Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the access point.

Guidelines for Using the Access Points

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.

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, or PoE-In). 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 side of the unit.

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.

Accessing the Console Port and the Reset Button

The console port and reset button are under a covering M25 plug located on the side of the access point, as shown in the following figure.

Figure 1: IW-6300H Access Point Console Port and Reset Button
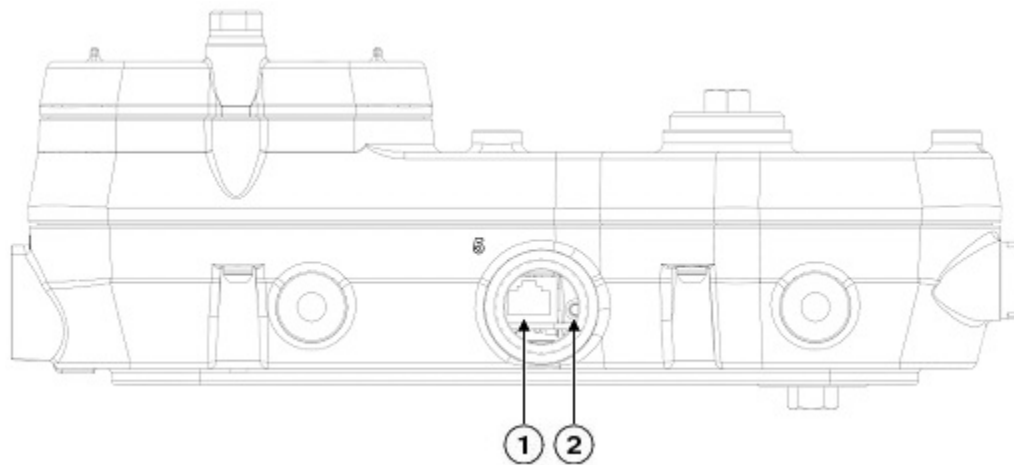
1	Console port	2	Reset button

Inspect the seal of the plug and properly tighten it at the time of installation, and also every time the plug is removed and replaced. Tighten the plug to 5-6 lb-ft. If you do not tighten the plug properly, it will not meet IP67 criteria, and may lead to water leaking into the unit.

Resetting the Access Point

Using the Reset button you can:

- Reset the AP to the default factory-shipped configuration.

- Clear the AP internal storage, including all configuration files.

To use the Reset button, press, and keep pressed, the Reset button on the access point during the AP boot cycle. Wait until the AP status LED changes to Amber. During this, the AP console shows a seconds counter, counting the number of seconds the Reset button is pressed. Then:

- To reset the AP to it's default factory-shipped configuration, keep the Reset button pressed for less than 20 seconds. The AP configuration files are cleared.

This resets all configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID.

- To clear the AP internal storage, including all configuration files and the regulatory domain configuration, keep the Reset button pressed for more than 20 seconds, but less than 60 seconds.

The AP status LED changes from Amber to Red, and all the files in the AP storage directory are cleared.

If you keep the Reset button pressed for more than 60 seconds, the Reset button is assumed faulty and no changes are made.

Monitoring the Access Point LEDs

If your access point is not working properly, look at the system LED and port LEDs. You can use them to quickly assess the status of the unit.

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 the following table.

Table 1: Access Point System LED Signals

LED Message Type	Color	Meaning
Boot loader status sequence	Blinking Green	Boot loader status sequence: • DRAM memory test in progress • DRAM memory test OK • Board initialization in progress • Initializing FLASH file system • FLASH memory test OK • Initializing Ethernet • Ethernet OK • Starting Cisco IOS • Initialization successful
Association status	Chirping (short blips) Green	This status indicates a normal operating condition. The unit is joined to a controller, but no wireless client is associated with it.
	Solid Green	Normal operating condition with at least one wireless client associated with the unit

LED Message Type	Color	Meaning
Operating Status	Blinking Amber	A software upgrade is in progress
	Cycling through Green, Red, and Amber	Discovery/join process is in progress
	Rapidly cycling through Red, Green, Amber, and Off	This status indicates that the Access Point location command has been invoked.
	Blinking Red	This status indicates that an Ethernet link is not operational
Boot loader warnings	Blinking Amber	Configuration recovery is in progress (the Reset button has been pushed for 2-3 seconds)
	Red	There is an Ethernet failure or an image recovery (the Reset button has been pushed for 20-30 seconds)
	Blinking Green	An image recovery is in progress (the Reset button has been released)
Boot loader errors	Red	There has been a DRAM memory test failure
	Blinking Red and Amber	There has been a FLASH file system failure
	Blinking Red and Off	This sequence may indicate any of the following: • Environment variable failure • Bad MAC address • Ethernet failure during image recovery • Boot environment failure • No Cisco image file • Boot failure
AP OS errors	Red	There has been a software failure; a disconnect then reconnect of the unit power may resolve the issue
	Cycling through Red, Green, Amber, and Off	This is a general warning of insufficient inline power

The access point port LED signals are listed in the following table.

Table 2: Access Point Port LED Signals

LED Message Type	Color	Meaning
Port link status	Green	Link on
	Blinking Green	Link activity
	Off	No link

Verifying Controller Association

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

Procedure

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:

Procedure

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.