自律アクセスポイントの Lightweight モードへの変換

自律アクセスポイントの Lightweight モードへの変換に関するガイドライン

- Lightweight モードに変換したアクセスポイントは、無線ドメインサービス（WDS）をサポートしません。変換したアクセスポイントは、Cisco ワイヤレス LAN device とのみ通信し、WDS デバイスとは通信できません。ただし、アクセスポイントがコントローラにアソシエートする際、device が WDS に相当する機能を提供します。
- すべての Cisco Lightweight アクセスポイントでは、無線ごとに 16 の Basic Service Set Identifier（BSSID）およびアクセスポイントごとに合計 16 のワイヤレス LAN をサポートします。変換されたアクセスポイントがdeviceにアソシエートすると、アクセスポイントがアクセスポイントグループのメンバーでない限り、ID 1 ～ 16 のワイヤレス LAN のみがアクセスポイントにプッシュされます。

- Lightweight モードに変換したアクセスポイントは、DHCP、DNS、または IP サブネットブロードキャストを使用して IP アドレスを取得し、device を検出する必要があります。

Lightweight モードに変換される Autonomous アクセスポイントについて

Autonomous Cisco Aironet アクセスポイントを Lightweight モードに変換できます。Lightweight モードにアクセスポイントをアップグレードすると、アクセスポイントはdeviceと通信し、deviceから設定とソフトウェアイメージを受信します。

Lightweight モードから Autonomous モードへの復帰

Autonomous アクセスポイントを Lightweight モードに変換してから、Autonomous モードをサポートする Cisco IOS リリース（Cisco IOS リリース 12.3(7)JA 以前のリリース）をロードして、そのアクセスポイントを Lightweight 装置から Autonomous 装置に戻すことができます。アクセスポイントがdeviceにアソシエートされている場合、deviceを使用して Cisco IOS リリースをロードできます。アクセスポイントがdeviceにアソシエートされていない場合、TFTP を使用して Cisco IOS リリースをロードできます。いずれの方法でも、ロードする Cisco IOS Release を含む TFTP サーバにアクセスポイントがアクセスできる必要があります。

DHCP オプション 43 および DHCP オプション 60 の使用

Cisco Aironet アクセスポイントは、DHCP オプション 43 に Type-Length-Value（TLV）形式を使用します。DHCP サーバは、アクセスポイントの DHCP ベンダー クラス ID（VCI）文字列に基づいてオプションを返すよう、プログラムする必要があります（DHCP オプション 60）。

DHCP オプション 43 の設定方法については、ご使用の DHCP サーバの製品ドキュメンテーションを参照してください。『Converting Autonomous Access Points to Lightweight Mode』には、には、DHCP サーバのオプション 43 の設定手順の例が記載されています。

アクセスポイントが、サービス プロバイダー オプション AIR-OPT60-DHCP を選択して注文された場合、そのアクセスポイントの VCI 文字列は、前の表にある VCI 文字列と異なります。VCI 文字列のサフィックスは ServiceProvider です。たとえば、このオプションを指定した 1260 は、VCI 文字列 Cisco AP c1260-ServiceProvider を返します。

（注） DHCP サーバから取得するdeviceの IP アドレスがユニキャスト IP アドレスであることを確認してください。DHCP オプション 43 を設定する場合は、マルチキャストアドレスとしてdeviceの IP アドレスを設定しないでください。

DHCP オプション 60 の制約事項

- Cisco Wave2 AP は、長さが最大 256 文字の文字列のみをサポートします。

（注） 文字列の長さが制限を超えると、DHCP 検出プロセス中にデフォルト値が送信されます。

変換したアクセスポイントがクラッシュ情報をDeviceに送信する方法

変換したアクセスポイントが予期せずリブートした場合、アクセスポイントではクラッシュ発生時にローカルフラッシュメモリ上にクラッシュファイルが保存されます。装置のリブート後、アクセスポイントはリブートの理由をdeviceに送信します。クラッシュにより装置がリブートした場合、deviceは既存の CAPWAP メッセージを使用してクラッシュファイルを取得し、deviceのフラッシュメモリにそれを保存します。クラッシュ情報コピーは、deviceがアクセスポイントからこれを取得した時点でアクセスポイントのフラッシュメモリから削除されます。

変換したアクセスポイントからのメモリコアダンプのアップロード

デフォルトでは、Lightweight モードに変換したアクセスポイントは、deviceにメモリコアダンプを送信しません。この項では、device GUI または CLI を使用してアクセスポイントコアダンプをアップロードする手順について説明します。

変換されたアクセスポイントの MAC アドレスの表示

コントローラが変換されたアクセス ポイントの MAC アドレスをコントローラ GUI の情報ページに表示する方法には、いくつか異なる点があります。

- [AP Summary] ウィンドウには、変換されたアクセス ポイントのイーサネット MAC アドレスのリストが、コントローラにより表示されます。
- [AP Detail] ウィンドウには、変換されたアクセス ポイントの BSS MAC アドレスとイーサネット MAC アドレスのリストが、コントローラにより表示されます。
- [Radio Summary] ページには、変換されたアクセスポイントのリストがdeviceにより無線 MAC アドレス順に表示されます。

Lightweight アクセスポイントの静的 IP アドレスの設定

DHCP サーバに IP アドレスを自動的に割り当てさせるのではなく、アクセス ポイントに IP アドレスを指定する場合は、コントローラ GUI または CLI を使用してアクセス ポイントに固定 IP アドレスを設定できます。静的 IP アドレスは、通常、AP 数の限られた導入でのみ使用されます。

固定 IP アドレスがアクセスポイントに設定されている場合は、DNS サーバとアクセスポイントが属するドメインを指定しない限り、アクセスポイントはドメインネームシステム（DNS）解決を使用してdeviceを検出できません。device CLI または GUI のいずれかを使用して、これらのパラメータを設定できます。

（注） アクセス ポイントを設定して、アクセス ポイントの以前の DHCP アドレスが存在したサブネット上にない固定 IP アドレスを使用すると、そのアクセス ポイントはリブート後に DHCP アドレスにフォール バックします。アクセス ポイントが DHCP アドレスにフォール バックした場合は、**show ap config general** *Cisco_AP* CLI コマンドを入力すると、アクセス ポイントがフォールバック IP アドレスを使用していることが表示されます。ただし、GUI は固定 IP アドレスと DHCP アドレスの両方を表示しますが、DHCP アドレスをフォールバック アドレスであるとは識別しません。

Lightweight アクセスポイントの Autonomous アクセスポイントへの再変換方法

Lightweight アクセスポイントを Autonomous モードに戻す方法（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *Cisco_AP* **tftp-downgrade** *tftp_server_ip_address tftp_server_image_filename* 例： `Device# ap name AP02 tftp-downgrade 10.0.0.1 tsrvname`	Lightweight アクセスポイントを Autonomous モードに戻します。 （注） このコマンドを入力したら、アクセスポイントが再起動するまで待機し、CLI または GUI を使用してアクセスポイントを再設定します。

モードボタンと TFTP サーバを使用して Lightweight アクセスポイントを Autonomous モードに戻す方法

手順

ステップ 1 TFTP サーバ ソフトウェアを実行している PC に、10.0.0.2 ～ 10.0.0.30 の範囲に含まれる固定 IP アドレスを設定します。

ステップ 2 コンピュータの TFTP サーバ フォルダにアクセスポイントのイメージファイル（たとえば、1140 シリーズ アクセスポイントの場合は *c1140-k9w7-tar.123-7.JA.tar* ）が存在すること、およびその TFTP サーバがアクティブであることを確認します。

ステップ 3 TFTP サーバフォルダ内の 1140 シリーズ アクセスポイントのイメージファイルの名前を c1140-k9w7-tar.default に変更します。

ステップ 4 カテゴリ 5（CAT5）のイーサネット ケーブルを使用して、PC をアクセス ポイントに接続します。

ステップ 5 アクセス ポイントの電源を切ります。

ステップ 6 MODE ボタンを押しながら、アクセスポイントに電源を再接続します。

（注） アクセスポイントの MODE ボタンを有効にしておく必要があります。

ステップ 7 [MODE] ボタンを押し続けて、ステータス LED が赤色に変わったら（約 20 ～ 30 秒かかります）、[MODE] ボタンを放します。

ステップ 8 アクセス ポイントがリブートしてすべての LED が緑色に変わり、ステータス LED が緑色に点滅するまで待ちます。

ステップ 9 アクセス ポイントがリブートしたら、GUI または CLI を使用してアクセス ポイントを再設定します。

アクセスポイントの認可

以降の項では、アクセスポイントを許可するさまざまな方法について説明します。

ローカルデータベースを使用したアクセスポイントの許可（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ap auth-list ap-policy authorize-ap** 例： `Device(config)# ap auth-list ap-policy authorize-ap`	アクセスポイントの許可ポリシーを設定します。
ステップ 4	**username** *user_name* **mac** ［**aaa attribute list** *list_name*］ 例： `Device(config)# username aaa.bbb.ccc mac aaa attribute list attrlist`	（任意）アクセスポイントの MAC アドレスをローカルで設定します。
ステップ 5	**aaa new-model** 例： `Device(config)# aaa new-model`	新しいアクセス コントロール コマンドと機能をイネーブルにします
ステップ 6	**aaa authorization credential-download** {*auth_list* | **default**} **local** 例： `Device(config)# aaa authorization credential-download auth_download local`	ローカルサーバから EAP 資格情報をダウンロードします。
ステップ 7	**aaa attribute list** リスト 例： `Device(config)# aaa attribute list alist`	（任意）AAA 属性リストの定義を設定します。
ステップ 8	**aaa session-id common** 例： `Device(config)# aaa session-id common`	AAA の共通セッション ID を設定します。
ステップ 9	**aaa local authentication default authorization default** 例： `Device(config)# aaa local authentication default authorization default`	（任意）ローカル認証方式リストを設定します。
ステップ 10	**end**	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**show ap name** *Cisco_AP* **config general** 例： `Device# show ap name AP01 config general`	特定のアクセスポイントに対応する設定情報を表示します。

RADIUS サーバを使用したアクセスポイントの許可（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server** *server-name* 例： `Device(config)# radius server ise`	RADIUS サーバ コンフィギュレーション モードを開始します。
ステップ 4	**address** {**ipv4** | **ipv6**} *radius-server-ipv4-address-or-name* **auth-port** *udp-port-auth-server* **acct-port** *udp-port-acct-server* 例： `Device(config-radius-server)# address ipv4 224.0.0.1 auth-port 1645 acct-port 1646`	RADIUS サーバや他のサーバのパラメータを設定します。
ステップ 5	**key** *0 cisco* 例： `Device(config-radius-server)# key 0 cisco`	RADIUS 認証サーバのクリア テキストの暗号キーを設定します。
ステップ 6	**exit** 例： `Device(config-radius-server)# exit`	特権 EXEC モードに戻ります。
ステップ 7	**aaa group server radius** *server-group* 例：	RADIUS サーバ グループの定義を設定します。

	コマンドまたはアクション	目的
	`Device(config)# aaa group server radius ise-group`	（注） *server-group* はサーバグループ名です。有効な範囲は 1 ～ 32 文字の英数字です。
ステップ 8	**server name** *ise* 例： `Device(config-sg-radius)# server name ise`	RADIUS サーバ名を設定します。
ステップ 9	**ip radius source-interface** *vlan* 例： `Device(config-sg-radius)# ip radius source-interface vlan`	RADIUS パケットでの送信元アドレスのインターフェイスを指定します。
ステップ 10	**exit** 例： `Device(cconfig-sg-radius)# exit`	特権 EXEC モードに戻ります。
ステップ 11	**aaa authorization network default group** *default-server-group* **local** 例： `Device(config)# aaa authorization network default group ise-group local`	許可の方法をローカルに設定します。
ステップ 12	**aaa authorization credential-download default group** *default-server-group* **local** 例： `Device(config)# aaa authorization credential-download default group ise-group local`	ローカルサーバ、RADIUS サーバ、または LDAP サーバから EAP クレデンシャルをダウンロードするようにローカルデータベースを設定します。

変換したアクセスポイントでの Reset ボタンのディセーブル化（CLI）

Lightweight モードに変換したアクセスポイントの [Reset] ボタンを有効または無効にすることができます。[Reset] ボタンには、アクセスポイントの外面に「MODE」と書かれたラベルが付けられています。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ap reset-button** 例： `Device(config)# no ap reset-button`	deviceに関連付けられ、変換したすべてのアクセスポイントの [Reset] ボタンを無効にします。 （注） deviceに関連付けられ、変換したすべてのアクセスポイントの [Reset] ボタンを有効にするには、**ap reset-button** コマンドを入力します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**ap name** *cisco_ap* **reset-button** 例： `Device# ap name AP02 reset-button`	指定した変換済みアクセスポイントの [Reset] ボタンを有効にします。

AP クラッシュ ログ情報のモニタリング

（注） device GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**show ap crash-file** 例： `Device# show ap crash-file`	クラッシュファイルがdeviceにダウンロードされているかどうかを確認します。

アクセスポイントでの固定 IP アドレスの設定方法

アクセスポイントでの固定 IP アドレスの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway* 例： `Device# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2`	アクセスポイントの固定 IP アドレスを設定します。このコマンドには、次のキーワードと引数が含まれます。 • **ip-address**：Ciscoアクセスポイントの固定 IP アドレスを指定します。 • *ip-address*：Ciscoアクセスポイントの固定 IP アドレス。 • **netmask**：Cisco アクセスポイントの固定 IP ネットマスクを指定します。 • *netmask*：Ciscoアクセス ポイントの固定 IP ネットマスク。 • **gateway**：Cisco アクセス ポイントゲートウェイを指定します。 • *gateway*：Cisco アクセス ポイントゲートウェイの IP アドレス。 アクセスポイントがリブートしてdeviceに再 join し、指定した固定 IP アドレスがアクセスポイントにプッシュされます。固定 IP アドレスがアクセスポイントに送信された後、DNS サーバの IP ア

	コマンドまたはアクション	目的
		ドレスおよびドメイン名を設定できます。アクセスポイントのリブート後にステップ 3 とステップ 4 を実行します。
ステップ 3	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 4	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 5	**ap static-ip name-server** *nameserver_ip_address* 例： `Device(config)# ap static-ip name-server 10.10.10.205`	特定のアクセスポイントまたはすべてのアクセスポイントが DNS 解決を使用してdeviceを検出できるよう DNS サーバを設定します。 （注） DNS サーバ設定を元に戻すには、**no ap static-ip name-server** *nameserver_ip_address* コマンドを入力します。
ステップ 6	**ap static-ip domain** *static_ip_domain* 例： `Device(config)# ap static-ip domain domain1`	特定のアクセスポイントまたはすべてのアクセスポイントが属するドメインを設定します。 （注） ドメイン名の設定を元に戻すには、**no ap static-ip domain** *static_ip_domain* コマンドを入力します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show ap name** *Cisco_AP* **config general** 例： `Device# show ap name AP03 config general`	アクセスポイントの IP アドレス設定を表示します。

アクセスポイントでの固定 IP アドレスの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。

ステップ 2 [All Access Points] セクションで、 [AP Name] をクリックします。

ステップ 3 表示される [Edit AP] ウィンドウで、[IP Config] セクションに移動します。

ステップ 4 [Static IP (IPv4/IPv6)] チェックボックスをオンにします。これでスタティック IP の詳細ペインがアクティブになります。

ステップ 5 [Static IP]、[Netmask]、[Gateway]、[DNS IP Address] を入力します。

ステップ 6 [Update & Apply to Device] をクリックします。

TFTPリカバリ手順を使用したアクセスポイントのリカバリ

手順

ステップ 1 必要なリカバリイメージを Cisco.com（ap3g2-k9w8-tar.152-2.JA.tar）からダウンロードし、ご利用の TFTP サーバのルートディレクトリにインストールします。

ステップ 2 TFTP サーバをターゲットのアクセスポイントと同じサブネットに接続して、アクセス ポイントをパワーサイクリングします。アクセスポイントは TFTP イメージから起動し、次にdeviceにジョインしてサイズの大きなアクセスポイントのイメージをダウンロードし、アップグレード手順を完了します。

ステップ 3 アクセスポイントが回復したら、TFTP サーバを削除できます。

Autonomous アクセスポイントを Lightweight モードに変換する場合の設定例

例：アクセスポイントの IP アドレス設定の表示

次に、アクセスポイントの IP アドレス設定を表示する例を示します。

```
Device# 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
...
```

例：アクセスポイントのクラッシュファイル情報の表示

次の例は、アクセスポイントのクラッシュファイル情報を表示する方法を示しています。このコマンドを使用して、ファイルがdeviceにダウンロードされたかどうかを確認できます。

```
Device# 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.
```

AP MAC 許可

AP 許可ポリシー機能により、許可された AP のみがコントローラにとの関連付けを行えるようになります。AP を許可するには、AP のイーサネット MAC アドレスを登録する必要があります。登録は、コントローラまたは外部 RADIUS サーバでローカルに行うことができます。

AP MAC 許可の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no] ap auth-list ap-policy authorize-ap** *profile-name* 例： `Device(config)# ap auth-list ap-policy authorize-ap`	AP 許可ポリシーを設定します。
ステップ 3	**end** 例：	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 4	**show ap auth-list** *value-in-dBm* 例： `Device# show ap auth-list`	AP MAC 許可のステータスを表示します。

設定例

1. ローカルデータベース設定：

   ```
   Device(config)# aaa authorization network default local
   Device(config)# aaa authorization credential-download default local
   ```

2. ユーザ名設定：

   ```
   Device(config)# username e4c72281151a mac
   ```

   ユーザ名は AP のイーサネット MAC アドレスであり、AP がコントローラに関連付けられる前に許可されます。AP のイーサネット MAC アドレスには英数字を使用できます。文字は小文字で指定する必要があります。スペースまたは特殊文字は使用できません。AP のイーサネット MAC アドレスを取得するには、**show ap summary** コマンドを使用します。

アクセスポイントでのイーサネット VLAN タギング

アクセスポイントでのイーサネット VLAN タギングについて

AP コンソールのまたはコントローラから直接イーサネット インターフェイスで VLAN タギングを設定できます。設定はフラッシュメモリに保存され、ローカルにスイッチングされるすべてのトラフィックとともに、すべての CAPWAP フレームは設定されるように VLAN タグを使用し、VLAN にはマッピングされていません。

アクセス ポイントでのイーサネット VLAN タギングの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] > > を選択します。

ステップ 2 AP join プロファイルの名前をクリックするか、[Add] をクリックして新しい AP join プロファイルを作成します。

ステップ 3 表示される [Add/Edit AP Join Profile] ウィンドウで、[CAPWAP] タブをクリックし、[Advanced] タブをクリックします。

ステップ 4 [Enable VLAN Tagging] チェックボックスをオンにして、AP join プロファイルの VLAN タギングを有効にします。

ステップ 5 [Update & Apply to Device] をクリックします。

アクセスポイントでのイーサネット VLAN タギングの設定（CLI）

AP でイーサネット VLAN タギングを設定するには、次の手順に従います。

始める前に

- ブリッジモードの MAP では、VLAN タギングはサポートされていません。AP がブリッジモードに設定されている場合、この機能は自動的に無効になります。
- VLAN タグ付けが有効になっている場合、flex ネイティブ VLAN ID を AP 用に設定することはできません。
- AP がフェールオーバー中にワイヤレスコントローラの検出に失敗した場合、FlexConnect スタンドアロンモードの AP（VLAN タグが有効になっている）が 10 分ごとにリロードされることがあります。

手順

	コマンドまたはアクション	目的

ステップ 1	**ap name** *ap-name* **vlan-tag** *vlan-id*
	例：
	`Device# ap name AP1 vlan-tag 12`
	`Device# ap name AP1 no vlan-tag`
		非ブリッジ AP の VLAN タギングを設定します。設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 2	**ap vlan-tag** *vlan-id*
	例：
	`Device# ap vlan-tag 1000`
	`Device# ap no vlan-tag`
		すべての非ブリッジ AP の VLAN タギングを設定します。設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 3	**show ap config general** **例**： `Device# show ap config general`	（任意）すべての AP に共通の情報を表示します。