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

- Understanding WDS, page 11-2
- Understanding Fast Secure Roaming, page 11-3
- Understanding Radio Management, page 11-4
- Configuring WDS and Fast Secure Roaming, page 11-4
- Configuring Radio Management, page 11-12
- Using Debug Messages, page 11-11
Understanding WDS

The following sections describe WDS even though the access point/bridge cannot be configured as a WDS server even when it is configured as an access point. However, when configured as an access point, the access point/bridge can use a WDS server and can act as a WDS authenticator (client).

When you configure an access point to provide WDS, other access points (such as your access point/bridge if it is configured as an access point) on your wireless LAN use the WDS access point to provide fast, secure roaming for client devices and to participate in radio management.

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 access point. The WDS access point aggregates the information and forwards it to a wireless LAN solution engine (WLSE) device on your network.

Role of the WDS Access Point

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

- Advertises its WDS capability and participates in electing the best WDS access point for your wireless LAN. When you configure your wireless LAN for WDS, 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.
- Authenticates all access points in the subnet and establishes a secure communication channel with each of them.
- Collects radio data from access points in the subnet, aggregates the data, and forwards it to the WLSE device on your network.
- Registers all client devices in the subnet, establishes session keys for them, and caches their security credentials. When a client roams to another access point, the WDS access point forwards the client’s security credentials to the new access point.

Role of Access Points Using the WDS Access Point

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.
- Report radio data to the WDS access point.
Understanding Fast Secure Roaming

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

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

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

When you configure your wireless LAN for fast, secure roaming, however, LEAP-enabled client devices roam from one access point to another without involving the main server. Using Cisco Centralized Key Management (CCKM), 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.
Understanding Radio Management

Access points participating in radio management scan the radio environment and send reports to the WDS access point on such radio information as potential rogue access points, associated clients, client signal strengths, and the radio signals from other access points. The WDS access point forwards the aggregated radio data to the WLSE device on your network. Access points participating in radio management also assist with the self-healing wireless LAN, automatically adjusting settings to provide coverage in case a nearby access point fails. Refer to the “Configuring Radio Management” section on page 11-12 for instructions on configuring radio management.

Configuring WDS and Fast Secure Roaming

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

- Guidelines for WDS, page 11-5
- Requirements for WDS and Fast Secure Roaming, page 11-5
- Configuring the Access Point/Bridge to use the WDS Access Point, page 11-5
- Configuring the Access Point/Bridge to use the WDS Access Point, page 11-5
- Configuring the Authentication Server to Support Fast Secure Roaming, page 11-6
Guidelines for WDS

You should be aware of these WDS guidelines:

- You cannot configure your access point/bridge as a WDS access point. However, when you configure your access point/bridge as an access point, you can also configure it to use the WDS access point.
- Repeater access points do not support WDS.

Requirements for WDS and Fast Secure Roaming

The wireless LAN on which your access point/bridge resides must meet these requirements:

- At least one access point available to be configured as the WDS access point
- An authentication server (or an access point configured as a local authenticator)
- Cisco Aironet client devices running Cisco client firmware version 5.20.17 or later

Configuring the Access Point/Bridge to use the WDS Access Point

Your access point/bridge must be configured as an access point before you can configure it to use WDS. Follow these steps to configure your access point/bridge to authenticate through the WDS access point and participate in CCKM:

**Step 1** Browse to the Wireless Services Summary page.

**Step 2** Click AP to browse to the Wireless Services AP page. **Figure 11-3** shows the Wireless Services AP page.
Configuring WDS and Fast Secure Roaming

Step 3 In the Participate in SWAN Infrastructure field, click Enabled.

Step 4 Choose one of the following options in the WDS Discovery field:
   a. Auto Discovery—The access point/bridge finds the WDS access point automatically.
   b. Specified Discovery—The access point/bridge discovers the WDS access point based on the IP address you enter.

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

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

Step 7 In the L3 Mobility Service via IP/GRE Tunnel, enter the value of the GRE Tunnel MTU.

Step 8 Click Apply.

Once you complete the configuration, the access point/bridge interacts with the WDS and automatically performs these steps:
- Discovers and tracks the current WDS access point and relays WDS advertisements to the wireless LAN.
- Authenticates with the WDS access point and establishes a secure communication channel to the WDS access point.
- Registers associated client devices with the WDS access point.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the “Configuring the Access Point/Bridge to use the WDS Access Point” section on page 11-5:

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

In this example, the access point/bridge is enabled to interact with the WDS access point, 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 Fast Secure Roaming

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

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 access point. Figure 11-4 shows the Network Configuration page.

![Network Configuration Page](image)

**Figure 11-4  Network Configuration Page**

Step 2  Click **Add Entry** under the AAA Clients table. The Add AAA Client page appears. Figure 11-5 shows the Add AAA Client page.
Chapter 11      Configuring WDS, Fast Secure Roaming, and Radio Management

Configuring WDS and Fast Secure Roaming

Step 3 In the AAA Client Hostname field, enter the name of the WDS access point.
Step 4 In the AAA Client IP Address field, enter the IP address of the WDS access point.
Step 5 In the Key field, enter exactly the same password that is configured on the WDS access point.
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 access point 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 access point. Figure 11-6 shows the User Setup page.
Step 10  Enter the name of the access point in the User field.
Step 11  Click Add/Edit.
Step 12  Scroll down to the User Setup box. Figure 11-7 shows the User Setup box.

**Figure 11-6  User Setup Page**

**Figure 11-7  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 access point.
Step 17  Browse to the System Configuration page, click Service Control, and restart ACS to apply your entries. Figure 11-8 shows the System Configuration page.

**Figure 11-8  ACS System Configuration Page**

**Viewing WDS Information**

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

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

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug wlc cp ap [ mn ] [ mobility ] [ rm ] [ state ] [ lws-discovery ]</td>
<td>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 access point (state).</td>
</tr>
<tr>
<td>debug wlc cp leap-client</td>
<td>Use this command to turn on display of debugging messages related to LEAP-enabled client devices.</td>
</tr>
<tr>
<td>debug wlc cp packet</td>
<td>Use this command to turn on display of packets to and from the WDS access point.</td>
</tr>
<tr>
<td>debug wlc cp wds [ state ] [ statistics ]</td>
<td>Use this command and the state option to turn on display of WDS debug and state messages. Use the statistics option to turn on display of failure statistics.</td>
</tr>
</tbody>
</table>
Configuring Radio Management

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

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

**Step 1**  Browse to the Wireless Services Summary page. *Figure 11-9* shows the Wireless Services Summary page.

![Figure 11-9 Wireless Services Summary Page](image)

*Figure 11-9 Wireless Services Summary Page*

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

**Step 3**  On the WDS/WNM Summary page, click **Settings** to browse to the General Setup page. *Figure 11-10* shows the General Setup page.

Click **Refresh**
Figure 11-10 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 “For complete descriptions of the commands used in this example, consult the Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges.” section on page 11-13:

```
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.