CHAPTER 4

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/cisco/web/support/index.html

Sections in this chapter include:

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 point only supports Layer 3 CAPWAP communications with the controllers.

  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. 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 CAPWAP 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 provides 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-CAPWAP-CONTROLLER. Use *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 access point MAC addresses and the MAC filter list is enabled.
  - If layer 3 functionality is enabled on your switch, make sure that DHCP broadcast and request can be passed.
- The access point PoE Out port should be connected only to a single peripheral customer device, such as a camera or sensor gateway. We recommend that the PoE Out port not be connected to a switch or hub.
- After the access points are associated to the controller, you should change the bridge group name (BGN) from the default value. With the default BGN, the mesh access points (MAPs) can potentially try to connect with other mesh networks and slow down the convergence of the network.

Important Notes

Convergence Delays

During deployment, the access points can experience convergence delays due to various causes. The following list identifies some operating conditions that can cause convergence delays:

- A root access point (RAP) attempts to connect to a controller using any of the wired ports (cable, fiber-optic, PoE In, or PoE Out). If the wired ports are operational, the RAP can potentially spend several minutes on each port prior to connecting to a controller.

- If a RAP is unable to connect to a controller over the wired ports, it attempts to connect using the wireless network. This results in additional delays when multiple potential wireless paths are available.
- If a MAP is unable to connect to a RAP using a wireless connection, it then attempts to connect using any available wired port. The access point can potentially spend several minutes for each connection method, before attempting the wireless network again.

Bridge Loop

The access point supports packet bridging between wired and wireless network connections. The same network must never be connected to multiple wired ports on an access point or on two bridged access points. A bridge loop causes network routing problems.

Controller DHCP Server

The controller DHCP server only assigns IP addresses to lightweight access points, Ethernet bridging clients on the mesh access points, and wireless clients associated to an access point. It does not assign an IP address to other devices.

MAP Data Traffic

If the signal on the access point backhaul channel has a high signal-to-noise ratio, it is possible for a MAP to connect to the controller, via parent node, but not be able to pass data traffic, such as pinging the access point. This can occur because the default data rate for backhaul control packets is set to 6 Mb/s, and the backhaul data rate set to auto by the user.

Controller MAC Filter List

Before activating your access point, you must ensure that the access point MAC address has been added to the controller MAC filter list and that **Mac Filter List** is enabled.

Note The access point MAC address and barcode is located on the bottom of the unit. When two MAC addresses are shown, use the top MAC address.

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 using a web browser, and choose **SECURITY > AAA > MAC Filtering** to view the MAC addresses added to the controller filter list.

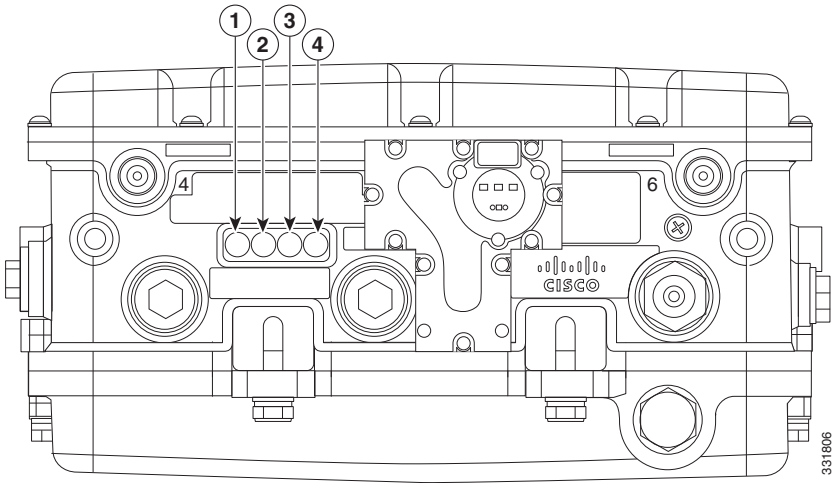
Using DHCP Option 43

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 Appendix F, "Configuring DHCP Option 43".

Monitoring the Access Point LEDs

If your access point is not working properly, look at the LEDs on the bottom of the unit. You can use them to quickly assess the status of the unit. Figure 4-1 shows the location of the access point LEDs.

Figure 4-1 Access Point LEDs - Shown on the Bottom of Model AIR-CAP1552SA/SD-x-K9



1	RF-2 LED—Status of the 5 GHz MIMO backhaul radio	**3**	Uplink LED—Ethernet, cable, or fiber status
2	RF-1 LED—Status of the 2.4 GHz MIMO access radio	**4**	Status LED—access point and software status

Note It is expected that there will be small variations in LED color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer specifications and is not a defect.

The access point LED signals are listed in Table 4-1.

Table 4-1 Access Point LED Signals

LED	Color[1, 2]	Meaning
Status	Black	No power applied or LED off.
	Steady green	Access point is operational.
	Blinking green	Download or upgrade of Cisco IOS image file in progress.
	Steady amber	Mesh neighbor access point discovery in progress.
	Blinking amber	Mesh authentication in progress.
	Blinking red / green /amber	CAPWAP discovery in progress.
	Steady red	Firmware failure. Contact your support organization for assistance.
Uplink	Black	All network ports down or LED off.
	Steady green	Uplink port is operational (cable, fiber optic, or Ethernet).
RF-1	Black	Radio turned off or LED off.
	Steady green	Radio is operational; network is good.
	Steady red	Firmware failure. Contact your support organization for assistance.
RF-2	Black	Radio is turned off or LED off.
	Steady green	Radio is operational; network is good.
	Steady red	Firmware failure. Contact your support organization for assistance.

1. If all LEDs off, the access point has no power.
2. When the access point power supply is initially turned on, all LEDs are amber.

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 using a web browser.

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 Log out of the controller, and close your web browser.

Changing the Bridge Group Name

The bridge group name (BGN) controls the association of the access points to a RAP. BGNs can be used to logically group the radios to avoid different networks on the same channel from communicating with each other. This setting is also useful if you have more than one RAP in your network in the same area.

If you have two RAPs in your network in the same area (for more capacity), we recommend that you configure the two RAPs with different BGNs and on different channels.

The BGN is a string of ten characters maximum. A factory-set bridge group name (NULL VALUE) is assigned during manufacturing. It is not visible to you, but allows new access point radios to join a network of new access points. The BGN can be reconfigured from the Controller CLI and GUI. After configuring the BGN, the access point reboots.

After the access points are deployed and associated to the controller, the BGN should be changed from the default value to prevent the MAPs from attempting to associate to other mesh networks.

The BGN should be configured very carefully on a live network. You should always start with the most distant access point (last node) from the RAP and move towards the RAP. If you start configuring the BGN in a different location, then the access points beyond this point (farther away) are dropped, as they have a different BGN. MAPS with unconfigured BGNs will periodically join to RAPs with configured BGNs. This prevents the stranding of MAPs.

To configure the BGN for the access points using the controller GUI, follow these steps:

Step 1 Log into your controller using a web browser.

Step 2 Click **Wireless**. When access points associates to the controller, the access point name appears in the AP Name list.

Step 3 Click on an access point name.

Step 4 Find the Mesh Information section, and enter the new BGN in the Bridge Group Name field.

Step 5 Click **Apply**.

Step 6 Repeat Steps 2 through 5 for each access point.

Step 7 Log out from your controller, and close your web browser.

Connecting to the Access Point Locally

If you need to monitor the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its console port using a DB-9 to RJ-45 serial cable.

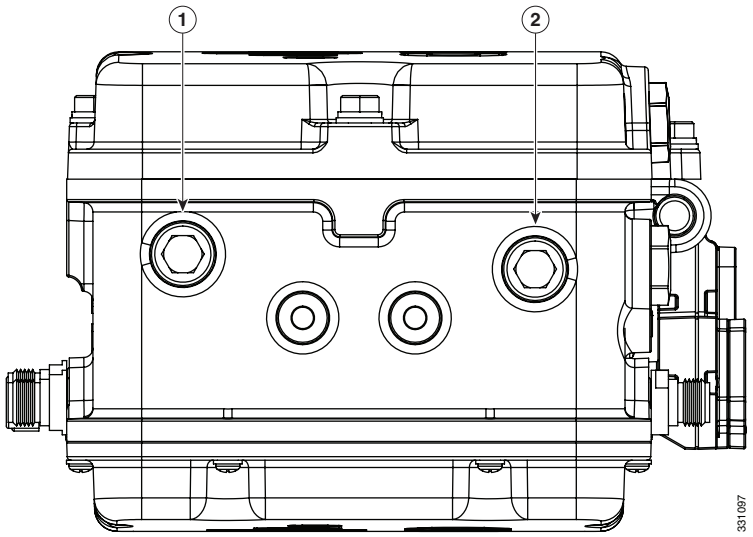
Note The console port should only be used for debugging in a lab environment.

Follow these steps to open the CLI by connecting to the access point console port:

Step 1 Open the hinged cover of the access point (if necessary) (see "Working with the Access Point Hinged Cover" section on page 3-58 for instructions).

Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 console port on the access point and to the COM port on a computer (see Figure 4-2 for the console port locations).

Figure 4-2 Console Port Location on Access Point Models (AIR-CAP1552SA/SD-x-K9 Shown)



1	Console port **Note** Not used for 1552WU. The 1552WU console is only available by opening the device and connecting to the internal console port.	2	Not used

Note The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. To order a serial cable, browse to:

http://www.cisco.com/pcgi-bin/marketplace/welcome.pl

Step 2 Set up a terminal emulator program on your PC to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Step 3 When finished, remove your serial cable, and close the hinged cover (see the "Working with the Access Point Hinged Cover" section on page 3-58 for instructions).

Access Point Power Injector

The power injector (AIR-PWRINJ1500-2=) has three LEDs on the front end of the case (see Figure 4-3). For detailed information on the power injector, see the *Cisco Aironet 1550 Series Outdoor Mesh Access Point Power Injector Installation Instructions*.

Caution Caution: Power injector (AIR-PWRINJ1500-2=) is not certified for installation within hazardous locations environments.

Figure 4-3 Power Injector Connectors and LEDs

1	Mounting tabs	**4**	AC POWER LED
2	AP POWER LED	**5**	TO AP—Ethernet connector (RJ-45) to access point (10/100/1000BASE-T)
3	FAULT LED	**6**	TO SWITCH—Ethernet connector (RJ-45) to switch (10/100/1000BASE-T)

Monitoring the Power Injector LEDs

You can use the power injector LEDs to check the power injector status. The LEDs provide the following status information:

- AP POWER—Turns solid green after successful discovery; indicates that power injector is supplying power to the access point.
- FAULT—Turns solid red when a fault occurs during discovery mode or power-up. Check Ethernet cables and connections before contacting your support organization for assistance.
- AC POWER—Turns solid green when power injector is receiving AC power and is ready to provide power to the access point.