Troubleshooting

Using the Mode Button

Using the **Mode** button (see C9136I Top View with Connectors and Ports) you can perform the following tasks:

- Reset the AP to the default factory-shipped configuration
- Clear AP's internal storage, including all the configuration files

To use the **Mode** button, press, and continue to press the **Mode** button on the access point during the AP boot cycle. Wait until the AP console shows a seconds counter. When the counter indicates the number of seconds for which the **Mode** button is pressed, the AP status LED changes to blinking red. Then reset the AP to the default factory-shipped configuration, keep the mode button pressed for less than 20 seconds. The AP configuration files are cleared.

Clear the AP internal storage, including all the configuration files, keep the **Mode** button pressed for more than 20 seconds, but less than 60 seconds. This resets all the configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID.

Note If the **Mode** button is pressed for more than 30 seconds, but less than 60 seconds, the FIPS mode flag is also cleared during the full factory reset of the AP. If the FIPS flag is set, the console access is disabled.

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

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

Troubleshooting the Access Point to Cisco Controller Join Process

Note As specified in the Cisco Wireless Solutions Software Compatibility Matrix, ensure that your controller is running controller software Cisco IOS-XE 17.7.1 or a later release to support C9136I AP.

Access points can fail to join a controller for many reasons—a RADIUS authorization is pending, self-signed certificates are not enabled on the controller, the access point and the controller regulatory domains do not match, and so on.

Controller software enables you to configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any **debug** commands on the controller because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the controller until it receives a CAPWAP join request from the access point. Therefore, it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining problems without enabling CAPWAP **debug** commands on the controller, the controller collects information for all the access points that send a discovery message to it and maintains information on any access points that have successfully joined it.

The controller collects all the join-related information for each access point that sends a CAPWAP discovery request to the controller. Collection begins with the first discovery message received from the access point and ends with the last configuration payload sent from the controller to the access point.

When the controller is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

An access point sends all the syslog messages to the IP address 255.255.255.255 by default.

You can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all the syslog messages to this IP address.

When the access point joins a controller for the first time, the controller sends the global syslog server IP address (the default is 255.255.255.255) to the access point.

- The access point is disconnected from the controller and joins another controller. In this case, the new controller sends its global syslog server IP address to the access point.
- Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all the syslog messages to the new IP address, provided the access point can reach the syslog server IP address.

Note You can configure the syslog server for access points and view the access point join information only from the controller CLI.

Important Information for Controller-Based Deployments

Keep these guidelines in mind when you use the C9136I Series AP:

- The AP can only communicate with Cisco wireless controllers.
- The AP does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the AP joins it.
- CAPWAP does not support Layer 2. The AP must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The AP console port is enabled for monitoring and debug purposes.
- All the configuration commands are disabled when the AP is connected to a controller.

Configuring DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling them to find and join a controller.

The following is a DHCP Option 43 configuration example on a Windows 2003 Enterprise DHCP server for use with Cisco Catalyst lightweight access points. For other DHCP server implementations, see the product documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.

Note DHCP Option 43 is limited to one access point type per DHCP pool. You must configure a separate DHCP pool for each access point type.

The C9136I AP uses the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point DHCP Vendor Class Identifier (VCI) string (DHCP Option 43). The VCI string for the C9136I Series access point is:

Cisco AP C9136I

The format of the TLV block is as follows:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses x 4
- Value: IP addresses of the wireless controller management interfaces listed sequentially in Hex code.

To configure DHCP Option 43 in the embedded Cisco IOS DHCP server, follow these steps:

Procedure

Step 1 Enter the configuration mode

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>
```

Here:

<*pool name*>: is the name of the DHCP pool, such as AP9136I

<*IP Network*>: is the network IP address where the controller resides, such as 10.0.15.1

<*Netmask*>: is the subnet mask, such as 255.255.255.0

<*Default router*>: is the IP address of the default router, such as 10.0.0.1

<*DNS Server*>: is the IP address of the DNS server, such as 10.0.10.2

Step 3 Add the Option 43 line using the following syntax:

```
option 43 hex <hex string>
```

The hex string is assembled by concatenating the following TLV values:

Type + Length + Value

For example, if there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2, the type is f1(hex), the length is 2 * 4 = 8 = 08 (hex), and the IP addresses translate to 0a7e7e02 and 0a7f7f02. Assembling the string then yields f1080a7e7e020a7f7f02. The resulting Cisco IOS command added to the DHCP scope is **option 43 hex f1080a7e7e020a7f7f02**.