



## Configuring Fast Reassociation

---

This chapter describes how to configure the access point for fast reassociation of roaming client devices. This chapter contains these sections:

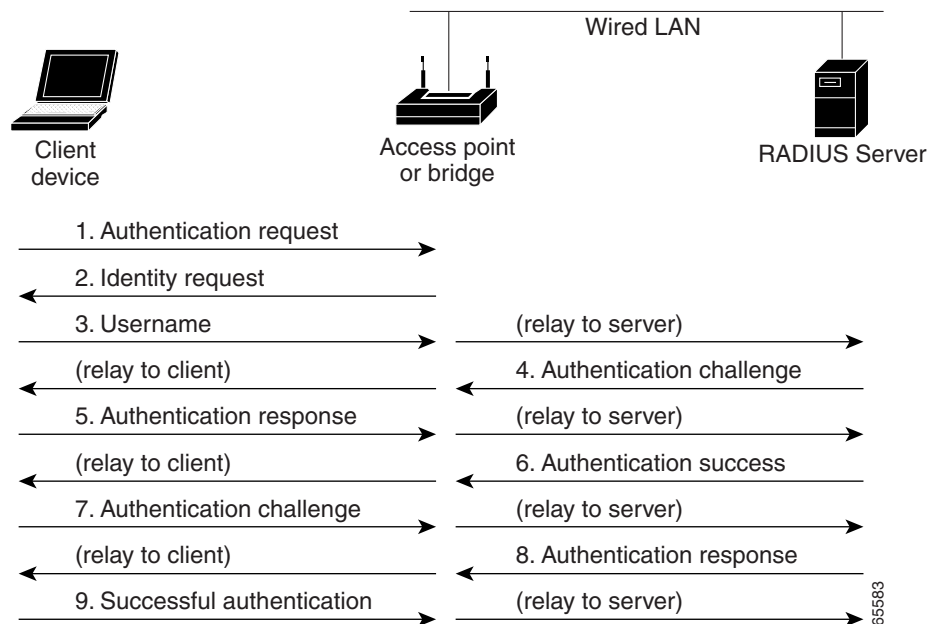
- [Understanding Fast Reassociation, page 11-2](#)
- [Configuring Fast Reassociation, page 11-4](#)

# Understanding Fast Reassociation

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

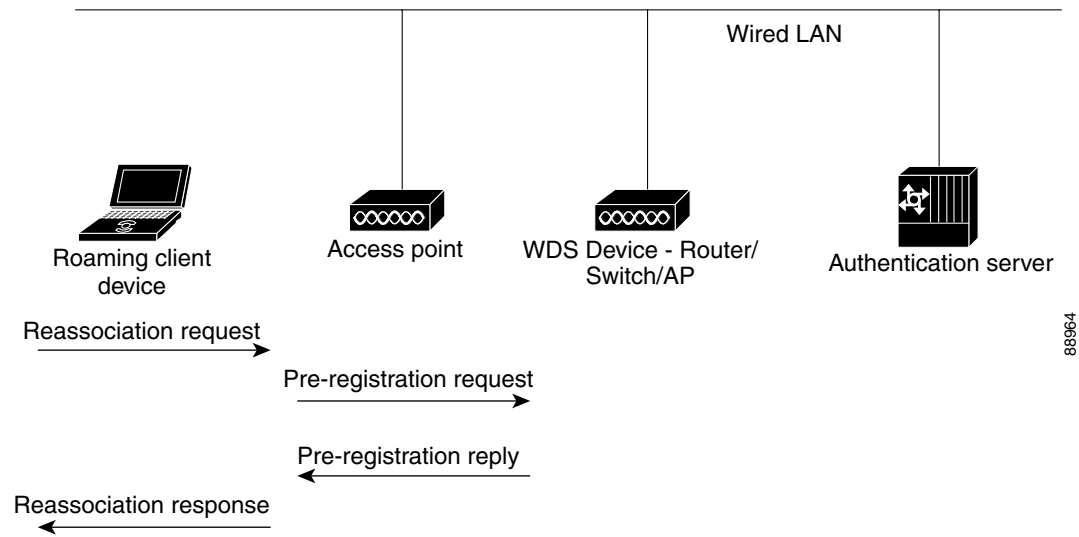
During normal operation, LEAP-enabled client devices mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server, as in [Figure 11-1](#).

**Figure 11-1 Client Authentication Using a RADIUS Server**



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

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



The WDS access point 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 access point. The WDS access point 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.

The WDS access point performs several tasks on your wireless LAN:

- Authenticates all access points in the subnet and establishes a secure communication channel with each of them.
- Registers all client devices in the subnet, establishes session keys for them, and caches their security credentials. When a client roams to another access point, the WDS access point forwards the client's security credentials to the new access point.
- Advertises its WDS capability and participates in electing the best WDS access point for your wireless LAN. When you configure your wireless LAN for fast reassociation, you set up one access point as the main WDS access point candidate and one or more additional access points as backup WDS access point candidates.

**Note**

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

**Note**

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

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

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

## Configuring Fast Reassociation

This section describes how to set up your wireless LAN to use fast reassociation for roaming client devices. This section includes these sections:

- [Requirements for Fast Reassociation, page 11-4](#)
- [Configuration Overview, page 11-4](#)
- [Configuring Access Points as Potential WDS Access Points, page 11-5](#)
- [Configuring Access Points to use the WDS Access Point, page 11-6](#)
- [Viewing WDS Information, page 11-7](#)
- [Using Debug Messages, page 11-7](#)

## Requirements for Fast Reassociation

To set up fast reassociation, you must have these items on your wireless LAN:

- At least one access point that you can configure as the WDS access point
- Cisco Aironet client devices running Cisco client firmware version 5.20.17 or later

## Configuration Overview

You must complete three major steps to set up fast reassociation:

1. Configure access points on your wireless LAN as potential WDS access points.
2. Configure the rest of your access points to use the WDS access point.
3. Enable access points on the subnet to allow CCKM authenticated key management for at least one SSID. See the [“Configuring Authentication Types” section on page 10-8](#) for complete instructions on enabling CCKM.

## Configuring Access Points as Potential WDS Access Points



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



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

Beginning in Privileged Exec mode 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:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>wlccp wds priority</b> <i>priority</i> <b>interface</b> <i>interface</i>	Enable the access point as a WDS access point candidate. <ul style="list-style-type: none"> <li>• <b>priority</b>—Enter a priority number from 1 to 255 to set the priority of this WDS candidate. The WDS access point candidate with the highest priority number becomes the acting WDS access point.</li> <li>• <b>interface</b>—Set the interface on which the access point sends out WDS advertisements. For this release, you must use <b>bvi 1</b> as the interface for WDS advertisements.</li> </ul>
Step 3	<b>wlccp authentication-server infrastructure</b> <i>list</i>	Configure the list of servers to be used for 802.1x authentication for your wireless infrastructure devices, such as access points and repeaters. See the <a href="#">“Defining AAA Server Groups”</a> section on page 12-9 for instructions on creating a list of servers.
Step 4	<b>wlccp authentication-server client</b> { <b>any</b>   <b>eap</b>   <b>leap</b>   <b>mac</b> } <i>list</i>	Configure the list of servers to be used for 802.1x authentication for CCKM-enabled client devices. You can specify a separate list for clients using a certain type of authentication, such as EAP, LEAP, or MAC-based, or specify a list for client devices using any type of authentication. See the <a href="#">“Defining AAA Server Groups”</a> section on page 12-9 for instructions on creating a list of servers.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no** form of the **wlccp wds** command to remove the access point from the list of WDS access point candidates. Use the **no** form of the **wlccp authentication-server** commands to disable server lists.

This example shows how to set up a high-priority WDS access point candidate using different server lists for authenticating infrastructure devices, client devices using LEAP, and client devices using MAC-based authentication:

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 100 interface bvi1
```

```
AP(config)# wlccp authentication-server infrastructure wlan-list1  
AP(config)# wlccp authentication-server client leap leap-list1  
AP(config)# wlccp authentication-server client mac mac-list1  
AP(config)# end
```

## Configuring Access Points to use the WDS Access Point

To configure an access point to authenticate through the WDS access point and participate in CCKM, enter this command in global configuration mode:

```
AP(config)# wlccp ap username username password [ 0 | 7 ] password
```

Enter the username and password that the access point uses to authenticate to the network. The 0 or 7 option determines whether the access point's password is encrypted (7) or unencrypted (0).

Use the no form of the command to disable participation in CCKM.

## Viewing WDS Information

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

Command	Description
<code>show wlccp ap</code>	Use this command on access points participating in CCKM to display the WDS access point's MAC address, the WDS access point'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.
<code>show wlccp wds { ap   mn } [ detail ] [ mac-addr mac-address ]</code>	<p>On the WDS access point only, use this command to display cached information about access points and client devices.</p> <ul style="list-style-type: none"> <li><b>ap</b>—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 <b>mac-addr</b> option to display information about a specific access point.</li> <li><b>mn</b>—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 <b>detail</b> option to display the client's lifetime (seconds remaining before the client must reauthenticate), SSID, and VLAN ID. Use the <b>mac-addr</b> option to display information about a specific client device.</li> </ul> <p>If you only enter <b>show wlccp wds</b>, the command displays the access point's IP address, MAC address, priority, and interface state (administratively standalone, active, backup, or candidate). If the state is backup, the command also displays the current WDS access point's IP address, MAC address, and priority.</p>

## Using Debug Messages

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

Command	Description
<code>debug wlccp ap { mn   wds-discovery   state }</code>	Use this command to turn on display of debug messages related to client devices ( <b>mn</b> ), the WDS discovery process, and access point authentication to the WDS access point ( <b>state</b> ).
<code>debug wlccp leap-client</code>	Use this command to turn on display of debugging messages related to LEAP-enabled client devices.

Command	Description
<code>debug wlccp packet</code>	Use this command to turn on display of packets to and from the WDS access point.
<code>debug wlccp wds [ state   statistics ]</code>	Use this command and the <b>state</b> option to turn on display of WDS debug and state messages. Use the <b>statistics</b> option to turn on display of failure statistics.