



CHAPTER 8

ワイヤレス デバイスの基本設定

このモジュールは、次の Cisco サービス統合型ルータ（ISR）の自律ワイヤレス デバイスの設定方法について説明します。

- Cisco 860 シリーズ
- Cisco 880 シリーズ
- Cisco 890 シリーズ



(注) 自律ソフトウェアを組み込みワイヤレス デバイス上で Cisco Unified ソフトウェアにアップグレードするには、「[Cisco Unified ソフトウェアへのアップグレード](#)」(P.8-9) で手順を参照してください。

ワイヤレス デバイスは組み込み型で、接続用の外部コンソール ポートはありません。ワイヤレス デバイスを設定するには、コンソール ケーブルでパーソナル コンピュータをホスト ルータのコンソール ポートに接続して次の手順に従って接続を確立し、ワイヤレス設定を行います。

- 「[無線コンフィギュレーションセッションの開始](#)」(P.8-2)
- 「[無線環境の設定](#)」(P.8-4)
- 「[ホットスタンバイ モードでのアクセス ポイントの設定](#)」(P.8-9) (任意)
- 「[Cisco Unified ソフトウェアへのアップグレード](#)」(P.8-9)
- 「[関連資料](#)」(P.8-12)

無線コンフィギュレーションセッションの開始



(注) ルータのセットアップでワイヤレス デバイスを設定する前に、後述の手順に従ってルータとアクセス ポイントとの間でセッションを開く必要があります。

以下のコマンドを、グローバル コンフィギュレーション モードでルータの Cisco IOS コマンドライン インターフェイス (CLI) に入力します。

手順の概要

1. `interface wlan-ap0`
2. `ip address subnet mask`
3. `no shut`
4. `interface vlan1`
5. `ip address subnet mask`
6. `exit`
7. `exit`
8. `service-module wlan-ap 0 session`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	interface wlan-ap0 例： <pre>Router(config)# interface wlan-ap0 Router(config-if)#</pre>	ワイヤレス デバイスへの、ルータのコンソール インターフェイスを定義します。 <ul style="list-style-type: none"> このインターフェイスは、ルータのコンソールとワイヤレス デバイス間の通信に使用します。 (注) 常にポート 0 を使用します。 <ul style="list-style-type: none"> 次のメッセージが表示されます。 <pre>The wlan-ap 0 interface is used for managing the embedded AP. Please use the service-module wlan-ap 0 session command to console into the embedded AP.</pre>
ステップ 2	ip address subnet mask 例： <pre>Router(config-if)# ip address 10.21.0.20 255.255.255.0</pre> または <pre>Router(config-if)# ip unnumbered vlan1</pre>	インターフェイス IP アドレスとサブネット マスクを指定します。 (注) この IP アドレスは、 ip unnumbered vlan1 コマンドを使用することで、Cisco ISR に割り当てられた IP アドレスと共有できます。
ステップ 3	no shut 例： <pre>Router(config-if)# no shut</pre>	内部インターフェイス接続を開いた状態を維持するように指定します。

	コマンドまたはアクション	目的
ステップ 4	interface vlan1 例: <pre>Router(config-if)# interface vlan1</pre>	データ通信のために、内部 Gigabit Ethernet (GE0; ギガビットイーサネット) 0 ポート上で仮想 LAN インターフェイスを別のインターフェイスに指定します。 <ul style="list-style-type: none"> • Cisco 860 シリーズ、Cisco 880 シリーズ、および Cisco 890 シリーズの ISR では、すべてのスイッチポートがデフォルトの vlan1 インターフェイスを継承します。
ステップ 5	ip address subnet mask 例: <pre>Router(config-if)# ip address 10.10.0.30 255.255.255.0</pre>	インターフェイス IP アドレスとサブネット マスクを指定します。
ステップ 6	exit 例: <pre>Router(config-if)# exit Router(config)#</pre>	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	exit 例: <pre>Router(config)# exit Router#</pre>	グローバル コンフィギュレーション モードを終了します。
ステップ 8	service-module wlan-ap 0 session 例: <pre>Router# service-module wlan-ap0 session Trying 10.21.0.20, 2002 ... Open ap></pre>	ワイヤレス デバイスとルータのコンソール間の接続をオープンにします。



ヒント

ワイヤレス デバイスとのセッションを開始するコンソールに Cisco IOS ソフトウェア エイリアスを作成する場合は、EXEC プロンプトから **alias exec dot11radio service-module wlan-ap 0 session** コマンドを入力します。このコマンドを入力すると、Cisco IOS ソフトウェアの **dot11 radio** レベルに自動的にスキップします。

セッションの終了

ワイヤレス デバイスとルータのコンソールとの間のセッションを閉じるには、次の手順に従います。

ワイヤレス デバイス

1. Control-Shift-6 x

ルータ

2. disconnect

3. Enter キーを 2 回押します。

無線環境の設定



(注)

ワイヤレス デバイスを初めて設定する場合は、基本のワイヤレス設定の前に、アクセス ポイントとルータとの間でコンフィギュレーション セッションを開始する必要があります。「無線コンフィギュレーションセッションの開始」(P.8-2) を参照してください。

ワイヤレス デバイスのソフトウェアに適合するツールを使用してデバイスを設定します。

- 「Cisco IOS コマンドライン インターフェイス」(P.8-5) : 自律ソフトウェア
- 「Cisco Express 設定」(P.8-4) : ユニファイド ソフトウェア



(注)

自律モードから Unified モードにアップグレードするには、アップグレード手順について、「Cisco Unified ソフトウェアへのアップグレード」(P.8-9) を参照してください。

Cisco Unified Wireless ソフトウェアへのアップグレード終了後、Web ブラウザのツールを使ってデバイスを設定します。手順については次の URL を参照してください。

http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap2-gui.html

Cisco Express 設定

Unified ワイヤレス デバイスを設定するには、次の手順に示すように、Web ブラウザ ツールを使用します。

- ステップ 1** ワイヤレス デバイスとのコンソール接続を確立し、**show interface bvi1** Cisco IOS コマンドを入力して、Bridge-Group Virtual Interface (BVI; ブリッジ グループ仮想インターフェイス) IP アドレスを取得します。
- ステップ 2** ブラウザのウィンドウを開き、ブラウザ ウィンドウのアドレス行にこの BVI IP アドレスを入力します。Enter を押します。[Enter Network Password] ウィンドウが表示されます。
- ステップ 3** ユーザ名を入力します。デフォルトのユーザ名は *Cisco* です。
- ステップ 4** ワイヤレス デバイスのパスワードを入力します。デフォルトのパスワードは *Cisco* です。[Summary Status] ページが表示されます。Web ブラウザの設定ページの使用方法の詳細については、次の URL を参照してください。

http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap4-first.html#wp1103336

Cisco IOS コマンドライン インターフェイス

自律ワイヤレス デバイスを設定するには、Cisco IOS CLI ツールを使用して次の作業を行います。

- 「無線の設定」(P.8-5)
- 「無線セキュリティ設定の実行」(P.8-5)
- 「無線 QoS の設定」(P.8-8) (任意)

無線の設定

Autonomous モードまたは Cisco Unified モードで信号を伝送するために、ワイヤレス デバイスの無線パラメータを設定します。特定の設定手順については、「第 9 章「無線の設定」」を参照してください。

無線セキュリティ設定の実行

- 「認証の設定」(P.8-5)
- 「WEP および暗号スイートの設定」(P.8-6)
- 「無線 VLAN の設定」(P.8-6)

認証の設定

認証の種類は、Service Set Identifiers (SSID; サービス セット識別子) に準拠します。SSID はアクセス ポイントに設定されます。同一のアクセス ポイントを持つ複数の種類のクライアント デバイスで使用するために、複数の SSID を設定します。

アクセス ポイントを介したワイヤレス クライアント デバイスとネットワークとの通信を開始する前に、クライアント デバイスは、公開キーまたは共有キーによる認証によってアクセス ポイントを認証する必要があります。安全性を最大限にするために、クライアント デバイスは MAC アドレスまたは Extensible Authentication Protocol (EAP; 拡張認証プロトコル) 認証を使用してネットワークも認証する必要があります。いずれの認証タイプもネットワークの認証サーバを信頼します。

認証タイプを選択するには、次の URL で『*Authentication Types for Wireless Devices*』を参照してください。

<http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html>

最大限のセキュリティ環境を設定するには、次の URL で『*RADIUS and TACACS+ Servers in a Wireless Environment*』を参照してください。

http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html

ローカル認証システムとしてのアクセス ポイント設定

ローカルの認証サービスまたはバックアップ認証サービスを障害が発生した WAN リンクまたはサーバに提供するために、アクセス ポイントをローカルの認証サーバとして機能するように設定できます。アクセス ポイントは、Lightweight Extensible Authentication Protocol (LEAP) 認証、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) 認証または MAC ベースの認証を使用して最大 50 のワイヤレス クライアント デバイスを認証することができます。このアクセス ポイントは毎秒最大 5 つの認証を実行できます。

ローカル オーセンティケータでのアクセス ポイントの設定は、クライアントのユーザ名とパスワードを使用して手動で行います。これは、ローカル オーセンティケータのデータベースが RADIUS サーバと同期化されないためです。クライアントが使用できる VLAN および SSID のリストを指定できます。

このロールの無線デバイスの設定に関する詳細については、次の URL で『*Using the Access Point as a Local Authenticator*』を参照してください。

<http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html>

WEP および暗号スイートの設定

Wired Equivalent Privacy (WEP) 暗号はワイヤレス デバイス間での伝送データをスクランブルして、通信機密を保持します。ワイヤレス デバイスおよびそのワイヤレス クライアント デバイスは、同一の WEP キーを使用してデータの暗号化および複合化を行います。WEP キーは、ユニキャストおよびマルチキャストの両方のメッセージを暗号化します。ユニキャスト メッセージとは、ネットワーク上の 1 個のデバイスに向けて送信されるメッセージです。マルチキャスト メッセージは、ネットワーク上の複数のデバイスに送信されます。

暗号スイートは、無線 LAN 上の無線通信を保護するように設計された、暗号と完全性アルゴリズムのセットです。Wi-Fi Protected Access (WPA) または Cisco Centralized Key Management (CCKM) を有効にするには、暗号スイートを使用する必要があります。

Temporal Key Integrity Protocol (TKIP) を含む暗号スイートは無線 LAN にとって最適な安全性を提供します。WEP だけしか含まない暗号化スイートでは、最低限のセキュリティしかありません。

暗号化の手順については、次の URL で『*Configuring WEP and Cipher Suites*』を参照してください。

<http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html>

無線 VLAN の設定

無線 LAN で VLAN を使用し、SSID を VLAN に割り当てると、「**セキュリティの種類**」(P.8-7) で定義されている 4 種類のセキュリティ設定のいずれかを使用して複数の SSID を作成できます。VLAN は、定義されたスイッチのセット内に存在するブロードキャスト ドメインと考えることができます。VLAN は、単一のブリッジング ドメインに接続されている複数のエンド システム (ホスト、またはブリッジやブリッジやルータなどのネットワーク装置) で構成されます。ブリッジング ドメインは、さまざまなネットワーク機器によりサポートされます。ネットワーク機器には、各 VLAN 用の別個のプロトコル グループとともに、ブリッジング プロトコルをそれらの間で動作させる LAN スイッチなどがあります。

無線 VLAN アーキテクチャの詳細については、次の URL で『*Configuring Wireless VLANs*』を参照してください。

http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html



(注) 無線 LAN で VLAN を使用しないと、SSID に割り当てることができるセキュリティ オプションが制限されます。これは、Express Security ページで暗号化設定と認証タイプが対応付けられているためです。

SSID の割り当て

アクセス ポイントとして機能するワイヤレス デバイスには最大 16 個の SSID を設定できます。また、SSID ごとに一意のパラメータ セットを設定できます。たとえば、ある SSID ではネットワーク アクセスだけをユーザーに許可し、別の SSID では認証したユーザであれば機密データへのアクセスを許可するといった利用法が可能です。

複数の SSID の作成の詳細については、次の URL で『*Service Set Identifiers*』を参照してください。

<http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html>



Read VLAN を使用しない場合、暗号化設定（WEP と暗号）が 2.4GHz 無線などのインターフェイスに適用されるため、1 つのインターフェイスで複数の暗号化設定を使用することはできません。たとえば、VLAN がディセーブルの状態スタティック WEP を使用する SSID を作成した場合は、WPA 認証を使用する SSID を別途作成できません。使用される暗号化設定が異なるためです。SSID のセキュリティ設定が別の SSID の設定と競合する場合、競合を解消するために 1 つ以上の SSID を削除します。

セキュリティの種類

表 8-1 は、SSID に割り当てられる 4 つのセキュリティ タイプについて説明しています。

表 8-1 SSID セキュリティの種類

セキュリティ タイプ	説明	有効になるセキュリティ機能
セキュリティなし	これは安全性が最も低いオプションです。このオプションは、パブリック スペースで SSID を使用する場合に限定して使用し、ネットワークへのアクセスを制限する VLAN に割り当てる必要があります。	なし。
スタティック WEP キー	このオプションは、「セキュリティなし」よりは安全です。ただし、スタティック WEP キーは攻撃に対して脆弱です。この設定を行う場合は、MAC アドレスに基づいてワイヤレス デバイスにアソシエーションを制限する必要があります。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html の『 <i>Cipher Suites and WEP</i> 』を参照してください。 または ネットワーク内に RADIUS サーバがない場合、アクセスポイントをローカル認証サーバとして使用するかを検討してください。 手順については、 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html の『 <i>Using the Access Point as a Local Authenticator</i> 』を参照してください。	WEP が必須。ワイヤレス デバイス キーに合う WEP キーがないと、この SSID を使用してもクライアント デバイスをアソシエートできません。

表 8-1 SSID セキュリティの種類 (続き)

セキュリティ タイプ	説明	有効になるセキュリティ機能
EAP ¹ 認証	<p>このオプションは、802.1X 認証 (LEAP²、PEAP³、EAP-TLS⁴、EAP-FAST⁵、EAP-TTLS⁶、EAP-GTC⁷、EAP-SIM⁸、およびその他の 802.1X/EAP ベースの製品) がイネーブルになります。</p> <p>この設定は、必須の暗号化、WEP、オープン認証プラス EAP、ネットワーク EAP 認証を使用し、キー管理なしで RADIUS サーバ認証ポート 1645 を使用します。</p> <p>ネットワーク上の認証サーバの IP アドレスと共有秘密キーを入力する必要があります (サーバ認証ポート 1645)。802.1x 認証ではダイナミック暗号キーが提供されるため、WEP キーを入力する必要がありません。</p>	<p>必須の 802.1X 認証。この SSID を使用してアソシエートするクライアント デバイスは、802.1X 認証を実行する必要があります。</p> <p>ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP によるオープン認証を設定していない場合、以下の警告メッセージが表示されます。</p> <p>SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.</p>
WPA ⁹	<p>このオプションは、データベース認証されたユーザにワイヤレス アクセスを許可します。アクセスは認証サーバのサービスを通じて行います。ユーザの IP トラフィックは WEP で使用されるものより強力なアルゴリズムで暗号化されます。</p> <p>この設定では暗号キー、TKIP¹⁰、オープン認証プラス EAP、ネットワーク EAP 認証、必須のキー管理 WPA、および RADIUS サーバ認証ポート 1645 を使用します。</p> <p>EAP 認証の場合と同じように、ネットワーク上の認証サーバの IP アドレスと共有秘密キーを入力する必要があります (サーバ認証ポート 1645)。</p>	<p>WPA 認証が必須。この SSID を使用して対応付けを行うクライアント デバイスは WPA 対応でなければなりません。</p> <p>ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP によるオープン認証を設定していない場合、以下の警告メッセージが表示されます。</p> <p>SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.</p>

1. EAP = Extensible Authentication Protocol
2. LEAP = Lightweight Extensible Authentication Protocol
3. PEAP = Protected Extensible Authentication Protocol
4. EAP-TLS = Extensible Authentication Protocol-Transport Layer Security
5. EAP-FAST = Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling
6. EAP-TTLS = Extensible Authentication Protocol-Tunneled Transport Layer Security
7. EAP-GTC = Extensible Authentication Protocol-Generic Token Card
8. EAP-SIM = Extensible Authentication Protocol-Subscriber Identity Module
9. WPA = Wi-Fi Protected Access
10. TKIP = Temporal Key Integrity Protocol

無線 QoS の設定

Quality of Service (QoS) を設定することで、別のトラフィックを犠牲にして特定のトラフィックを優先させることができます。QoS がない場合、デバイスは各パケットに最善のサービスを提供します (パケットの内容やサイズは問いません)。信頼性、遅延限度、またはスループットに関して保証することなく、パケットを送信します。ワイヤレス デバイスに QoS を設定するには、<http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html> の『Quality of Service in a Wireless Environment』を参照してください。

ホットスタンバイ モードでのアクセス ポイントの設定

ホットスタンバイ モードでは、アクセス ポイントは別のアクセス ポイントのバックアップとして指定されます。スタンバイ アクセス ポイントは、アクセス ポイントのそばに配置され、それをモニタします（設定は、このアクセス ポイントとまったく同じにします）。スタンバイ アクセス ポイントは、クライアントとしてモニタ対象のアクセス ポイントとアソシエートします。またモニタ対象のアクセス ポイントに、イーサネットおよび無線ポートを通して Internet Access Point Protocol (IAPP; インターネット アクセス ポイント プロトコル) クエリを送信します。モニタするアクセス ポイントから応答がない場合、スタンバイ アクセス ポイントはオンラインに切り替わり、そのアクセス ポイントの役割をネットワーク上で引き継ぎます。

スタンバイ アクセス ポイントの設定は、IP アドレスを除き、モニタするアクセス ポイントの設定と一致している必要があります。モニタ対象アクセス ポイントがオフラインになり、スタンバイ アクセス ポイントがそれを引き継いだ場合、両アクセス ポイントの設定が同一であれば、クライアントデバイスは簡単かつ確実にスタンバイ アクセス ポイントに切り替わることができます。詳細については、次の URL で『Hot Standby Access Points』を参照してください。

<http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html>

Cisco Unified ソフトウェアへのアップグレード

アクセス ポイントを Cisco Unified モードで実行するには、次の手順に従ってソフトウェアをアップグレードする必要があります。

- 「アップグレードの準備」 (P.8-9)
- 「アップグレードの実行」 (P.8-10)
- 「アクセス ポイントへのソフトウェアのダウンロード」 (P.8-11)
- 「アクセス ポイントでのソフトウェア リカバリ」 (P.8-12)

ソフトウェア前提条件

- アクセス ポイントが組み込まれた Cisco 890 シリーズ ISR は、IP Base フィーチャセットと Cisco IOS 12.4(22)YB ソフトウェアを実行している場合、自律ソフトウェアから Cisco Unified ソフトウェアにアップグレードできます。
- アクセス ポイントが組み込まれた Cisco 880 シリーズ ISR は、advipservices フィーチャセットと Cisco IOS 12.4(20)T ソフトウェアを実行している場合、自律ソフトウェアから Cisco Unified ソフトウェアにアップグレードできます。
- Cisco Unified アーキテクチャの中で組み込み型アクセス ポイントを使用するには、バージョン 5.1 以降のシスコ Wireless LAN Configuration (WLC) を実行している必要があります。

アップグレードの準備

アップグレードを準備するには次の作業を行います。

- 「アクセス ポイントの IP アドレスの保護」 (P.8-10)
- 「モード設定がイネーブルになっていることの確認」 (P.8-10)

アクセス ポイントの IP アドレスの保護

アクセス ポイントの IP アドレスを保護することにより、アクセス ポイントは WLC と通信でき、起動時に Unified イメージをダウンロードできます。ホスト ルータは、DHCP プールを通じてアクセス ポイント DHCP サーバ機能を提供します。このアクセス ポイントは WLC と通信し、DHCP プール コンフィギュレーションのコントローラ IP アドレスのオプション 43 を設定します。次の例は、設定サンプルを示しています。

```
ip dhcp pool embedded-ap-pool
network 60.0.0.0 255.255.255.0
dns-server 171.70.168.183
default-router 60.0.0.1
option 43 hex f104.0a0a.0a0f (single WLC IP address(10.10.10.15) in hex format)
int vlan1
ip address 60.0.0.1 255.255.255.0
```

WLC 検出プロセスの詳細については、

<http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html> の『Cisco Wireless LAN Configuration Guide』を参照してください。

モード設定がイネーブルになっていることの確認

モードの設定が有効になっていることを確認するには、次の手順を実行します。

-
- ステップ 1** ルータから WLC サーバに ping を実行し、接続を確認します。
 - ステップ 2** **service-module wlan-ap 0 session** コマンドを実行し、アクセス ポイントへのセッションを確立します。
 - ステップ 3** アクセス ポイントが自律起動イメージを動作させているか確認します。
 - ステップ 4** **show boot** コマンドを入力してアクセス ポイントのモード設定がイネーブルになっていることを確認します。コマンドの出力例を示します。

```
Autonomous-AP# show boot
BOOT path-list:      flash:ap801-k9w7-mx.124-10b.JA3/ap801-k9w7-mx.124-10b.JA3
Config file:        flash:/config.txt
Private Config file: flash:/private-config
Enable Break:       yes
Manual Boot:        yes
HELPER path-list:
NVRAM/Config file
buffer size:       32768
Mode Button:       on
```

アップグレードの実行

自律ソフトウェアを Cisco Unified ソフトウェアにアップグレードするには、次の手順に従います。

-
- ステップ 1** アクセス ポイントの起動イメージを Cisco Unified アップグレード イメージ (回復イメージとも呼びます) に変更するには、グローバル コンフィギュレーション モードで **service-module wlan-ap 0 bootimage unified** コマンドを実行します。

```
Router# conf terminal
Router(config)# service-module wlan-ap 0 bootimage unified
Router(config)# end
```



(注) **service-module wlan-ap 0 bootimage unified** コマンドを実行しても正しく処理されない場合は、ソフトウェア ライセンスがまだ有効であるか確認してください。

アクセス ポイントの起動イメージのパスを識別するには、アクセス ポイントのコンソールから EXEC モードで **show boot** コマンドを使用します。

```
autonomous-AP# show boot
BOOT path-list:      flash:/ap801-rcvk9w8-mx/ap801-rcvk9w8-mx
```

- ステップ 2** グレースフル シャットダウンを行ってアクセス ポイントをリポートし、アップグレードプロセスを完了するには、グローバル コンフィギュレーション モードで **service-module wlan-ap 0 reload** コマンドを実行します。アクセス ポイントとのセッションを確立し、アップグレードプロセスをモニタします。GUI の設定ページを使用したワイヤレス デバイスのセットアップの詳細については、「[Cisco Express 設定](#)」(P.8-4) を参照してください。

AP から自律モードへアップグレードまたは復帰する際のトラブルシューティング

- Q.** 私のアクセス ポイントでは、自律ソフトウェアから Cisco Unified ソフトウェアへのアップグレードに失敗し、回復モードに陥ったままになっているようです。どうすればいいでしょうか。
- A.** アクセス ポイントで自律ソフトウェアから Unified ソフトウェアにアップグレードできなかった場合は、次の操作を実行してください。
- 回復イメージを起動する前に、自律アクセス ポイントのスタティック IP アドレスが BVI インターフェイスに設定されていないことを確認します。
 - ルータ/アクセス ポイントと WLC 間で ping を実行して、接続が確立されているか確認します。
 - アクセス ポイントと WLC クロック（時刻と日付）が正しく設定されているか確認します。
- Q.** アクセス ポイントが起動を試行しているのですが、何度やってもうまくいきません。どうしてですか。またアクセス ポイントがリカバリ イメージでスタックしたまま、Unified ソフトウェアにアップグレードしません。どうしてですか。
- A.** アクセス ポイントでは、起動を試みて失敗したり、回復モードに陥ってしまい、Unified ソフトウェアにアップグレードできない場合があります。このいずれかの状態になった場合は、**service-module wlan-ap0 reset bootloader** コマンドを実行してアクセス ポイントをブートローダに戻し、手動でイメージを復帰させてください。

アクセス ポイントへのソフトウェアのダウンロード

アクセス ポイントの起動イメージを直前の自律イメージにリセットするには、グローバル コンフィギュレーション モードで **service-module wlan-ap0 bootimage autonomous** コマンドを使用します。自律ソフトウェア イメージをアクセス ポイントにリロードするには、**service-module wlan-ap 0 reload** コマンドを使用します。

アクセス ポイントでのソフトウェア リカバリ

アクセス ポイントにイメージを回復するには、グローバル コンフィギュレーション モードで **service-module wlan-ap0 reset bootloader** コマンドを使用します。このコマンドを使用すると、アクセス ポイントがブートローダに戻り、手動でイメージをリカバリできるようになります。



注意

このコマンドの使用に当たっては、十分注意してください。この操作では通常のシャットダウンが実行されないことから、実行中のファイル操作に影響が生じる場合があります。このコマンドは、シャットダウンまたは障害状態から回復する目的に限り使用してください。

関連資料

自律およびユニファイド設定手順の詳細については、次のマニュアルを参照してください。

- 「シスコの自律ソフトウェアのマニュアル」 — 表 8-2
- 「Cisco Unified ソフトウェアのマニュアル」 — 表 8-3

表 8-2 シスコの自律ソフトウェアのマニュアル

ネットワーク デザイン	リンク
ワイヤレスの概要	第 2 章「ワイヤレス デバイス概要」
設定	リンク
無線の設定	第 9 章「無線の設定」
セキュリティ	リンク
『Authentication Types for Wireless Devices』	本マニュアルでは、アクセス ポイントに設定する認証の種類について説明しています。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html
『RADIUS and TACACS+ Servers in a Wireless Environment』	このマニュアルは、RADIUS および TACACS+ のイネーブルと設定の方法、アカウント情報の詳細説明、さらに、管理側が行う認証と認証プロセスの柔軟な制御方法について説明します。RADIUS および TACACS+ は、AAA ¹ を通じて活用され、AAA コマンドを使用する場合だけイネーブルにできます。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html
『Using the Access Point as a Local Authenticator』	本マニュアルでは、ローカル認証を担当するアクセス ポイントというロールにおいて、無線デバイスを使用する方法について説明しています。アクセス ポイントは小規模無線 LAN のスタンドアロン認証システムとして機能するか、あるいはバックアップ認証サービスを提供します。ローカル認証を担当するアクセス ポイントは、LEAP、EAP-FAST および MAC ベースの認証を最大 50 個のクライアント デバイスに対して実行します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html

表 8-2 シスコの自律ソフトウェアのマニュアル（続き）

ネットワーク デザイン	リンク
『Cipher Suites and WEP』	このマニュアルは、WPA および CCKM ² 、WEP、および WEP 機能 (AES ³ 、MIC ⁴ 、TKIP、およびブロードキャスト キーのローテーションなど) を使用するために必要な暗号スイートの設定方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html
『Hot Standby Access Points』	本マニュアルでは、ホットスタンバイ ユニットとしてワイヤレス デバイスを設定する方法を説明しています。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html
『Configuring Wireless VLANs』	このマニュアルは、ワイヤード LAN に設定された VLAN とともにアクセス ポイントを使用するための設定方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html
『Service Set Identifier』	ワイヤレス デバイスは、アクセス ポイントとして最大 16 の SSID をサポートできます。本マニュアルでは、ワイヤレス デバイス上の SSID の設定および管理方法について説明します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html
管理	リンク
アクセス ポイントの管理	第 10 章「無線デバイスの管理」
Quality of Service	このマニュアルは、ユーザのシスコ無線インターフェイスでの QoS の設定方法について解説します。この機能により、別のトラフィックを犠牲にして特定のトラフィックを優先させることができます。QoS がない場合、デバイスは各パケットに最善のサービスを提供します (パケットの内容やサイズは問いません)。信頼性、遅延限度、またはスループットに関して保証することなく、パケットを送信します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html
『Regulatory Domains and Channels』	本マニュアルには、世界中の規制ドメイン内の Cisco アクセス製品でサポートしている無線チャンネルが記載されています。 http://www.cisco.com/en/US/customer/docs/routers/access/wireless/software/guide/RadioChannelFrequencies.html
『System Message Logging』	本マニュアルでは、ユーザのワイヤレス デバイス上でシステム メッセージ ロギングを設定する方法について説明しています。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SystemMsgLogging.html

1. AAA = Authentication, Authorization, and Accounting
2. CCKM = Cisco Centralized Key Management
3. AES = Advanced Encryption Standard
4. MIC = Message Integrity Check

表 8-3 Cisco Unified ソフトウェアのマニュアル

ネットワーク デザイン	リンク
『Why Migrate to the Cisco Unified Wireless Network?』	http://www.cisco.com/en/US/solutions/ns175/networking_solutions_products_genericcontent0900aecd805299ff.html
『Wireless LAN Controller (WLC) FAQ』	http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008064a991.shtml
『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, versions 12.4(10b) JA and 12.3(8) JEC』	http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr2410b.html
『Cisco Aironet 1240AG Access Point Support Documentation』	http://www.cisco.com/en/US/docs/wireless/access_point/1240/quick/guide/ap1240qs.html
『Cisco 4400 Series Wireless LAN Controllers Support Documentation』	http://www.cisco.com/en/US/products/ps6366/tsd_products_support_series_home.html