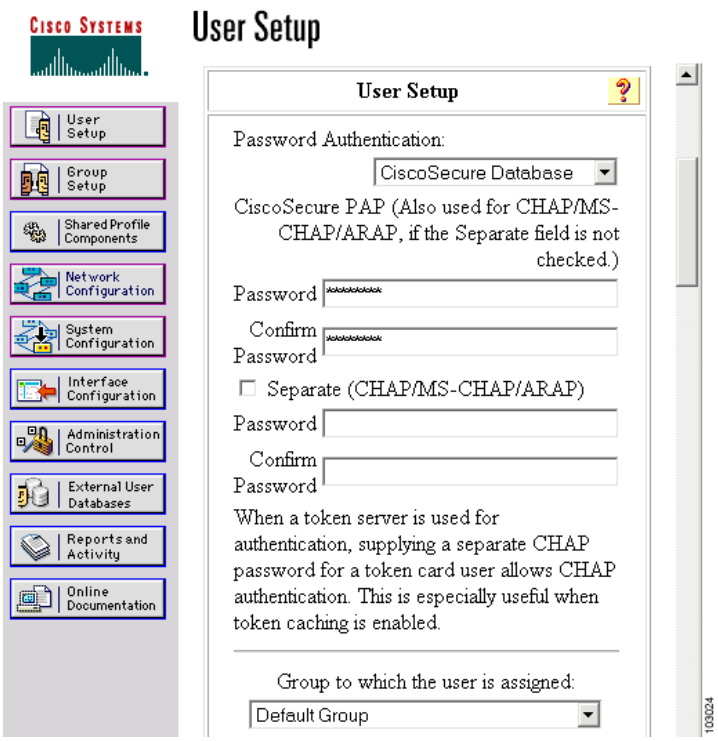


Step 10 Enter the name of the access point in the User field.

Step 11 Click **Add/Edit**.

Step 12 Scroll down to the User Setup box. Figure 11-13 shows the User Setup box.

Figure 11-13 ACS User Setup Box



Step 13 Select **CiscoSecure Database** from the Password Authentication drop-down menu.

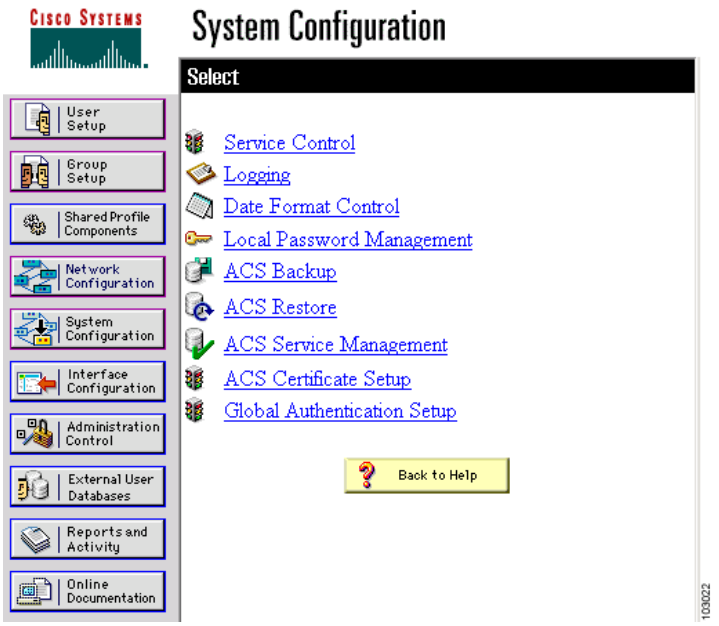
Step 14 In the Password and Confirm Password fields, enter exactly the same password that you entered on the access point on the Wireless Services AP page.

Step 15 Click **Submit**.

Step 16 Repeat Step 10 through Step 15 for each access point that uses the WDS device.

Step 17 Browse to the System Configuration page, click **Service Control**, and restart ACS to apply your entries. Figure 11-14 shows the System Configuration page.

Figure 11-14 ACS System Configuration Page



Viewing WDS Information

On the web-browser interface, browse to the Wireless Services Summary page to view a summary of WDS status.

On the CLI in privileged exec mode, use these commands to view information about the current WDS device and other access points participating in CCKM:

Command	Description
show wlccp ap	Use this command on access points participating in CCKM to display the WDS device's MAC address, the WDS device's IP address, the access point's state (authenticating, authenticated, or registered), the IP address of the infrastructure authenticator, and the IP address of the client device (MN) authenticator.
show wlccp wds { **ap** | **mn** } [**detail**] [**mac-addr** *mac-address*]	On the WDS device only, use this command to display cached information about access points and client devices. • **ap**—Use this option to display access points participating in CCKM. The command displays each access point's MAC address, IP address, state (authenticating, authenticated, or registered), and lifetime (seconds remaining before the access point must reauthenticate). Use the **mac-addr** option to display information about a specific access point. • **mn**—Use this option to display cached information about client devices, also called mobile nodes. The command displays each client's MAC address, IP address, the access point to which the client is associated (cur-AP), and state (authenticating, authenticated, or registered). Use the **detail** option to display the client's lifetime (seconds remaining before the client must reauthenticate), SSID, and VLAN ID. Use the **mac-addr** option to display information about a specific client device. If you only enter **show wlccp wds**, the command displays the access point's IP address, MAC address, priority, and interface state (administratively standalone, active, backup, or candidate). If the state is backup, the command also displays the current WDS device's IP address, MAC address, and priority.

Using Debug Messages

In privileged exec mode, use these debug commands to control the display of debug messages for devices interacting with the WDS device:

Command	Description
debug wlccp ap {**mn** | **wds-discovery** | **state**}	Use this command to turn on display of debug messages related to client devices (**mn**), the WDS discovery process, and access point authentication to the WDS device (**state**).
debug wlccp dump	Use this command to perform a dump of WLCCP packets received and sent in binary format.
debug wlccp packet	Use this command to turn on display of packets to and from the WDS device.
debug wlccp wds [**aggregator** | **authenticator** | **nm** | **state** | **statistics**]	Use this command and its options to turn on display of WDS debug messages. Use the **statistics** option to turn on display of failure statistics.
debug wlccp wds authenticator {**all** | **dispatcher** | **mac-authen** | **process** | **rxdata** | **state-machine** | **txdata**}	Use this command and its options to turn on display of WDS debug messages related to authentication.

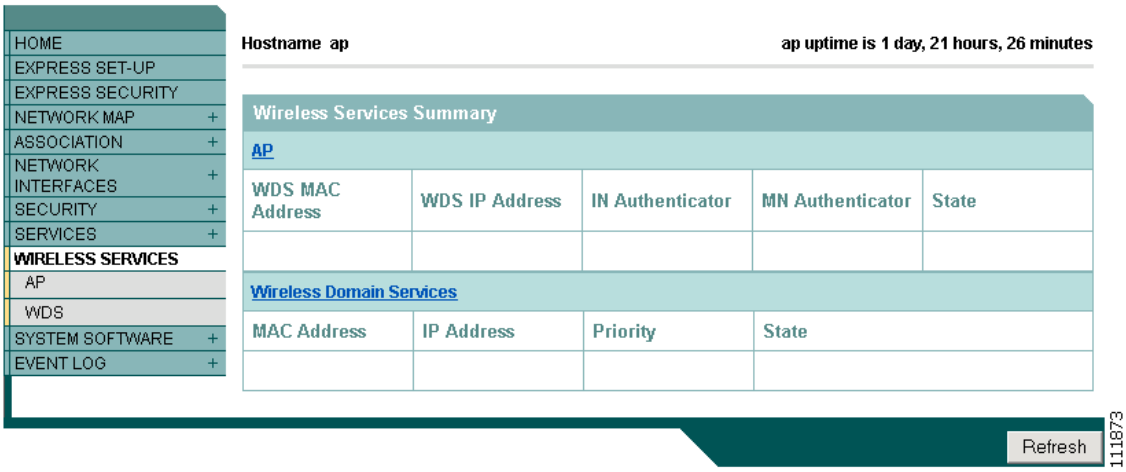
Configuring Radio Management

When you configure access points on your wireless LAN to use WDS, the access points automatically play a role in radio management when they interact with the WDS device. To complete the radio management configuration, you configure the WDS device to interact with the WLSE device on your network.

Follow these steps to enable radio management on an access point configured as a WDS device:

Step 1 Browse to the Wireless Services Summary page. Figure 11-15 shows the Wireless Services Summary page.

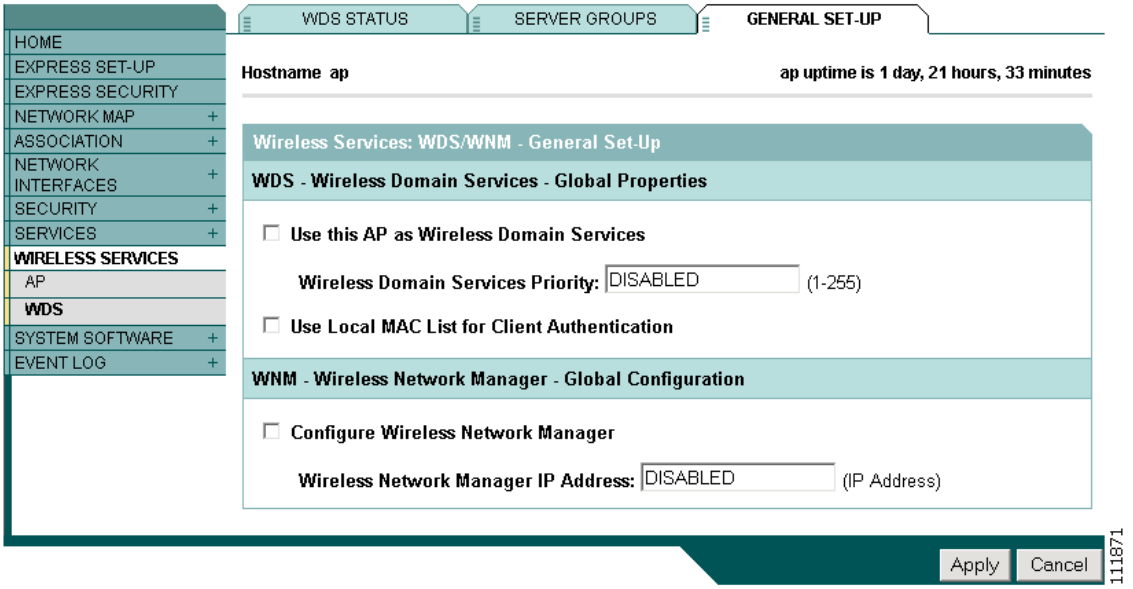
Figure 11-15 Wireless Services Summary Page



Step 2 Click **WDS** to browse to the General Setup page.

Step 3 On the WDS/WNM Summary page, click **Settings** to browse to the General Setup page. Figure 11-16 shows the General Setup page.

Figure 11-16 WDS/WNM General Setup Page



Step 4 Check the *Configure Wireless Network Manager* check box.

Step 5 In the *Wireless Network Manager IP Address* field, enter the IP address of the WLSE device on your network.

Step 6 Click **Apply**. The WDS access point is configured to interact with your WLSE device.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Radio Management" section on page 11-23:

```
AP# configure terminal
AP(config)# wlccp wnm ip address 192.250.0.5
AP(config)# end
```

In this example, the WDS access point is enabled to interact with a WLSE device with the IP address 192.250.0.5.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.