



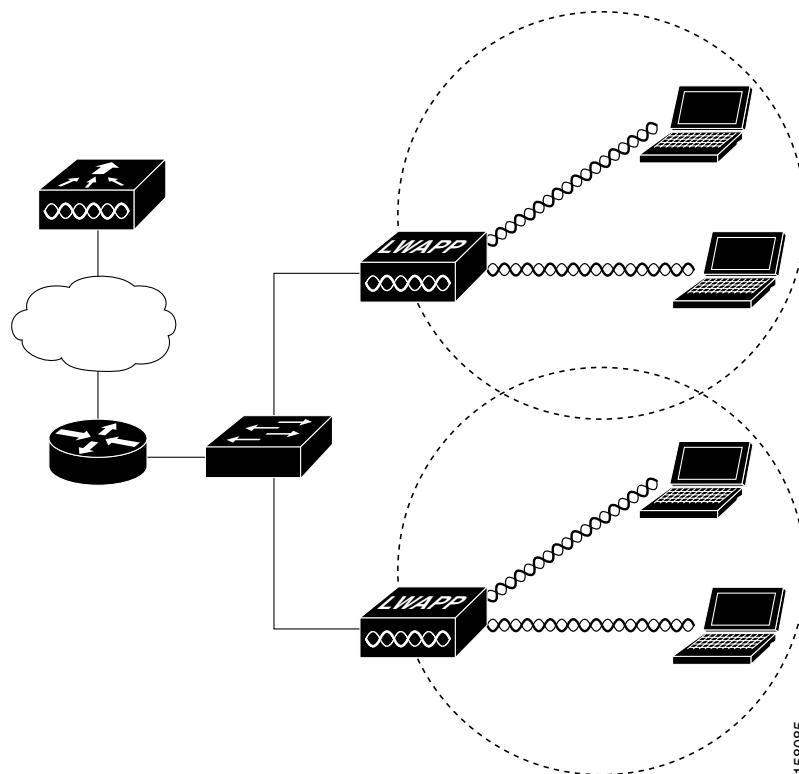
APPENDIX **E**

Priming Access Points Prior to Deployment

This section describes an optional procedure designed to prime or stage your access points in a convenient location rather than after they are installed in possibly difficult to reach locations. This helps limit potential installation problems to primarily Ethernet and power areas.

[Figure E-1](#) illustrates a typical priming configuration for your access points.

Figure E-1 Typical Priming Configuration



Before deploying your access points to their final locations, follow these steps to prime your access points:

- Step 1** In a Layer 2 environment, where the access points are located on the same subnet as the controller, the access point communicates directly with the controller.
- Step 2** In a Layer 3 environment, ensure a DHCP server (typically on your switch) is enabled on the same subnet as your access points. The access points will receive its IP address and controller information using DHCP Option 43.

The access point must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, OTAP, or IP subnet broadcast. This guide describes the DHCP method to convey the controller IP address. For other methods, refer to the product documentation. See also the [“Using DHCP Option 43” section on page 3-2](#) for more information.



Note For a Layer 3 access point on a different subnet than the controller, ensure ensure the route to the controller has destination UDP ports 12222 and 12223 open for LWAPP communications. Ensure the routes to the primary, secondary, and tertiary controllers allow IP packet fragments.

- Step 3** Ensure that your controller is connected to a switch trunk port.
- Step 4** Configure the controller in LWAPP Layer 3 mode and ensure that its DS Port is connected to the switch. Use the CLI, web-browser interface, or Cisco WCS procedures as described in the appropriate controller guide.

- a. In multi-controller environments, You can set one controller’s DS port to **Master** (you can use the *config network master-base disable* CLI command or you can use the controller GUI) so that new access points always associate with it. You can use the **show network config** CLI command to determine if the controller DS port is the master.

All access points associate to the master controller. From one location, you can configure access point settings such as primary, secondary, and tertiary controllers. This allows you to redistribute your access points to other controllers on the network.

You can also use a Cisco WCS server to control, configure, and redistribute all your access points from a single location.

- Step 5** Apply power to the access points:
- a. Connect your access points to untagged access ports on your POE capable switch. You can optionally use power modules (AIR-PWR-1000=) or power injectors (AIR-PWRINJ-1000AF=) to power your access points.
- b. After you power up the access point, it begins a power-up sequence that you can check by observing the access point LEDs. The red Alarm LED turns on for about 15 to 20 seconds and then all LEDs blink sequentially back an forth, indicating that the access point is trying to find a controller.



Note If the access point remains in this mode for more than 5 minutes, the access point is unable to find the master controller. Check the connection between the access point and the controller and ensure they are on the same subnet.

- c. If the access point shuts down (all LEDs off), check to ensure that sufficient power is available.
- d. When the access point associates with the controller, if the access point code version differs from the controller code version, the access point downloads the operating system code from the controller. All the access point LEDs blink simultaneously during the download.

- Step 6** If the operating system download is successful, the access point reboots. Normal operation is indicated when the Alarm LED is off, the Power LED is green, and the 2.4 GHz and 5 GHz LEDs are blinking to indicate radio activity.



Note If the Alarm LED remains red for more than a minute, remove power from the access point and contact Cisco Technical Support for assistance.

- Step 7** Use the controller CLI, controller GUI, or Cisco WCS to configure the access point with primary, secondary, and tertiary controller names.
- Step 8** If the access point is in a Controller Mobility Group, use the controller CLI, controller GUI, or Cisco WCS to configure the Controller Mobility Group name.
- Step 9** Use controller CLI, controller GUI, or Cisco WCS to configure the access point-specific 802.11a, 802.11b, and 802.11g network settings.
- Step 10** If the configuration priming was successful, the Power LED is green, the Alarm LED is off, and the radio LEDs are blinking to indicate normal operation.
- Step 11** Repeat Steps 4 to 9 for each access point.

When you successfully complete the configuration priming of all your access points, ensure the Master setting is disabled on your controller. You can begin deploying the access points to their final destinations (refer to the [“Deploying the Access Points on the Wireless Network”](#) section on page 2-7).
