



アクセス ポイントの最初の設定

この章では、最初に wireless device 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、wireless device 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 Command-Line Interface (CLI; コマンドライン インターフェイス) を使用して実行できますが、wireless device 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。

この章の内容は、次のとおりです。

- [始める前に \(P. 4-2\)](#)
- [IP アドレスの取得と割り当て \(P. 4-5\)](#)
- [1100 シリーズのアクセス ポイントへのローカル接続 \(P. 4-6\)](#)
- [1130 シリーズのアクセス ポイントへのローカル接続 \(P. 4-7\)](#)
- [1200、1230、1240、1250 シリーズのアクセス ポイントへのローカル接続 \(P. 4-8\)](#)
- [1300 シリーズのアクセス ポイント / ブリッジへのローカル接続 \(P. 4-9\)](#)
- [デフォルトの無線設定 \(P. 4-10\)](#)
- [基本設定の割り当て \(P. 4-10\)](#)
- [基本的なセキュリティ設定 \(P. 4-18\)](#)
- [1130 および 1240 シリーズ アクセス ポイントのシステム電力の設定 \(P. 4-29\)](#)
- [CLI を使用した IP アドレスの割り当て \(P. 4-30\)](#)
- [CLI を使用した IP アドレスの割り当て \(P. 4-30\)](#)
- [Telnet セッションを使用した CLI へのアクセス \(P. 4-31\)](#)
- [802.1X サブリカントの設定 \(P. 4-32\)](#)



(注)

このリリースでは、アクセス ポイントの無線インターフェイスがデフォルトで無効に設定されています。

始める前に

wireless device を設置する前に、使用しているコンピュータがこの wireless device 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。

- wireless device 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、wireless device の一意の IP アドレス (172.17.255.115 など)
- wireless device 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
- Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) 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、wireless device の IP アドレスを検索する場合、アクセスポイントの Media Access Control (MAC; メディア アクセス制御) 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。

モード ボタン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モード 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を切ります (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)。
 - ステップ 2** モード 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** モード 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) ボタンを離します。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。Web ブラウザ インターフェイスは、Windows プラットフォーム (98、2000、および XP) 上の Microsoft Internet Explorer バージョン 6.0 と、Windows プラットフォーム (98、2000、および XP) および Solaris プラットフォーム上での Netscape バージョン 7.0 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 wireless device の IP アドレスを入力し、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** 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 wireless device のパスワードを入力し、Enter キーを押します。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** System 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

システム ファイルを削除するには、デフォルト設定へリセットするか、ソフトウェアのリロードを必ず行ってください。

アクセス ポイントをデフォルト設定と静的 IP アドレスにリセットする場合は、`write erase` または `erase /all nvram` コマンドを使用します。静的 IP アドレスも含めすべてを消去する場合は、上記のコマンドに加えて `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アクセス ポイント / ブリッジ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:` と入力して、起動コンフィギュレーションを含む NVRAM ファイルをすべて消去します。



(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 アドレスとサブネット マスクを消去する手順は、次のとおりです。それ以外は、手順 3 に進んでください。

a. `write default-config` と入力します。

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

- ステップ 4** 次の CLI メッセージが表示されたら、`reload` と入力します。Erase of nvram: complete このコマンドを入力すると、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** 次の CLI メッセージが表示されたら、`Y` と入力します。Proceed with reload? [confirm]

**注意**

コンフィギュレーション ファイルを損失しないよう、このブート プロセスを中断しないでください。アクセス ポイント / ブリッジのインストール モード LED が緑色に点滅してから、CLI の設定変更を進めてください。また、ロード プロセスが完了すると、次の CLI メッセージが表示されます。*Line protocol on Interface Dot11Radio0, changed state to up*

- ステップ 6** アクセス ポイント / ブリッジのリポートが完了したら、アクセス ポイントを再設定できます。静的 IP アドレスを既に割り当てている場合は Web ブラウザ インターフェイスから、静的 IP アドレスをまだ割り当ていない場合は CLI から再設定してください。

アクセス ポイントは、IP アドレスも含めてデフォルト値に設定されます (Dynamic Host Configuration Protocol (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)。アクセス ポイント / ブリッジの新 IP アドレスを取得するには、*show interface bvi1* の CLI コマンドを使用します。

IP アドレスの取得と割り当て

wireless device 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 wireless device の IP アドレスを取得するか、割り当てる必要があります。

- 1130AG、1200、1240 シリーズ アクセスポイント、または 1300 シリーズ アクセスポイント / ブリッジの場合は、アクセスポイント 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。本体のコンソールポートに接続するには、該当する項から次の手順を実行します。
 - 1100 シリーズのアクセスポイントへのローカル接続 (P. 4-6)
 - 1130 シリーズのアクセスポイントへのローカル接続 (P. 4-7)
 - 1200、1230、1240、1250 シリーズのアクセスポイントへのローカル接続 (P. 4-8)
 - 1300 シリーズのアクセスポイント / ブリッジへのローカル接続 (P. 4-9)



(注) ターミナルエミュレータのアプリケーションの中には、Flow 制御パラメータを Xon/Xoff に設定しなくてはならないものがあります。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。
 - 1200 シリーズのアクセスポイントの場合は、wireless device 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、「1100 シリーズのアクセスポイントへのローカル接続」の項 (P.4-6) または「1200、1230、1240、1250 シリーズのアクセスポイントへのローカル接続」の項 (P.4-8) の手順を実行します。
 - 組織のネットワーク管理者に、wireless device の 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

1130AG、1200、1240、1250 アクセスポイント、または 1300 シリーズ アクセスポイント / ブリッジ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。

1100 シリーズ 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、1100 シリーズ アクセスポイントは DHCP サーバからの IP アドレスの取得を何度か試みます。アドレスを受信できない場合、アクセスポイントは 5 分間 IP アドレス 10.0.0.1 を自分自身に割り当てます。この 5 分間の時間枠内に、デフォルトの IP アドレスを参照し、静的アドレスを設定できます。5 分経過してもアクセスポイントが再設定されなかった場合、アクセスポイントはアドレス 10.0.0.1 を廃棄し、DHCP サーバからのアドレスの取得を再び要求し始めます。アドレスを受信できない場合には、要求を無期限に送信します。10.0.0.1 でアクセスポイントを参照できる 5 分間の時間枠を逃した場合、電源をいったん切り、改めて投入することでアクセスポイントにこの過程を繰り返させることができます。

1300 シリーズ アクセスポイント / ブリッジは、ルート アクセスポイントの無線ネットワークとして機能していると判断します。ブリッジとして設定するには、手動でインストールモードを指定して、アンテナの位置を合わせて無線リンクを確立します。リンクを確立するには、2 台のアクセスポイント / ブリッジをインストールモードに設定しておく必要があります。インストールモードでは、1 台のアクセスポイント / ブリッジをルートブリッジに、もう 1 台の方を非ルートブリッジと

して設定してください。設定しやすいよう、アクセスポイント/ブリッジをインストールモードにすると自動オプションが利用できます。無線リンクを確立してブリッジアンテナの位置を合わせた後、アクセスポイント/ブリッジ両方のインストールモードを解除して、ルートブリッジと非ルートブリッジとしてLANに配置してください。

1100 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をアクセスポイント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、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) PCをアクセスポイントに接続するのに、特別なクロスケーブルは不要です。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。

アクセスポイントがデフォルト値に設定され、DHCPサーバからIPアドレスを受信できない場合、IPアドレス10.0.0.1がデフォルトとして5分間設定されます。その5分間で、そのIPアドレスを参照して装置を設定できます。5分経過しても装置が再設定されなかった場合、アクセスポイントはアドレス10.0.0.1を廃棄し、DHCPサーバからのアドレスの取得を再び要求し始めます。アドレスを受信できない場合には、要求を無期限に送信します。10.0.0.1でアクセスポイントを参照できる5分間の時間枠を逃した場合、電源をいったん切り、改めて投入することでアクセスポイントにこの過程を繰り返させることができます。

アクセスポイント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** アクセスポイントの設定に使用するPCが10.0.0.2～10.0.0.10のIPアドレスに設定されていることを確認します。
- ステップ2** カテゴリ5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。クロスケーブルまたはストレート型ケーブルのいずれかを使用できます。
- ステップ3** アクセスポイントの電源を投入します。
- ステップ4** 「基本設定の割り当て」の項(P.4-10)の手順に従って操作します。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」の項(P.4-2)の手順に従ってください。
- ステップ5** アクセスポイントの設定後、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をアクセスポイントに接続するか、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、お使いのPCのオペレーティングマニュアルを参照してください。

1130 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、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 アクセスポイントのカバーを開きます。

ステップ 2 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 Cisco 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 3 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 フロー制御でうまくいかない場合は、フロー制御なしを使用してください。

ステップ 4 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続いて特権 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。

1200、1230、1240、1250 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、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Cisco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フロー制御でうまくいかない場合は、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続いて特権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。

1300 シリーズのアクセスポイント/ブリッジへのローカル接続

アクセスポイント/ブリッジを（アクセスポイント/ブリッジを有線 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)

PC をパワー インジェクタに接続するのに、特別なクロス ケーブルは不要です。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されていることを確認します。そうでない場合は、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型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 インジェクタをアクセスポイント/ブリッジに接続します。

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、アクセスポイント/ブリッジの電源を入れます。

ステップ 5 「基本設定の割り当て」の項 (P.4-10) の手順に従って操作します。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」(P.4-2) の手順に従ってください。

ステップ 6 アクセスポイント/ブリッジの設定後、PC からイーサネット ケーブルを抜いて、パワー インジェクタを有線 LAN に接続します。



(注)

PC をアクセスポイント/ブリッジに接続するか、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、お使いの PC のオペレーティング 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 リリース 12.3(8)JA を初めて起動した時点では、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。

詳細は、第6章「無線の設定」を参照してください。

基本設定の割り当て

wireless device 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 wireless device 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。wireless device の Web ブラウザインターフェイスは、Windows プラットフォーム(98、2000、および XP)上の Microsoft Internet Explorer バージョン 6.0 と、Windows プラットフォーム(98、2000、および XP)および Solaris プラットフォーム上での Netscape バージョン 7.0 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 wireless device の IP アドレスを入力し、**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** キーを押して、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** キーを押します。Summary Status ページが表示されます。一般的な Summary Status ページは、[図 4-1](#) に示されています。このページは、ご使用になっているアクセスポイントのモデルによって異なる場合があります。

図 4-1 Summary Status ページ

The screenshot displays the 'Summary Status' page for a Cisco 1200 Access Point. The page is organized into several sections:

- Header:** Cisco Systems logo, 'Cisco 1200 Access Point', and a 'Refresh' button.
- Navigation Menu:** A sidebar on the left with options: HOME, EXPRESS SETUP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG.
- Hostname:** 'ap' with an 'up' status and 'up uptime is 1 day, 1 hour, 36 minutes'.
- Associations:** A section with links for 'Clients: 0' and 'Resumes: 0'.
- Network Identity:** A table showing IP and MAC addresses.

| | |
|-------------|----------------|
| IP Address | 10.81.104.91 |
| MAC Address | 0005.9a38.42c0 |
- Network Interfaces:** A table listing interfaces, MAC addresses, and transmission rates.

| Interface | MAC Address | Transmission Rate |
|----------------|----------------|-------------------|
| Ethernet0 | 0005.9a38.42c0 | 100Mbps |
| Radio0.002.11B | 0001.8445.93e6 | 11.0Mbps |
| Radio0.002.11A | 0005.9a38.2451 | 54.0Mbps |
- Event Log:** A table showing system events with columns for Time, Severity, and Description.

| Time | Severity | Description |
|--------------------|--------------|---|
| Mar 1 00:00:50.231 | Notification | Line protocol on interface Dot11Radio0, changed state to up |
| Mar 1 00:00:57.250 | Error | Interface Dot11Radio0, changed state to up |
| Mar 1 00:00:57.231 | Information | Interface Dot11Radio0, frequency 2447 selected |
| Mar 1 00:00:57.231 | Information | Interface Dot11Radio0, frequency 2457 is in use |
| Mar 1 00:00:57.231 | Information | Interface Dot11Radio0, frequency 2437 is in use |
| Mar 1 00:00:57.231 | Information | Interface Dot11Radio0, frequency 2427 is in use |
| Mar 1 00:00:57.230 | Information | Interface Dot11Radio0, frequency 2422 is in use |
| Mar 1 00:00:57.230 | Information | Interface Dot11Radio0, frequency 2417 is in use |
| Mar 1 00:00:57.230 | Information | Interface Dot11Radio0, frequency 2412 is in use |
| Mar 1 00:00:55.232 | Notification | Line protocol on interface Dot11Radio1, changed state to up |
- Footer:** 'Close Window' button, 'Copyright (c) 1992-2004 by Cisco Systems, Inc.', and a version number '1.1.10001'.

ステップ 5 Express Setup をクリックします。Express Setup ページが表示されます。図 4-2 および図 4-3 は、1100 シリーズ アクセス ポイントの Express Setup ページを示しています。このページは、ご使用になっているアクセスポイントのモデルによって異なる場合があります。

図 4-2 1100 シリーズ アクセスポイントの Express Setup ページ



図 4-3 1130、1200、1240 シリーズ アクセスポイントの Express Setup ページ



(注) 図 4-3 は、1130 シリーズ アクセスポイントの Express Setup ページを示しています。1200 シリーズも同様ですが、ユニバーサルワークグループブリッジの役割をサポートしていません。

図 4-4 1250 シリーズ アクセスポイントの Express Setup ページ

HOME
EXPRESS SETUP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK
INTERFACES
SECURITY
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG

Hostname: ap ip uptime is 15 minutes

Express Set Up

Host Name:
MAC Address: 0017.54cc.d98

Configuration Server Protocol: DHCP Static IP

IP Address:
IP Subnet Mask:
Default Gateway:

SNMP Community:
 Read-Only Read-Write

Radio 0/2, 11N[™]

Role in Radio Network: Access Point Repeater
 Root Bridge Non-Root Bridge
 Workgroup Bridge Universal Workgroup Bridge Client MAC:
 Scanner

Optimize Radio Network for: Throughput Range Default Custom

Aironet Extensions: Enable Disable

Radio 1/0/2, 11N[™]

Role in Radio Network: Access Point Repeater
 Root Bridge Non-Root Bridge
 Workgroup Bridge Universal Workgroup Bridge Client MAC:
 Scanner

Optimize Radio Network for: Throughput Range Default Custom

Aironet Extensions: Enable Disable

Apply Cancel

図 4-5 1300 シリーズ アクセス ポイント / ブリッジの Express Setup ページ

The screenshot shows the 'Express Setup' configuration page for a Cisco BR1310G. The left sidebar contains a navigation menu with options like HOME, EXPRESS SETUP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOGS. The main content area is titled 'Express Set-Up' and includes the following fields and options:

- Host Name: BR1310G
- MAC Address: 000b.f4b.adce
- Configuration Server Protocol: DHCP Static IP
- IP Address: 10.91.107.17
- IP Subnet Mask: 255.255.255.192
- Default Gateway: 10.91.107.1
- SNMP Community: defaultCommunity
- SNMP Read-Write: Read-Only Read-Write
- Radio 802.11G:
 - Role in Radio Network: Access Point Repeater Root Bridge Non-Root Bridge Install Mode Workgroup Bridge Universal Workgroup Bridge Client MAC: <NONE>
 - Optimize Radio Network for: Throughput Range Default Custom
 - About Extensions: Enable Disable

At the bottom right, there are 'Apply' and 'Cancel' buttons.

ステップ 6 システム管理者から入手した設定を入力します。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 wireless device の識別に役立ちます。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、wireless device 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。クライアント ユーザが wireless device どうしを区別することが重要な場合、システム名の一意的部分が最初の 15 文字に現れるようにしてください。



(注) システム名を変更すると、wireless device 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、すばやく再度、アソシエートされます。

- **Configuration 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** : wireless device 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** : wireless device 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 wireless device の設定をしている間に wireless device の IP アドレスが変更されると、その wireless device 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 wireless device 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](#)」の項 (P.4-2) 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。
- **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。
- **Role in Radio Network** : ネットワークでの wireless device の役割を示したボタンをクリックします。wireless device 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。
 - **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。この設定は、1200 および 1240 シリーズ アクセスポイントにのみ可能です。
 - **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。この設定は、1200 および 1240 シリーズ アクセスポイントにのみ可能です。
 - **Install Mode** : 1300 シリーズ 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、最適な効率を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** : Cisco Aironet 350 シリーズ ワークグループブリッジのエミュレートを行います。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。ワークグループブリッジは、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している無線クライアントが他に無ければ、最大 254 台までのクライアントを接続できます。この設定は、1100、1200 および 1300 シリーズ アクセスポイントで可能です。
 - **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。この設定は、1130、1240 シリーズ アクセスポイント、および 1300 シリーズ アクセスポイント / ブリッジで可能です。
 - **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。
 - **Scanner** : ネットワーク監視モードとして機能します。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。絶え間なくスキャンを行い、無線 LAN に接続中の他の無線装置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** : wireless device の無線に対して設定済みの設定か、カスタマイズされた設定のいずれかを選択します。
 - **Throughput** : wireless device で処理されるデータ量が最大限に増えます。ただし、その通信範囲は縮小される可能性があります。
 - **Range** : wireless device の通信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 wireless device に使用されます。**Custom** をクリックすると、Network Interfaces: に次のページが表示されます。
 - Radio-802.11b Settings ページ
 - Radio-802.11b Settings ページ
 - Radio-802.11n Settings ページ (1250)
 - Radio-802.11n Settings ページ (1250)
- **Aironet Extensions** : 無線 LAN 上に Cisco Aironet デバイスだけがある場合には、この設定を有効にします。

ステップ7 **Apply** をクリックして、設定を保存します。

ステップ8 **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9 **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10 **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11 **Enable** をクリックして、無線を有効に設定します。

ステップ12 **Apply** をクリックします。

これで wireless device 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。設定を完了するの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) 1100、1200、1240、および 1250 シリーズの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。そのためには、ステータス LED がオレンジになるまで、モード ボタンを数秒間押ししながら、電源ジャックを抜いて再び差し込みます。

Express 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 」の項 (P.4-5) 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。 |
| Default Gateway | 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。 |
| SNMP Community | defaultCommunity (Read-only) |
| 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 | Throughput |
| Aironet Extensions | Enable |

基本的なセキュリティ設定

wireless device に基本設定を割り当てたら、セキュリティ設定を行い、ネットワークを不正アクセスから保護する必要があります。wireless device は、作業場所の物理的な境界を超えて通信することができます。

Express Setup ページを使用して基本設定を割り当てる場合と同じように、Express Security ページを使用して一意の SSID を作成し、これに 4 つのセキュリティ タイプのうちのいずれかを割り当てることができます。図 4-6 は、一般的な Express Security ページを示しています。

図 4-6 Express Security ページ

Express Security Setup

SSID Configuration

1. SSID Broadcast SSID in Beacon

2. VLAN

No VLAN Enable VLAN ID: (1-4094) Native VLAN

3. Security

No Security

Static WEP Key

Key 1 128 bit

EAP Authentication

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

WPA

Apply Cancel

SSID Table

| Delete | SSID | VLAN | Encryption | Authentication | Key Management | Native VLAN | Broadcast SSID |
|-----------------------|-------|------|------------|----------------|----------------|-------------|-------------------------------------|
| <input type="radio"/> | wlan1 | none | none | open | none | | <input checked="" type="checkbox"/> |

Express Security ページは、基本的なセキュリティ設定の設定に役立ちます。Web ブラウザ インターフェイスのメイン Security ページを使用して、詳細なセキュリティ設定を設定できます。

Express Security 設定の概要

Express Security ページから作成した SSID は、Express Security ページ下部の SSID Table に表示されます。wireless device には最大 16 の SSID を作成できます。デュアル無線の wireless device では、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 リリース 12.4(10b)JA および 12.3(8)JEC 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。

先頭の文字に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 に使用することはできません。

- 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 (Wired Equivalent Privacy (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。

■ 基本的なセキュリティ設定

Express Security のタイプ

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 のみに使用し、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 wireless device 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（「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」の項（P. 16-8）を参照）。または、ネットワークに Remote Authentication Dial-In User Service（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。wireless device のキーと一致する WEP キーが存在しないと、クライアントデバイスがこの SSID を使用してアソシエートすることはできません。 |
| EAP Authentication | 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鍵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化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。 | 802.1X 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、802.1X 認証を実行する必要があります。 無線クライアントで 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。Open 認証 + EAP 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. |

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 |
|------------|---|--|
| WPA | <p>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。</p> <p>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。</p> <p>Extensible Authentication Protocol (EAP; 拡張認証プロトコル) 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鍵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。</p> <p>無線クライアントで 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。Open 認証 + EAP を設定しないと、次の GUI 警告メッセージが表示されます。</p> <p>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.</p> <p>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。</p> <p>SSID CONFIG WARNING:[SSID]:If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.</p> |

Express Security の制限

Express Security ページは単純な基本のセキュリティ設定用に設計されているため、使用できるオプションは wireless device のセキュリティ機能のサブセットになります。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。
- SSID を特定の無線インターフェイスに割り当てることはできません。作成した SSID はすべての無線インターフェイスで有効になります。SSID を特定の無線インターフェイスに割り当てる場合は、Security SSID Manager ページを使用します。
- 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。
- wireless device 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る場合は、Security SSID Manager ページを使用します。

Express Security ページの使用方法

Express Security ページを使用して SSID を作成する手順は、次のとおりです。

-
- ステップ 1** SSID の入力フィールドに 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。
- ステップ 2** wireless device のビーコンで SSID をブロードキャストするには、Broadcast SSID in Beacon チェックボックスをオンにします。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 wireless device にアソシエートできるようになります。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、クライアントデバイスは wireless device にアソシエートできません。wireless device のビーコンに追加できる SSID は 1 つだけです。
- ステップ 3** (オプション) Enable VLAN ID チェックボックスをオンにして、SSID を VLAN に割り当てるための VLAN 番号 (1 ~ 4095) を入力します。既存の VLAN に SSID を割り当てることはできません。
- ステップ 4** (オプション) Native VLAN チェックボックスをオンにして、VLAN をネイティブ VLAN として指定します。
- ステップ 5** 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 を選択した場合は、ネットワーク上の認証サーバの IP アドレスと共有秘密鍵を入力します。



(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。詳細は、「[VLAN の使用](#)」の項 (P.4-19) を参照してください。

- ステップ 6** Apply をクリックします。ページ下部の SSID Table に SSID が表示されます。
-

CLI の設定例

ここでは、Express Security ページで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：No Security (P. 4-23)
- 例：Static WEP (P. 4-24)
- 例：EAP Authentication (P. 4-25)
- 例：WPA (P. 4-27)

例 : No Security

次の例は、Express Security ページを使用して *no_security_ssid* という名前の SSID を作成した結果として行われる設定の一部を示しています。ここでは、ビーコンにこの SSID を追加し、これを VLAN 10 に割り当て、ネイティブ VLAN として VLAN 10 を選択しています。

```
!  
dot11 ssid no_security_ssid  
authentication open  
vlan 10  
!  
interface Dot11Radio0.10  
encapsulation dot1Q 10 native  
no ip route-cache  
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  
bridge-group 1 spanning-disabled  
!  
interface Dot11Radio1  
no ip address  
no ip route-cache  
!  
ssid no_security_ssid  
!  
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0  
rts threshold 2312  
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 block-unknown-source  
no bridge-group 1 source-learning  
no bridge-group 1 unicast-flooding  
bridge-group 1 spanning-disabled
```

例 : Static WEP

次の例は、Express Security ページを使用して *static_wep_ssid* という名前の SSID を作成した結果として行われる設定の一部を示しています。ここでは、この SSID をビーコンから除外し、この SSID を 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 キーを入力しています。

```
ssid static_wep_ssid
    vlan 20
    authentication open
!
interface Dot11Radio0
    no ip address
    no ip route-cache
    !
    encryption vlan 20 key 3 size 128bit 7 FFD518A21653687A4251AEE1230C transmit-key
    encryption vlan 20 mode wep mandatory
!
    speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
    rts threshold 2312
    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
    bridge-group 1 spanning-disabled

    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 block-unknown-source
    no bridge-group 20 source-learning
    no bridge-group 20 unicast-flooding
    bridge-group 20 spanning-disabled
!
interface Dot11Radio1
    no ip address
    no ip route-cache
    !
    encryption vlan 20 key 3 size 128bit 7 741F07447BA1D4382450CB68F37A transmit-key
    encryption vlan 20 mode wep mandatory
!
    ssid static_wep_ssid
!
    speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
    rts threshold 2312
    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
    bridge-group 1 spanning-disabled
!
interface Dot11Radio1.20
    encapsulation dot1Q 20
    no ip route-cache
    bridge-group 20
    bridge-group 20 subscriber-loop-control
    bridge-group 20 block-unknown-source
    no bridge-group 20 source-learning
    no bridge-group 20 unicast-flooding
    bridge-group 20 spanning-disabled
```

例 : EAP Authentication

次の例は、Express Security ページを使用して *eap_ssid* という名前の SSID を作成した結果として行われる設定の一部を示しています。ここでは、SSID をビーコンから除外し、SSID を VLAN 30 に割り当てています。



(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
!
interface Dot11Radio0/1
    no ip address
    no ip route-cache
    !
    encryption vlan 30 mode wep mandatory
    !
    ssid eap_ssid
!
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
rts threshold 2312
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
bridge-group 1 spanning-disabled
!
interface Dot11Radio0/1.30
    encapsulation dot1Q 30
    no ip route-cache
    bridge-group 30
    bridge-group 30 subscriber-loop-control
    bridge-group 30 block-unknown-source
    no bridge-group 30 source-learning
    no bridge-group 30 unicast-flooding
    bridge-group 30 spanning-disabled
!
interface Dot11Radio0/1
    no ip address
    no ip route-cache
    !
    encryption vlan 30 mode wep mandatory
    !
    ssid eap_ssid
!
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
rts threshold 2312
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
bridge-group 1 spanning-disabled
!
```

```
interface Dot11Radio0/1.30
  encapsulation dot1Q 30
  no ip route-cache
  bridge-group 30
  bridge-group 30 subscriber-loop-control
  bridge-group 30 block-unknown-source
  no bridge-group 30 source-learning
  no bridge-group 30 unicast-flooding
  bridge-group 30 spanning-disabled
!
interface FastEthernet0
  mtu 1500
  no ip address
  ip mtu 1564
  no ip route-cache
  duplex auto
  speed auto
  bridge-group 1
  no bridge-group 1 source-learning
  bridge-group 1 spanning-disabled
!
interface FastEthernet0.30
  mtu 1500
  encapsulation dot1Q 30
  no ip route-cache
  bridge-group 30
  no bridge-group 30 source-learning
  bridge-group 30 spanning-disabled
!
interface BVI1
  ip address 10.91.104.91 255.255.255.192
  no ip route-cache
!
ip http server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
ip radius source-interface BVI1
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.91.104.92 auth-port 1645 acct-port 1646 key 7 091D1C5A4D5041
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
```

例：WPA

次の例は、Express Security ページを使用して *wpa_ssid* という名前の SSID を作成した結果として行われる設定の一部を示しています。ここでは、SSID をビーコンから除外し、SSID を VLAN 40 に割り当てています。

```
ssid wpa_ssid
  vlan 40
  authentication open eap eap_methods
  authentication network-eap eap_methods
  authentication key-management wpa
!
aaa new-model
!
!
aaa group server radius rad_eap
  server 10.91.104.92 auth-port 1645 acct-port 1646
!
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 authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
!
bridge irb
!
!
interface Dot11Radio0/1
  no ip address
  no ip route-cache
!
  encryption vlan 40 mode ciphers tkip
!
  ssid wpa_ssid
!
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
rts threshold 2312
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
bridge-group 1 spanning-disabled
!
interface Dot11Radio0/1.40
  encapsulation dot1Q 40
  no ip route-cache
  bridge-group 40
  bridge-group 40 subscriber-loop-control
  bridge-group 40 block-unknown-source
  no bridge-group 40 source-learning
  no bridge-group 40 unicast-flooding
  bridge-group 40 spanning-disabled
!
```

```
    ssid wpa_ssid
!
interface FastEthernet0
  no ip address
  no ip route-cache
  duplex auto
  speed auto
  bridge-group 1
  no bridge-group 1 source-learning
  bridge-group 1 spanning-disabled
!
interface FastEthernet0.40
  encapsulation dot1Q 40
  no ip route-cache
  bridge-group 40
  no bridge-group 40 source-learning
  bridge-group 40 spanning-disabled
```

1130 および 1240 シリーズ アクセスポイントのシステム電力の設定

1130 および 1240 アクセスポイントは、接続先の電源が十分な電力を供給しないことを検知すると、無線インターフェイスを無効にします。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の System Software: System Configuration ページで、電力オプションを選択できます。図 4-7 は、System Configuration ページの System Power Settings セクションを示しています。

図 4-7 System Software: System Configuration ページの電力オプション

| System Power Settings | |
|--------------------------------------|--|
| Power State: | FULL POWER |
| Power Source: | AC_ADAPTOR |
| Power Settings: | <input checked="" type="radio"/> Power Negotiation <input type="radio"/> Pre-standard Compatibility |
| Power Injector: | <input type="checkbox"/> Installed on Port with MAC Address: <input type="text" value="DISABLED"/> (#####.####.####) |
| <input type="button" value="Apply"/> | |

| Locate Access Point | |
|--------------------------------------|---|
| Blink the Access Point LEDs: | <input checked="" type="radio"/> Disable <input type="radio"/> Enable |
| <input type="button" value="Apply"/> | |

AC 電源アダプタの使用

AC 電源アダプタを使用して 1130 または 1240 アクセスポイントに電力を供給する場合、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

Power over Ethernet (PoE) を 1130 または 1240 アクセスポイントに供給するスイッチを使用し、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

Power over Ethernet (PoE) を 1130 アクセスポイントに供給するスイッチを使用し、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、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 1130 または 1240 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。

CLI を使用した IP アドレスの割り当て

wireless device は、有線 LAN に接続されると、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。ネットワークでは、wireless device のイーサネットポートと無線ポートに個別の IP アドレスがトラッキングされるのではなく、BVI が使用されます。

CLI を使用して wireless device 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。特権 EXEC モードから開始し、次の手順に従って wireless device の BVI に IP アドレスを割り当てます。

| | コマンド | 目的 |
|--------|--------------------------------------|--|
| ステップ 1 | <code>configure terminal</code> | 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 | <code>interface bvi1</code> | BVI のインターフェイス設定モードに切り替えます。 |
| ステップ 3 | <code>ip address address mask</code> | IP アドレスとアドレス マスクを BVI に割り当てます。 |
| | |  <p>(注) Telnet セッションを使用して wireless device 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 wireless device への接続が失われます。Telnet を使用して wireless device 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 wireless device への別の Telnet セッションを開始します。</p> |

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、お使いの 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 キーを押します。

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 メニューが表示されません。Windows 2000 で Telnet セッションを起動するには、open と入力してから、wireless device 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 wireless device の IP アドレスを入力して、Connect をクリックします。

802.1X サブリカントの設定

ネットワークにアクセスするため認証が必要なのは PC ユーザのため、従来、dot1x 認証サーバ/クライアントの関係にはネットワーク機器と PC クライアントがそれぞれ使用されていました。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、プラグが抜かれてもおかしくない、ネットワーク接続が部外者から使用されるかもしれない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み、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れるように設定します。



(注)

802.1X サブリカントは、1130AG、1240AG、1250、および 1300 シリーズのアクセスポイントで使用できます。1100 シリーズおよび 1200 シリーズのアクセスポイントでは利用できません。

サブ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、サブ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 | <code>configure terminal</code> | 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 | <code>dot1x credentials profile</code> | dot1x クレデンシャル プロファイルを作成し、dot1x クレデンシャルの設定サブモードに入ります。 |
| ステップ 3 | <code>anonymous-id description</code> | (オプション): 使用する匿名 ID を入力します。 |
| ステップ 4 | <code>description description</code> | (オプション): 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 | <code>username username</code> | 認証ユーザ ID を入力します。 |
| ステップ 6 | <code>password {0 7 LINE}</code> | <p>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。</p> <p>0: 続けて、暗号化されていないパスワードを入力します。</p> <p>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、既に保存済みの設定を適用する場合に使用します。</p> <p>LINE: 暗号化されていない(クリアテキストの)パスワード。</p> |
| | | <p>(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。</p> |

| | コマンド | 目的 |
|--------|---|--|
| ステップ 7 | <code>pki-trustpoint pki-trustpoint</code> | (オプション。EAP-TLS にのみ使用。): 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 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ 9 | <code>copy running config startup-config</code> | (オプション) コンフィギュレーション ファイルに入力内容を保存します。 |

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。


```
ap1240AG>enable
Password:xxxxxxx
ap1240AG#config terminal
Enter configuration commands, one per line. End with CTRL-Z.
ap1240AG(config)# dot1x credentials test
ap1240AG(config-dot1x-creden)#username Cisco
ap1240AG(config-dot1x-creden)#password Cisco
ap1240AG(config-dot1x-creden)#exit
ap1240AG(config)#
```

インターフェイスまたは SSID にクレデンシャルを適用する方法

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 | <code>configure terminal</code> | 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 | <code>interface fastethernet 0</code> | アクセス ポイントのファースト イーサネット ポートのインターフェイス設定モードを開始します。  (注) <code>interface fa0</code> を使用してファースト イーサネット設定モードを開始することもできます。 |
| ステップ 3 | <code>dot1x credentials profile name</code> | 既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 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ 5 | <code>copy running config startup-config</code> | (オプション) コンフィギュレーション ファイルに入力内容を保存します。 |


次の例では、アクセスポイントのファーストイーサネットポートまで、クレデンシャルプロファイル *test* を適用しています。

```
ap1240AG>enable
Password:xxxxxxx
ap1240AG#config terminal
Enter configuration commands, one per line. End with CTRL-Z.
ap1240AG(config)#interface fa0
ap1240AG(config-if)#dot1x credentials test
ap1240AG(config-if)#end
ap1240AG#
```

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 サブ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 サブ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 | <code>configure terminal</code> | 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 | <code>dot11 ssid ssid</code> | 802.11 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。SSID では、大文字と小文字が区別されます。  (注) 先頭の文字に !、#、; の文字は使用できません。 +,], /, ", TAB、末尾のスペースは、SSID には無効な文字です。 |
| ステップ 3 | <code>dot1x credentials profile</code> | 既に設定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 | <code>end</code> | 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 | <code>copy running config startup-config</code> | (オプション) コンフィギュレーション ファイルに入力内容を保存します。 |

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、サブ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 サブリカントの EAP 方式プロファイルの作成と適用」の項 (P. 11-18) を参照してください。