アクセス ポイントの最初の設定

この章では、最初にワイヤレス デバイスの基本設定を行うときの手順について説明します。この章の内容は、ワイヤレス デバイスに付属するクイック スタート ガイドの説明と共通する箇所があります。この章で説明する設定はすべて CLI を使用して実行できますが、ワイヤレス デバイスの Web ブラウザ インターフェイスで初期設定を完了してから、CLI を使用して詳細設定を追加入力する方が簡単な場合があります。

(注) アクセス ポイントの無線インターフェイスはデフォルトで無効になっています。

はじめる前に

ワイヤレス デバイスを設置する前に、使用しているコンピュータがこのワイヤレス デバイスと同じネットワークに接続されていることを確認し、ネットワーク管理者から次の情報を取得してください。

- ワイヤレス デバイスのシステム名
- 大文字と小文字を区別する、無線ネットワークの無線 Service Set Identifier（SSID; サービス セット ID）
- DHCP サーバに接続されていない場合は、ワイヤレス デバイスの一意の IP アドレス（172.17.255.115 など）
- ワイヤレス デバイスが PC と同じサブネット上にない場合、デフォルト ゲートウェイ アドレスとサブネット マスク
- 簡易ネットワーク管理プロトコル（SNMP）コミュニティ名と SNMP ファイル属性（SNMP を使用している場合）
- Cisco IP Setup Utility（IPSU）を使用して、ワイヤレス デバイスの IP アドレスを検索する場合、アクセス ポイントの MAC アドレス。MAC アドレスは、アクセス ポイントの底面ラベルに記載されています（00164625854c など）。

デバイスのデフォルト設定へのリセット

初期設定時に最初からやり直す必要がある場合は、アクセス ポイントをデフォルト設定にリセットすることができます。

MODE ボタンを使用したデフォルト設定へのリセット

（注）　MODE ボタンを使用したデフォルト設定へのリセットは、自律モードのアクセス ポイントにのみ適用されます。Lightweight モードのアクセス ポイントには適用されません。

アクセス ポイントの MODE ボタンを使用して、アクセス ポイントをデフォルト設定にリセットする手順は、次のとおりです。

ステップ 1　アクセス ポイントの電源（外部電源用の電源ジャックまたはインライン パワー用のイーサネット ケーブル）を切ります。

ステップ 2　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。

ステップ 3　MODE ボタンを押し続けて、ステータス LED がオレンジに変わったら（約 1 ～ 2 秒かかります）ボタンを放します。アクセス ポイントのすべての設定が、デフォルトに戻ります。

GUI を使用したデフォルト設定へのリセット

アクセス ポイントの GUI を使用してデフォルトの設定に戻す手順は、次のとおりです。

ステップ 1　インターネット ブラウザを開きます。
無線デバイスの Web ブラウザ インターフェイスは、Microsoft Internet Explorer バージョン 9.0 と Mozilla Firefox バージョン 17 と完全に互換性があります。

ステップ 2　ブラウザのアドレス入力用ボックスにワイヤレス デバイスの IP アドレスを入力して、**Enter** キーを押します。[Enter Network Password] ウィンドウが表示されます。

ステップ 3　[User Name] フィールドに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　[Password] フィールドにワイヤレス デバイスのパスワードを入力し、Enter を押します。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。

ステップ 5　[Software] をクリックして [System Software] 画面を表示します。

ステップ 6　[System Configuration] をクリックして、[System Configuration] 画面を表示します。

ステップ 7　[Reset to Defaults] ボタンをクリックすると、IP アドレスを含むすべての設定がデフォルト値にリセットされます。IP アドレスを除いたすべての設定をデフォルト値にリセットするには、[Reset to Defaults (Except IP)] ボタンをクリックします。

CLI を使用したデフォルト設定へのリセット

注意　デフォルトにリセットまたはソフトウェアをリロードする前に、システム ファイルを削除しないでください。

アクセス ポイントをデフォルト設定および静的 IP アドレスにリセットする場合、*write erase* または *erase /all nvram* コマンドを使用します。静的 IP アドレスなどすべてを消去する場合、上記のコマンドの他に、*erase* および *erase boot static-ipaddr static-ipmask* コマンドを使用します。

特権 EXEC モードからは、CLI を使用して次の手順でaccess point/bridgeの設定をデフォルト値にリセットできます。

ステップ 1　**erase nvram** を入力して、スタートアップ コンフィギュレーションを含むすべての NVRAM ファイルを消去します。

（注）　**erase nvram** コマンドでは、静的 IP アドレスは消去されません。

ステップ 2　静的 IP アドレスおよびサブネット マスクを消去するには、次の手順を実行します。それ以外の場合は、ステップ 3 に進みます。

a. **write default-config** と入力します。

ステップ 3　「*Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]*」という CLI メッセージが表示されたら、Y と入力します。

ステップ 4　「*Erase of nvram: complete.*」という CLI メッセージが表示されたら、**reload** と入力します。このコマンドにより、オペレーティング システムがリロードされます。

ステップ 5　「*Proceed with reload? [confirm]*」という CLI メッセージが表示されたら、Y と入力します。

注意　コンフィギュレーション ファイルの損傷を防ぐため、ブート プロセスは中断しないでください。CLI コンフィギュレーションの変更を続ける前に、access point/bridge Install Mode LED が緑色に点滅するまで待ちます。ロード プロセスが完了すると、「*Line protocal on Interface Dot11Radio0, changed state to up.*」という CLI メッセージが表示されます。

ステップ 6　access point/bridgeがリブートしたら、静的 IP アドレスを割り当てている場合は WEB ブラウザ インターフェイスを使用して、割り当てていない場合は CLI を使用して、アクセス ポイントを再設定できます。

アクセス ポイントは、特権 EXEC モードから、IP アドレスも含めてデフォルト値に設定されています（DHCP を使用して IP アドレスを受信するように設定されます）。access point/bridgeの新しい IP アドレスを取得するには、*show interface bvi1* CLI コマンドを使用します。

アクセス ポイントへのログイン

ユーザは、次のいずれかの方法を使用してアクセス ポイントにログインできます。

- グラフィカル ユーザ インターフェイス（GUI）
- Telnet（IP アドレスを使用して AP が設定されている場合）
- コンソール ポート

（注）　Cisco Aironet アクセス ポイントのすべてのモデルにコンソール ポートが用意されているわけではありません。アクセス ポイントにコンソール ポートが用意されていない場合は、GUI または Telnet を使用してアクセスしてください。

GUI を使用して AP にログインする方法については、初めて Web ブラウザ インターフェイスを使用する場合（2-1 ページ）を参照してください。

CLI を使用して AP にログインする方法については、CLI のアクセス（3-8 ページ）を参照してください。

コンソール ポートを使用して AP にログインする方法については、アクセス ポイントへのローカル接続（4-4 ページ）を参照してください。

IP アドレスの取得と割り当て

ワイヤレス デバイスの [Express Setup] ページにアクセスするには、次のいずれかの方法でワイヤレス デバイスの IP アドレスを取得するか、割り当てる必要があります。

- アクセス ポイントのコンソール ポートに接続し、静的 IP アドレスを割り当てます。デバイスのコンソール ポートに接続するには、次の項の手順を実行します。
  - アクセス ポイントへのローカル接続（4-4 ページ）。
  - 1550 シリーズのアクセス ポイントへのローカル接続（4-5 ページ）

（注）　ターミナル エミュレータ アプリケーションによっては、フロー制御パラメータを Xon/Xoff に設定する必要があります。フロー制御値が none に設定されているためにデバイスのコンソール ポートに接続できない場合は、フロー制御値を Xon/Xoff に変更してみてください。

- DHCP サーバを使用すると（使用できる場合）、自動的に IP アドレスが割り当てられます。次のいずれかの方法により、DHCP によって割り当てられた IP アドレスを検索できます。
  - まず、ワイヤレス デバイスのコンソール ポートに接続し、**show ip interface brief** コマンドを使用して IP アドレスを表示します。

    コンソール ポートに接続するには、「アクセス ポイントへのローカル接続」セクション（4-4 ページ）の手順に従います。
  - 組織のネットワーク管理者に、ワイヤレス デバイスのメディア アクセス コントロール（MAC）アドレスを知らせます。ネットワーク管理者は、MAC アドレスを使用して DHCP サーバに照会し、IP アドレスを確認します。アクセス ポイントの MAC アドレスは、アクセス ポイントの底面ラベルに記載されています。

デフォルトの IP アドレスの動作

1040、1140、1240、2600 アクセス ポイントをデフォルトの設定で LAN に接続している場合、アクセス ポイントは DHCP サーバに IP アドレスを要求し、アドレスを受信できない場合、要求を無期限に送信し続けます。

アクセス ポイントへのローカル接続

（注）　次の情報は、1550 シリーズ AP を除くすべての AP に適用されます。

アクセス ポイントを（有線 LAN に接続せずに）ローカルに設定する必要がある場合、DB-9 to RJ-45 のシリアル ケーブルを使用して PC をアクセス ポイントのコンソール ポートに接続できます。次の手順に従ってアクセス ポイントのコンソール ポートに接続し、CLI を開きます。

ステップ 1　9 ピンのメスの DB-9 to RJ-45 シリアル ケーブルを、アクセス ポイントの RJ-45 シリアル ポートと、コンピュータの COM ポートに接続します。DB-9 to RJ-45 シリアル ケーブルのシスコ製品番号は AIR-CONCAB1200 です。シリアル ケーブルは、http://www.cisco.com/go/marketplace で注文できます。

ステップ 2　アクセス ポイントと通信できるようにターミナル エミュレータを設定します。ターミナル エミュレータの接続では、9600 ボー、データ ビット 8、パリティなし、ストップ ビット 1 の設定を使用します。フロー制御はなしです。

（注）　xon/xoff フロー制御で正常に機能しない場合は、フロー制御なしを使用してください。

ステップ 3　接続したら、enter を押すか、**en** と入力して、コマンド プロンプトを表示します。enter を押すと、ユーザ EXEC モードになります。**en** と入力すると、パスワードを入力するよう求められ、パスワードを入力すると特権 EXEC モードになります。デフォルトのパスワードは *Cisco* です。大文字と小文字は区別されます。

（注）　設定の変更が完了したら、アクセス ポイントからシリアル ケーブルを取り外してください。

1550 シリーズのアクセス ポイントへのローカル接続

アクセス ポイントを（有線 LAN に接続せずに）ローカルに設定する必要がある場合、カテゴリ 5 のイーサネット ケーブルを使用して PC を長距離用パワー インジェクタのイーサネット ポートに接続できます。シリアル ポート接続を使用するのと同じように、パワー インジェクタのイーサネット ポートへのローカル接続を使用できます。

（注）　特別なクロス ケーブルを使用しなくても、PC をパワー インジェクタに接続できます。また、ストレートケーブルまたはクロス ケーブルのいずれも使用できます。

ブリッジをローカルで接続する手順は、次のとおりです。

ステップ 1　使用する PC が IP アドレスを自動的に取得するように設定します。または、アクセス ポイント/ブリッジの IP アドレスと同じサブネット内の IP アドレスを手動で割り当てます。たとえば、アクセス ポイント/ブリッジに IP アドレス 10.0.0.1 を割り当てた場合、PC に IP アドレス 10.0.0.20 を割り当てます。

ステップ 2　パワー インジェクタから電源ケーブルを抜いた状態で、カテゴリ 5 のイーサネット ケーブルを使用して PC をパワー インジェクタに接続します。クロス ケーブルまたはストレート ケーブルのいずれかを使用できます。

（注）　イーサネット ポート 0 を使用して、パワー インジェクタとアクセス ポイント/ブリッジ間で通信が実行されます。イーサネット ポート 0 の設定は何も変更しないようにしてください。

ステップ 3　二重同軸ケーブルで、パワー インジェクタをaccess point/bridgeに接続します。

ステップ 4　パワー インジェクタの電源ケーブルを接続して、access point/bridgeの電源を入れます。

ステップ 5　「基本設定の割り当て」セクション（4-6 ページ）の手順を実行します。操作を間違えたため、最初からやり直す必要がある場合は、「デバイスのデフォルト設定へのリセット」の手順（ 4-1ページ）の手順に従ってください。

ステップ 6　access point/bridgeの設定後、PC からイーサネット ケーブルを抜いて、アクセス ポイントを有線 LAN に接続します。

（注）　PC をaccess point/bridgeに接続するか、PC を有線 LAN に再接続する場合は、PC の IP アドレスを解放または更新しなければならない場合があります。ほとんどの PC では、PC をリブートするか、コマンド プロンプト画面で **ipconfig /release** および **ipconfig /renew** コマンドを入力することによって、IP アドレスを解放および更新できます。手順の詳細は、ご使用の PC の操作マニュアルを参照してください。

デフォルトの無線設定

Cisco IOS Release 12.3(8)JA から、アクセス ポイントの無線は無効に設定され、デフォルトの SSID は何も割り当てられていません。これは、権限のないユーザが、デフォルトの SSID を使用してセキュリティを設定していないこのアクセス ポイントからお客様の無線ネットワークにアクセスするのを防ぐための措置です。アクセス ポイントの無線インターフェイスを有効にする前に、SSID を作成する必要があります。

基本設定の割り当て

ワイヤレス デバイスの IP アドレスを決定または割り当てた後、次の手順に従って、このワイヤレス デバイスの [Express Setup] ページにアクセスし、初期設定を行います。

ステップ 1　インターネット ブラウザを開きます。

ステップ 2　ブラウザのアドレス入力用ボックスにワイヤレス デバイスの IP アドレスを入力して、**Enter** キーを押します。
[Enter Network Password] 画面が表示されます。

ステップ 3　Tab を押して、[Username] フィールドの次の [Password] フィールドに進みます。

ステップ 4　大文字/小文字を区別して *Cisco* というパスワードを入力し、Enter を押します。
[Summary Status] ページが表示されます。

ステップ 5　[Easy Setup] をクリックします。
[Express Setup] 画面が表示されます。

ステップ 6　[Network Configuration] をクリックします。

ステップ 7　システム管理者から入手した設定を [Network Configuration] に入力します。
設定可能な項目は、次のとおりです。

- [Host Name]：ホスト名は必須設定ではありませんが、ネットワーク上のワイヤレス デバイスを識別するのに役立ちます。ホスト名は、管理システム ページのタイトルに表示されます。

(注)　システム名には、32 文字まで入力することができます。しかし、ワイヤレス デバイスでは、クライアント デバイスに自分自身を識別させる際に、システム名の最初の 15 文字だけを使用します。異なるワイヤレス デバイスを区別することがクライアント ユーザにとって重要な場合、最初の 15 文字に、システム名の固有の部分を含めてください。

(注)　システム名を変更すると、ワイヤレス デバイスにより無線がリセットされます。この結果、アソシエートされたクライアント デバイスのアソシエーションが解除され、ただちに再アソシエートされます。

- [Server Protocol]：ネットワークの IP アドレスの割り当て方法に対応するオプション ボタンをクリックします。
  - [DHCP]：IP アドレスは、ネットワークの DHCP サーバによって自動的に割り当てられます。
  - [Static IP]：ワイヤレス デバイスでは、[IP Address] フィールドに入力された静的 IP アドレスが使用されます。
- [IP Address]：ワイヤレス デバイスの IP アドレスを割り当てたり、変更したりします。DHCP がネットワークで有効な場合、このフィールドは空白のままにします。

(注)　有線 LAN 上で Web ブラウザ インターフェイスや Telnet セッションを使用してワイヤレス デバイスの設定をしている間にワイヤレス デバイスの IP アドレスが変更されると、そのワイヤレス デバイスへの接続は解除されます。接続が解除された場合は、新しい IP アドレスを使用してワイヤレス デバイスに再接続してください。もう一度、最初からやり直す必要がある場合は、「デバイスのデフォルト設定へのリセット」セクション（4-1 ページ）の手順に従ってください。

- [IP Subnet Mask]：IP アドレスが LAN 上で認識されるように、ネットワーク管理者から提供された IP サブネット マスクを入力します。DHCP が有効な場合、このフィールドは空白のままにします。
- [Default Gateway]：ネットワーク管理者から提供されたデフォルト ゲートウェイ IP アドレスを入力します。DHCP が有効な場合、このフィールドは空白のままにします。
- **[IPv6 ProtocolP]**：適用するプロトコルに対応する対応するチェックボックスをオンにして、そのプロトコルを指定します。次のオプションを選択できます。
  - DHCP
  - Autoconfig
  - Static IP
- **[IPv6 Address]**：IPv6 アドレスを入力します。
- **[Username]**：ネットワークへのアクセスに必要なユーザ名を入力します。
- **[Password]**：ネットワークへのアクセスに必要なユーザ名に対応するパスワードを入力します。
- [SNMP Community]：ネットワークで SNMP が使用されている場合、ネットワーク管理者により用意された SNMP コミュニティ名を入力して、（同じくネットワーク管理者により用意された）SNMP データの属性を選択します。
- **[Current SSID List]（読み取り専用）**

ステップ 8　アクセス ポイントでサポートされる無線帯域について、次の [Network Configuration] 設定を入力します。2.4 GHz 無線と 5 GHz の無線には共通して次のオプションがあります。

- [SSID]：[SSID] 入力フィールドに SSID を入力します。SSID には、最大 32 文字の英数字を使用できます。
  - [Broadcast SSID in Beacon]：SSID を指定していないデバイスをアクセス ポイントにアソシエートできるようにするには、このチェックボックスをオンにします。このチェックボックスがオンになっている場合、アクセス ポイントは Broadcast SSID プローブ要求に応答すると共に、ビーコンと併せて自身の SSID をブロードキャストします。SSID をブロードキャストすると、SSID を指定していないデバイスがこの無線デバイスとアソシエートできます。このオプションは、パブリック スペースでゲストやクライアント デバイスが SSID を使用する場合に便利です。SSID をブロードキャストしない場合、クライアント デバイスの SSID がこの SSID と一致しない限り、そのクライアント デバイスは無線デバイスとアソシエートできません。無線デバイス ビーコンに組み込める SSID は 1 つだけです。
- [VLAN]：無線のVLAN を有効にするには、[Enable VLAN ID] オプション ボタンをクリックし、VLAN ID を 1 ～ 4095 の範囲で入力します。この VLAN をネイティブ VLAN として指定する場合は、[Native VLAN] チェックボックスをオンにします。VLAN を無効にするには、[No VLAN] オプション ボタンをクリックします。
- [Security]：SSID のセキュリティ設定を選択します。この設定は、[No Security] から [WPA] まで堅牢性の順に並んでいます。[WPA] が最も強力なセキュリティ設定です。[EAP Authentication] または [WPA] を選択する場合は、ネットワーク上の認証サーバの IP アドレス（RADIUS サーバの IP アドレス）と共有秘密（RADIUS サーバ シークレット）を入力します。

（注）　無線 LAN で VLAN を使用しない場合、複数の SSID に割り当てることのできるセキュリティ オプションが制限されます。詳細については、「VLAN の使用」セクション（4-12 ページ）を参照してください。

  - [No Security]：このセキュリティ設定では、暗号キーやキー管理は使用されず、Open 認証が使用されます。
  - [WEP Key]：このセキュリティ設定では、WEP 暗号化が必須となり、キー管理や Open 認証は使用されません。最大 4 つの WEP キー（つまり、キー 1、2、3、および 4）を指定できます。キーごとに値を入力し、128 ビットまたは 40 ビットのどちらであるかを指定します。
  - [EAP Authentication]：拡張認証プロトコル（EAP）認証では、認証サーバのサービスを通じてデータベースに対して認証されたユーザに無線アクセスを許可します。その上で、認証済みユーザに許可されているトラフィックを暗号化します。LEAP、PEAP、EAP-TLS、EAP-TTLS、EAP-GTC、EAP-SIM、およびその他の 802.1x/EAP ベースのプロトコルには、この設定を使用します。この設定では、暗号化必須 WEP、Open 認証 + EAP、ネットワーク EAP 認証、キー管理なし、RADIUS サーバ認証ポート 1645 が使用されます。RADIUS サーバおよび RADIUS サーバ シークレットを指定します。
  - [WPA]：Wi-Fi Protected Access（WPA）は、認証サーバのサービスを通じてデータベースに対して認証されたユーザへの無線アクセスを許可します。その上で、WEP で使用されるアルゴリズムよりも強力なアルゴリズムを使用して、認証済みユーザに許可されている IP トラフィックを暗号化します。このオプションを選択する前に、クライアントが WPA 認定済みであることを確認してください。この設定では、暗号スイート tkip、Open 認証 + EAP、ネットワーク EAP 認証、キー管理 WPA 必須、RADIUS サーバ認証ポート 1645 が使用されます。RADIUS サーバおよび RADIUS サーバ シークレットを指定します。

（注）　ここで使用されるセキュリティ設定の詳細については、「セキュリティ設定の概要」セクション（4-11 ページ）を参照してください。

- [Role in Radio Network]：ネットワークでのワイヤレス デバイスの役割を示すボタンをクリックします。ワイヤレス デバイスが有線 LAN に接続されている場合は、[Access Point (Root)] を選択します。アクセス ポイントが有線 LAN に接続されていない場合は、[Repeater (Non-Root)] を選択します。Airlink でサポートされている役割は、ルートのみです。無線ネットワークの異なる AP でサポートされる役割の詳細については、無線ネットワークの役割の設定（6-2 ページ）を参照してください。無線ネットワークでは、次の役割が有効です。
  - [Access Point]：ルート デバイス。クライアントからのアソシエーションを受け入れ、クライアントから無線 LAN までの無線トラフィックを仲介します。この設定は、どのアクセス ポイントにも適用できます。
  - [Repeater]：非ルート デバイス。クライアントからのアソシエーションを受け入れ、クライアントから、無線 LAN に接続中のルート アクセス ポイントまでの無線トラフィックを仲介します。この設定は、どのアクセス ポイントにも適用できます。
  - [Root Bridge]：非ルート ブリッジとのリンクを確立します。このモードでは、クライアントからのアソシエーションも受け入れます。
  - [Non-Root Bridge]：このモードでは、ルート ブリッジとのリンクを確立します。
  - [Install Mode]：アクセス ポイント/ブリッジを自動インストール モードに指定することで、最適な効率が得られるようにブリッジのリンクを位置合わせして調整できます。
  - [Workgroup Bridge]：ワークグループ ブリッジ モードの場合、アクセス ポイントは、Cisco Aironet アクセス ポイントまたはブリッジにアソシエートするクライアント デバイスとして機能します。他の無線クライアントがルート ブリッジまたはアクセス ポイントにアソシエートされていないと仮定すると、ワークグループ ブリッジは最大 254 のクライアントを持つことができます。
  - [Universal Workgroup Bridge]：アクセス ポイントを、シスコ以外のアクセス ポイントとアソシエートできるワークグループ ブリッジとして設定します。
  - [Client MAC]：ユニバーサル ワークグループ ブリッジに接続されているクライアントのイーサネット MAC アドレス。このフィールドが表示されるのは、ユニバーサル ワークグループ ブリッジ モードの場合のみです。
  - [Scanner]：ネットワーク モニタリング デバイスとして機能します。スキャナ モードでは、アクセス ポイントはクライアントからのアソシエーションを受け入れません。継続的にスキャンを行い、無線 LAN に接続中の他の無線デバイスから検出した無線トラフィックをレポートします。すべてのアクセス ポイントは、スキャナとして設定できます。
- [Optimize Radio Network for]：ワイヤレス デバイスの無線の設定済みの設定か、ワイヤレス デバイスの無線のカスタマイズされた設定のいずれかを選択します。
  - [Throughput]：ワイヤレス デバイスで処理されるデータ量が最大限に増えます。ただし、その範囲は縮小される可能性があります。
  - [Range]：ワイヤレス デバイスの範囲が最大限に拡張されます。ただし、スループットは減少する可能性があります。
  - [Default]：アクセス ポイントに使用するデフォルト値のセット。
  - [Custom]：[Network Interfaces] で入力した設定がワイヤレス デバイスに使用されます。[Custom] をクリックすると、次のネットワーク インターフェイスのページに移動します。
- [Aironet Extensions]：無線 LAN 上に Cisco Aironet ワイヤレス デバイスしかない場合は、この設定を有効にします。

- [Channel]：無線デバイスの無線のデフォルト チャネル設定は Least Congested です。この場合、無線デバイスは、起動時に最も混雑の少ないチャネルをスキャンして選択します。ただし、サイト調査の後も一貫したパフォーマンスが維持されるように、各アクセス ポイントにスタティック チャネル設定を指定することを推奨します。
  - 2.4 GHz 無線に対応するオプションは、Least Congested を設定したチャネル 1-2412、チャネル 2-2417、チャネル 3-2422、チャネル 4-2427、チャネル 5-2432、チャネル 6-2437、チャネル 7-2442、チャネル 8-2447、チャネル 9-2452、チャネル 10-2457、チャネル 11-2462 です。
  - 5 GHz 無線に対応するオプションは、動的周波数選択を設定したチャネル 36-5180、チャネル 40-5200、チャネル 44-5220、チャネル 48-5240、チャネル 149-5745、チャネル 153-5765、チャネル 157-5785、チャネル 161-5805、チャネル 165-5825 です。
- [Power]：[Power] ドロップダウン リストから電力レベルを選択します。
  - 2.4 GHz 無線に対応するオプションは、Maximum、22、19、16、13、10、7、および 4 です。
  - 5 GHz 無線に対応するオプションは、Maximum、14、11、8、5、および 2 です。

ステップ 9　[Apply] をクリックして設定値を保存します。

ステップ 10　[Network Interfaces] をクリックして [Network Interfaces Summary] ページを表示します。

ステップ 11　[Radio Interface] をクリックして [Network Interfaces: Radio Status] ページを表示します。

ステップ 12　[Settings] タブをクリックして無線インターフェイスの [Settings] ページを表示します。

ステップ 13　[Enable] をクリックして、無線を有効に設定します。

ステップ 14　[Apply] をクリックします。

これでワイヤレス デバイスは稼働しますが、ネットワークの運用およびセキュリティに関する要件を満たすための追加の設定が必要になる場合があります。設定の完了に必要な情報については、このマニュアルの該当する章を参照してください。

(注)　アクセス ポイントは、工場出荷時の設定に戻すことができます。それには、MODE ボタンを数秒間（ステータス LED がオレンジになるまで）押しながら、電源ジャックを抜いて再び差し込みます。

[Easy Setup] ページのデフォルト設定

表 4-1 は、[Express Setup] ページのデフォルト設定一覧です。

表 4-1　[Express Setup] ページのデフォルト設定

設定	デフォルト
Host Name	ap
Configuration Server Protocol	DHCP
IP Address	デフォルトで DHCP により割り当てられます。アクセス ポイントにおけるデフォルトの IP アドレスの動作については、「デフォルトの IP アドレスの動作」セクション（4-4 ページ）を参照してください。
IP Subnet Mask	デフォルトで DHCP により割り当てられます。DHCP が無効の場合、デフォルト設定は 255.255.255.224 です。

表 4-1　[Express Setup] ページのデフォルト設定（続き）

設定	デフォルト
デフォルト ゲートウェイ	デフォルトで DHCP により割り当てられます。DHCP が無効の場合、デフォルト設定は 0.0.0.0 です。
IPv6 Protocol	DHCP および Autoconfig
SNMP Community	defaultCommunity（Read-only）
VLAN	No VLAN
セキュリティ	No Security
Role in Radio Network（インストール済みの無線ごとに設定）	Access Point
Optimize Radio Network for	デフォルト
Aironet Extensions	Enable
チャネル	Least-Congested（2.4GHz の場合）および Dynamic Frequency Selection（5GHz の場合）
電源	最大

セキュリティ設定の概要

基本的なセキュリティ設定は、[Easy Setup] > [Radio Configuration] セクションで設定できます。このセクションに提供されているオプションを使用して、固有の SSID を作成し、4 つのセキュリティ タイプのいずれかを割り当てることができます。

ワイヤレス デバイスには最大 16 の SSID を作成できます。作成した SSID は、[Current SSID List] に表示されます。デュアル無線のワイヤレス デバイスでは、デフォルトで、作成した SSID が両方の無線インターフェイスで有効になります。

（注） Cisco IOS Release 12.4(23c)JA および 12.xxx には、デフォルトの SSID は存在しません。クライアント デバイスからアクセス ポイントにアソシエートする前に、SSID を設定しておく必要があります。

SSID には、最大 32 文字の英数字を使用でき、大文字と小文字が区別されます。

最初の文字として次の文字は使用できません。

- 感嘆符（!）
- ポンド記号（#）
- セミコロン（;）

次の文字は無効とされ、SSID には使用できません。

- プラス記号（+）
- 閉じ大カッコ（]）
- スラッシュ（/）
- 引用符（"）
- タブ
- 末尾のスペース

VLAN の使用

無線 LAN で VLAN を使用し、VLAN に SSID を割り当てる場合、[Express Security] ページの 4 つのセキュリティ設定のうちのいずれかを使用して複数の SSID を作成できます。ただし、無線 LAN で VLAN を使用しない場合、SSID に割り当てることのできるセキュリティ オプションは制限されます。[Express Security] ページでは暗号化設定と認証タイプがリンクしているためです。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 を無効にし、静的 WEP によって SSID を作成した場合、Wi-Fi Protected Access（WPA）認証によって追加の SSID を作成することはできません。これらは異なる暗号化設定を使用しているためです。SSID のセキュリティ設定が別の SSID と競合していることがわかった場合、1 つ以上の SSID を削除して競合を解消することができます。

SSID のセキュリティ タイプ

表 4-2 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 4-2　[Express Security Setup] ページのセキュリティ タイプ

セキュリティ タイプ	説明	有効になるセキュリティ機能
No Security	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 スペースで使用されている SSID だけに使用し、ネットワークへのアクセスを制限している VLAN に割り当てる必要があります。	なし。
Static WEP Key	このオプションは、[No Security] よりは安全です。ただし、静的 WEP キーは攻撃に対して脆弱です。この設定を行う場合、MAC アドレスに基づいてワイヤレス デバイスへのアソシエーションを制限することを考慮してください（第 16 章「MAC アドレス ACL を使用したアクセス ポイントへのクライアント アソシエーションの許可と禁止」を参照）。または、ネットワークに RADIUS サーバが存在しない場合、アクセス ポイントをローカルの認証サーバとして使用することを考慮してください（第 9 章「ローカル認証サーバとしてのアクセス ポイントの設定」を参照）。	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 4-2　[Express Security Setup] ページのセキュリティ タイプ(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 認証	このオプションでは、802.1X 認証(LEAP、PEAP、EAP-TLS、EAP-FAST、EAP-TTLS、EAP-GTC、EAP-SIM、その他 802.1X/EAP ベースの製品)が有効になります。 この設定では、暗号化必須、WEP、Open 認証 + EAP、ネットワーク EAP 認証、キー管理なし、RADIUS サーバ認証ポート 1645 を選択します。 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 認証によって動的暗号キーが提供されるため、WEP キーを入力する必要はありません。	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。 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 を使用したオープン認証を設定しないと、次の GUI 警告メッセージが表示されます。 「WARNING: Network EAP is used for LEAP authentication only.If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.」 CLI を使用している場合は、次の警告メッセージが表示されます。 「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」
WPA	Wi-Fi Protected Access(WPA)は、認証サーバのサービスを通じてデータベースに対して認証されたユーザへの無線アクセスを許可し、WEP で使用されるアルゴリズムよりも強力なアルゴリズムを使用して IP トラフィックを暗号化します。 この設定では、暗号スイート、TKIP、Open 認証 + EAP、ネットワーク EAP 認証、キー管理 WPA 必須、RADIUS サーバ認証ポート 1645 を選択します。 拡張認証プロトコル(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)。	WPA 認証が必須。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、WPA 対応でなければなりません。 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 を使用したオープン認証を設定しないと、次の GUI 警告メッセージが表示されます。 「WARNING: Network EAP is used for LEAP authentication only.If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.」 CLI を使用している場合は、次の警告メッセージが表示されます。 「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」

セキュリティ設定の制限事項

[Easy Setup] の [Radio Configuration] セクションでのセキュリティ設定は、基本セキュリティの簡易設定として設計されています。使用可能なオプションは、ワイヤレス デバイスのセキュリティ機能のサブセットです。[Express Security] ページの使用にあたっては、次の制限事項に留意してください。

- [No VLAN] オプションを選択している場合、静的 WEP キーを一度設定することができます。[Enable VLAN] を選択した場合は、静的 WEP キーを無効にする必要があります。
- SSID を編集することはできません。ただし、SSID を削除して再作成することはできます。
- 複数の認証サーバは設定できません。複数の認証サーバを設定する場合は、[Security Server Manager] ページを使用します。
- 複数の WEP キーは設定できません。複数の WEP キーを設定する場合は、[Security Encryption Manager] ページを使用します。
- ワイヤレス デバイス上にすでに設定されている VLAN に SSID を割り当てることはできません。既存の VLAN に SSID を割り当てる場合は、[Security SSID Manager] ページを使用します。
- 同一の SSID 上で認証タイプを組み合わせて設定することはできません（MAC アドレス認証と EAP 認証など）。認証タイプを組み合わせて設定する場合は、[Security SSID Manager] ページを使用します。

CLI の設定例

ここでは、各セキュリティ タイプを使用して SSID を作成するのと同じ働きをする CLI コマンドの例を示します。この項で取り上げる設定例は次のとおりです。

- 例：2.4GHz 無線の [No Security]（4-14 ページ）
- 例：2.4 GHz 無線の静的 WEP（4-15 ページ）
- 例：[EAP Authentication]（4-16 ページ）
- 例：2.4GHz 無線の WPA2（4-18 ページ）

例：2.4GHz 無線の [No Security]

次の例は、*no_security_ssid* という名前の SSID を作成し、その SSID をビーコンに組み込んで VLAN 10 に割り当ててから、VLAN 10 をネイティブ VLAN として選択した場合の設定の一部を示しています。

```
!
dot11 ssid no_security_ssid
   vlan 10
   authentication open
   guest-mode
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
 ssid no_security_ssid
 !
 antenna gain 0
 station-role root
!
```

```
interface Dot11Radio0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
!
interface Dot11Radio1.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
```

例：2.4 GHz 無線の静的 WEP

次の例は、*static_wep_ssid* という名前の SSID を作成し、その SSID をビーコンから除外して VLAN 20 に割り当て、キー スロットとして 3 を選択し、128 ビット キーを入力した場合の設定の一部を示しています。

```
!
dot11 ssid static_wep_ssid
   vlan 20
   authentication open
!
!
!
encryption vlan 20 key 3 size 128bit 7 76031220D71D63394A6BD63DE57F transmit-key
encryption vlan 20 mode wep mandatory
 !
ssid static_wep_ssid
!
!
interface Dot11Radio0.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 spanning-disabled
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
!
interface Dot11Radio0.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
```

```
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption vlan 20 key 3 size 128bit 7 E55F05382FE2064B7C377B164B73 transmit-key
encryption vlan 20 mode wep mandatory
 !
ssid static_wep_ssid
!
!
interface Dot11Radio1.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 spanning-disabled
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
!
interface Dot11Radio1.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface GigabitEthernet0.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 spanning-disabled
no bridge-group 20 source-learning
!
interface GigabitEthernet0.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
```

例：[EAP Authentication]

次の例は、*eap_ssid* という名前の SSID を作成し、その SSID をビーコンから除外して、SSID を VLAN 30 に割り当てた場合の設定の一部を示しています。

(注)　無線クライアントで EAP-FAST を使用していて、設定の中に Open 認証 + EAP を含めていないと、次の警告メッセージが表示されます。

「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」

```
dot11 ssid eap_ssid
   vlan 30
   authentication open eap eap_methods
   authentication network-eap eap_methods
!
dot11 guest
!
username apuser password 7 096F471A1A0A
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
 encryption vlan 30 mode wep mandatory
 !
 ssid eap_ssid
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
```

```
interface Dot11Radio1.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 spanning-disabled
 no bridge-group 30 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server 10.10.11.100
 address ipv4 10.10.11.100 auth-port 1645 acct-port 1646
 key 7 00271A150754
!
bridge 1 route ip
```

例：2.4GHz 無線の WPA2

次の例は、*wpa_ssid* という名前の SSID を作成し、その SSID をビーコンから除外して、SSID を VLAN 40 に割り当てた場合の設定の一部を示しています。

```
aaa new-model
!
aaa group server radius rad_eap
 server name 10.10.11.100
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
```

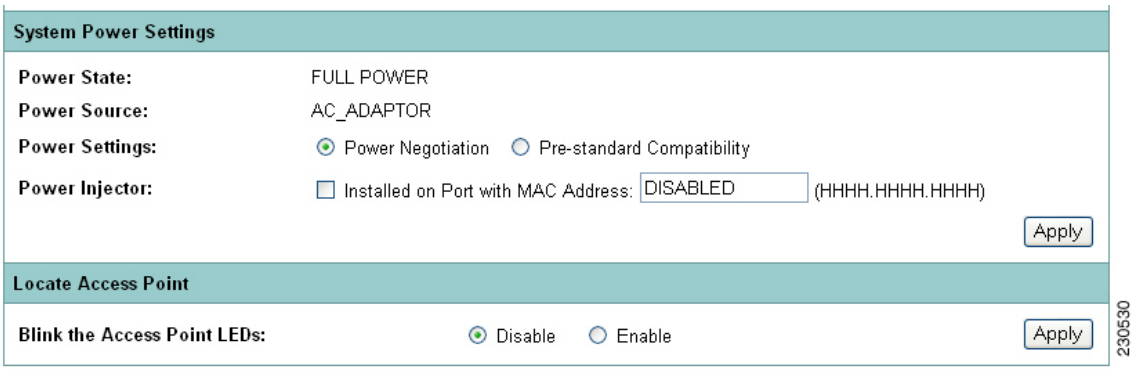
```
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
aaa session-id common
!
dot11 ssid wpa_ssid
   vlan 40
   authentication open eap eap_methods
   authentication network-eap eap_methods
    authentication key-management wpa version 2
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
encryption vlan 40 mode ciphers aes-ccm
 !
 ssid wpa_ssid
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 spanning-disabled
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
```

```
interface Dot11Radio1.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 spanning-disabled
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 spanning-disabled
 no bridge-group 40 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server 10.10.11.100
 address ipv4 10.10.11.100 auth-port 1645 acct-port 1646
 key 7 0....F175804
!
```

アクセス ポイントでのシステム電力の設定

AP 1040、AP 802、AP 1140、AP 1550、AP 1600、AP 2600、AP 3500、AP 3600、および AP 1260 は、ユニットの接続先電源が十分に電力を供給していないことを感知すると、無線インターフェイスをディセーブルにします。使用している電源によっては、アクセス ポイントの設定で電源のタイプを入力する必要がある場合があります。Web ブラウザ インターフェイスで [Software] > [System Configuration] ページを選択し、電力オプションを選択します。図 4-1 は、[System Configuration] ページの [System Power Settings] セクションを示しています。

図 4-1　[System Software: System Configuration] ページの電力オプション



AC 電源アダプタの使用

AC 電源アダプタを使用してアクセス ポイントに電力を供給する場合は、アクセス ポイントの設定を調整する必要はありません。

IEEE 802.3af 電力ネゴシエーションのスイッチ機能の使用

1040、1140、および 1260 アクセス ポイントに Power over Ethernet（PoE）を供給するスイッチを使用していて、そのスイッチが IEEE 802.3af 電力ネゴシエーション標準に対応している場合、[System Software: System Configuration] ページで [Power Negotiation] を選択します。

IEEE 802.3af 電力ネゴシエーションに対応していないスイッチの使用

1040 または 1140 アクセス ポイントに Power over Ethernet（PoE）を供給するスイッチを使用していて、そのスイッチが IEEE 802.3af 電力ネゴシエーション標準に対応していない場合は、[System Software: System Configuration] ページで [Pre-Standard Compatibility] を選択します。

電力インジェクタの使用

電力インジェクタを使用して 1040、1140、または 1260 アクセス ポイントに電力を供給している場合、[System Software: System Configuration] ページで [Power Injector] を選択し、アクセス ポイントを接続しているスイッチ ポートの MAC アドレスを入力します。

dot11 extension power native コマンド

有効になっている場合、**dot11 extension power native** によって、無線で使用中のパワー テーブルが IEEE 802.11 テーブルからネイティブ パワー テーブルへシフトされます。無線装置は、このテーブル値を CISCO-DOT11-1F-MIB の NativePowerTable および NativePowerSupportedTable から取り出します。[Native Power] テーブルは、-1dBm レベルをサポートする Cisco Aironet の無線機器で使用できるよう、電源を -1dBm 近辺に低く設定するよう厳密に設計されています。

802.11ac のサポート

802.11ac は 802.11 の次世代ワイヤレス標準です。高いスループットを実現し、5 GHz 帯域で動作するように設計されています。802.11ac は 3700、2700、および 1700 シリーズ アクセス ポイントでサポートされています。802.11ac 無線が完全に機能するには、802.11n 無線が必要です。802.11n 無線をシャットダウンすると、802.11ac の機能に影響します。

802.11ac のチャネル幅

802.11n 無線と 802.11ac 無線は、同じ帯域で動作します。ただし、802.11n のチャネル帯域幅のほうを低く設定した場合に限り、それぞれのチャネル帯域幅を個別に設定できます。サポートされるチャネル帯域幅の組み合わせの詳細については、表 4-3を参照してください。

表 4-3　　サポートされるチャネル帯域幅の組み合わせ

802.11n のチャネル帯域幅	802.11ac のチャネル帯域幅
20	20
20	40
20	80
40	40
40	80

オフ チャネル スキャンまたは伝送はサポートされません。802.11ac 無線でオフ チャネル スキャン機能を利用するには、802.11n 無線が必要です。

たとえば、80 Mhz のチャネル幅を設定するには次のようにします。

```
ap# configure terminal
ap(config)# interface dot11Radio 1
ap(config-if)# channel width 80
ap(config-if)# end
```

802.11ac の電源管理

3700、2700、および 1700 の 802.11ac シリーズ アクセス ポイントは、Power over Ethernet（PoE）ソース、ローカル電源、またはパワー インジェクタで電力供給できます。AP が PoE から電力供給される場合、AP にはインライン電源から供給される場合より多くの電力が必要になるため、AP はソース（PoE+（802.3at）または PoE（802.3af））に応じて特定の無線設定を調整します。

たとえば、PoE+（802.3at）から電力供給される 3700 シリーズ AP は両方の無線に 4x4:3 設定を指定します。一方、PoE（802.3af）から電力供給される場合は、両方の無線に 3x3:3 設定を指定します。以下の表を参照してください。

ヒント　たとえば 4x4:3 の無線設定は、4 台のトランスミッタと 4 台のレシーバで 3 つの空間ストリームに対応できることを意味します。

(注)　AP が高電力の PoE または低電力（15.4W）の電源のどちらで動作しているかを判別するには、AP の GUI で [Home] ページを表示します。AP が低電力で動作している場合は、[Home:Summary Status] に次の警告が表示されます。

Due to insufficient inline power.Upgrade inline power source or install power injector.

屋外メッシュ製品を除くすべてのアクセス ポイントは、Power over Ethernet 対応です。Power over Ethernet を使用する無線を 2 台使用するアクセス ポイントは、完全に機能し、すべての機能をサポートします。使用可能なさまざまな電源管理オプションについては、表 4-4を参照してください。

表 4-4　電源に基づくインライン パワー オプション

給電規格	説明	AP の機能	PoE バジェット（ワット）[1]	802.3af	E-PoE	802.3at PoE+ PWRINJ4
PoE + 802.3at	AP3700 初期状態	4x4:3（2.4/5 GHz）	16.1	No	Yes	Yes
PoE 802.3af	AP3700 初期状態	3x3:3（2.4/5 GHz）	15.4	Yes	該当なし	該当なし
PoE 802.3at	AP2700 初期状態	3x4:3（2.4/5 GHz）および補助イーサネット ポート使用可能	16.8	No	No	Yes
PoE 802.3af	AP2700 初期状態	3x4:3（5 GHz）、2x2:2（2.4 GHz）および補助イーサネット ポート使用可能	15.4	Yes	Yes	該当なし

1. PSE（スイッチまたはインジェクタ）で必要な電力です。

802.11n と 802.11ac は、802.11n に設定された電力レベルを使用します。802.11ac に個別に電力レベルを設定することはできません。

CLI を使用した IP アドレスの割り当て

ワイヤレス デバイスを有線 LAN に接続すると、ワイヤレス デバイスは、自動的に生成される Bridge Virtual Interface（BVI; ブリッジ仮想インターフェイス）を使用してネットワークにリンクします。ネットワークは、ワイヤレス デバイスのイーサネットと無線ポートの IP アドレスを個別に記録せずに、BVI を使用します。

CLI を使用してワイヤレス デバイスに IP アドレスを割り当てる場合、そのアドレスを BVI に割り当てる必要があります。ワイヤレス デバイスの BVI に IP アドレスを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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	**interface bvi1**	BVI 対応のインターフェイス コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 3	**ip address** *address mask*	BVI に IP アドレスとアドレス マスクを割り当てます。 (注)　Telnet セッションを使用してワイヤレス デバイスに接続している場合は、BVI に新しい IP アドレスを割り当てると、このワイヤレス デバイスへの接続が失われます。Telnet を使用してワイヤレス デバイスの設定を続ける必要がある場合は、新しい IP アドレスで、そのワイヤレス デバイスへの別の Telnet セッションを開始します。

Telnet セッションを使用した CLI へのアクセス

Telnet セッションを使用して CLI にアクセスする手順は、次のとおりです。これらの手順は、Microsoft Windows を実行する PC で Telnet 端末アプリケーションを使用する場合を想定しています。オペレーティング システムの詳細な操作方法については、ご使用の PC の操作マニュアルを確認してください。

ステップ 1　[Start] > [Programs] > [Accessories] > [Telnet] の順に選択します。

[Accessories] メニューに Telnet がない場合は、[Start] > [Run] の順に選択し、入力フィールドに **Telnet** と入力して Enter を押します。

ステップ 2　[Telnet] ウィンドウが表示されたら、[Connect] をクリックして、[Remote System] を選択します。

(注)　Windows 2000 では、[Telnet] ウィンドウにドロップダウン リストが表示されません。Windows 2000 で Telnet セッションを起動するには、**open** と入力してから、ワイヤレス デバイスの IP アドレスを入力します。

ステップ 3　[Host Name] フィールドにワイヤレス デバイスの IP アドレスを入力して、[Connect] をクリックします。

802.1X サプリカントの設定

dot1x 認証サーバ/クライアントの関係には、従来、ネットワーク デバイスと PC クライアントがそれぞれ使用されていました。これは、ネットワークへのアクセスに認証が必要なのは PC ユーザであるためです。しかし、無線ネットワークになってから、今までの認証サーバ/クライアントの関係とは違う手法が取り入れられました。まず、プラグが抜かれる可能性や、ネットワーク接続が部外者から使用される可能性がある公衆の場にアクセス ポイントを設置できるようになりました。次に、リピータ アクセス ポイントを無線ネットワークに組み込む場合、そのリピータ アクセス ポイントをクライアントと同様にルート アクセス ポイントで認証させる必要があります。

サプリカントの設定には、次の 2 段階があります。

- クレデンシャル プロファイルを作成して設定する
- このクレデンシャルをインターフェイスまたは SSID に適用する

どちらの手順を先に完了してもかまいませんが、サプリカントを使用する前に完了しておく必要があります。

クレデンシャル プロファイルの作成

特権 EXEC モードから、次の手順に従って 802.1X クレデンシャル プロファイルを作成します。

	コマンド	目的
ステップ 1	**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	**dot1x credentials** *profile*	dot1x クレデンシャル プロファイルを作成し、dot1x クレデンシャルのコンフィギュレーション サブモードに入ります。
ステップ 3	**anonymous-id** *description*	(任意):使用する匿名 ID を入力します。
ステップ 4	**description** *description*	(任意):クレデンシャル プロファイルの名称を入力します。
ステップ 5	**username** *username*	認証ユーザ ID を入力します。
ステップ 6	**password {0 | 7 | LINE}**	クレデンシャルに、暗号化されていないパスワードを入力します。 **0**:続けて、暗号化されていないパスワードを入力します。 **7**:続けて、非表示のパスワードを入力します。非表示のパスワードは、すでに保存済みの設定を適用する場合に使用します。 **LINE**:暗号化されていない(クリア テキストの)パスワード。 (注)　暗号化されていないテキストとクリア テキストは同じものです。クリア テキストのパスワードの後に 0 を入力してください。または、0 を省略してクリア テキストのパスワードを入力してください。
ステップ 7	**pki-trustpoint** *pki-trustpoint*	(オプション。EAP-TLS だけに使用):デフォルトの PKI トラストポイントを入力します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**copy running config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

パラメータを無効にするには、**dot1x credentials** コマンドの **no** 形式を使用します。

次に、クレデンシャル プロファイルの作成例を示します。名称を *test*、ユーザ名を *Cisco*、暗号化されていないパスワードを *Cisco* とします。

```
ap>enable
Password:xxxxxxx
ap#config terminal
Enter configuration commands, one per line.End with CTRL-Z.
ap(config)# dot1x credentials test
ap(config-dot1x-creden)#username Cisco
ap(config-dot1x-creden)#password Cisco
ap(config-dot1x-creden)#exit
ap(config)#
```

インターフェイスまたは SSID へのクレデンシャルの適用

クレデンシャル プロファイルの適用方法は、インターフェイスに対しても SSID に対しても同じです。

クレデンシャル プロファイルを有線ポートに適用する方法

特権 EXEC モードから、次の手順に従ってクレデンシャルをアクセス ポイントの有線ポートに適用します。

	コマンド	目的
ステップ 1	**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	**interface gigabitethernet 0**	アクセス ポイントのギガビット イーサネット ポートのインターフェイス コンフィギュレーション モードを開始します。 (注)　**interface fa0** を使用してギガビット イーサネット コンフィギュレーション モードを開始することもできます。
ステップ 3	**dot1x credentials** *profile name*	すでに作成しておいたクレデンシャル プロファイル名を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

次の例では、アクセス ポイントのギガビット イーサネット ポートに、クレデンシャル プロファイル *test* を適用します。

```
ap>enable
Password:xxxxxxx
ap#config terminal
Enter configuration commands, one per line.End with CTRL-Z.
ap(config)#interface Gig0
ap(config-if)#dot1x credentials test
ap(config-if)#end
```

アップリンクに使用する SSID にクレデンシャル プロファイルを適用する方法

無線ネットワーク内にリピータ アクセス ポイントがあり、ルート アクセス ポイントで 802.1X サプリカントを使用している場合、リピータがルート アクセス ポイントとアソシエートして認証に使用する SSID に、802.1X サプリカントのクレデンシャルを適用する必要があります。

特権 EXEC モードから、次の手順に従って、アップリンクに使用する SSID にクレデンシャルを適用します。

	コマンド	目的
ステップ 1	**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	**dot11 ssid** *ssid*	802.11 SSID と入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。 (注)　先頭の文字に !、#、; は使用できません。 +、]、/、"、TAB、末尾のスペースは、SSID で無効な文字です。
ステップ 3	**dot1x credentials** *profile*	設定済みのクレデンシャル プロファイル名を入力します。

	コマンド	目的
ステップ 4	**end**	dot1x クレデンシャルの設定サブモードを終了します。
ステップ 5	**copy running config startup-config**	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、*test* という名前のクレデンシャル プロファイルを適用しています。リピータ アクセス ポイント上の適用先 SSID を *testap1* としています。

```
repeater-ap>enable
Password:xxxxxxx
repeater-ap#config terminal
Enter configuration commands, one per line.End with CTRL-Z.
repeater-ap(config-if)#dot11 ssid testap1
repeater-ap(config-ssid)#dot1x credentials test
repeater-ap(config-ssid)#end
repeater-ap(config)
```

EAP 方式プロファイルの作成と適用

EAP 方式リストを設定して、サプリカントを有効にし、特定の EAP 方式を認識するオプションも用意されています。「802.1X サプリカントの EAP 方式プロファイルの作成と適用」セクション (11-18 ページ) を参照してください。

IPv6 の設定

IPv6 は、膨大な数のアドレスを提供するために開発された、最新のインターネット プロトコルです。IPv4 では 32 ビットのアドレスが使用されますが、このプロトコルは 128 ビットのアドレスを使用します。

無線ネットワークでの展開では多数の IP 無線デバイスやスマートフォンを使用することから、128 ビットのアドレス形式を使用する IPv6 のアドレス空間では、3.4 x 1038 個のアドレスをサポートできます。

IPv6 アドレスは、x:x:x:x:x:x:x:x のようにコロン (:) で区切られた一連の 16 ビットの 16 進フィールドで表されます。

IPv6 アドレス タイプには、次の 3 つのタイプがあります。

- ユニキャスト

  Cisco IOS ソフトウェアでは、次の IPv6 ユニキャスト アドレス タイプがサポートされます。

  - 集約可能グローバル アドレス

    集約可能グローバル ユニキャスト アドレスは、インターネットの IPv6 部分でグローバルにルーティングおよび到達することができます。これらのグローバル アドレスは、アドレス形式のプレフィックス 001 で識別されます。

  - リンクローカル アドレス

    リンクローカル アドレスは、リンクローカル プレフィックス FE80::/10 (1111 1110 10) を使用して自動的にインターフェイスに設定されます。インターフェイス ID は、Modified EUI-64 形式になります。

- エニーキャストを使用できるのは、ルータだけです。ホストでは使用できません。エニーキャスト アドレスは、IPv6 パケットの送信元アドレスには使用しないでください。

- マルチキャスト アドレスは、指定のネットワーク サービスにマルチキャストされるように意図されたフレームを処理するホスト グループの論理 ID です。IPv6 のマルチキャスト アドレスは、プレフィックス FF00::/8 (1111 1111) を使用します。

  IPv6 設定では、次のマルチキャスト グループを使用します。

  - 送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00::/104
  - 全ノード リンクローカル マルチキャスト グループ FF02::1
  - 全ルータ リンクローカル マルチキャスト グループ FF02::2

表 4-5に、IPv6 アドレスのタイプと形式を示します。

表 4-5　　IPv6 アドレスの形式

IPv6 アドレス タイプ	優先形式	圧縮形式
ユニキャスト	2001:0:0:0:DB8:800:200C:417A	2001::DB8:800:200C:417A
マルチキャスト	FF01:0:0:0:0:0:0:101	FF01::101
ループバック	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

サポートされるモード

- ルート
- ルート ブリッジ
- 非ルート ブリッジ
- Repeater
- WGB

サポートされないモード

- スペクトル モード
- Monitor mode

IPv6 アドレスを有効にするには、特権 EXEC モードから、次のコマンドを使用します。

- ap(config)# **int bv1**
- ap(config-if)# **ipv6 address**

ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

ステートレス自動設定をイネーブルにするには、特権 EXEC モードから、次のコマンドを使用します。

ap(config-if)# **ipv6 address autoconfig**

他の IPv6 アドレスをインターフェイスに割り当てることなくリンクローカル アドレスを設定するには、特権 EXEC モードから、次のコマンドを使用します。

ap(config-if)# **ipv6 address ipv6-address link-local**

サイトローカル アドレスまたはグローバル アドレスをインターフェイスに割り当てるには、特権 EXEC モードから、次のコマンドを使用します。

ap(config-if)# **ipv6 address ipv6-address [eui-64]**

(注)　オプションの eui-64 キーワードは、アドレスの下位 64 ビットに Modified EUI-64 インターフェイス ID を使用する場合に使用します。

DHCPv6 アドレスの設定

DHCPv6 は、IPv6 ネットワークで動作するために必要な IP アドレス、IP プレフィックス、およびその他のコンフィギュレーションを使用して IPv6 ホストを設定するために使用するネットワーク プロトコルです。DHCPv6 クライアントは、迅速な 2 つのメッセージ交換（送信要求、応答）または通常の 4 つのメッセージ交換（送信要求、アドバタイズ、要求、応答）によって、サーバから設定パラメータを取得します。デフォルトでは、4 つのメッセージ交換が使用されます。rapid-commit オプションをクライアントとサーバの両方でイネーブルにすると、2 つのメッセージ交換が使用されます。

アクセス ポイントの DHCPv6 クライアントをイネーブルにするには、特権 EXEC モードから、次のコマンドを使用します。

- ap# c**onf t**
- ap(config)**# int bv1**
- ap(config)**# ipv6 address dhcp rapid-commit(optional)**

自律 AP は、ステートフルおよびステートレス DHCPv6 アドレッシングの両方をサポートします。

ステートフル アドレッシング

ステートフル アドレッシングでは、DHCP サーバが使用されます。DHCP クライアントはステートフル DHCPv6 アドレッシングを使用して IP アドレスを取得します。

ステートフル アドレッシングを設定するには、特権 EXEC モードから、次のコマンドを使用します。

ap(config)**# ipv6 address dhcp**

ステートレス アドレッシング

ステートレス アドレッシングでは、DHCP サーバを使用せずに IP アドレスを取得します。DHCP クライアントは、ルータ アドバタイズメントに基づいて、自身の IP アドレスを自動的に設定します。

ステートレス アドレッシングを設定するには、特権 EXEC モードから、次のコマンドを使用します。

ap(config)# **ipv6 address autoconfig**

IPv6 ネイバー探索

IPv6 ネイバー探索プロセスでは、同じネットワーク上のネイバーのリンク層アドレスを決定するために、ICMP メッセージと送信要求ノード マルチキャスト アドレスを使用します。

IPv6 ネイバー探索を設定するには、特権 EXEC モードから、次のコマンドを使用します。

コマンド	目的
ipv6 nd ?	ネイバー探索プロトコルを設定します。
ipv6 nd ns-interval *value*	このコマンドは、ブリッジ グループ仮想インターフェイス（BVI）に対してのみ有効です。 インターフェイスに IPv6 ネイバー送信要求の再送信する間隔を設定します。
ipv6 nd reachable-time *value*	リモートの IPv6 ノードに到達可能な時間を設定します。
ipv6 nd dad attempts *value*	このコマンドは、ブリッジ グループ仮想インターフェイス（BVI）に対してのみ有効です。 ユニキャスト IPv6 アドレスで、重複アドレス検出を行う際に連続して送信するネイバー送信要求メッセージの数を設定します。
ipv6 nd dad time *value*	重複アドレス検出の際の IPv6 ネイバー送信要求の送信間隔を設定します。
ipv6 nd autoconfig default-router	このコマンドは、ブリッジ グループ仮想インターフェイス（BVI）に対してのみ有効です。 ネイバー検出によって導出されるデフォルト ルータへのデフォルト ルートを設定します。
ipv6 nd autoconfig prefix	このコマンドは、ブリッジ グループ仮想インターフェイス（BVI）に対してのみ有効です。 次の定期ルータ アドバタイズメントの待機中に遅延を発生させないようにルータ アドバタイズメントの送信要求を行うルータ送信要求メッセージを設定します。
ipv6 nd cache expire *expire-time-in-seconds*	IPv6 ネイバー探索キャッシュ エントリの期限が切れるまでの時間を設定します。
ipv6 nd cache interface-limit size [log rate]	指定したインターフェイスにネイバー探索キャッシュ制限を設定します。
ipv6 nd na glean	このコマンドは、ブリッジ グループ仮想インターフェイス（BVI）に対してのみ有効です。 非送信要求ネイバー アドバタイズメントからエントリを収集するネイバー探索を設定します。
ipv6 nd nsf {**convergence** *time-in-seconds*| **dad** [**suppress**]| **throttle** *resolutions*}	IPv6 ネイバー探索ノンストップ フォワーディングを設定します。コンバージェンス時間を秒単位で設定したり（10 ～ 600 秒）、重複アドレス検出（DAD）を抑止したり、ノンストップ フォワーディング（NSF）で使用する解決の数を設定したりすることもできます。
ipv6 nd nud limit *limit*	ネイバー到達不能検出（NUD）の再送信回数を設定し、未解決の再送信回数の制限を設定します。
ipv6 nd resolution data limit *limit-in-packets*	キュー内でネイバー探索（ND）解決を待機するデータ パケット数の制限を設定します。
ipv6 nd route-owner	ネイバー探索で学習したルートを「ND」ステータスのルーティング テーブルに挿入し、ND 自動構成動作を有効にします。

IPv6 アクセス リストの設定

IPv6 アクセス リスト（ACL）は、トラフィックをフィルタリングしてルータへのアクセスを制限するために使用します。IPv6 プレフィックスのリストを使用して、ルーティング プロトコル アップデートをフィルタリングします。

アクセス リストをグローバルに設定してインターフェイスに割り当てるには、特権 EXEC モードから、次のコマンドを使用します。

- ap(config)# **ipv6 access-list** *acl-name*

IPv6 アクセス リストの設定には、特権 EXEC モードから、表 4-6に記載されているコマンドを使用できます。

表 4-6　IPv6 アクセス リストの設定コマンド

コマンド	目的
default	コマンドをデフォルト値に設定します。
deny	拒否するパケットを指定します。
evaluate	アクセス リストを評価します。
exit	アクセス リスト コンフィギュレーション モードを終了します。
no	コマンドを無効にするか、そのデフォルトに設定します。
permit	転送するパケットを指定します。
remark	アクセス リスト エントリのコメントを設定します。
sequence	このエントリのシーケンス番号を設定します。

グローバルに設定された ACL をレイヤ 3 インターフェイスの発信トラフィックと着信トラフィックに割り当てるには、特権 EXEC モードから、次のコマンドを使用します。

- ap(config)# **interface** *interface*
- ap(config)# **ipv6 traffic-filter** *acl-name* **in/out**

RADIUS の設定

RADIUS サーバは、次の 3 つの機能を提供するバックグラウンド プロセスです。

- ネットワークへのアクセスを許可する前に、ユーザを認証する
- 特定のネットワーク サービスに対してユーザを許可する
- 特定のネットワーク サービスの使用状況を把握する

RADIUS によるアクセス ポイントへのアクセスの制御（5-11 ページ）を参照してください。

IPv6 WDS のサポート

WDS およびインフラストラクチャ アクセス ポイントは、WLAN Context Control Protocol（WLCCP）と呼ばれるマルチキャスト プロトコルで通信します。

Cisco IOS Release 15.2(4)JA は、IPv6 アドレスを使用して、WDS とアクセス ポイント間の通信をサポートします。WDS はデュアル スタックで動作します。つまり、IPv4 と IPv6 の両方の登録を受け入れます。

IPv6 WDS AP 登録

最初のアクティブな IPv6 アドレスが WDS の登録に使用されます。表 4-7に、IPv6 WDS AP 登録プロセスでのさまざまなシナリオを示します。

表 4-7　IPv6 WDS-AP 登録

	WDS			AP			
シナリオ	デュアル	IPv6	IPv4	デュアル	IPv6	IPv4	通信モード
1	Yes			yes			IPv6
2	Yes				yes		IPv6
3	Yes					yes	IPv4
4		yes		yes			IPv6
5		yes			yes		IPv6
6		yes				yes	失敗
7			yes	yes			IPv4
8			yes		yes		失敗
9			yes			yes	IPv4

（注）　IPv4 および IPv6 のアクセス ポイント間の 11r ローミングは、MDIE が異なるため、サポートされません。AP および WDS は両方とも、BV1 の最初のアクティブな IPv6 アドレスを使用して登録し、アドバタイズします。リンクローカルは登録に使用されません。

CDPv6 サポート：

CDP は、隣接するネイバーのデバイス ID、機能、MAC アドレス、IP アドレスまたはデュプレックスに関する情報を取得するために使用されるレイヤ 2 プロトコルです。各 CDP 対応デバイスは、隣接するネイバーに自身の情報を送信します。ネイティブ IPv6 の一部として、アクセス ポイントはアドレス TLV の一部と併せて自身の IPv6 アドレスを cdp メッセージで送信すると共に、隣接スイッチから取得した IPv6 アドレス情報を解析します。

次のコマンドは、接続されている IPv6 ネイバーを表示します。

ap# **show cdp neighbors detail**

RA フィルタリング

RA フィルタリングにより、無線クライアントから送信された RA をドロップすることで、IPv6 ネットワークのセキュリティが強化されます。RA フィルタリングは、設定に誤りがあるか、悪意のある IPv6 クライアント（正規の IPv6 ルータよりも優先される高い優先順位が設定されている場合がよくあります）が、ネットワークに接続できないようにします。いずれの場合も、IPv6 RA はある時点でドロップされ、悪意または設定の誤りがある IPv6 デバイスから、他の無線デバイスやアップストリームにある有線ネットワークが保護されます。

ただし、RA フィルタリングはアップリンクの方向ではサポートされません。

アクセス ポイントの自動設定

自律アクセス ポイントの Autoconfig 機能を使用することで、AP は自身の設定を Secure Copy Protocol（SCP）サーバから定期的にダウンロードするようになります。Autoconfig 機能が有効にされている場合、AP は事前に設定された時点でサーバから設定情報ファイルをダウンロードし、その設定を適用します。それと同時に、次回の設定のダウンロードもスケジュールされます。

（注）　設定が最後にダウンロードした設定と変わらない場合、AP はその設定を適用しません。

Autoconfig の有効化

Autoconfig を有効にする手順は次のとおりです。

ステップ 1　設定情報ファイルの準備

ステップ 2　環境変数の有効化

ステップ 3　設定情報ファイルのダウンロードのスケジューリング

設定情報ファイルの準備

Autoconfig 対応の AP は、SCP サーバから構成情報ファイルをダウンロードします。設定情報ファイルは、次の情報が含まれる XML ファイルです。

- 新規スタートアップ コンフィギュレーション。
- 絶対時間および範囲の値。AP は、次回の情報ファイルのダウンロードを、この絶対時間に 0 から範囲値までの間の乱数値を足した時刻にスケジュールします。

設定情報ファイルの形式は次のとおりです。

```
<?xml version="1.0" encoding="UTF-8"?>
<l2tp_cfg>
    <cfg_fetch_start_time>Absolute Time</cfg_fetch_start_time>
    <cfg_fetch_time_range>Random Jitter</cfg_fetch_time_range>
    <cfg_fetch_config>
        <![CDATA[
        <Startup config>
        ]]>
    </cfg_fetch_config>
```

```
</l2tp_cfg>
```

以下で、設定情報ファイルで使用される xml タグについて説明します。

XML タグ	目的
cfg_fetch_start_time	このタグには、絶対時間が DAY HH:MM の形式で含まれます。 • DAY には、Sun、Mon、Tue、Wed、Thu、Fri、Sat、All のいずれかを設定できます。 • HH は時間を表します。0 ～ 23 の数値を設定できます。 • MM は分を表します。0 ～ 59 の数値を設定できます。 例：「Sun 10:30」、「Thu 00:00」、「All 12:40」
cfg_fetch_time_range	次回の情報ファイルのダウンロード時刻をランダム化するために、0 からこの値までの間の乱数値が開始時刻に加算されます。
cfg_fetch_config	このタグには、AP の次のスタートアップ コンフィギュレーションが含まれます。

環境変数の有効化

設定情報ファイルを SCP サーバに準備して保管した後は、次の環境変数を設定する必要があります。

環境変数	目的
AUTO_CONFIG_AP_FUNCTIONALITY	Autoconfig を有効にするには、この変数を「YES」に設定する必要があります。
AUTO_CONFIG_USER	SCP サーバにアクセスするためのユーザ名
AUTO_CONFIG_PASSWD	SCP サーバにアクセスするためのパスワード
AUTO_CONFIG_SERVER	SCP サーバのホスト名/IP
AUTO_CONFIG_INF_FILE	SCP サーバからフェッチする設定情報ファイルの名前

環境変数を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

dot11 autoconfig add *environment-variable-name* **val** *value.*
次に例を示します。

```
dot11 autoconfig add AUTO_CONFIG_SERVER val 206.59.246.199
```

設定情報ファイルのダウンロードのスケジューリング

環境変数を設定した後、SCP サーバからの設定情報ファイルのダウンロードをスケジュールする必要があります。手順は次のとおりです。

ステップ 1　AP のクロック時刻を SNTP（Simple Network Time Protocol）サーバに同期させる必要があります。SNTP サーバを設定するには、コマンド **sntp server** *sntp-server-ip* を使用します。ここで、*sntp-server-ip* は SNTP サーバの IP アドレスです。

ステップ 2　AP に正確な時刻を使用させるには、正確なタイム ゾーンを設定する必要があります。それには、コマンド **clock timezone** *TIMEZONE HH MM* を使用します。

- TIMEZONE はタイム ゾーンの名前です（IST、UTC など）。
- HH はタイムゾーンからの時間のオフセットです。
- MM は、タイムゾーンからの分のオフセットです

ステップ 3　SCP サーバから設定情報ファイルをダウンロードできなかった場合にダウンロードを再試行するまでの時間間隔を設定できます。この再試行間隔を設定するには、コマンド **dot11 autoconfig download retry interval min** *MIN* **max** *MAX* を使用します。

- MIN は再試行間隔の最小秒数です。
- MAX は再試行間隔の最大秒数です。ダウンロードが失敗するたびに、再試行間隔は 2 倍になります。ただし、再試行間隔が MAX に達すると、再試行は停止されます。

ブート ファイルを使用した Autoconfig の有効化

ブート ファイルで次のコマンドを DHCP IP 設定の一部として指定することでも、Autoconfig を有効にできます。

DHCP/BootTP サーバから返されるブート ファイルには、次の例に示す形式の内容が含まれます。

```
dot11 autoconfig add env var AUTO_CONFIG_AP_FUNCTIONALITY val YES
dot11 autoconfig add env var AUTO_CONFIG_USER val someusername
dot11 autoconfig add env var AUTO_CONFIG_PASSWD val somepasswd
dot11 autoconfig add env var AUTO_CONFIG_SERVER val scp.someserver.com
dot11 autoconfig add env var AUTO_CONFIG_INF_FILE val some_inf_file.xml
sntp server 208.210.12.199
clock timezone IST 5 30
dot11 autoconfig download retry interval min 100 max 400
end
```

Autoconfig ステータスの確認

Autoconfig ステータスを調べるには、**show dot11 autoconfig status** コマンドを使用します。

例

```
AP1600-ATT# show dot11 autoconfig status
Dot11 l2tp auto config is disabled

1600-89-absim# show dot11 autoconfig status
Auto configuration download will occur after
45 秒

1600-89-absim# show dot11 autoconfig status
Trying to download information file from server
```

Autoconfig のデバッグ

必要に応じて、次のデバッグ コマンドを使用できます。

- Autoconfig ステート マシンの移行を確認するためのデバッグ コマンド:
  Deb dot11 autoconfigsm
- Autoconfig イベントを確認するためのデバッグ コマンド:
  Deb dot11 autoconfigev

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。