

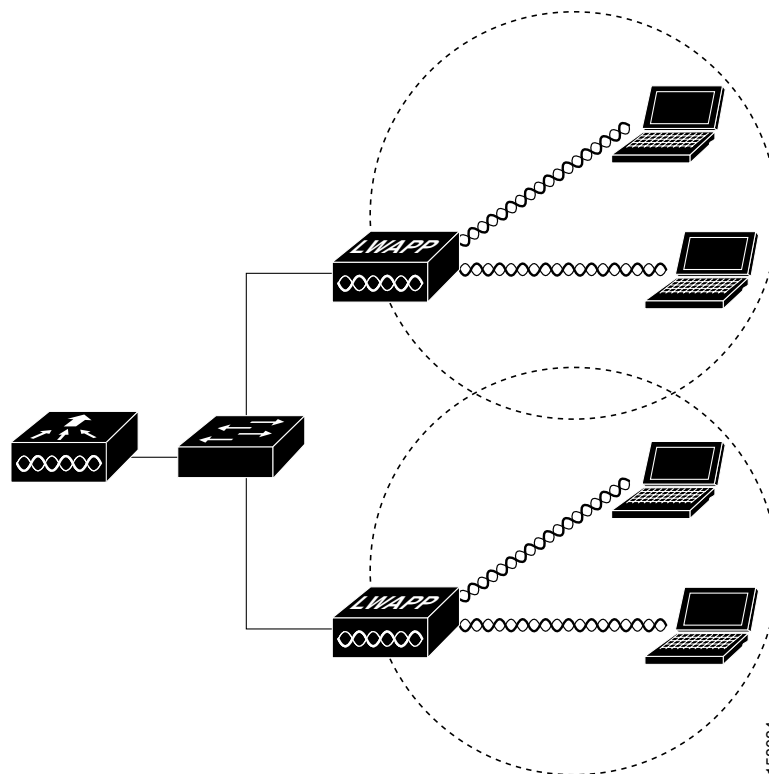


## Priming Access Points Prior to Deployment

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

**Figure F-1** Typical Priming Configuration



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

- 
- Step 1** Use the controller CLI, controller GUI, or Cisco WCS to configure your controller:
- a. Add the MAC addresses of your access points in controller filter list (refer to the [“Adding the Access Point MAC Addresses to the Controller Filter List”](#) section on page 2-10).
  - b. Enable Zero Touch Configuration on your controller (refer to the [“Enabling Zero Touch Configuration on the Controller”](#) section on page 2-10).
- Step 2** 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. In this environment, you don’t need a DHCP server on the same subnet as the access points because the access points receive IP address information from the controller.
- Step 3** In a Layer 3 environment, ensure that 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. Refer to the [“Controller MAC Filter List”](#) section on page 3-2 for more information.




---

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

---

- Step 4** Ensure that your controller is connected to a switch trunk port.
- Step 5** 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 6** 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 injectors (AIR-PWRINJ1500=) to power your access points.
  - b. 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.
  - c. When the operating system download is successful, the access point reboots.

- 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** Repeat Steps 4 to 9 for each access point.
- When you successfully complete the configuration priming of all your access points, ensure that Master setting is disabled on your controller. You can begin deploying the access points to their final destinations.
-

