



## Troubleshooting

---

This chapter provides troubleshooting procedures for basic problems with the access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

[http://www.cisco.com/en/US/products/hw/wireless/tsd\\_products\\_support\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html)

Sections in this chapter include:

- [Guidelines for Using the Access Points](#), page 3-2
- [Controller MAC Filter List](#), page 3-2
- [Using DHCP Option 43](#), page 3-3
- [Misconfigured Bridge Shared Secret Key](#), page 3-3
- [Misconfigured MESH Access Point IP address](#), page 3-3
- [Verifying Controller Association](#), page 3-4
- [Access Point Power](#), page 3-4

## Guidelines for Using the Access Points

You should keep these guidelines in mind when you use the access points:

- The access point can only communicate with controllers and cannot operate independently.
- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.
- The access points support Layer 2 or Layer 3 LWAPP communications with the controllers. In Layer 2 operation, the access point and the controller must be on the same subnet and communicate with each other using MAC addresses in encapsulated Ethernet frames. This operation is not scalable to larger networks and not recommended by Cisco.

In Layer 3 operation, the access point and the controller can be on the same or different subnets. The access point communicates with the controller using standard IP packets. Layer 3 operation is scalable and is recommended by Cisco. A Layer 3 access point on a different subnet than the controller requires a DHCP server on the access point subnet and a route to the controller. The route to the controller must have destination UDP ports 12222 and 12223 open for LWAPP communications. The route to the primary, secondary, and tertiary controllers must allow IP packet fragments.

- Before deploying your access points ensure that the following has been done:
  - Your controllers are connected to switch ports that are configured as trunk ports.
  - Your access points are connected to switch ports that are configured as untagged access ports.
  - A DHCP server is reachable by your access points and has been configured with Option 43. Option 43 is used to provide the IP addresses of the Management Interfaces of your controllers. Typically, a DHCP server can be configured on a Cisco switch.
  - Optionally a DNS server can be configured to enable `CISCO-LWAPP-CONTROLLER.<local domain>` to resolve to the IP address of the Management Interface of your controller.
  - Your controllers are configured and reachable by the access points.
  - Your controllers are configured with the MAC addresses of the access points and Zero Touch Configuration is enabled.

## Controller MAC Filter List

Prior to activating your access point, you must ensure that the access point MAC address has been added to the controller MAC Filter list. To view the MAC addresses added to the controller MAC filter list, you can use the controller CLI or the controller GUI:

- Controller CLI—Use the **show macfilter summary** controller CLI command to view the MAC addresses added to the controller filter list.
- Controller GUI—Log into your controller web interface (HTTPS) using a web browser and choose **SECURITY > MAC Filters** to view the MAC addresses added to the controller filter list.

## Using DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling the access point to find and join a controller. Refer to the product documentation for your DHCP server for instructions on configuring DHCP Option 43. For additional information, refer to the [“Configuring DHCP Option 43” section on page G-1](#).

## Misconfigured Bridge Shared Secret Key

If an access point has a misconfigured bridge shared secret key, it is not allowed to join the mesh network. If **Enable Zero Touch Configuration** is checked on your controller, the access point can obtain the shared secret key from the controller or a neighbor access point.

If **Enable Zero Touch Configuration** is not checked, you might need to check the feature to allow the access point to get a new bridge shared secret key (refer to the [“Enabling Zero Touch Configuration on the Controller” section on page 2-10](#)).

## Misconfigured MESH Access Point IP address

IP address misconfiguration can occur when you are re-addressing a segment of your mesh network and your first IP address change is the IP addresses of the RAP connected to the wired network. To avoid this problem, always start the IP addressing changes from the farthest access point and work your way back to the RAP. This problem might also happen if you move equipment; for example, you uninstall an access point and redeploy it in another physical location on the mesh network with a different IP subnet.

Another option to fix this misconfigured IP address is to physically take a controller in L2 mode with a RAP to the location of the misconfigured MAP. Set the bridge group name for the RAP to match the misconfigured MAP. Add the MAP's MAC address to the controller's filter list and check **Enable Zero Tough Configuration**. When the misconfigured MAP displays on the controller's Summary page, you can properly configure the access point.

## Verifying Controller Association

To verify that your access point is associated to the controller, follow these steps:

---

**Step 1** Log into your controller web interface (HTTPS) using a web browser.



**Note** You can also use the controller CLI **show ap summary** command from the controller console port.

---

**Step 2** Click **Wireless** and verify that your access point MAC address is listed under Ethernet MAC.

**Step 3** Logout of the controller and close your web browser.

---

## Access Point Power

The access point does not have an LED to indicate available power.



**Caution**

No serviceable parts inside. Do not open.

---

To ensure that your access point has power after installation, perform these steps:

---

**Step 1** Ensure that the access point power source is turned-off.

**Step 2** Remove and reconnect the AC power or Ethernet connector that supplies power to the access point.



**Note** Hand-tighten the connector until the connector locks.

---

**Step 3** Ensure that all other cable connectors are properly connected.

**Step 4** Turn-on the power source for the access point.

---