Converting Autonomous Access Points to Lightweight Mode

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Converting Autonomous Access Points to Lightweight Mode

- Access points that are converted to lightweight mode do not support Wireless Domain Services (WDS). Converted access points communicate only with Cisco wireless LAN switchs and cannot communicate with WDS devices. However, the switch provides functionality that is equivalent to WDS when the access point associates to it.
- All Cisco lightweight access points support 16 Basic Service Set Identifiers (BSSIDs) per radio and a total of 16 wireless LANs per access point. When a converted access point associates to a switch, only wireless LANs with IDs 1 through 16 are pushed to the access point unless the access point is a member of an access point group.
- Access points that are converted to lightweight mode must get an IP address and discover the switch using DHCP, DNS, or IP subnet broadcast.

Information About Autonomous Access Points Converted to Lightweight Mode

You can convert autonomous Cisco Aironet access points to lightweight mode. When you upgrade the access points to lightweight mode, the access point communicates with the switch and receives a configuration and software image from the switch.

See the *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* document for instructions to upgrade an autonomous access point to lightweight mode:

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html

Reverting from Lightweight Mode to Autonomous Mode

After you use the upgrade tool to convert an autonomous access point to lightweight mode, you can convert the access point from a lightweight unit back to an autonomous unit by loading a Cisco IOS release that supports autonomous mode (Cisco IOS Release 12.3(7)JA or earlier releases). If the access point is associated to a switch, you can use the switch to load the Cisco IOS release. If the access point is not associated to a switch, you can load the Cisco IOS release using TFTP. In either method, the access point must be able to access a TFTP server that contains the Cisco IOS release to be loaded.

Using DHCP Option 43 and DHCP Option 60

Cisco Aironet access points use the type-length-value (TLV) format for DHCP option 43. You must program the DHCP servers to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP option 60).

The following table lists the VCI strings for Cisco access points that can operate in lightweight mode.

Access Point	VCI String
Cisco Aironet 1140 Series	Cisco AP c1140
Cisco Aironet 3500 Series	Cisco AP c3500
Cisco Aironet 3600 Series	Cisco AP c3600

The format of the TLV block is as follows:

- Type: 0xf1 (decimal 241)
- Length: Number of switch IP addresses * 4
- Value: List of the IP addresses of switch management interfaces

See the product documentation for your DHCP server for instructions on configuring DHCP option 43. The *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* document contains example steps for configuring option 43 on a DHCP server.

If the access point is ordered with the Service Provider Option - AIR-OPT60-DHCP selected, the VCI string for that access point will be different than those strings listed in the previous table. The VCI string has the following suffix: ServiceProvider. For example, a 1260 with this option returns this VCI string: Cisco AP c1260-ServiceProvider.

Note The switch IP address that you obtain from the DHCP server should be a unicast IP address. Do not configure the switch IP address as a multicast address when configuring DHCP option 43.

How Converted Access Points Send Crash Information to the Switch

When a converted access point unexpectedly reboots, the access point stores a crash file on its local flash memory at the time of the crash. After the unit reboots, it sends the reason for the reboot to the switch. If the unit rebooted because of a crash, the switch pulls up the crash file using existing CAPWAP messages and stores it in the switch flash memory. The crash information copy is removed from the access point flash memory when the switch pulls it from the access point.

How Converted Access Points Send Radio Core Dump Information to the Switch

When a radio module in a converted access point generates a core dump, the access point stores the core dump file of the radio on its local flash memory at the time of the radio crash. It sends a notification message to the switch indicating which radio generated a core dump file. The switch sends a trap that alerts you so that you can retrieve the radio core file from the access point.

The retrieved core file is stored in the switch flash and can be uploaded through TFTP or FTP to an external server for analysis. The core file is removed from the access point flash memory when the switch pulls it from the access point.

Uploading Memory Core Dumps from Converted Access Points

By default, access points converted to lightweight mode do not send memory core dumps to the switch. This section provides instructions to upload access point core dumps using the switch GUI or CLI.

Displaying MAC Addresses for Converted Access Points

There are some differences in the way that controllers display the MAC addresses of converted access points on information pages in the controller GUI:

- On the AP Summary page, the controller lists the Ethernet MAC addresses of converted access points.
- On the AP Detail page, the controller lists the BSS MAC addresses and Ethernet MAC addresses of converted access points.
- On the Radio Summary page, the switch lists converted access points by the radio MAC address.

Configuring a Static IP Address for a Lightweight Access Point

If you want to specify an IP address for an access point rather than having one assigned automatically by a DHCP server, you can use the controller GUI or CLI to configure a static IP address for the access point. Static IP addresses are generally used only for deployments with a limited number of users.

An access point cannot discover the switch using domain name system (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs. You can configure these parameters using either the switch CLI or the GUI.

Note If you configure an access point to use a static IP address that is not on the same subnet on which the access point's previous DHCP address was, the access point falls back to a DHCP address after the access point reboots. If the access point falls back to a DHCP address, enter the **show ap config general** *Cisco_AP* CLI command to show that the access point is using a fallback IP address. However, the GUI shows both the static IP address and the DHCP address, but it does not identify the DHCP address as a fallback address.

How to Revert to a Previous Release

Reverting to a Previous Release (CLI)

SUMMARY STEPS

1. **enable**
2. **ap name** *Cisco_AP* **tftp-downgrade** *tftp_server_ip_address tftp_server_image_filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco_AP* **tftp-downgrade** *tftp_server_ip_address tftp_server_image_filename* **Example:** `Switch# ap name AP02 tftp-downgrade 10.0.0.1 tsrvname`	Reverts the access point converted to lightweight mode to autonomous mode. **Note** After entering this command, you must wait until the access point reboots and then reconfigure the access point using the CLI or GUI.

Reverting to a Previous Release (Using the Mode Button and a TFTP Server)

Step 1 Configure the PC on which your TFTP server software runs with a static IP address in the range of 10.0.0.2 to 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as *c1140-k9w7-tar.123-7.JA.tar* for a 1140 series access point) in the TFTP server folder and that the TFTP server is activated.

Step 3 Rename the access point image file in the TFTP server folder to **c1140-k9w7-tar.default** for a 1140 series access point.

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power from the access point.

Step 6 Press and hold the **MODE** button while you reconnect power to the access point.

Note The **MODE** button on the access point must be enabled.

Step 7 Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.

Step 8 Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, reconfigure the access point using the GUI or the CLI.

Authorizing Access Points (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap auth-list ap-policy authorize-ap**
4. **ap auth-list ap-policy mic**
5. **username** *user_name* **mac aaa attribute list** *list_name*
6. **aaa new-model**
7. **aaa authorization credential-download** *auth_list* **local**
8. **aaa attribute list** *list*
9. **aaa session-id common**
10. **aaa local authentication default authorization default**
11. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ap auth-list ap-policy authorize-ap** **Example:** `Switch(config)# ap auth-list ap-policy authorize-ap`	Configures an access point authorization policy.
Step 4	**ap auth-list ap-policy mic** **Example:** `Switch(config)# ap auth-list ap-policy mic`	Configures an access point to accept manufactured-installed certificates (MICs), self-signed certificates (SSCs), or local significant certificates (LSCs).
Step 5	**username** *user_name* **mac aaa attribute list** *list_name* **Example:** `Switch(config)# username aaa.bbb.ccc mac aaa attribute list attrlist`	Configures the MAC address of an access point locally.
Step 6	**aaa new-model** **Example:** `Switch(config)# aaa new-model`	Enables new access control commands and functions.

	Command or Action	Purpose
Step 7	**aaa authorization credential-download** *auth_list* **local** **Example:** `Switch(config)# aaa authorization credential-download auth_download local`	Downloads EAP credentials from the local server.
Step 8	**aaa attribute list** *list* **Example:** `Switch(config)# aaa attribute list alist`	Configures AAA attribute list definitions.
Step 9	**aaa session-id common** **Example:** `Switch(config)# aaa session-id common`	Configures the AAA common session ID.
Step 10	**aaa local authentication default authorization default** **Example:** `Switch(config)# aaa local authentication default authorization default`	Configures the local authentication method list.
Step 11	**show ap name** *Cisco_AP* **config general** **Example:** `Switch(config)# show ap name AP01 config general`	Displays the configuration information that corresponds to a specific access point.

Retrieving Radio Core Dumps (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **ap name** *Cisco_AP* **crash-file get-radio-core-dump slot 0**
3. **show ap crash-file**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco_AP* **crash-file get-radio-core-dump slot 0** **Example:** `Switch# ap name AP02 crash-file get-radio-core-dump slot 0`	Transfers the radio core dump file from the access point to the switch. For the slot parameter, enter the slot ID of the radio that crashed.
Step 3	**show ap crash-file** **Example:** `Switch# show ap crash-file`	Displays access point crash file information. Using this command, you can verify whether the file is downloaded to the switch.

How to Upload Access Point Core Dumps

Uploading Access Point Core Dumps (CLI)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ap core-dump** *tftp_server_ip_address tftp_server_image_filename* **compress**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ap core-dump** *tftp_server_ip_address tftp_server_image_filename* **compress** **Example:** `Switch(config)# ap core-dump 10.0.0.1 cdpname compress`	Uploads a core dump of the access point. The following parameters must be specified with the command: • *tftp_server_ip_address*—IP address of the TFTP server to which the access point sends core dump files. • *filename*—Name that the access points uses to label the core file. • **compress**—Configures the access point to send compressed core files. **Note** When you choose compress, the file is saved with a .gz extension (for example, dump.log.gz). This file can be opened with WinZip. • **uncompress**—Configures the access point to send uncompressed core files.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.

Uploading Access Point Core Dumps (GUI)

Step 1 Choose **Configuration > AP Summary.**
The **All APs** page appears with a list of access points.

Step 2 Click the access point for which you want to upload the core dumps.
The **AP > Edit** page appears.

Step 3 Click the **Advanced** tab.

Step 4 In the **AP Core Dump** area, select the **AP Core Dump** check box to upload a core dump of the access point.

Step 5 In the **TFTP Server IP** text box, enter the IP address of the TFTP server.

Step 6 In the **File Name** text box, enter a name of the access point core dump file (such as dump.log).

Step 7 Select the **File Compression** check box to compress the access point core dump file.
When you enable this option, the file is saved with a .gz extension (such as dump.log.gz). This file can be opened with WinZip.

Step 8 Click **Apply** to commit your changes.

Disabling the Reset Button on Converted Access Points (CLI)

You can enable or disable the Reset button on access points that are converted to lightweight mode. The Reset button is labeled MODE on the outside of the access point.

Note The procedure to perform this task using the controller GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no ap reset-button**
4. **end**
5. **ap name** *Cisco_AP* **reset-button**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**no ap reset-button** **Example:** `Switch(config)# no ap reset-button`	Disables the Reset buttons on all converted access points that are associated to the switch. **Note** To enable the Reset buttons on all converted access points that are associated to the switch, enter the **ap reset-button** command.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.
Step 5	**ap name** *Cisco_AP* **reset-button** **Example:** `Switch# ap name AP02 reset-button`	Enables the Reset button on the converted access point that you specify.

Monitoring the AP Crash Log Information

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **show ap crash-file**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show ap crash-file** **Example:** `Switch# show ap crash-file`	Verifies whether the crash file is downloaded to the switch.

How to Configure a Static IP Address on an Access Point

Configuring a Static IP Address on an Access Point (CLI)

SUMMARY STEPS

1. **enable**
2. **ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway*
3. **enable**
4. **configure terminal**
5. **ap static-ip name-server** *nameserver_ip_address*
6. **ap static-ip domain** *static_ip_domain*
7. **end**
8. **show ap name** *Cisco_AP* **config dot11 24ghz general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway* **Example:** `Switch# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2`	Configures a static IP address on the access point. This command contains the following keywords and arguments: • **ip-address—** Specifies the Cisco access point static IP address. • *ip-address***—** Cisco access point static IP address. • **netmask—**Specifies the Cisco access point static IP netmask. • *netmask***—** Cisco access point static IP netmask. • **gateway—**Specifies the Cisco access point gateway. • *gateway***—** IP address of the Cisco access point gateway. The access point reboots and rejoins the switch, and the static IP address that you specify is pushed to the access point. After the static IP address has been sent to the access point, you can configure the DNS server IP address and domain name. You must perform Steps 3 and 4 after the access points reboot.
Step 3	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 4	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 5	**ap static-ip name-server** *nameserver_ip_address* **Example:** `Switch(config)# ap static-ip name-server 10.10.10.205`	Configures a DNS server so that a specific access point or all access points can discover the switch using DNS resolution. **Note** To undo the DNS server configuration, enter the **no ap static-ip name-server** *nameserver_ip_address* command.
Step 6	**ap static-ip domain** *static_ip_domain* **Example:** `Switch(config)# ap static-ip domain domain1`	Configures the domain to which a specific access point or all access points belong. **Note** To undo the domain name configuration, enter the **no ap static-ip domain** *static_ip_domain* command.

	Command or Action	Purpose
Step 7	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-z** to exit global configuration mode.
Step 8	**show ap name** *Cisco_AP* **config dot11 24ghz general** **Example:** `Switch# show ap name AP03 dot11 24ghz config general`	Displays the IP address configuration for the access point.

Configuring a Static IP Address on an Access Point (GUI)

Step 1 Choose **Configuration** > **Wireless** > **AP Summary**
The **All APs** page appears with a list of all access points that are associated with the switch.

Step 2 Click the name of the access point for which you want to configure a static IP address.
The **AP > Edit** page appears.

Step 3 In the **IP Config** area, select the **Static IP** check box if you want to assign a static IP address to the access point. The default value is unselected.
Options that enable you to configure a static IP address for the access point appear in the **IP Config** area.

Step 4 In the **Netmask** field, enter the network mask.

Step 5 In the **Gateway** field, enter the default gateway address.

Step 6 Click **Apply** to commit your changes.
The access point reboots and rejoins the switch, and the static IP address that you specified in Step 4 is sent to the access point.

Step 7 After the static IP address has been sent to the access point, you can configure the DNS server IP address and domain name by performing the following steps:

a) In the **DNS IP Address** field, enter the IP Address of the DNS server.
b) In the **Domain Name** field, enter the name of the domain to which the access points belongs.
c) Click **Apply** to commit the changes.

Recovering the Access Point Using the TFTP Recovery Procedure

Step 1 Download the required recovery image from Cisco.com (ap3g2-k9w8-tar.152-2.JA.tar) and install it in the root directory of your TFTP server.

Step 2 Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the switch to download the oversized access point image and complete the upgrade procedure.

Step 3 After the access point has been recovered, you can remove the TFTP server.

Configuration Examples for Converting Autonomous Access Points to Lightweight Mode

Displaying LSC Information: Example

This example shows how to display the LSC summary:

```
Switch# show wireless certificate lsc summary
<?xml version="1.0"?>
 <iossr-response
  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'>
  <cmd-response>
   <res0>
    <properties>
     <lscEnable type="boolean">false</lscEnable>
     <key_size type="unsignedInt">2048</key_size>
     <lscApProvision type="unsignedByte">0</lscApProvision>
     <rebootNum type="unsignedByte">3</rebootNum>
     <trustpoint
      type="string">default_lsc_trustpoint</trustpoint>
     <country type="string"></country>
     <state type="string"></state>
     <city type="string"></city>
     <orgn type="string"></orgn>
     <dept type="string"></dept>
     <email type="string"></email>
    </properties>
   </res0>
  </cmd-response>
 </iossr-response>
LSC Enabled                    : No
LSC AP-Provisioning            : No
TrustPoint                     : default_lsc_trustpoint
LSC Params:
    Country                    :
    State                      :
    City                       :
    Orgn                       :
    Dept                       :
```

```
    Email                           :
    KeySize                         : 2048
```

This example shows how to display details about the access points that are provisioned using LSC:

```
Switch# show wireless certificate lsc ap-provision
<?xml version="1.0"?>
 <iossr-response
  xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'>
  <cmd-response>
   <res0>
    <properties>
     <lscApProvision type="unsignedByte">0</lscApProvision>
    </properties>
   </res0>
   <res1>  </res1>
  </cmd-response>
 </iossr-response>
LSC AP-Provisioning                  : No
```

Displaying the IP Address Configuration for Access Points: Example

This example shows how to display the IP address configuration for the access point:

```
Switch# show ap name AP03 dot11 24ghz config general
Cisco AP Identifier.............. 4
Cisco AP Name.................... AP6
IP Address Configuration..... Static IP assigned
IP Address.......................... 10.10.10.118
IP NetMask.......................... 255.255.255.0
Gateway IP Addr..... 10.10.10.1
Domain.................... Domain1
Name Server.......... 10.10.10.205
...
```

Displaying Access Point Crash File Information: Example

This example shows how to display access point crash file information. Using this command, you can verify whether the file is downloaded to the switch:

```
Switch# show ap crash-file
Local Core Files:
lrad_AP1130.rdump0 (156)

The number in parentheses indicates the size of the file. The size should
be greater than zero if a core dump file is available.
```