Configuring Other Services

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

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 configured as the WDS device) to provide fast, secure roaming for client devices in a given subnet and to participate in radio management. 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.

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 in the same subnet, 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.

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, over the wired interface.
- 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 registered to the WDS device, 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.

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
Integrated Services Router (ISR)	100 (depending on ISR platform)

Role of Access Points Using the WDS Device

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

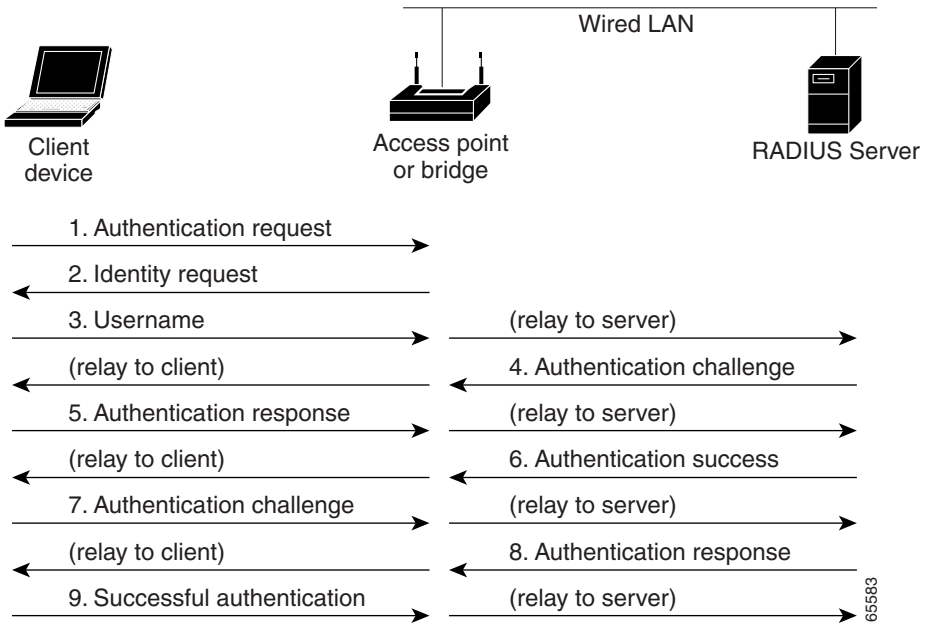
- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.
- Report radio data to the WDS device.

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.

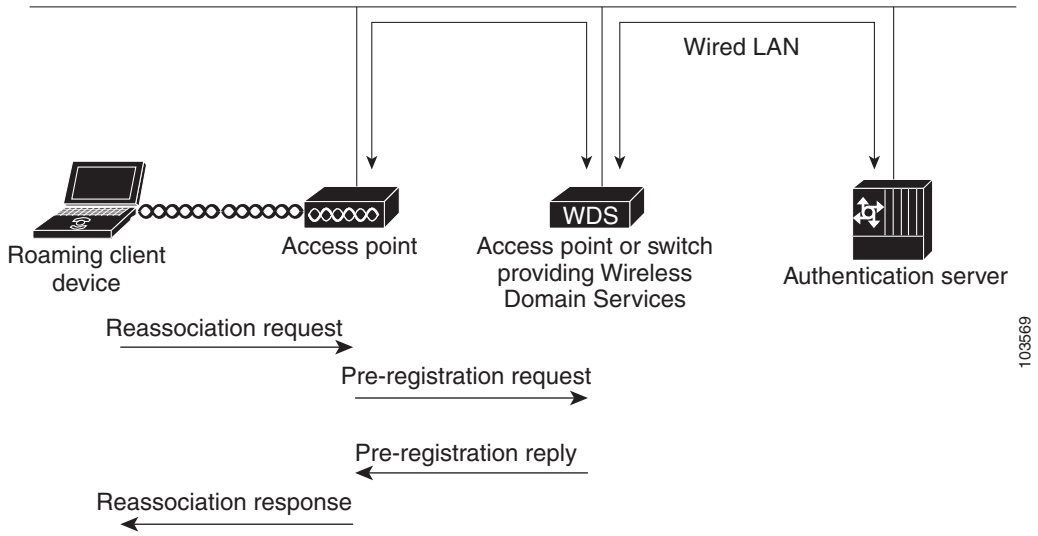
During normal operation, EAP/802.1x-enabled client devices mutually authenticate with a new access point by performing a complete EAP/802.1x authentication, including communication with the main RADIUS server, as in Figure 12-1.

Figure 12-1 Example of Client Authentication Exchange using a RADIUS Server (LEAP case)



When you configure your wireless LAN for fast, secure roaming, however, EAP/802.1x-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 12-17 for instructions on configuring access points to support fast, secure roaming.

Note This mechanism also requires the client to accept the credentials that are being passed from one AP to the other. Make sure that you enable CCKM on the access points, and also make sure that your wireless client supports CCKM for the authentication mechanism (with CCX) used in your network. Without CCKM support, the client may refuse the fast roaming mechanism and force a re-authentication through the RADIUS server.
To know the CCX versions needed for each authentication mechanism, go to the following URL:
http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html
To know the CCX version supported by each client type, go to the following URL:
http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_partners_0900aecd800a7907.html

Understanding Wireless Intrusion Detection Services

When you implement Wireless Intrusion Detection Services (WIDS) on your wireless LAN, your access points, 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 (non-Cisco) WIDS engine, 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 (non-Cisco) WIDS engine derives a wired-side MAC address from the wireless MAC address and uses it to search the switch's BRIDGE MIB.
- 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 non-Cisco) WIDS engine.
- 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 12-26 for instructions on configuring the access point to participate in WIDS and Configuring Management Frame Protection, page 12-21 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.

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.

Requirements for WDS

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

- At least one access point, Integrated Services Router (ISR)
- An authentication server (or an access point or ISR configured as a local authenticator)

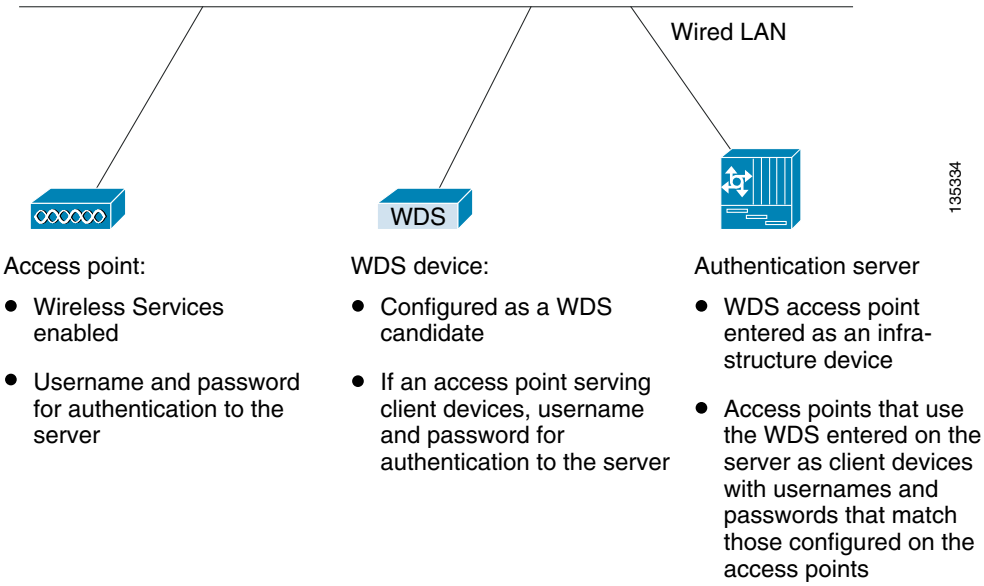
Configuration Overview

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.
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 12-3 shows the required configuration for each device that participates in WDS.

Figure 12-3 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.

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 Choose **Wireless > WDS**.

Step 2 Click **General Set-Up** tab.

Figure 12-4 General Setup Hostname ap page

Step 3 Check the ***Use this AP as Wireless Domain Services*** check box.

Step 4 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 5 (Only for WDS clients) Check the **Use Local MAC List for Client Authentication** check box to authenticate client AP devices using MAC addresses in the local list of addresses configured on the WDS device.
If you do not check 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 Checking 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 6 Click **Apply**.

Step 7 Click **Server Groups** tab to go to the WDS Server Groups page.

Step 8 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 9 Select the primary server from the Priority 1 drop-down list. (If a server that you need to add to the group does not appear in the Priority drop-down lists, 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 do not 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 10 (Optional) Select backup servers from the Priority 2 and 3 drop-down lists.

Step 11 Click **Apply**.

Step 12 Configure the list of servers to be used for 802.1x authentication for wireless client devices. You can specify a separate list for clients using a certain type of authentication, such as EAP, LEAP, other EAP types, 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 check box is present specifically for the Cisco clients identified below:

- Cisco 7920, 7921, and 7925 phones using LEAP
- Autonomous APs configured as wireless clients (workgroup bridge or non-root bridge) and using LEAP authentication

Unchecking the LEAP authentication check box prevents these client devices from authenticating to the wireless network using LEAP and the WDS service. The clients can connect using any other form of EAP authentication if the EAP option is selected. However, this does not prevent other client cards or supplicant combinations from connecting, because these clients use the 802.1X standard for all form of EAP authentications, including LEAP. This information does not apply to non-Cisco clients.

Step 13 Select the primary server from the Priority 1 drop-down list. (If a server that you need to add to the group does not appear in the Priority drop-down lists, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)

Step 14 (Optional) Select backup servers from the Priority 2 and 3 drop-down lists.

Step 15 (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 16 Click **Apply**.

Step 17 Configure the WDS access point for EAP authentication. See Chapter 11, "Configuring Authentication Types," for instructions on configuring EAP.

Note This authentication uses LEAP by default. Infrastructure access points using the WDS service need to be authenticated through the WDS device. If your WDS access point serves client devices, follow the instructions in the "Configuring Access Points to use the WDS Device" section on page 12-10 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 12-7:

```
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*. If you do not specify the SSID list, all SSIDs are included.

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

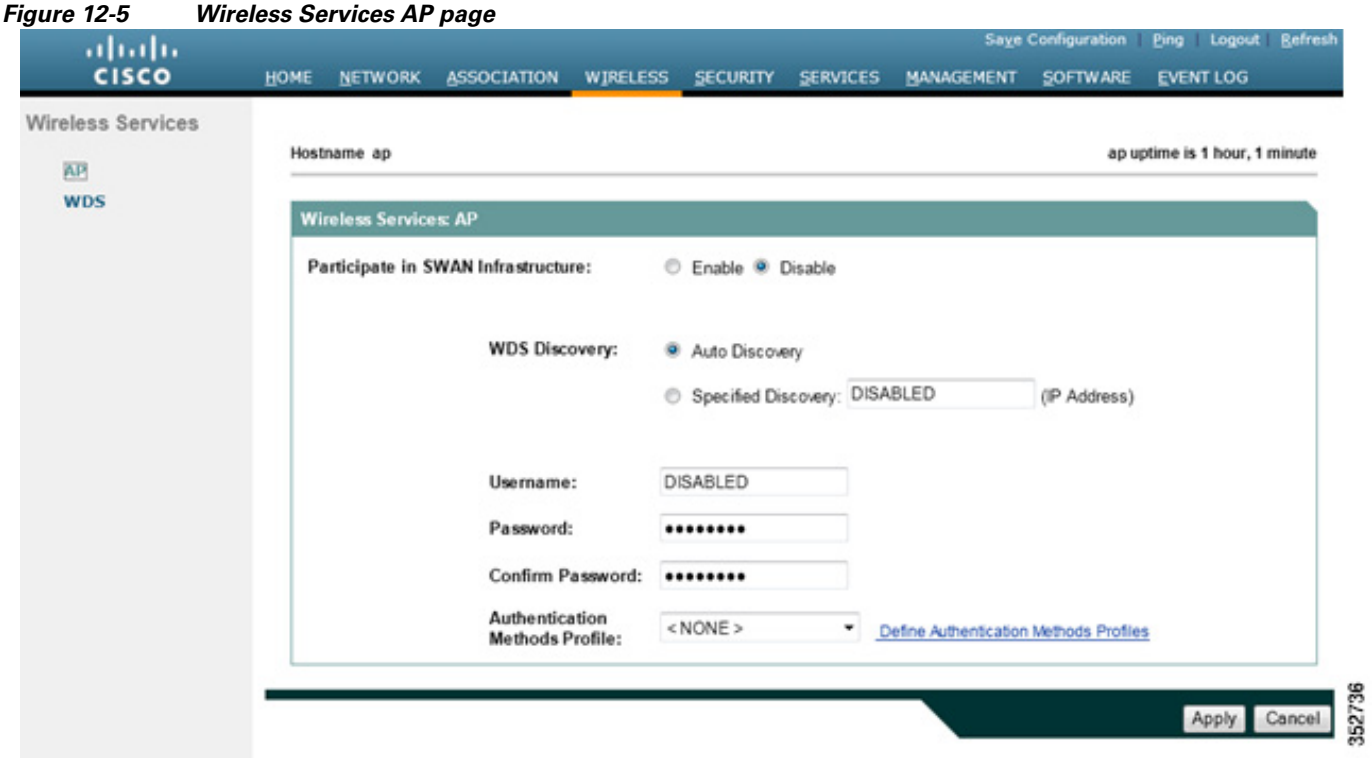
Configuring Access Points to use the WDS Device

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 Choose **Wireless > AP**. The Wireless Services AP page appears.

Figure 12-5 Wireless Services AP page



Step 2 Click **Enable** for the *Participate in SWAN Infrastructure* setting, to enable the AP to use the WDS service for client authentication.

Step 3 (Optional) Select **Specified Discovery** and enter the IP address of the WDS 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 4 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 5 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. When configuring the username and password in this page, the AP uses LEAP to authenticate through the WDS server.

Step 6 (Optional) If you do not want your infrastructure AP to be authenticated through the WDS using LEAP, but want to use another EAP authentication method (for example EAP-FAST), select another authentication method profile from the Authentication Methods Profile drop down list. If you have not defined Authentication Method Profiles yet, click the **Define Authentication Method Profiles** link, configure a profile, then return to the Wireless Services AP configuration page to select the profile. See the Creating and Applying EAP Method Profiles for the 802.1X Supplicant, page 11-17 for more details on how to create a new profile.

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 12-10:

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 0 wes7win8
AP(config)# wlccp ap eap profile Myfast
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.

An optional Myfast EAP profile is called to authenticate using another method than LEAP. In this example, the profile uses EAP-FAST, and is configured as follows:

```
ap(config)# eap profile myfast
ap(config-eap-profile)# method fast
ap(config-eap-profile)# end
```

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 Identity Services Engine (ISE).

Step 2 Choose **Administration > Network Resources > Network devices**.
The Network Devices page appears.
Here you can add the WDS as a AAA client.

Figure 12-6 Cisco ISE Network Devices Page

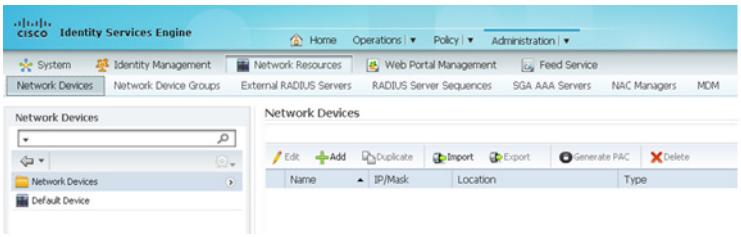
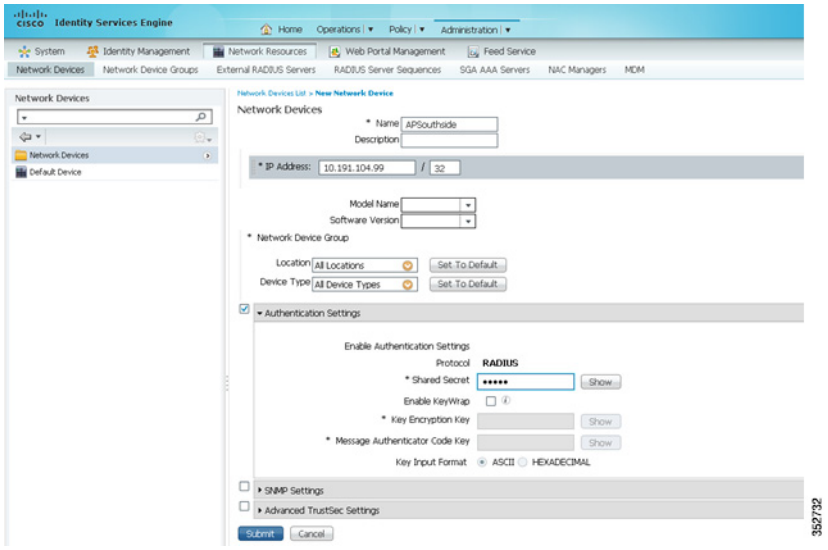


Figure 12-7 Cisco ISE Network Devices Page Detailed



Step 3 Click **Add** to add the WDS as a new AAA client.

Step 4 In the Name field, enter the WDS device name. This name is significant only locally.
Optionally, enter a description for the WDS device.

Step 5 In the IP address field, enter the IP address of the WDS device.
Optionally, specify the device location and device type, but only if these categories have been configured on the ISE.

Step 6 Check the **Authentication Settings** check box. The fields in the Authentication Settings area get enabled.

Step 7 For the RADIUS protocol, in the Shared Secret field, enter a shared secret value. This value will be entered identically on the WDS device when configuring the ISE as a RADIUS server.

Step 8 Click **Submit** to validate your entries.

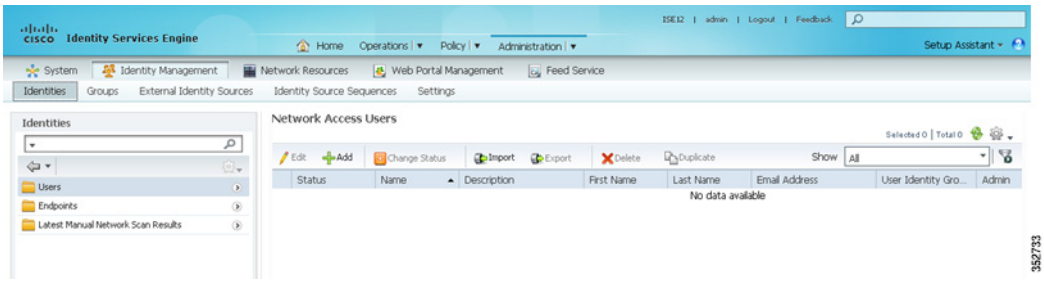
Step 9 Repeat Step 3 to Step 8 for each WDS device candidate.

Step 10 Choose **Administration > Identities Management > Identities**.
The Network Access Users page appears.

Note This procedure shows configuration of users in the ISE internal database. ISE can also use an external database. Please see the ISE guide for more details.

Step 11 Click **Add** to add a new user.

Figure 12-8 Network Access Users page



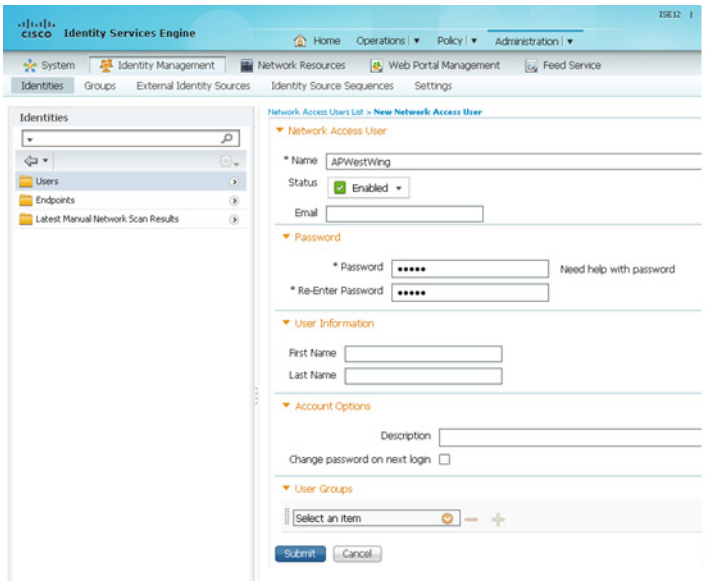
Step 12 In the Name field, enter the username configured for the access point client to the WDS.

Step 13 In the Password and Confirm Password fields, enter the exact same password that you entered on the access point on the Wireless Services AP page.

Step 14 Click **Submit**.

Step 15 Repeat Step 11 to Step 14 for each access point that uses the WDS device.

Figure 12-9 Cisco ISE Network Access Users page detailed



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** form of this command to turn off WDS only 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 reloads, the dot11 radio subsystems 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 [**cdp-neighbor** | **mac-address** *mac-address* | **order ip**]	On the WDS device only, use this command to display cached information about access points participating in CCKM. • cdp-neighbor—displays the CDP neighbors reported by each AP authenticated through the WDS. • mac-address *mac-address*—displays information only on the AP specified byt the entered MAC address. • order ip—changes the order used to display the AP, from ascending using the AP MAC address, to ascending using the AP IP address.
show wlccp wds mn [**detail**] [**mac-addr** *mac-address*]	Use this command 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-address** option to display information about a specific client device.
show wlccp wds	Use this command to display 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.
show wlccp wds nm	Use this command to display the list of all configure network management platforms, along with statistics (transmitted and received messages, retransmissions, and dropped messages).

Command	Description
show wlccp wds statistics	Use this command to display statistics about the WDS. This includes Current AP count, Current client count on connected APs, AAA Authentication Attempt count, AAA Authentication Success count, AAA Authentication Failure count, MAC Spoofing Block count, Roaming without AAA Authentication count (Pre-shared key and Open networks), Roaming with full AAA Authentication count (for non-CCX devices not supporting fast secure roaming), Fast Secured Roaming count, MSC Failure count, KSC Failure count, MIC Failure count (to detect WPA/WPA2 replay attacks), and RN Mismatch count (to detect WPA2 mismatches)
show wlccp wds aggregator statistics	Use this command to display statistics about Radio Measurement information collected from participating APs (received and forwarded updates)

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** | **nm** | **wds-discovery** | **state**}	Use this command to turn on display of debug messages related to client devices (**mn**), configured management platforms (**nm**), 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 rmlib { errors | packets }	Use this command to debug radio measurement messages exchanged between the AP and the WDS, and between the WDS and the Network management platform, when applicable.

Command	Description
debug wlccp wds [aggregator | all | ap | authenticator | mn | nm | recovery | state | statistics]	Use this command and its options to turn on display of WDS debug messages. Use the **ap** option for debugging WDS events for all APs. You can optionally specify a mac-address also to debug the events of that specific AP. Use the **all** option to debug all WDS events. Use the **nm** option to debug messages exchanged with the network management platform when applicable Use the **recovery** option to debug the WDS failover (graceful recovery) process. 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 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 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

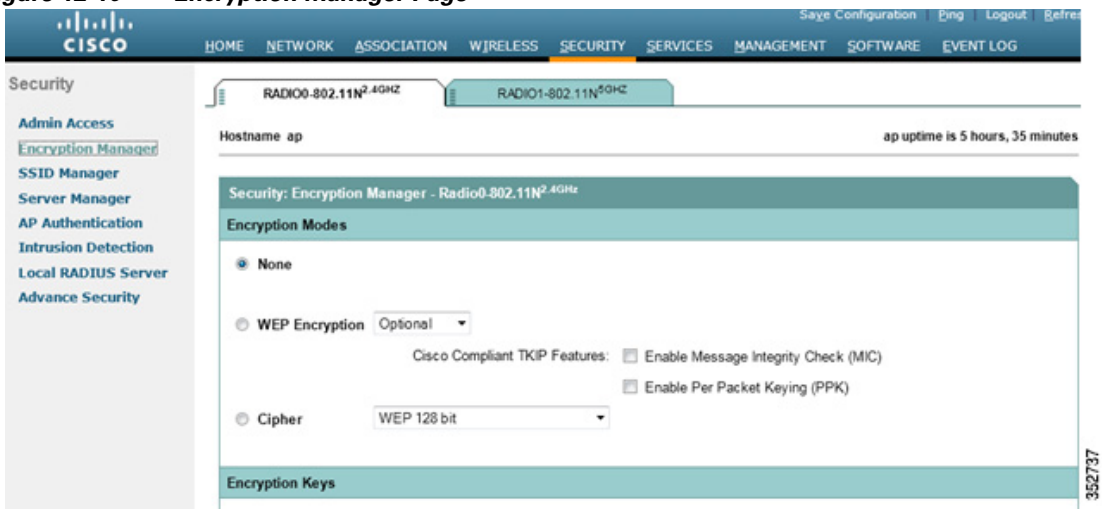
For instructions on configuring WDS, refer to the "Configuring WDS" section on page 12-5.

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 the target SSIDs. Follow these steps to configure CCKM for an SSID:

Step 1 Browse to the Encryption Manager page on the access point GUI. Figure 12-10 shows the top section of the Encryption Manager page.

Figure 12-10 Encryption Manager Page



Step 2 Click the **Cipher** button.

Step 3 Configure the encryption mechanism of your choice. Cisco recommends using WPA2 (except if you need to support legacy clients not supporting WPA2). To set the encryption mechanism to WPA2, choose AES CCMP from the Cipher drop-down list.

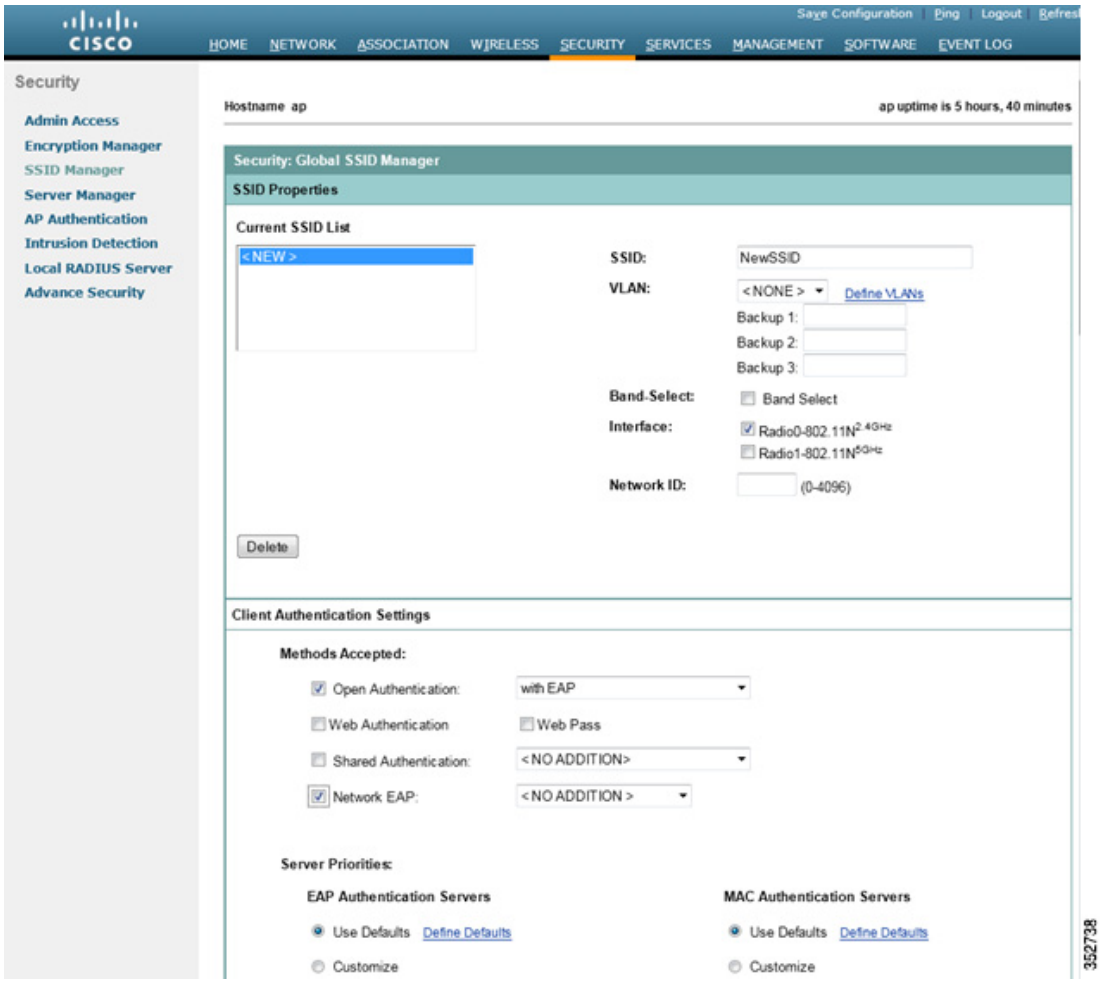
Note Cisco does not recommend configuring mixed modes (AES CCMP with TKIP and or WEP), as these modes are being deprecated and lower the security of your network.

Step 4 Select **CKIP + CMIC** from the Cipher drop-down list.

Step 5 Click **Apply**.

Step 6 Browse to the Global SSID Manager page. Figure 12-11 shows the top sections of the Global SSID Manager page.

Figure 12-11 Global SSID Manager Page



Step 7 On the target SSID where CCKM (fast secure roaming) needs to be supported, select these settings:

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

b. Under network settings, choose the 802.1X/EAP methods to be supported. **Network EAP** should be selected for LAP support with Cisco IP phones 7920, 7921, 7925 and 7926, and for client access points. **Open Authentication with EAP** should be selected for any other EAP type (e.g. PEAP, EAP-FAST, or EAP-TLS), and for all EAP types (including LEAP) for all other clients.

c. Under Client Authenticated Key Management area, in the Key Management drop-down list choose **Mandatory** or **Optional** as required. 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.

d. Check the **CCKM** check box.

e. If you have selected the AES CCMP Cipher, check the Enable WPA check box, and choose the **WPAv2 option** from the drop-down list

Step 8 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 12-18:

```
AP# configure terminal
AP(config)# dot11 ssid NewSSID
AP(config-ssid)# authentication open eap eap_methods
AP(config-ssid)# authentication key-management wpa version 2 cckm
AP(config-ssid)# exit
AP(config)# interface dot11radio0
AP(config-if)# encryption mode ciphers aes-ccm
AP(config-if)# ssid NewSSID
AP(config-if)# exit
AP(config)# end
```

In this example, the SSID *NewSSID* is configured to support EAP with CCKM, the AES CCMP cipher suite is enabled on the 2.4-GHz radio interface, and the SSID *NewSSID* 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*.

Support for 802.11r

Support for 802.11r is provided in Autonomous access points. WGB, Non-root bridge, and repeaters are not supported in 802.11r. It supports only clients.

These types of roaming are supported over the wireless domain services:

- Fast transition over Distributed System (DS)
- Fast transition over Air

802.11r differs from Cisco Centralized Key Management (CCKM) and Pairwise Master Key Identifier (PMKID) roaming in these ways:

- Initial authentication occurs before roaming
- Authentication with the target AP over the Air, or through the DS uses the existing access point's communication channel

Enabling 802.11r

To enable 802.11r, perform these steps:

Step 1 Choose **Network > Network interface**.

Step 2 Click the **Settings** tab.

Step 3 Choose **Radio0-802.11n 2G.Hz** or **Radio0-802.11n 5G.Hz**.

Step 4 Click the **enable** radio button for 11r Configuration.

Step 5 Click the **over-air** or **over-ds** radio button.

Step 6 Enter the reassociation time.

The values range from 20 to 1200.

Step 7 Click **Apply**.

Beginning in privileged EXEC mode, perform these steps to configure 802.11r using the access point CLI:

	Command	Purpose
Step 1	**configure terminal**	Enters the global configuration mode.
Step 2	**dot11 ssid** <*ssid*>	Configures the SSID.
Step 3	**authentication key-management wpa version 2 dot11r**	Configures 802.11r on an access point.
Step 4	**interface dot11radio** {*0* | *1*}	Enters interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 5	**dot11 dot11r pre-authentication {over-air | over-ds}**	Enables or disables the over-air or over-ds transition.
Step 6	**dot11 dot11r re-association timer** <*value*>	Configures the reassociation timer.

Configuring Management Frame Protection

Management Frame Protection operation requires a WDS. You can configure MFP on an access point and WDS manually.

Note Without a management platform, MFP cannot report detected intrusions and so has limited effectiveness.

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.

Client MFP 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.

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.

In order to prevent attacks using broadcast frames, access points supporting CCXv5 and configured for Client MFP, 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.

Note Cisco recommends using WPA2, and not implementing TKIP with WPA version 2, as this mode is being deprecated.

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

Command	Description
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. The **no** form of this 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.
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.
dot11 ids mfp {generator | detector}	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. 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.
sntp server *server IP address*	Enter the name or ip address of the SNTP server.
dot11 ids mfp distributor	Beginning in global configuration mode, use this command to configure 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.

The following CLI commands can be used to display and clear Client MFP statistics on the access point console for a Dot11Radio interface.

Command	Description
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.

Protection of Management Frames with 802.11w

The current 802.11 standard defines frame types for use in the management and control of wireless links. The management frames, included in the 802.11 protocol, are neither authenticated nor encrypted, even when the highest level of WLAN security are used. 802.11w is the Protected Management Frames standard for the IEEE 802.11 family of standards.

802.11w increases the security of the management frames by offering three new security pieces:

- Data Origin Authenticity
- Replay Detection
- Robust Management Frame Protection.

The Management frames that can be protected are:

- Disassociation
- Deauthentication
- Robust Action frames excluding Public Action frames

802.11w is also used to prevent association request replay attack. The protection offered by 802.11w is somewhat comparable to the protection offered by Cisco Client MFP. However, 802.11w does not offer a mechanism comparable to Cisco Infrastructure MFP.

To enable Cisco Client MFP, you need to make sure that the clients to be protected support CCXv5. To enable 802.11w, you need to make sure that the clients to be protected support 802.11w.

Both Cisco Infrastructure MFP and 802.11w can be enabled on the same SSID. However, you should not enable Cisco Client MFP and 802.11w on both the same SSID and the same radio.

Perform these steps to enable 802.11w:

Step 1 Browse to the Security page on the access point GUI.

Step 2 Select SSID Manager.

Step 3 From the Client Authenticated Key Management page, you can:

- Click the **11w Configuration Required** radio button, to allow only clients that support 802.11w to join the SSID.
- Click the **11w Configuration Optional** radio button, to allow both clients supporting 802.11w and clients not supporting 802.11w to join the SSID.

Step 4 Enter the **11w Association-comeback** time.

Step 5 Enter the **11w Saquery-retry** time.

This CLI command is used to enable 802.11w on the access point:

ap(config-ssid)# **11w-pmf client** *required/optional*

This CLI command is used to configure the association time out and saquery retry time interval:

ap(config-ssid)# **11w-pmf association-comeback** *1000-20000ms*

ap(config-ssid)# **11w-pmf saquery-retry** *100-500ms*

These commands are optional. Default time intervals are configured if these commands are not used. To configuring 802.11w on an access point, mfp client should be disable

Note WPAv2/AES is mandatory for 802.11w.

Note After 802.11r is enabled, the CCKM, 11r fast roaming, DLS, Radio Measurement and Protected Dual of Public Action frames are not supported.

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 management platform 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.

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

Step 3 Check the ***Configure Wireless Network Manager*** check box.

Step 4 In the ***Wireless Network Manager IP Address*** field, enter the IP address of the management platform on your network.

Step 5 Click **Apply**. The WDS access point is configured to interact with your management platform.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Radio Management" section on page 12-25:

```
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 management platform 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 12-10 and in the "Configuring Radio Management" section on page 12-25 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.

Beginning in privileged EXEC mode, follow these steps to set the access point radio network role to scanner:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**station role scanner**	Set the access point role to scanner.
Step 4	**end**	Return to privileged EXEC mode.

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.

Beginning in privileged EXEC mode, follow these steps to configure the access point to capture and forward 802.11 frames:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1**}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**monitor frames endpoint ip address** *IP-address* **port** *UDP-port* [**truncate** *truncation-length*]	Configure the radio for monitor mode. Enter the IP address and the UDP port on the WIDS engine on your network. • (Optional) Configure a maximum length in bytes for each forwarded frame. The access point truncates frames longer than this value. The default length is 128 bytes.
Step 4	**end**	Return to privileged EXEC mode.

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

Beginning in privileged EXEC mode, follow these steps to set authentication limits that trigger a fault on the access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ids eap attempts** *number* **period** *seconds*	Configure the number of authentication attempts and the number of seconds of EAPOL flooding that trigger a fault on the access point.
Step 3	**end**	Return to privileged EXEC mode.

Configuring 802.11u Hotspot and Hotspot 2.0

The 802.11u Hotspot feature enables IEEE 802.11 devices to interwork with external networks. It is used in hotspots or other public networks irrespective of whether the service is subscription based or free.

Wi-Fi Certified Passpoint, also known as Hotspot 2.0, streamlines network access in hotspots and eliminates the need for users to find and authenticate a network each time they connect. In Wi-Fi networks that do not support Passpoint, users must search for and choose a network, request the connection to the access point each time, and in many cases, must re-enter their authentication credentials. Passpoint automates that entire process, enabling a seamless connection between hotspot networks and mobile devices, with the highest WPA2 security.

The 802.11u Hotspot feature aids network discovery and selection, enabling information transfer from external networks. It provides information to the stations about the networks prior to association. Interworking not only helps users within the home, enterprise, and public access, but also assists manufacturers and operators to provide common components and services for IEEE 802.11 customers.

Before configuring an 802.11u Hotspot, ensure that you have:

- WPA key management
- Multiple Basic SSIDs

Follow these steps to configure an 802.11u Hotspot and Hotspot 2.0:

Step 1 Enter the ap(config-ssid)# mode.

Step 2 Enter the following commands to enable and configure 802.11u Hotspot:

a. hotspot dot11u enable

b. hotspot dot11u domain *index domain_name*

c. hotspot dot11u network-type *network_type internet_availabily_status(0 or 1)*

d. hotspot dot11u auth-type *auth_type*

e. hotspot dot11u ipaddr-type *ipv4type ipv6type*

f. hotspot dot11u hessid *h.h.h*

g. hotspot dot11u nai-realm *index* realm-name *name_string*

h. hotspot dot11u nai-realm *index* eap-method *eap-index eap_method*

i. hotspot dot11u nai-realm *index* auth-method *eap-index auth-index auth_type auth_subtype*

j. hotspot dot11u roam-oi *index hex-string isbeacon*

k. hotspot dot11u 3gpp-info *index mobile_country_code mobile_network_code*

Example:Enabling 802.11u Hotspot

```
ap(config-ssid)# hotspot dot11u enable
ap(config-ssid)# hotspot dot11u domain 1 cisco
ap(config-ssid)# hotspot dot11u network-type  2   1
ap(config-ssid)# hotspot dot11u auth-type  1
ap(config-ssid)# hotspot dot11u ipaddr-type 2 2
```

```
ap(config-ssid)# hotspot dot11u hessid 1234.5678.1234
ap(config-ssid)# hotspot dot11u nai-realm 1 realm-name cisco
ap(config-ssid)# hotspot dot11u nai-realm 1 eap-method 1 17
ap(config-ssid)# hotspot dot11u nai-realm 1 auth-method  1 1 1 2
ap(config-ssid)# hotspot dot11u roam-oi 1 004096 1
ap(config-ssid)# hotspot dot11u 3gpp-info 1 123 123
```

Step 3 Enter the following commands to enable and configure 802.11u Hotspot 2.0 :

a. hotspot hs2 enable

b. hotspot hs2 operator-name *index language_code operator_name*

c. hotspot hs2 wan-metrics *link_status symmetric_link_status uplink_speed downlink_speed*

d. hotspot hs2 port-config *ip_protocol port_number port_status*

Example:Enabling 802.11u Hotspot 2.0

```
ap(config-ssid)# hotspot hs2 enable
ap(config-ssid)# hotspot hs2 operator-name 1 eng cisco
ap(config-ssid)# hotspot hs2 wan-metrics 1 1 2345 3434
ap(config-ssid)# hotspot hs2 port-config 1 23 34 2
```

Step 4 Enter the following global configuration commands:

a. dot11 dot11u ap-venue name *name_string*

b. dot11 dot11u ap-venue type *venue_group venue_type*

Example:Global configuration commands:

```
ap(config)# dot11 dot11u ap-venue name cisco_odc
ap(config)# dot11 dot11u ap-venue type 2 2
```

To debug the 802.11u Hotspot and Hotspot 2.0 configuration, use the command **debug dot11 dot11u**.

To enable and configure 802.11u Hotspot and Hotspot 2.0 via the GUI, go to **Security > Dot11u Manager**.