CHAPTER 12

Configuring WDS, Fast Secure Roaming, Radio Management, and Wireless Intrusion Detection Services

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

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*.

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, an Integrated Services Router, 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, an Integrated Services Router (ISR) configured as the WDS devices supports up to 100 participating access points, and a WLSM-equipped switch supports up to 600 participating access points and up to 240 mobility groups.

Note A single access point supports up to 16 mobility groups.

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.
- Acts as a pass-through for all 802.1x-authenticated client devices associated to participating access points.
- Registers all client devices in the subnet that use dynamic keying, 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 12-1 lists the number of participating access points supported by the platforms that can be configured as a WDS device: an access point, an ISR, or a WLSM-equipped switch.

Table 12-1 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

Table 12-1 Participating Access Points Supported by WDS Devices (continued)

Unit Configured as WDS Device	Participating Access Points Supported
Integrated Services Router (ISR)	100 (depending on ISR platform)
WLSM-equipped switch	600

Role of Access Points Using the WDS Device

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

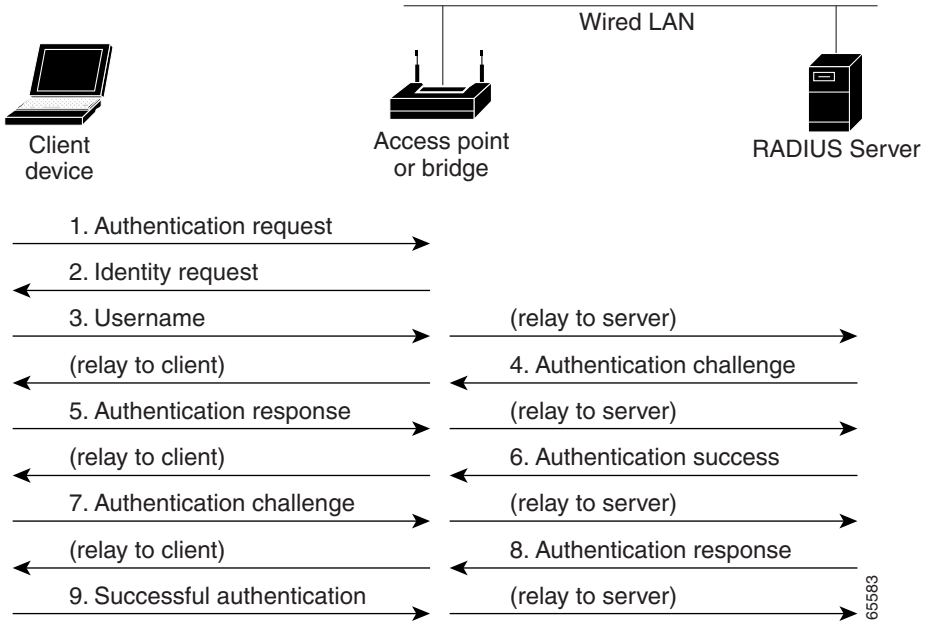
- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.
- Report radio data to the WDS device.

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.

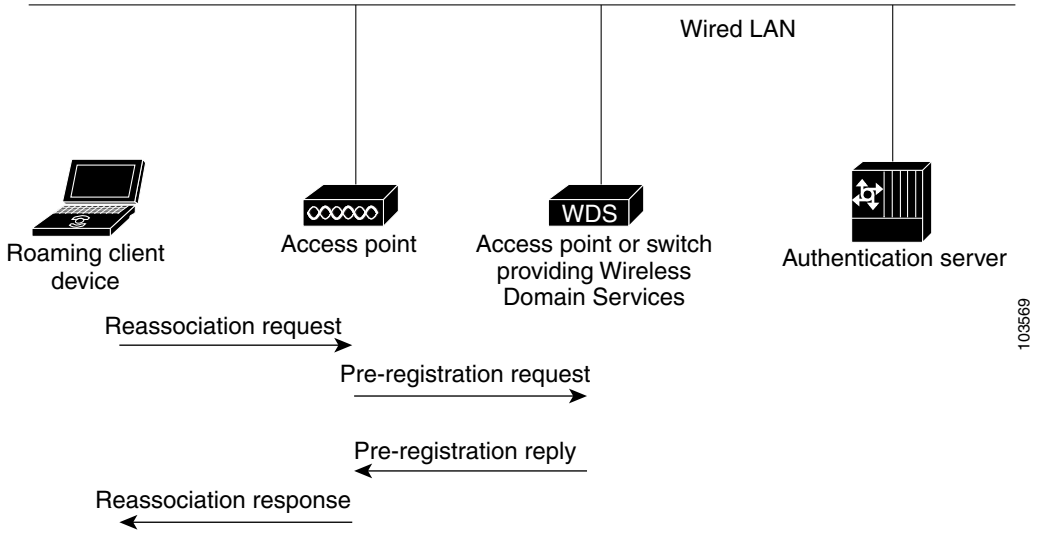
During normal operation, LEAP-enabled client devices mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server, as in Figure 12-1.

Figure 12-1 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 RADIUS 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 12-2 shows client authentication using CCKM.

Figure 12-2 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. Refer to the "Configuring Fast Secure Roaming" section on page 12-21 for instructions on configuring access points to support fast, secure roaming.

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 12-28 for instructions on configuring radio management.

Click this URL to browse to the WLSE documentation:

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/index.html

This link takes you to the Tools and Resources Downloads page. Select **Wireless LAN Management** to access the WLSE documentation.

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.

For instructions on configuring WDS on a switch equipped with a Wireless LAN Services Module (WLSM), refer to the *Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide.*

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

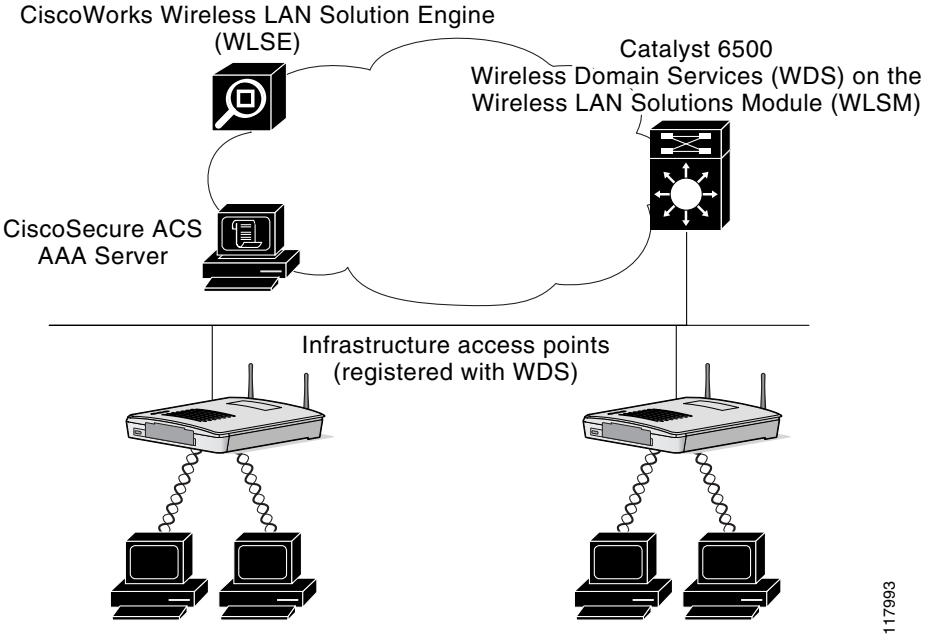
- 1100 or 1200 series access points participating in WDS
- Catalyst 6500 switch with Supervisor Module and WLSM configured as the WDS device

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

- Client devices

Figure 12-3 shows the components that interact to perform Layer 3 mobility.

Figure 12-3 Required Components for Layer 3 Mobility



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/networking_solutions_large_enterprise_home.html

Note If you enable Layer 3 mobility for an SSID and your WDS device does not support Layer 3 mobility, client devices cannot associate using that SSID.

Note Repeater access points and access points in workgroup bridge mode cannot associate to an SSID on which Layer 3 mobility is enabled.

Understanding Wireless Intrusion Detection Services

When you implement Wireless Intrusion Detection Services (WIDS) on your wireless LAN, your access points, WLSE, and an optional (non-Cisco) WIDS engine work together to detect and prevent attacks on your wireless LAN infrastructure and associated client devices.

Working with the WLSE, access points can detect intrusions and take action to defend the wireless LAN. WIDS consists of these features:

- Switch port tracing and rogue suppression—Switch port tracing and suppression uses an RF detection method that produces the radio MAC address of an unknown radio (a potential rogue device). The WLSE derives a wired-side MAC address from the wireless MAC address and uses it to search the switch's BRIDGE MIB. When one or more searchable MAC addresses are available, the WLSE uses CDP to discover any switches connected up to two hops away from the detecting

access points. The WLSE examines the BRIDGE MIB of each CDP-discovered switch to determine if they contain any of the target MAC addresses. If CDP finds any of the MAC addresses, WLSE suppresses the corresponding switch port number.

- Excessive management frame detection—Excessive management frames indicate an attack on your wireless LAN. An attacker might carry out a denial-of-service attack by injecting excessive management frames over the radio to overwhelm access points which have to process the frames. As part of the WIDS feature set, access points in scanning mode and root access points monitor radio signals and detect excessive management frames. When they detect excessive management frames, the access points generate a fault and send it through the WDS to the WLSE.
- Authentication/protection failure detection—Authentication/protection failure detection looks for attackers who are either trying to overcome the initial authentication phase on a wireless LAN or to compromise the ongoing link protection. These detection mechanisms address specific authentication attacks:
  - EAPOL flood detection
  - MIC/encryption failures detection
  - MAC spoofing detection
- Frame capture mode—In frame capture mode, a scanner access point collects 802.11 frames and forwards them to the address of a WIDS engine on your network.

Note See the "Configuring Access Points to Participate in WIDS" section on page 12-30 for instructions on configuring the access point to participate in WIDS and Configuring Management Frame Protection, page 12-24 for instructions on configuring the access point for MFP.

- 802.11 Management Frame Protection (MFP)—Wireless is an inherently broadcast medium enabling any device to eavesdrop and participate either as a legitimate or rogue device. Since control and management frames are used by client stations to select and initiate a session with an AP, these frames must be open. While management frames cannot be encrypted, they must be protected from forgery. MFP is a means by which the 802.11 management frames can be integrity protected.

Note MFP requires WLSE for reporting intrusion events.

Note MFP is available only on 32 Mb platforms: 1130 and 1240 series access points, and 1300 series access points in AP mode.

Configuring WDS

This section describes how to configure WDS on your network. This section contains these sections:

Guidelines for WDS

Follow these guidelines when configuring WDS:

- 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.
- In WDS only mode, the WDS supports up to 60 infrastructure access points and 1200 clients.
- 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 your main WDS device. However, you can configure 350 series access points to participate in WDS.

Requirements for WDS

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

- At least one access point, Integrated Services Router (ISR), or switch (equipped with a Wireless LAN Services Module) that you can configure as the WDS device
- An authentication server (or an access point or ISR configured as a local authenticator)

Note The 1300 access point/bridge cannot be configured as a WDS master, but can participate in a WDS network. This functionality is not supported on the 1300 access point/Bridge.

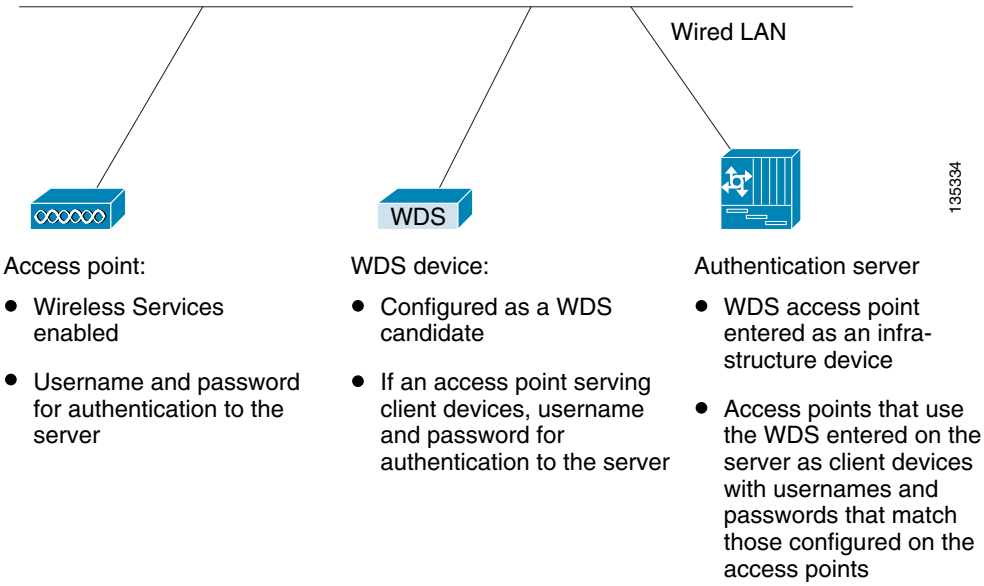
Configuration Overview

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

1. Configure access points, ISRs, or switches as potential WDS devices. This chapter provides instructions for configuring an access point as a WDS device. For instructions on configuring WDS on a switch equipped with a Wireless LAN Services Module (WLSM), refer to the *Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide.*
2. Configure the rest of your access points to use the WDS device.
3. Configure the authentication server on your network to authenticate the WDS device and the access points that use the WDS device.

Figure 12-4 shows the required configuration for each device that participates in WDS.

Figure 12-4 Configurations on Devices Participating in WDS



Configuring Access Points as Potential WDS Devices

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 several 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.

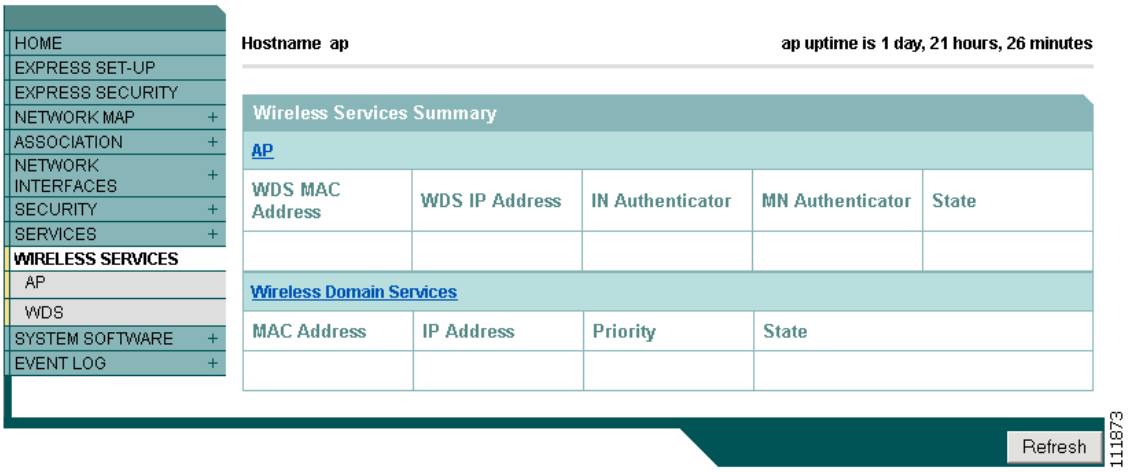
Note When WDS is enabled, the WDS access point performs and tracks all authentications. Therefore, you must configure EAP security settings on the WDS access point. See Chapter 11, "Configuring Authentication Types," for instructions on configuring EAP on the access point.

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

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 12-5 shows the Wireless Services Summary page.

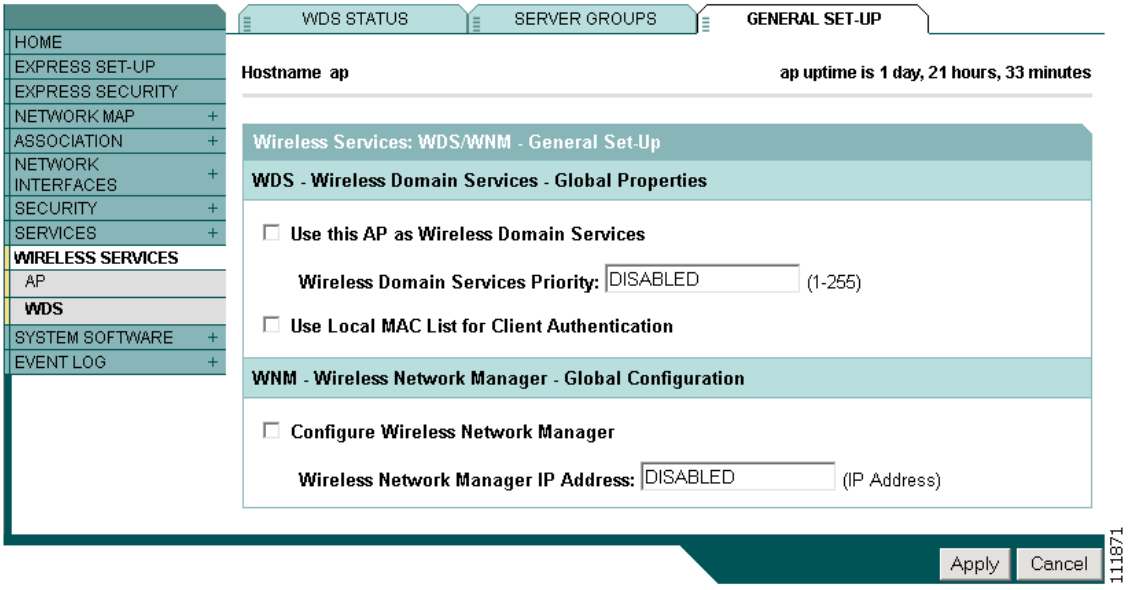
Figure 12-5 Wireless Services Summary Page



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 12-6 shows the General Setup page.

Figure 12-6 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.

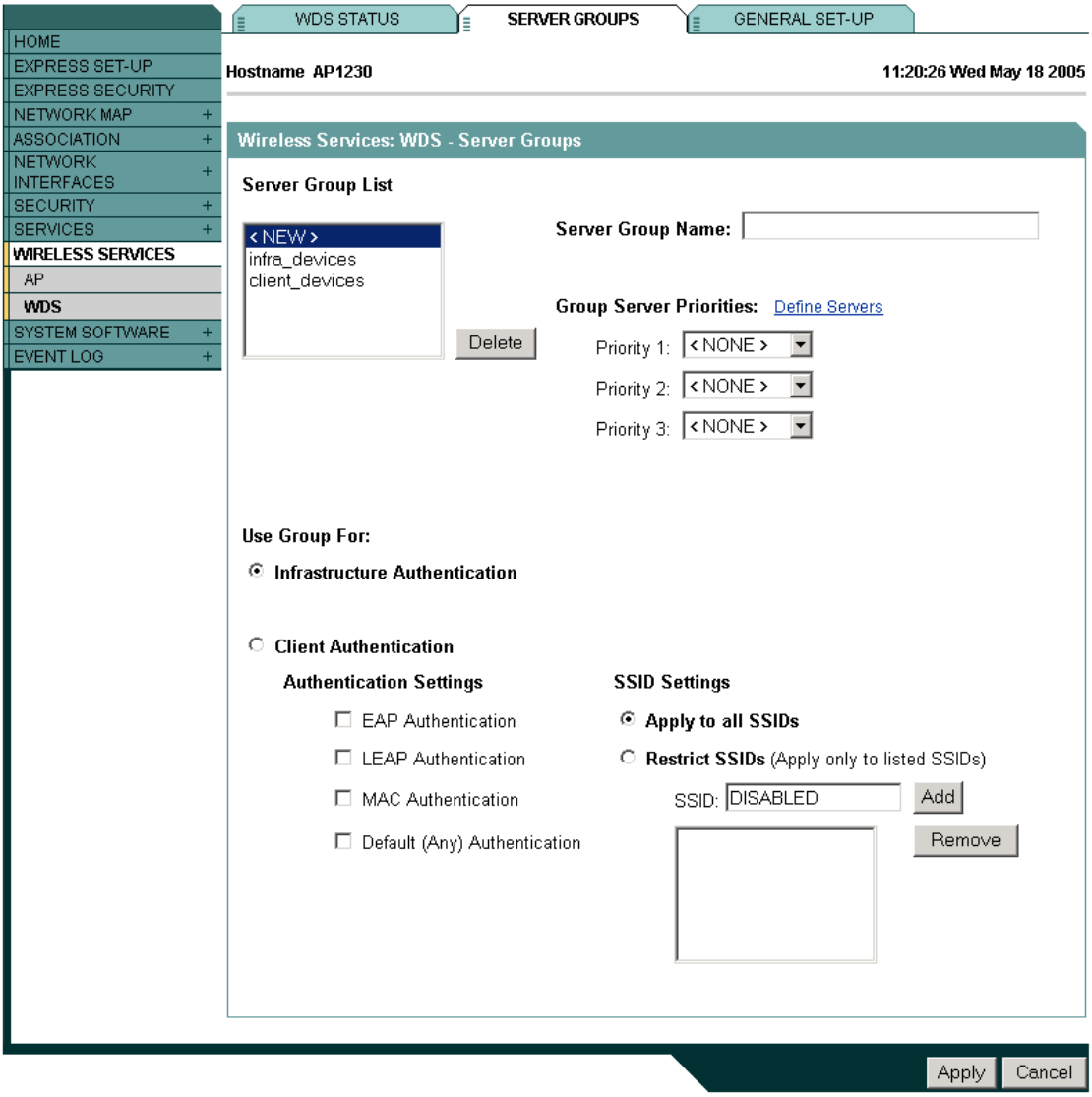
Note Selecting the *Use Local MAC List for Client Authentication* check box does not force client devices to perform MAC-based authentication. It provides a local alternative to server-based MAC-address authentication.

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 12-7 shows the WDS Server Groups page.

Figure 12-7 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 or an ISR as a local authentication server. See Chapter 9, "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 client devices. You can specify a separate list for clients using a certain type of authentication, such as EAP, LEAP, PEAP, 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.

The LEAP Authentication checkbox is present specifically for the Cisco clients identified below:

- Cisco Aironet 350 series cards using LEAP and EAP-FAST
- Cisco 7920, 7921, and 7925 phones using LEAP, EAP-FAST, PEAP, & EAP-TLS
- ADU using LEAP

Unchecking the LEAP Authentication checkbox prevents these client devices from connecting to a wireless network, but does not prevent other client cards or supplicant combinations from connecting because these clients use network-EAP for authentication under the various EAP types identified above. All other clients use the 802.1x standard for open authentication.

The information above does not apply to non-Cisco clients.

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 11, "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 12-14 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 Devices" section on page 12-9:

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bvi1
AP(config)# wlccp authentication-server infrastructure infra_devices
AP(config)# wlccp authentication-server client any client_devices
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 *infra_devices*; client devices using SSIDs *fred* or *ginger* are authenticated using server group *client_devices*.

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

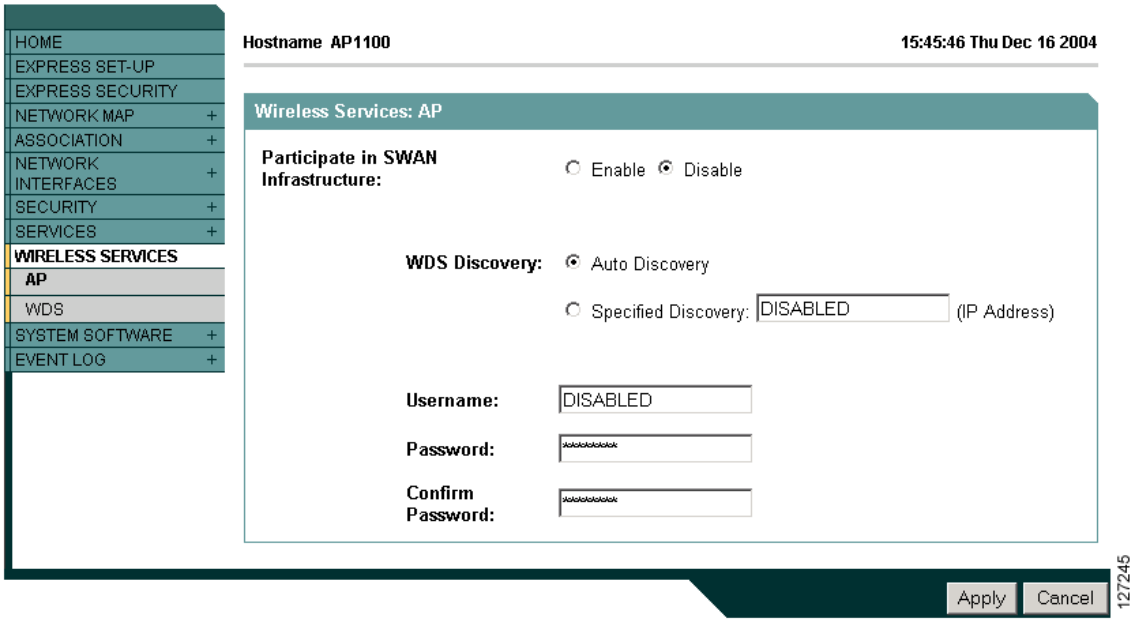
Follow these steps to configure an access point to authenticate through the WDS device and participate in WDS:

Note To participate in WDS, infrastructure access points should run the same version of IOS as the one that WDS runs.

Step 1 Browse to the Wireless Services Summary page.

Step 2 Click **AP** to browse to the Wireless Services AP page. Figure 12-8 shows the Wireless Services AP page.

Figure 12-8 Wireless Services AP Page



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

Step 4 (Optional) If you use a WLSM switch module as the WDS device on your network, select **Specified Discovery** and enter the IP address of the WLSM in the entry field. 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 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 12-14:

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

In this example, the access point is enabled to interact with the WDS device, and it authenticates to your 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*.

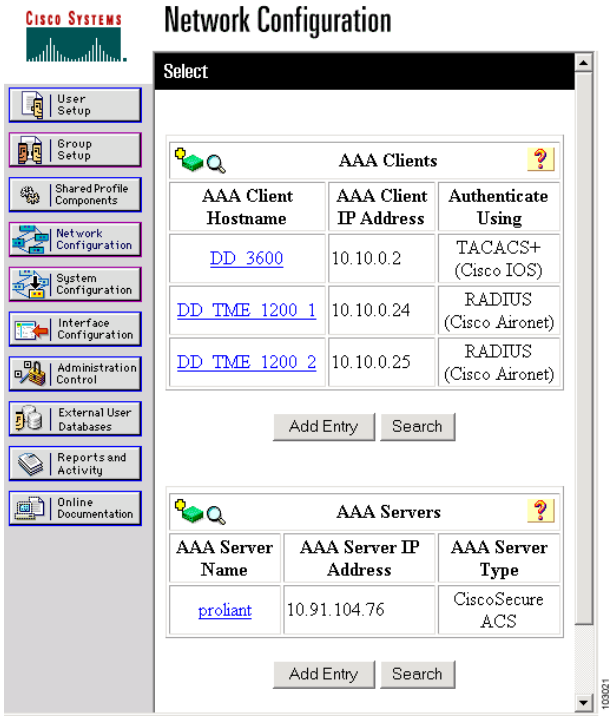
Configuring the Authentication Server to Support WDS

The WDS device and all access points participating in WDS 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:

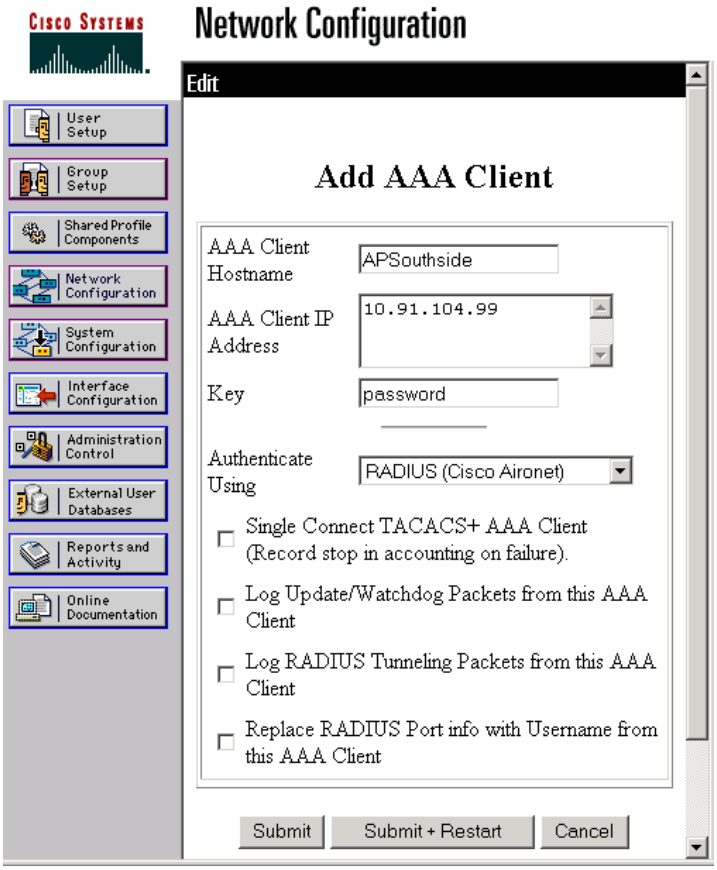
Step 1 Log into Cisco Secure ACS and click **Network Configuration** to browse to the Network Configuration page. You must use the Network Configuration page to create an entry for the WDS device. Figure 12-9 shows the Network Configuration page.

Figure 12-9 Network Configuration Page



Step 2 Click **Add Entry** under the AAA Clients table. The Add AAA Client page appears. Figure 12-10 shows the Add AAA Client page.

Figure 12-10 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.

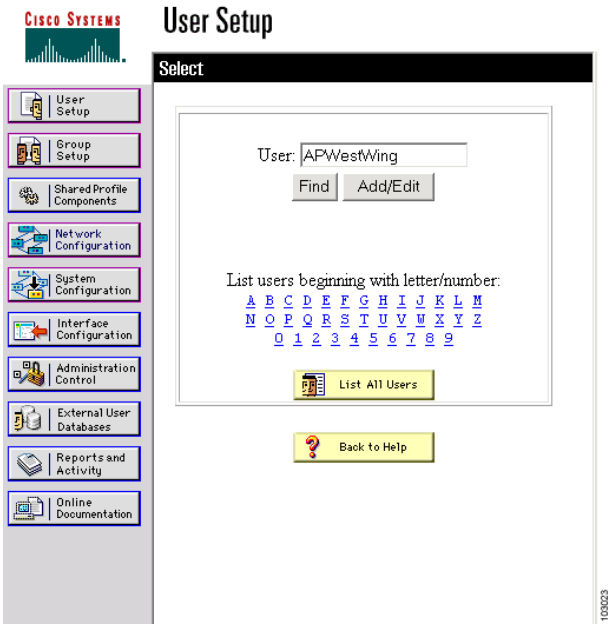
Step 6 From the Authenticate Using drop-down menu, select **RADIUS (Cisco Aironet)**.

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 12-11 shows the User Setup page.

Figure 12-11 User Setup Page

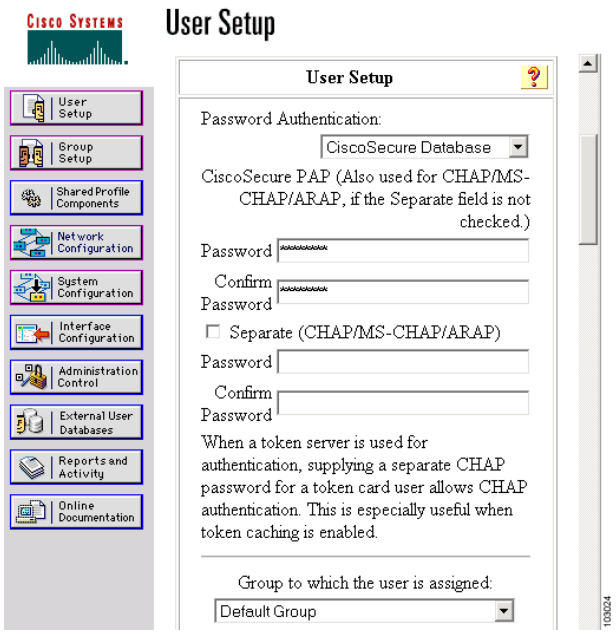


Step 10 Enter the name of the access point in the User field.

Step 11 Click **Add/Edit**.

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

Figure 12-12 ACS User Setup Box



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

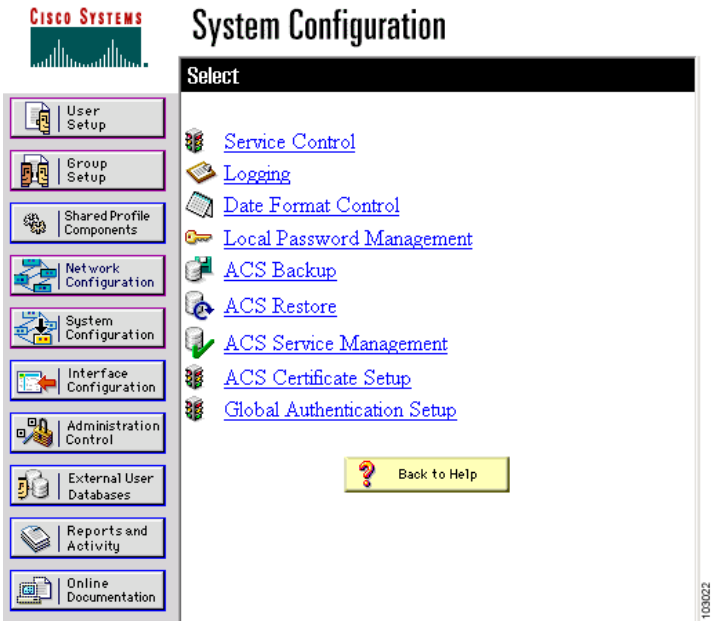
Step 14 In the Password and Confirm Password fields, enter exactly the same password that you entered on the access point on the Wireless Services AP page.

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 12-13 shows the System Configuration page.

Figure 12-13 ACS System Configuration Page



Configuring WDS Only Mode

WDS access points can operate in WDS only mode using the **wlccp wds mode wds-only** command. After issuing this command and reloading, the access point starts working in the WDS only mode. In WDS only mode, the dot11 subsystems are not initialized and the dot11 interface related commands cannot be configured. In WDS only mode, the WDS supports up to 60 infrastructure access points and up to 1200 clients. Use the **no** command to turn off WDS onlly mode. Use the **show wlccp wds** command to display the working mode of the WDS access point.

To set the WDS access point to operate in both AP and WDS modes, use the **no wlccp wds mode wds-only** command and use the **write erase** command to reload the access point immediately. After the access point reloadss, the dot11 radio subsytems initialize. The access point and WDS associate directly to wireless clients. In this mode, the WDS supports 30 infrastructure access points and 600 clients in addition to 20 direct wireless client associations.

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, candidate, or WDS-only). If the state is backup, the command also displays the current WDS device's IP address, MAC address, and priority. If the state is WDS-only, the command displays the device's MAC address, IP address, interface state, access point count, and mobile node count.

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 Fast Secure Roaming

After you configure WDS, access points configured for CCKM can provide fast, secure roaming for associated client devices. This section describes how to configure fast, secure roaming on your wireless LAN. This section contains these sections:

- Requirements for Fast Secure Roaming
- Configuring Access Points to Support Fast Secure Roaming

Requirements for Fast Secure Roaming

To configure fast secure roaming, you must have these items on your wireless LAN:

- At least one access point, ISR, or switch (equipped with a WLSM) configured as the WDS device
- Access points configured to participate in WDS
- Access points configured for fast, secure roaming
- An authentication server (or an access point, ISR, or switch configured as a local authenticator)
- Cisco Aironet client devices, or Cisco-compatible client devices that comply with Cisco Compatible Extensions (CCX) version 2 or later

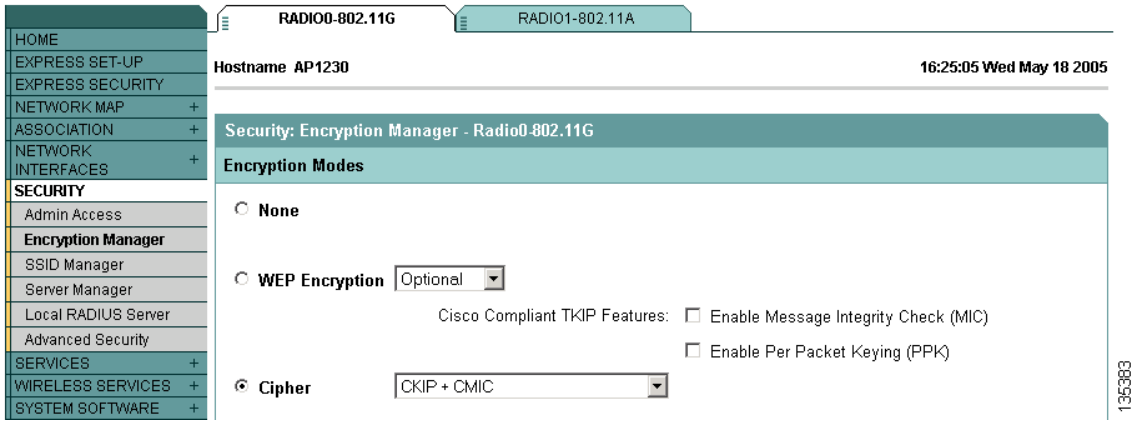
For instructions on configuring WDS, refer to the "Configuring WDS" section on page 12-7.

Configuring Access Points to Support Fast Secure Roaming

To support fast, secure roaming, the access points on your wireless LAN must be configured to participate in WDS and they must allow CCKM authenticated key management for at least one SSID. Follow these steps to configure CCKM for an SSID:

Step 1 Browse to the Encryption Manager page on the access point GUI. Figure 12-14 shows the top section of the Encryption Manager page.

Figure 12-14 Encryption Manager Page



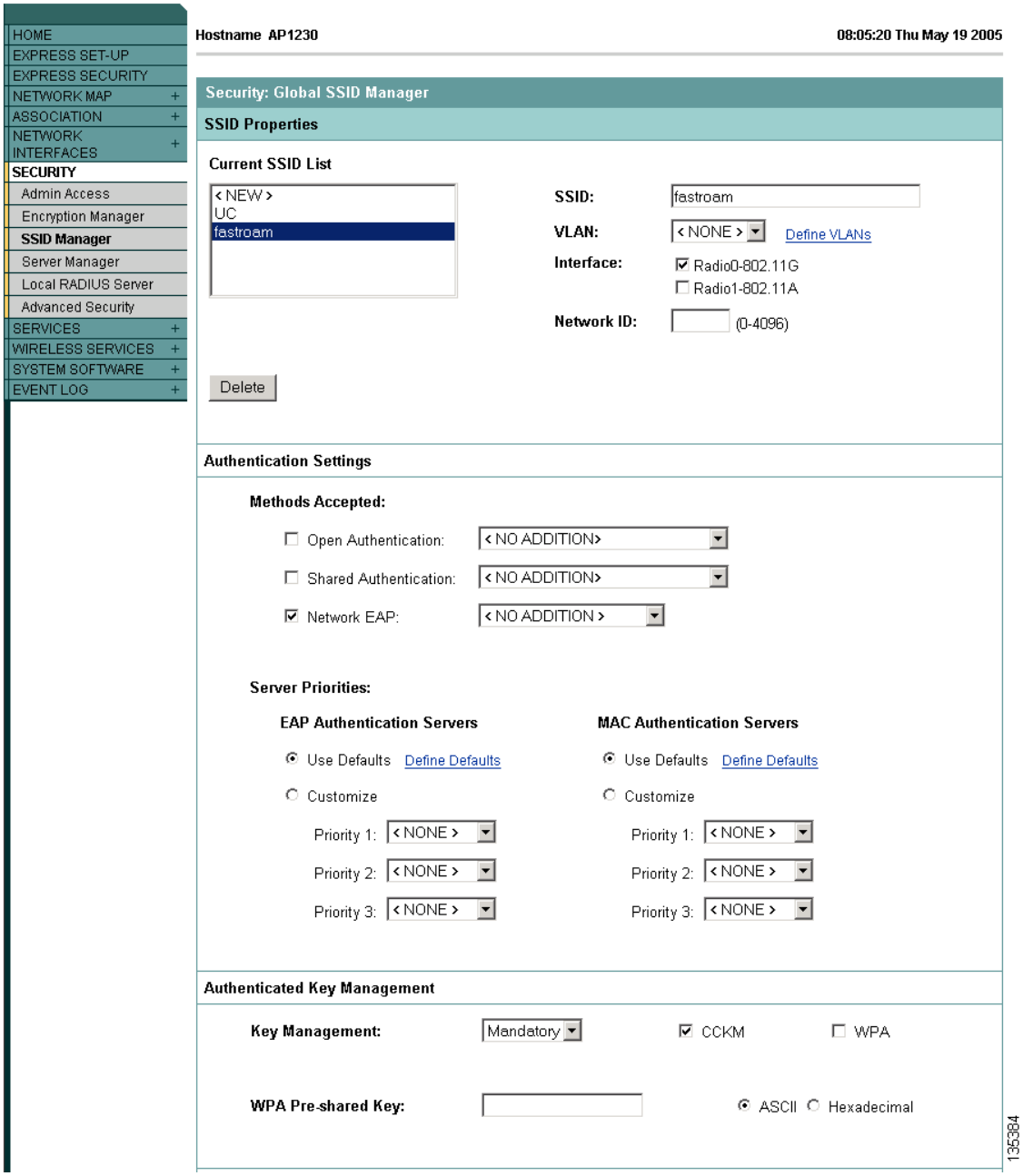
Step 2 Click the **Cipher** button.

Step 3 Select **CKIP + CMIC** from the Cipher drop-down menu.

Step 4 Click **Apply**.

Step 5 Browse to the Global SSID Manager page. Figure 12-15 shows the top sections of the Global SSID Manager page.

Figure 12-15 Global SSID Manager Page



Step 6 On the SSID that supports CCKM, select these settings:

b. If your access point contains multiple radio interfaces, select the interfaces on which the SSID applies.

c. Select **Network EAP** under Authentication Settings. When you enable CCKM, you must enable Network EAP as the authentication type.

d. Select **Mandatory** or **Optional** under Authenticated Key Management. If you select **Mandatory**, only clients that support CCKM can associate using the SSID. If you select Optional, both CCKM clients and clients that do not support CCKM can associate using the SSID.

e. Check the **CCKM** check box.

Step 7 Click **Apply**.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Access Points to Support Fast Secure Roaming" section on page 12-22:

```
AP# configure terminal
AP(config)# dot11 ssid fastroam
AP(config-ssid)# authentication network-eap eap_methods
AP(config-ssid)# authentication key-management cckm
AP(config-ssid)# exit
AP(config)# interface dot11radio0
AP(config-if)# encryption mode ciphers ckip-cmic
AP(config-if)# ssid fastroam
AP(config-if)# exit
AP(config)# end
```

In this example, the SSID *fastroam* is configured to support Network EAP and CCKM, the CKIP-CMIC cipher suite is enabled on the 2.4-GHz radio interface, and the SSID *fastroam* is enabled on the 2.4-GHz radio interface.

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

Configuring Management Frame Protection

Management Frame Protection operation requires a WDS and is available on 32 Mb platforms only (s: 1130 and 1240 series access points, and 1300 series access points in AP mode.). MFP is configured at the WLSE, but you can configure MFP on an access point and WDS manually.

Note If a WLSE is not present, then MFP cannot report detected intrusions and so has limited effectiveness. If a WLSE is present, you should perform the configuration from the WLSE.

For complete protection, you should also configure an MFP access point for Simple Network Transfer Protocol (SNTP).

Management Frame Protection

Management Frame Protection provides security features for the management messages passed between Access Point and Client stations. MFP consists of two functional components: Infrastructure MFP and Client MFP.

Infrastructure MFP provides Infrastructure support. Infrastructure MFP utilizes a message integrity check (MIC) across broadcast and directed management frames which can assist in detection of rogue devices and denial of service attacks. Client MFP provides client support. Client MFP protects authenticated clients from spoofed frames, by preventing many of the common attacks against WLANs from becoming effective.

Management Frame Protection operation requires a WDS and is available on 32 Mb platforms only (1130, 1240, 1250 series access points, and 1300 series access points in AP mode). MFP is configured at the WLSE, but you can configure MFP on an access point and WDS manually.

Note If a WLSE is not present, then MFP cannot report detected intrusions and so has limited effectiveness. If a WLSE is present, you should perform the configuration from the WLSE.

For complete protection, you should also configure an MFP access point for Simple Network Transfer Protocol (SNTP).

Overview

Client MFP encrypts class 3 management frames sent between access points and CCXv5-capable client stations, so that both AP and client can take preventative action by dropping spoofed class 3 management frames (i.e. management frames passed between an AP and a client station that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect class 3 Unicast management frames. The unicast cipher suite negotiated by the STA in the reassociation request's RSNIE is used to protect both unicast data and class 3 management frames. An access point in workgroup bridge, repeater, or non-root bridge mode must negotiate either TKIP or AES-CCMP to use Client MFP.

Protection of Unicast Management Frames

Unicast class 3 management frames are protected by applying either AES-CCMP or TKIP in a similar manner to that already used for data frames. Client MFP is enabled for autonomous access points only if the encryption is AES-CCMP or TKIP and key management WPA version 2.

Protection of Broadcast Management Frames

In order to prevent attacks using broadcast frames, access points supporting CCXv5 do not emit any broadcast class 3 management frames. An access point in workgroup bridge, repeater, or non-root bridge mode discards broadcast class 3 management frames if Client MFP is enabled.

Client MFP is enabled for autonomous access points only if the encryption is AES-CCMP or TKIP and key management WPA version 2.

Client MFP For Access Points in Root mode

Autonomous access points in root mode support mixed mode clients. Clients capable of CCXv5 with negotiated cipher suite AES or TKIP with WPAv2 are Client MFP enabled. Client MFP is disabled for clients which are not CCXv5 capable. By default, Client MFP is optional for a particular SSID on the access point, and can be enabled or disabled using the CLI in SSID configuration mode.

Client MFP can be configured as either required or optional for a particular SSID. To configure Client MFP as required, you must configure the SSID with key management WPA version 2 mandatory. If the key management is not WPAv2 mandatory, an error message is displayed and your CLI command is rejected. If you attempt to change the key management with Client MFP configured as required and key management WPAv2, an error message displays and rejects your CLI command. When configured as optional, Client MFP is enabled if the SSID is capable of WPAv2, otherwise Client MFP is disabled.

Configuring Client MFP

The following CLI commands are used to configure Client MFP for access points in root mode.

ids mfp client required

This SSID configuration command enables Client MFP as required on a particular SSID. The Dot11Radio interface is reset when the command is executed if the SSID is bound to the Dot11Radio interface. The command also expects that the SSID is configured with WPA version 2 mandatory. If the SSID is not configured with WPAv2 mandatory, an error message displays and the command is rejected.

no ids mfp client

This ssid configuration command disables Client MFP on a particular SSID. The Dot11Radio interface is reset when the command is executed if the SSID is bound to the Dot11Radio interface.

ids mfp client optional

This ssid configuration command enables Client MFP as optional on a particular SSID. The Dot11Radio interface is reset when the command is executed if the SSID is bound to the Dot11Radio interface. Client MFP is enabled for this particular SSID if the SSID is WPAv2 capable, otherwise Client MFP is disabled.

show dot11 ids mfp client statistics

Use this command to display Client MFP statistics on the access point console for a Dot11Radio interface.

clear dot11 ids mfp client statistics

Use this command to clear the Client MFP statistics.

authentication key management wpa version {1|2}

Use this command to explicitly specify which WPA version to use for WPA key management for a particular SSID.

	Command	Description
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ids mfp generator**	Configures the access point as an MFP generator. When enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame will invalidate the MIC, causing any receiving access point that is configured to detect (validate) MFP frames to report the discrepancy. The access point must be a member of a WDS.

	Command	Description
Step 3	**dot11 ids mfp detector**	Configures the access point as an MFP detector. When enabled, the access point validates management frames it receives from other access points. If it receives any frame that does not contain a valid, and expected, MIC IE, it will report the discrepancy to the WDS. The access point must be a member of a WDS.
Step 4	**sntp server** *server IP address*	Enter the name or ip address of the SNTP server.
Step 5	**end**	Return to the privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Beginning in privileged EXEC mode, follow these steps to configure the WDS:

	Command	Description
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ids mfp distributor**	Configures the WDS as an MFP distributor. When enabled, the WDS manages signature keys, used to create the MIC IEs, and securely transfers them between generators and detectors.
Step 3	**end**	Return to the privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

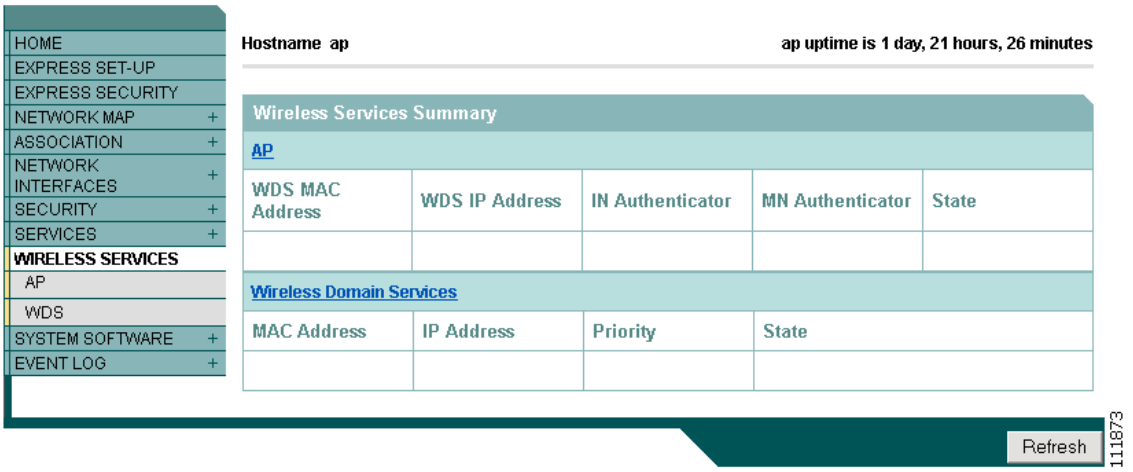
Configuring Radio Management

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 12-16 shows the Wireless Services Summary page.

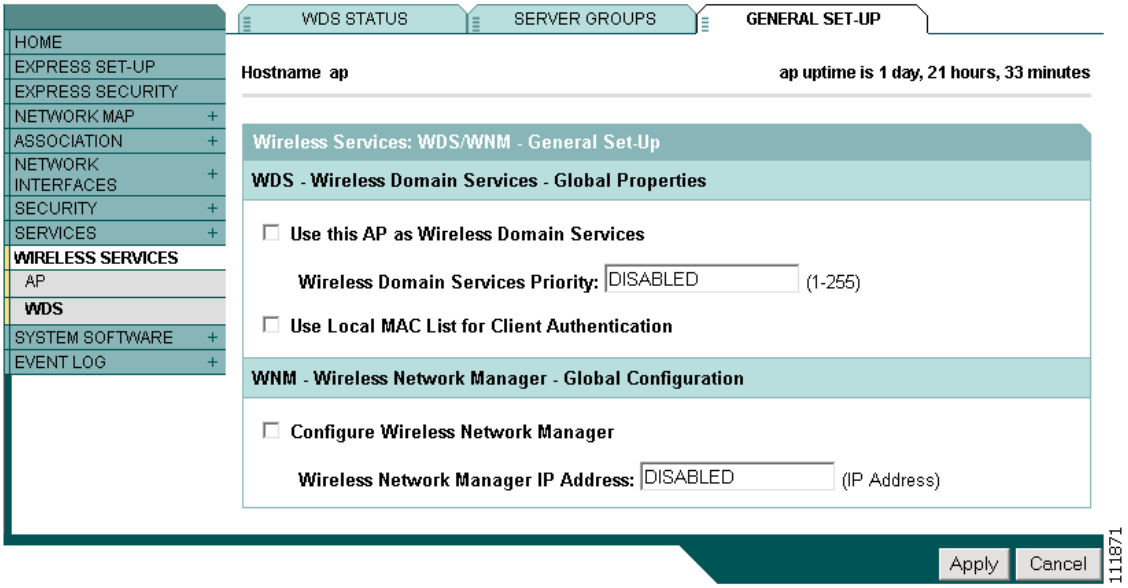
Figure 12-16 Wireless Services Summary Page



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 12-17 shows the General Setup page.

Figure 12-17 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 12-28:

```
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*.

Configuring Access Points to Participate in WIDS

To participate in WIDS, access points must be configured to participate in WDS and in radio management. Follow the steps in the "Configuring Access Points to use the WDS Device" section on page 12-14 and in the "Configuring Radio Management" section on page 12-28 to configure the access point to participate in WDS and in radio management.

Configuring the Access Point for Scanner Mode

In scanner mode, the access point scans all of its channels for radio activity and reports the activity to the WDS device on your network. A scanner access point does not accept client associations.

Configuring the Access Point for Monitor Mode

When an access point is configured as a scanner it can also capture frames in monitor mode. In monitor mode, the access point captures 802.11 frames and forwards them to the WIDS engine on your network. The access point adds a 28-byte capture header to every 802.11 frame that it forwards, and the WIDS engine on your network uses the header information for analysis. The access point uses UDP packets to forward captured frames. Multiple captured frames can be combined into one UDP packet to conserve network bandwidth.

In scanner mode the access point scans all channels for radio activity. However, in monitor mode the access point monitors only the channel for which the access point radio is configured.

Note If your access point contains two radios, both radios must be configured for scanner mode before you can configure monitor mode on the interfaces.

Displaying Monitor Mode Statistics

Use the **show wlccp ap rm monitor statistics** global configuration command to display statistics on captured frames.

This example shows output from the command:

```
ap# show wlccp ap rm monitor statistics

Dot11Radio 0
====================
WLAN Monitoring           : Enabled
Endpoint IP address       : 10.91.107.19
Endpoint port             : 2000
Frame Truncation Length   : 535 bytes

Dot11Radio 1
====================
WLAN Monitoring           : Disabled

WLAN Monitor Statistics
=========================
```

```
Total No. of frames rx by DOT11 driver      : 58475
Total No. of Dot11 no buffers               : 361
Total No. of Frames Q Failed                : 0
Current No. of frames in SCAN Q             : 0

Total No. of frames captured                : 0
Total No. of data frames captured           : 425
Total No. of control frames captured        : 1957
Total No. of Mgmt frames captured           : 20287
Total No. of CRC errored frames captured: 0

Total No. of captured frames forwarded      : 23179
Total No. of captured frames forward failed : 0
```

Use the **clear wlccp ap rm statistics** command to clear the monitor mode statistics.

Configuring Monitor Mode Limits

You can configure threshold values that the access point uses in monitor mode. When a threshold value is exceeded, the access point logs the information or sends an alert.

Configuring an Authentication Failure Limit

Setting an authentication failure limit protects your network against a denial-of-service attack called *EAPOL flooding*. The 802.1X authentication that takes place between a client and the access point triggers a series of messages between the access point, the authenticator, and an authentication server using EAPOL messaging. The authentication server, typically a RADIUS server, can quickly become overwhelmed if there are too many authentication attempts. If not regulated, a single client can trigger enough authentication requests to impact your network.

In monitor mode the access point tracks the rate at which 802.1X clients attempt to authenticate through the access point. If your network is attacked through excessive authentication attempts, the access point generates an alert when the authentication threshold has been exceeded.

You can configure these limits on the access point:

- Number of 802.1X attempts through the access point
- EAPOL flood duration in seconds on the access point

When the access point detects excessive authentication attempts it sets MIB variables to indicate this information:

- An EAPOL flood was detected
- Number of authentication attempts
- MAC address of the client with the most authentication attempts

to set authentication limits that trigger a fault on the access point:

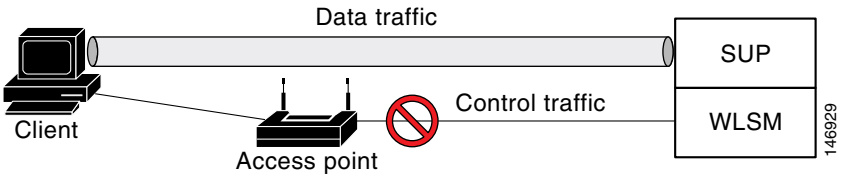
Configuring WLSM Failover

To ensure near hot standby in cases of WLSM failure, the WLSM Version 2.13 Release supports resilient tunnel recovery and active and standby WLSMs.

Resilient Tunnel Recovery

In the case of a single chassis scenario (only one WLSM per chassis), if the WLSM software fails, existing access point clients connected to the SUP continue to be connected to the SUP and won't notice any interruption in service. When an access point detects a WLSM failure, it doesn't tear down the active tunnels, which keeps data traffic going between client and SUP. But because of the WLSM failure, the control traffic going between the access point and the WLSM is disrupted (as shown in Figure 12-18), which prevents the access points from accepting new client connections until the WLSM software is back online. Resilient tunnel recovery is automatic and does not require any configuration.

Figure 12-18 Resilient Tunnel Recovery



Active/Standby WLSM Failover

In addition to resilient tunnel recovery, WLSM supports another level of resiliency by allowing you to deploy two WLSMs per chassis: an active WLSM and a standby WLSM. If the active WLSM fails, the standby WLSM becomes active and takes over the control traffic for existing and new access point clients without interrupting data traffic. This feature in addition to resilient tunnel recovery provide near-hot standby in case of WLSM failure.