CHAPTER 12

WDS、高速安全ローミング、無線管理、および Wireless Intrusion Detection Services の設定

この章では、Wireless Domain Services（WDS; 無線ドメイン サービス）、クライアント デバイスの高速安全ローミング、無線管理、および Wireless Intrusion Detection Services（WIDS）のためにアクセス ポイントを設定する方法について説明します。この章の内容は、次のとおりです。

スイッチの Wireless LAN Services Module（WLSM）に WDS を設定する方法は、『Catalyst 6500 Series Wireless LAN Services Module Installation and Configuration Note』を参照してください。

WDS の概要

ネットワークに WDS を設定すると、無線 LAN 上のアクセス ポイントは WDS デバイス（WDS デバイスとして設定されたアクセス ポイント、Integrated Services Router、またはスイッチ）を使用してクライアント デバイスに高速安全ローミングを提供し、無線管理に参加します。スイッチを WDS デバイスとして使用する場合、そのスイッチは Wireless LAN Services Module（WLSM）を備えている必要があります。WDS デバイスとして設定したアクセス ポイントは、最大 60 個のアクセス ポイントの参加をサポートします。WDS デバイスとして設定した Integrated Services Router（ISR）は、最大 100 個のアクセス ポイントの参加をサポートします。WLSM を備えたスイッチは、最大 600 個のアクセス ポイント、および 240 個までのモビリティ グループの参加をサポートします。

（注）　単一アクセス ポイントは 16 個までのモビリティ グループをサポートします。

高速安全ローミングによって、クライアント デバイスがアクセス ポイント間をローミングするときに速やかに再認証でき、音声やその他の時間に敏感なアプリケーションにおける遅延を回避できます。

無線管理に参加しているアクセス ポイントは、無線環境に関する情報（潜在的な不正アクセス ポイント、クライアント アソシエーション、アソシエーション解除など）を WDS デバイスに転送します。WDS デバイスはこの情報を集約し、ネットワーク上の Wireless LAN Solution Engine（WLSE; 無線 LAN ソリューション エンジン）デバイスに転送します。

WDS デバイスの役割

WDS デバイスは無線 LAN 上で次のようないくつかの作業を実行します。

- WDS 機能をアドバタイズして、無線 LAN に最適な WDS デバイスの選択に参加します。WDS 用に無線 LAN を設定する場合は、1 つのデバイスをメインの WDS 候補として設定し、1 つ以上の追加デバイスをバックアップの WDS 候補として設定します。メインの WDS デバイスがオフラインになったら、バックアップの WDS デバイスの 1 つがその役割を引き継ぎます。
- サブネット中の全アクセス ポイントを認証して、そのうちのそれぞれと安全な通信チャネルを設定します。
- サブネット中のアクセス ポイントから無線データを収集して、データを集約し、これをネットワーク上の WLSE デバイスに転送します。
- 参加しているアクセス ポイントにアソシエートされているすべての 802.1x 認証クライアントに対するパススルーとして機能します。
- 動的キーを使用するサブネット中の全クライアント　デバイスを登録して、それにセッション キーを設定し、セキュリティ クレデンシャルをキャッシュします。クライアントが別のアクセス ポイントにローミングする場合、WDS デバイスはクライアントのセキュリティ クレデンシャルを新しいアクセス ポイントに転送します。

表 12-1 は、WDS デバイスとして設定できるプラットフォーム（アクセス ポイント、ISR、WLSM 装備スイッチ）でサポート可能な参加アクセス ポイント数を示しています。

表 12-1　WDS デバイスでサポートされる参加アクセス ポイント数

WDS デバイスとして設定されたユニット	サポートされる参加アクセス ポイント数
クライアント デバイスからも接続できるアクセス ポイント	30
無線インターフェイスが無効になっているアクセス ポイント	60
Integrated Services Router（ISR）	100（ISR プラットフォームに応じて異なる）
WLSM を備えたスイッチ	600

WDS デバイスを使用したアクセス ポイントの役割

無線 LAN 上のアクセス ポイントは、次の動作において WDS デバイスと対話します。

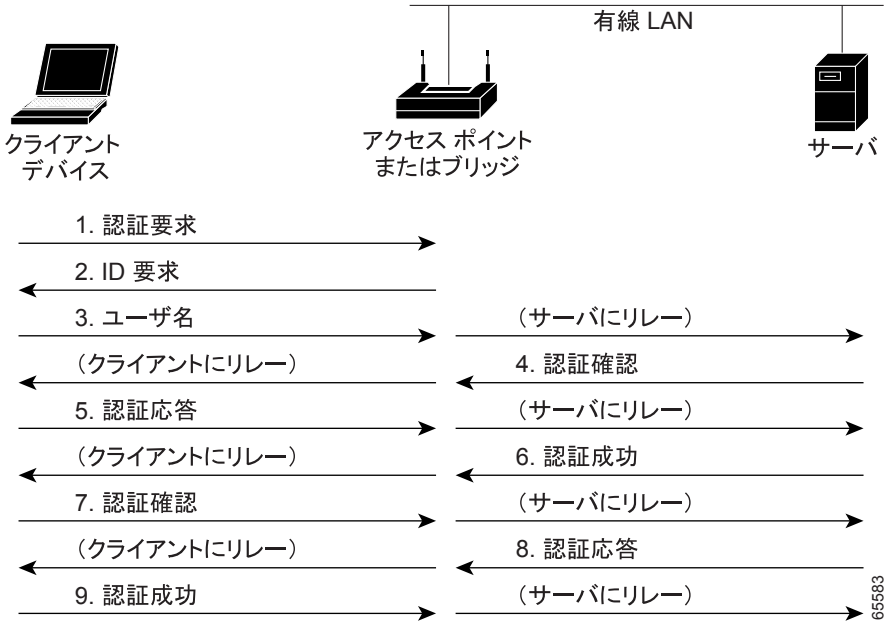
- 現在の WDS デバイスを検出、トラッキングし、WDS アドバタイズメントを無線 LAN に中継します。
- WDS デバイスを認証して、認証した WDS デバイスと安全な通信チャネルを確立します。
- WDS デバイスとアソシエートしたクライアント デバイスを登録します。
- 無線データを WDS デバイスに報告します。

高速安全ローミングの概要

多くの無線 LAN 内のアクセス ポイントは、システム全体においてアクセス ポイントからアクセス ポイントへローミングするモバイル クライアント デバイスに対応します。クライアント デバイスで稼働するアプリケーションの中には、異なるアクセス ポイントにローミングする場合、高速な再アソシエーションを必要とするものがあります。たとえば、音声アプリケーションでは、会話の遅延やギャップを防ぐために、シームレスなローミングが必要です。

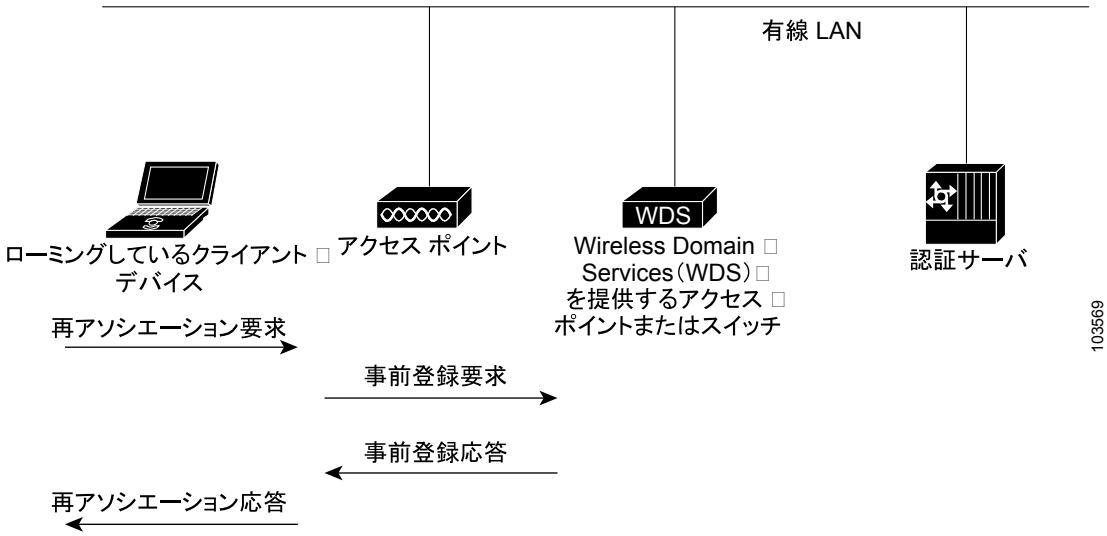
通常稼働時、Light Extensible Authentication Protocol （LEAP; 拡張認証プロトコル）対応クライアント デバイスは、図 12-1 に示すように、メイン Remote Authentication Dial-In User Service （RADIUS）サーバとの通信をはじめとする完全な LEAP 認証を実行することによって、新しいアクセス ポイントとの間の相互認証を実行します。

図 12-1　RADIUS サーバを使ったクライアント認証



無線 LAN に高速安全ローミングを設定すれば、LEAP 使用可能クライアント デバイスはメイン RADIUS サーバを利用することなく、あるアクセス ポイントから別のアクセス ポイントへのローミングを行うことが可能です。Cisco Centralized Key Management （CCKM）を使用すると、Wireless Domain Service （WDS; 無線ドメイン サービス）の提供が設定されたデバイスは、RADIUS サーバの代わりにクライアントを短時間で認証するため、音声などの時間が重要なアプリケーションではほとんど遅延が発生しません。図 12-2 は、CCKM を使用したクライアント認証を示しています。

図 12-2　CCKM と WDS アクセス ポイントを使用するクライアント再アソシエーション



WDS デバイスは、無線 LAN 上の CCKM 利用可能クライアント デバイスに対するクレデンシャルのキャッシュを維持します。CCKM 利用可能クライアントは、1 つのアクセス ポイントから別のアクセス ポイントへローミングする場合、クライアントが新しいアクセス ポイントへ再アソシエーションの要求を送信し、新しいアクセス ポイントはその要求を WDS デバイスへ中継します。WDS デバイスはクライアントのクレデンシャルを新しいアクセス ポイントへ転送し、新しいアクセス ポイントは再アソシエーション応答をクライアントに送信します。クライアントと新しいアクセス ポイントとの間で渡されるパケットは 2 つだけなので、再アソシエーションの時間が大幅に短縮されます。クライアントは再アソシエーション応答をユニキャスト キーの生成にも使用します。高速安全ローミングをサポートするアクセス ポイントの設定方法については、「高速安全ローミングの設定」の項（P.12-24）を参照してください。

無線管理の概要

無線管理に参加しているアクセス ポイントは、無線環境をスキャンし、潜在的な不正アクセス ポイント、アソシエートされたクライアント、クライアントの信号強度、他のアクセス ポイントからの無線信号などの無線情報に関するレポートを WDS デバイスに送信します。WDS デバイスは集約した無線データを、ネットワーク上の WLSE デバイスに転送します。無線管理に参加しているアクセス ポイントは、近くのアクセス ポイントに障害が発生した場合のカバレッジを提供するための無線 LAN の自己修復や自動設定調整についてもサポートしています。無線管理の設定方法については、「無線管理の設定」の項（P.12-31）を参照してください。

次の URL をクリックして、WLSE ドキュメントを参照します。

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/prod_technical_documentation.html

レイヤ 3 モビリティの概要

WLSM をネットワーク上の WDS デバイスとして使用すると、特定のサブネットを 1 つ設定したり、有線スイッチ インフラストラクチャ全体に VLAN を設定したりしなくても、大規模なレイヤ 3 ネットワークの任意の場所にアクセス ポイントを設置できます。クライアント デバイスは、マルチポイント GRE（mGRE）トンネルを使用して、異なるレイヤ 3 サブネットに存在するアクセス ポイントにローミングします。ローミングしているクライアントは、IP アドレスを変更しなくてもネットワークに接続されたままとなっています。

Wireless LAN Services Module（WLSM）を備えたスイッチに WDS を設定する方法については、『*Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide*』を参照してください。

レイヤ 3 モビリティ無線 LAN ソリューションは、次のハードウェア コンポーネントおよびソフトウェア コンポーネントで構成されています。

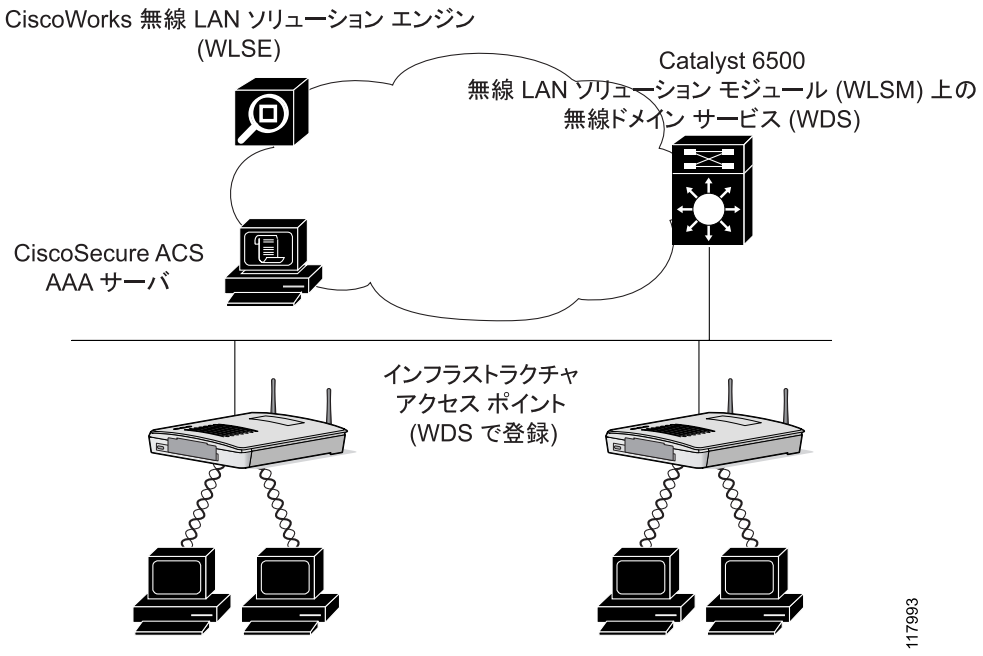
- WDS に参加している 1100 シリーズまたは 1200 シリーズのアクセス ポイント
- スーパーバイザ モジュールおよび WDS デバイスとして設定されている WLSM を備えた Catalyst 6500 スイッチ

（注）　レイヤ 3 モビリティを適切に設定するには、WLSM を WDS デバイスとして使用する必要があります。アクセス ポイントを WDS デバイスとして使用すると、レイヤ 3 モビリティはサポートされません。

- クライアント デバイス

図 12-3 は、相互に対話してレイヤ 3 モビリティを実行するコンポーネントを示しています。

図 12-3　レイヤ 3 モビリティに必要なコンポーネント



Cisco Structured Wireless-Aware Network（SWAN）に関する情報については、次のリンクをクリックしてください。

http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html

（注）　ある Service Set Identifier（SSID; サービス セット ID）にレイヤ 3 モビリティを設定していて、WDS デバイスでレイヤ 3 モビリティがサポートされていない場合、クライアント デバイスはその SSID を使用してもアソシエートできません。

（注）　リピータ アクセス ポイント、およびワークグループ ブリッジ モードのアクセス ポイントは、レイヤ 3 モビリティが設定された SSID にはアソシエートできません。

Wireless Intrusion Detection Services の概要

無線 LAN 上に Wireless Intrusion Detection Services（WIDS）を実装すると、アクセス ポイント、WLSE、およびオプションの（Cisco 製品ではない）WIDS エンジンが同時に動作して、無線 LAN インフラストラクチャ、およびアソシエートされたクライアント デバイスに対する攻撃を探知および防止します。

WLSE と同時に動作する場合、アクセス ポイントは侵入を探知し、無線 LAN を防御するアクションを実行します。WIDS の機能は次のとおりです。

- スイッチ ポートのトレースと不正抑制：スイッチ ポートのトレースと抑制では、RF 検出方法を使用して、不明な無線（潜在的な不正デバイス）の無線 Media Access Control（MAC; メディア アクセス制御）アドレスを生成します。WLSE は、無線 MAC アドレスから有線側 MAC アドレスを取り出し、これを使用してスイッチの BRIDGE Management Information Bases（MIB; 管理情報ベース）を検索します。1 つまたは複数の検索可能な MAC アドレスが利用できる場合、WLSE は Cisco Discovery Protocol（CDP）を使用して、検出元のアクセス ポイントから最大 2 ホップ離れて接続しているすべてのスイッチを発見します。WLSE は CDP で発見された各スイッチの BRIDGE MIB を調べて、ターゲット MAC アドレスが含まれているかどうかを判断します。CDP でいずれかの MAC アドレスが見つかると、WLSE は対応するスイッチ ポート番号を抑制します。
- 過剰管理フレーム検出：過剰管理フレームは、無線 LAN が攻撃されたことを示します。攻撃者は、無線上で大量の管理フレームを注入し、そのフレームを処理する必要があるアクセス ポイントに大きな負荷を加えることにより、サービス拒否攻撃を実行する場合があります。スキャン モードのアクセス ポイントとルート アクセス ポイントは、WIDS の機能セットの一部として無線信号を監視して、過剰管理フレームを検出します。アクセス ポイントが過剰管理フレームを検出すると、障害を生成し、WDS を介して WLSE にこれを送信します。
- 認証 / 保護失敗検出：認証 / 保護失敗検出は、無線 LAN 上での最初の認証フェーズを回避するかまたは、進行中のリンク保護を侵害しようとする攻撃者を探します。これらの検出メカニズムは、次の特定の認証攻撃に対応します。
  - EAPOL フラッド検出
  - MIC/ 暗号化失敗検出
  - MAC スプーフィング検出
- フレーム キャプチャ モード：フレーム キャプチャ モードでは、スキャナ アクセス ポイントが 802.11 フレームを収集し、ネットワーク上の WIDS エンジンのアドレスに送信します。

（注）　アクセス ポイントの WIDS への参加の設定方法については、「アクセスポイントの WIDS 参加の設定」の項（P.12-33）を、アクセス ポイントに対する Management Frame Protection（MFP; 管理フレーム保護）の設定方法については、「管理フレーム保護の設定」（P.12-27）を参照してください。

- 802.11 Management Frame Protection （MFP）：本来的に、無線は正当なデバイスか、不法デバイスであるかを問わず、あらゆるデバイスで傍受または参加が可能なブロードキャスト メディアです。制御 / 管理フレームは、クライアント ステーションが AP とのセッションを選択または開始する際に使用されるため、これらのフレームはオープンであることが要求されます。管理フレームは暗号化できませんが、偽造 / 改ざんできないように保護する必要があります。MFP は、802.11 管理フレームの完全性を保護するための手段です。

（注）　MFP で侵入イベントをレポートするには Wireless LAN Solutions Engine （WLSE）が必要です。

（注）　MFP は、1130 シリーズおよび 1240 シリーズのアクセス ポイント、および AP モードの 1300 シリーズ アクセス ポイントなどの 32MB プラットフォームでのみ利用できます。

WDS の設定

この項では、ネットワーク上で WDS を設定する方法について説明します。この項の構成は、次のとおりです。

WDS のガイドライン

WDS を設定する場合は、次のガイドラインに従います。

- クライアント デバイスも収容している WDS アクセス ポイントでは最大 30 のアクセス ポイントの参加をサポートできますが、無線を無効にした WDS アクセス ポイントでは、最大 60 までサポートできます。
- WDS 専用モードの場合、WDS では 60 個までのインフラストラクチャ アクセス ポイントと 1200 個までのクライアントがサポートされます。
- リピータ アクセス ポイントは、WDS をサポートしません。リピータ アクセス ポイントを WDS 候補として設定しないでください。また WDS アクセス ポイントを、イーサネット障害時にリピータ モードに戻るように設定しないでください。
- 350 シリーズ アクセス ポイントはメインの WDS デバイスとして設定できません。ただし、350 シリーズ アクセス ポイントを WDS に参加するように設定できます。

WDS の要件

WDS を設定するには、無線 LAN 上に次の項目を含める必要があります。

- WDS デバイスとして設定可能なアクセス ポイント、Integrated Services Router（ISR）、またはスイッチ（Wireless LAN Services Module を装備）が 1 つ以上
- 認証サーバ（またはローカル認証サーバとして設定されたアクセス ポイントまたは ISR）

（注）　1300 アクセス ポイント / ブリッジは、WDS マスタとして設定することはできませんが、WDS ネットワークに参加することはできます。この機能は、1300 AP/ ブリッジではサポートされていません。

設定概要

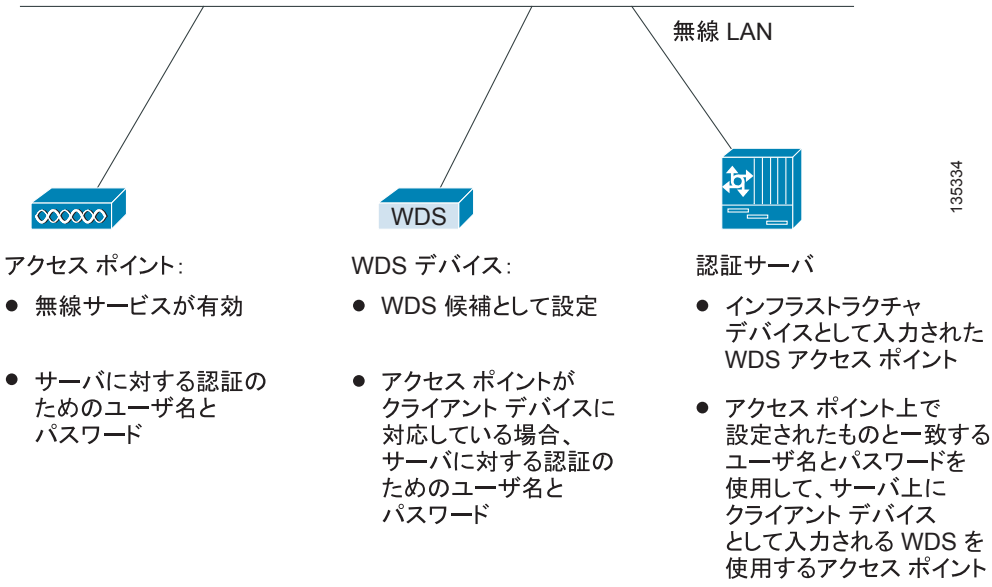
WDS および高速安全ローミングの設定には、次の 3 つの主要手順を完了する必要があります。

1. アクセス ポイント、ISR、またはスイッチを潜在的な WDS デバイスとして設定します。この項では、アクセス ポイントを WDS デバイスとして設定する方法について説明します。Wireless LAN Services Module（WLSM）を備えたスイッチに WDS を設定する方法については、*『Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide』*を参照してください。
2. 他のアクセス ポイントが、この WDS デバイスを使用するように設定します。

3. ネットワーク上の認証サーバが WDS デバイスと、WDS デバイスを使用するアクセス ポイントを認証するように設定します。

図 12-4 は、WDS に参加する各デバイスに必要な設定を示しています。

図 12-4　WDS に参加するデバイスの設定



アクセス ポイントを潜在的な WDS デバイスとして設定する

（注） メインの WDS 候補用に、多数のクライアント デバイスを収容する必要のないアクセス ポイントを設定します。クライアント デバイスが WDS アクセス ポイントの起動時にアソシエートした場合、そのクライアントは認証のために数分待たされる可能性があります。

（注） リピータ アクセス ポイントは、WDS をサポートしません。リピータ アクセス ポイントを WDS 候補として設定しないでください。また、WDS アクセス ポイントを、イーサネット障害時にリピータ モードに戻るように設定しないでください。

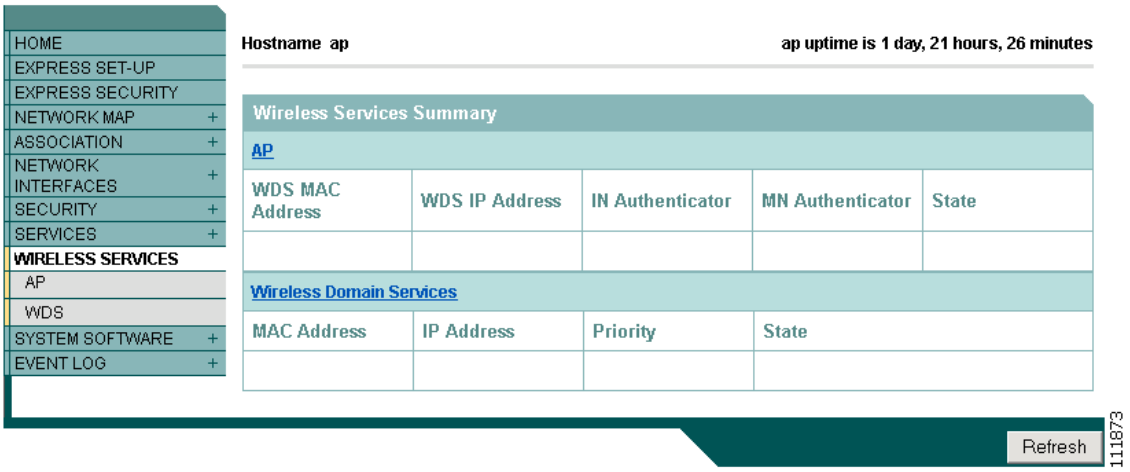
（注） WDS が有効な場合、WDS アクセス ポイントはすべての認証を実行、トラッキングします。したがって、WDS アクセス ポイントでは Extensible Authentication Protocol（EAP; 拡張認証プロトコル）セキュリティ設定を行う必要があります。アクセス ポイントでの EAP の設定方法については、第 11 章「認証タイプの設定」を参照してください。

（注） 350 シリーズ アクセス ポイントはメインの WDS デバイスとして設定できません。ただし、350 シリーズ アクセス ポイントを WDS に参加するように設定できます。

プライマリ WDS アクセス ポイントとして設定するアクセス ポイント上で、次の手順に従ってメインの WDS 候補としてアクセス ポイントを設定します。

ステップ 1　Wireless Services Summary ページを表示します。図 12-5 は、Wireless Services Summary ページを示しています。

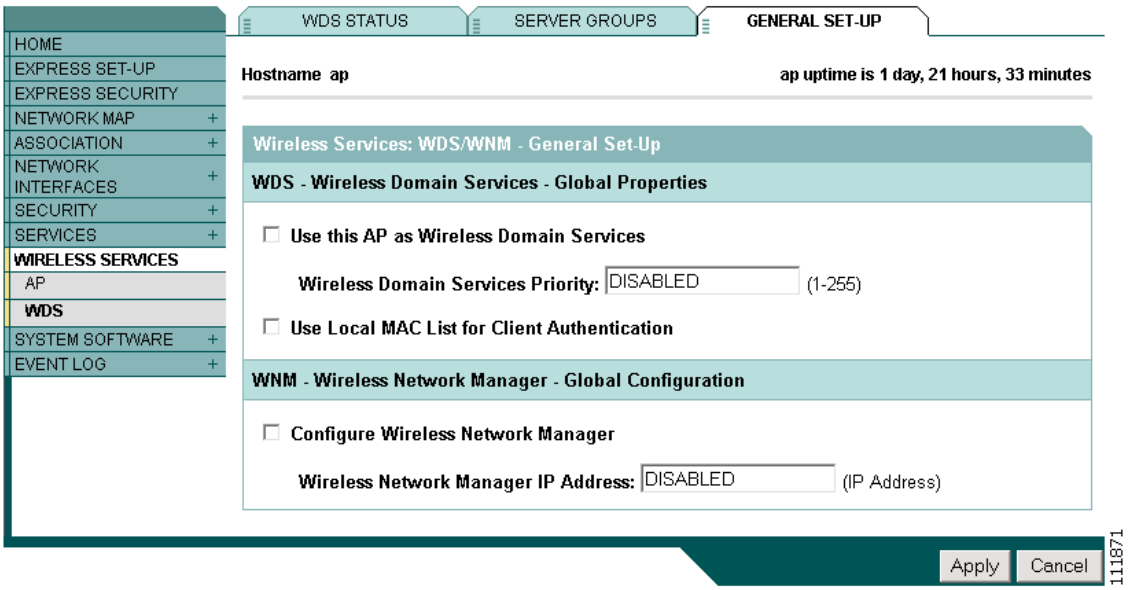
図 12-5　Wireless Services Summary ページ



ステップ 2　**WDS** をクリックして WDS/WNM Summary ページを表示します。

ステップ 3　WDS/WNM Summary ページで、**General Setup** をクリックして WDS/WNM General Setup ページに移動します。図 12-6 は、General Setup ページを示しています。

図 12-6　WDS/WNM General Setup ページ



ステップ 4　*Use this AP as Wireless Domain Services* チェックボックスをオンにします。

ステップ 5　Wireless Domain Services Priority フィールドに 1 ～ 255 の優先順位数を入力して、WDS 候補の優先順位を設定します。Wireless Domain Services Priority フィールド内の数字が最も大きい WDS アクセス ポイント候補が、WDS アクセス ポイントとして機能します。たとえば、1 つの WDS 候補には優先順位に 255 が割り当てられており、もう 1 つの候補には優先順位に 100 が割り当てられている場合は、優先順位が 255 の候補が WDS アクセス ポイントとして機能します。

ステップ 6　（オプション）*Use Local MAC List for Client Authentication* チェックボックスをオンにして、WDS デバイス上で設定されたアドレスのローカル リストにある MAC アドレスを使用してクライアント デバイスを認証します。このチェックボックスをオンにしない場合、WDS デバイスは Server Groups ページで MAC アドレス認証用に指定したサーバを使用して、MAC アドレスに基づくクライアント認証を行います。

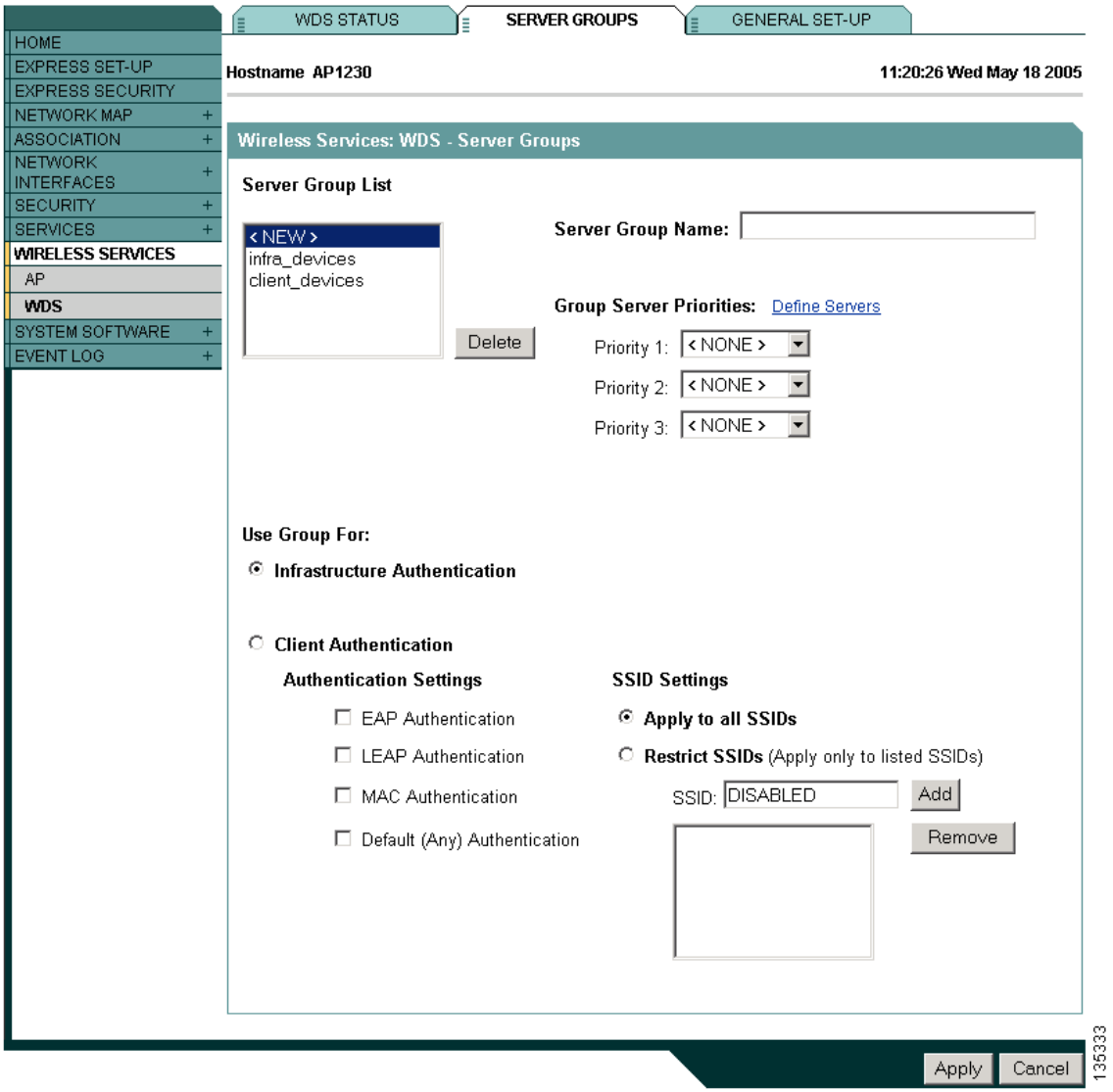
（注）　*Use Local MAC List for Client Authentication* チェックボックスをオンにしても、クライアント デバイスに対して MAC ベースの認証が強制されるわけではありません。サーバ ベースの MAC アドレス認証に対するローカルの代替方法が提供されるだけです。

ステップ 7　（オプション）ネットワーク上で Wireless LAN Solutions Engine（WLSE）を使用している場合、*Configure Wireless Network Manager* チェックボックスをオンにして、*Wireless Network Manager IP Address* フィールドに WLSE デバイスの IP アドレスを入力します。WDS アクセス ポイントは、アクセス ポイントとクライアント デバイスから無線計測情報を収集し、集約したデータを WLSE デバイスに送信します。

ステップ 8　**Apply** をクリックします。

ステップ 9　**Server Groups** をクリックして、WDS Server Groups ページを表示します。図 12-7 は、WDS Server Groups ページを示しています。

図 12-7　WDS Server Groups ページ



ステップ 10　WDS アクセス ポイントを使用するインフラストラクチャ デバイス（アクセス ポイント）の 802.1x 認証に使用するサーバ グループを作成します。Server Group Name フィールドにグループ名を入力します。

ステップ 11　Priority 1 ドロップダウン メニューからプライマリ サーバを選択します。（グループに追加する必要のあるサーバが Priority ドロップダウン メニューに表示されない場合は、**Define Servers** をクリックして、Server Manager ページを表示します。そのページでサーバを設定してから、WDS Server Groups ページに戻ります。）

（注）　ネットワーク上に認証サーバが存在しない場合、アクセス ポイントまたは ISR をローカル認証サーバとして設定できます。設定方法については、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」を参照してください。

ステップ 12　（オプション）Priority 2 ドロップダウン メニューおよび Priority 3 ドロップダウン メニューからバックアップ サーバを選択します。

ステップ 13　**Apply** をクリックします。

ステップ 14　クライアント デバイス用の 802.1x 認証に使用するサーバのリストを設定します。EAP、LEAP、PEAP、または MAC ベースのような特定タイプの認証を使ってクライアント用の別のリストを指定したり、任意のタイプの認証を使ってクライアント デバイス用のリストを指定したりできます。Server Group Name フィールドに、サーバのグループ名を入力します。

ステップ 15　Priority 1 ドロップダウン メニューからプライマリ サーバを選択します。（グループに追加する必要のあるサーバが Priority ドロップダウン メニューに表示されない場合は、**Define Servers** をクリックして、Server Manager ページを表示します。そのページでサーバを設定してから、WDS Server Groups ページに戻ります。）

ステップ 16　（オプション）Priority 2 ドロップダウン メニューおよび Priority 3 ドロップダウン メニューからバックアップ サーバを選択します。

ステップ 17　（オプション）**Restrict SSIDs** を選択すると、使用するサーバ グループを、特定の SSID を使用するクライアント デバイスに制限できます。SSID フィールドに SSID を入力して、**Add** をクリックします。SSID を削除するには、SSID リスト内で削除する SSID を選択して **Remove** をクリックします。

ステップ 18　**Apply** をクリックします。

ステップ 19　LEAP 認証用に WDS アクセス ポイントを設定します。LEAP の設定方法については、第 11 章「認証タイプの設定」を参照してください。

（注）　WDS アクセス ポイントでクライアント デバイスを使用する場合は、「アクセス ポイントを WDS デバイスを使用するように設定する」の項（P.12-15）の手順に従って、WDS アクセス ポイントで WDS が使用されるように設定します。

CLI の設定例

次の例は、「アクセス ポイントを潜在的な WDS デバイスとして設定する」の項（P.12-10）に記載された手順と同じ機能を果たす CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bvi1
AP(config)# wlccp authentication-server infrastructure infra_devices
AP(config)# wlccp authentication-server client any client_devices
AP(config-wlccp-auth)# ssid fred
AP(config-wlccp-auth)# ssid ginger
AP(config)# end
```

次の例では、サーバ グループ *infra_devices* を使用してインフラストラクチャ デバイスを認証しています。SSID *fred* または *ginger* を使用するクライアント デバイスは、サーバ グループ *client_devices* を使用して認証されます。

この例で使用されているコマンドの詳細は、『Cisco Aironet アクセス ポイント / ブリッジ Cisco IOS コマンド リファレンス』を参照してください。

アクセス ポイントを WDS デバイスを使用するように設定する

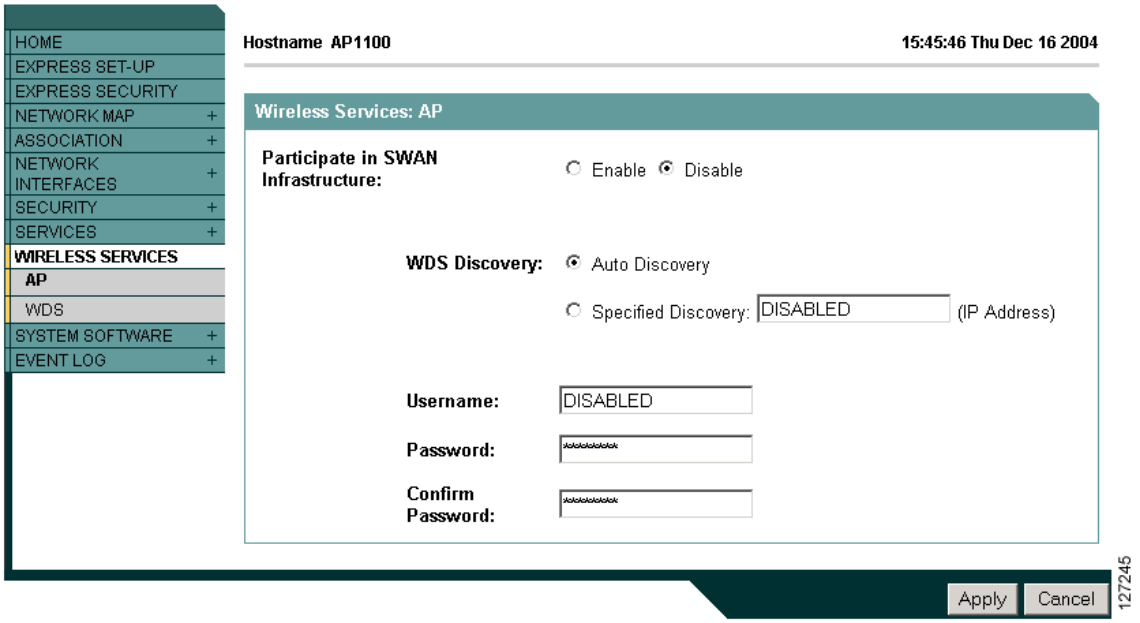
WDS デバイスを通じて認証し、WDS 内に参加するようにアクセス ポイントを設定する手順は、次のとおりです。

（注）　インフラストラクチャ アクセス ポイントが WDS に参加するには、WDS が実行している IOS と同じバージョンを実行する必要があります。

ステップ 1　Wireless Services Summary ページを表示します。

ステップ 2　**AP** をクリックして Wireless Services AP ページを表示します。図 12-8 は、Wireless Services AP ページを示しています。

図 12-8　Wireless Services AP ページ



ステップ 3　*Participate in SWAN Infrastructure* 設定で **Enable** をクリックします。

ステップ 4　（オプション）ネットワーク上で WDS デバイスとして WLSM スイッチ モジュールを使用する場合は、**Specified Discovery** を選択して、入力フィールドに WLSM の IP アドレスを入力します。Specified Discovery を有効にすると、アクセス ポイントは WDS アドバタイズメントを待たずに、WDS デバイスを使用して即座に認証します。指定した WDS デバイスが応答しない場合、アクセス ポイントは WDS アドバタイズメントを待ちます。

ステップ 5　Username フィールドにアクセス ポイントのユーザ名を入力します。このユーザ名は、認証サーバ上でアクセス ポイント用に作成したユーザ名と一致していなければなりません。

ステップ 6　Password フィールドにアクセス ポイントのパスワードを入力し、Confirm Password フィールドに同じパスワードをもう一度入力します。このパスワード名は、認証サーバ上でアクセス ポイント用に作成したパスワードと一致していなければなりません。

ステップ 7　**Apply** をクリックします。

WDS と対話するように設定したアクセス ポイントは、自動的に次の手順を実行します。

- 現在の WDS デバイスを検出、トラッキングし、WDS アドバタイズメントを無線 LAN に中継します。
- WDS デバイスを認証して、認証した WDS デバイスと安全な通信チャネルを確立します。
- WDS デバイスとアソシエートしたクライアント デバイスを登録します。

CLI の設定例

次の例は、「アクセス ポイントを WDS デバイスを使用するように設定する」の項（P.12-15）に記載された手順と同じ機能を果たす CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 7 wes7win8
AP(config)# end
```

この例では、アクセス ポイントは WDS デバイスと対話できるように設定されており、ユーザ名に *APWestWing*、パスワードに *wes7win8* を使用して認証サーバに対する認証を行います。認証サーバ上でクライアントとしてアクセス ポイントを設定するときには、同じユーザ名とパスワードの組み合わせで設定する必要があります。

この例で使用されているコマンドの詳細は、『Cisco Aironet アクセス ポイント / ブリッジ Cisco IOS コマンド リファレンス』を参照してください。

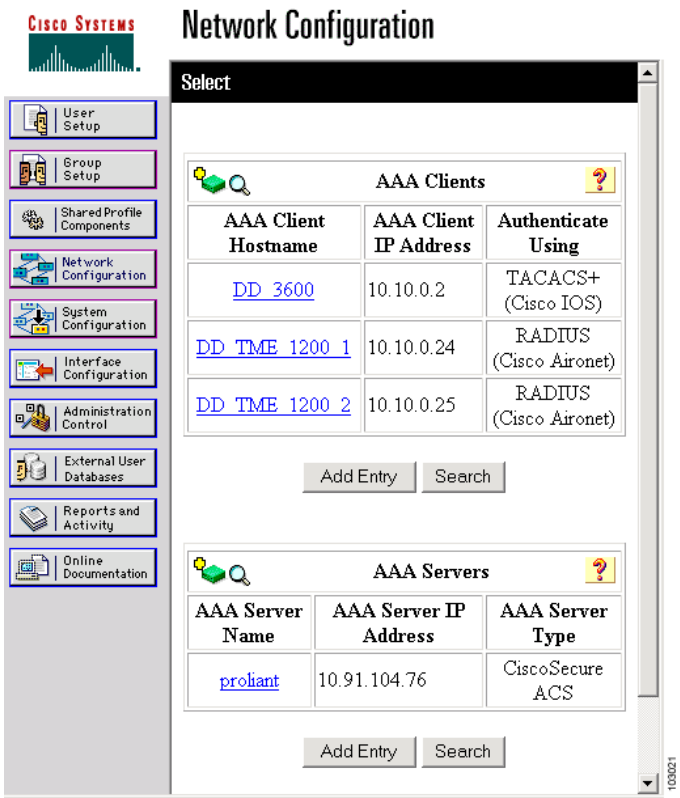
認証サーバが WDS をサポートするように設定する

WDS デバイスと WDS に参加している全アクセス ポイントは、認証サーバに対する認証を行う必要があります。サーバ上で、アクセス ポイント用のユーザ名とパスワードと、WDS デバイス用のユーザ名とパスワードを設定します。

サーバが Cisco ACS を実行している場合は、次の手順に従ってサーバ上でアクセス ポイントを設定します。

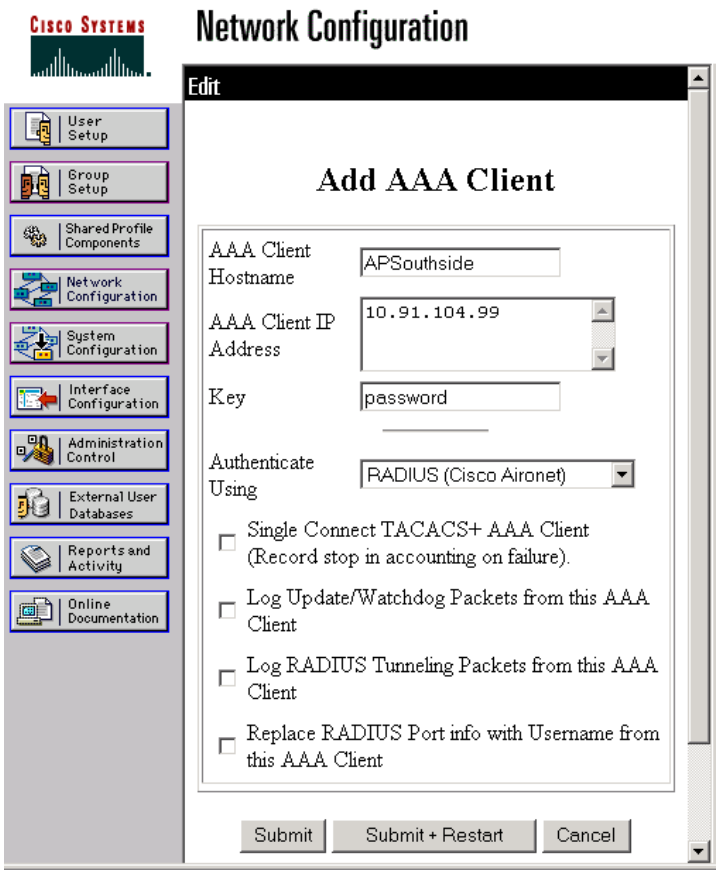
ステップ 1　Cisco Secure ACS にログインし、**Network Configuration** をクリックして Network Configuration ページを表示します。WDS デバイス用のエントリを作成するには、Network Configuration ページを使用する必要があります。図 12-9 は、Network Configuration ページを示しています。

図 12-9　Network Configuration ページ



ステップ 2　AAA Clients テーブルで、**Add Entry** をクリックします。Add AAA Client ページが表示されます。図 12-10 は、Add AAA Client ページを示しています。

図 12-10　Add AAA Client ページ



ステップ 3　AAA Client Hostname フィールドに、WDS デバイスの名前を入力します。

ステップ 4　AAA Client IP Address フィールドに、WDS デバイスの IP アドレスを入力します。

ステップ 5　Key フィールドに、WDS デバイスで設定したのとまったく同じパスワードを入力します。

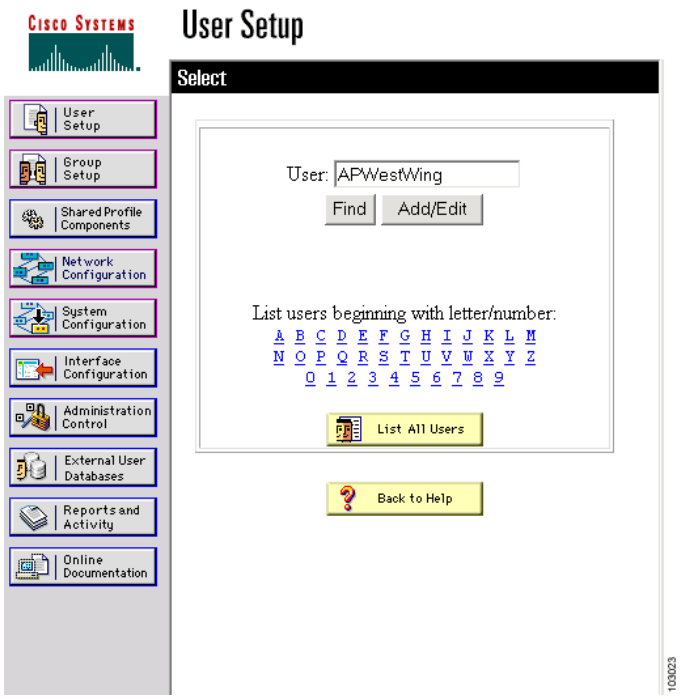
ステップ 6　Authenticate Using ドロップダウン メニューから、**RADIUS (Cisco Aironet)** を選択します。

ステップ 7　**Submit** をクリックします。

ステップ 8　WDS デバイス候補のそれぞれに対して、ステップ 2 からステップ 7 の手順を実行します。

ステップ 9　**User Setup** をクリックして User Setup ページを表示します。WDS デバイスを使用するアクセス ポイント用のエントリを作成するには、User Setup ページを使用する必要があります。図 12-11 は、User Setup ページを示しています。

図 12-11　User Setup ページ

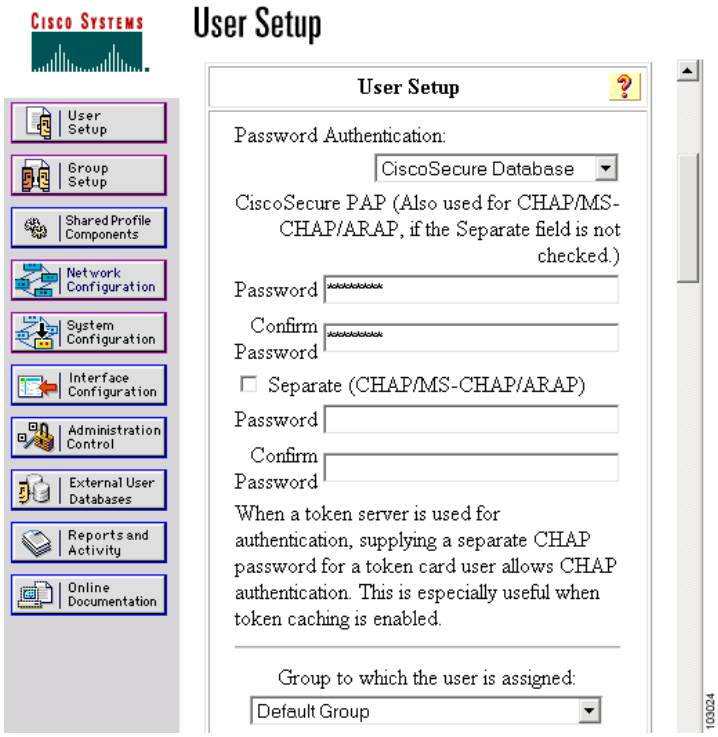


ステップ 10　User フィールドに、アクセス ポイントの名前を入力します。

ステップ 11　**Add/Edit** をクリックします。

ステップ 12　User Setup ボックスが表示されるまで、画面を下にスクロールします。図 12-12 は、User Setup ボックスを示しています。

図 12-12　ACS User Setup ボックス



ステップ 13　Password Authentication ドロップダウン メニューから **CiscoSecure Database** を選択します。

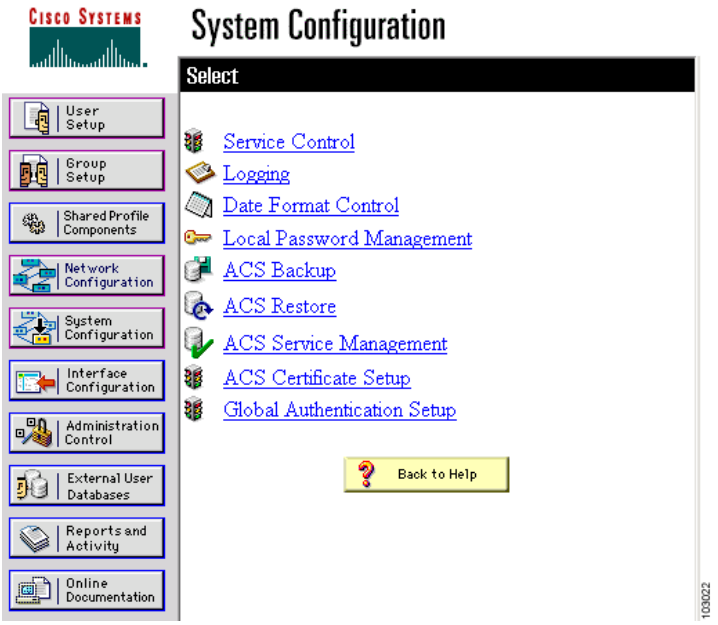
ステップ 14　Password フィールドと Confirm Password フィールドに、Wireless Services AP ページでアクセス ポイントに対して入力したのとまったく同じパスワードを入力します。

ステップ 15　**Submit** をクリックします。

ステップ 16　WDS デバイスを使用するアクセス ポイントそれぞれに対して、ステップ 10 からステップ 15 の手順を実行します。

ステップ 17　System Configuration ページを表示して **Service Control** をクリックし、ACS を再起動してエントリ内容を適用します。図 12-13 は、System Configuration ページを示しています。

図 12-13　ACS System Configuration ページ



WDS 専用モードの設定

WDS アクセス ポイントは、コマンド **wlccp wds mode wds-only** を使用して WDS 専用モードで稼動できます。このコマンドを発行してリロードすると、アクセス ポイントは WDS 専用モードで機能を開始します。WDS 専用モードでは、dot11 サブシステムが初期化されず、dot11 インターフェイス関連のコマンドを設定できません。WDS 専用モードは、WDS で 60 個までのインフラストラクチャ アクセス ポイントと 1200 個までのクライアントをサポートします。WDS 専用モードをオフにするには、コマンド **no** を使用します。WDS アクセス ポイントの実行中のモードを表示するには、コマンド **show wlccp wds** を使用します。

WDS アクセス ポイントが AP および WDS の両モードで稼動するように設定するには、コマンド **no wlccp wds mode wds-only** を使用し、さらにコマンド **write erase** を使用してアクセス ポイントをただちにリロードします。アクセス ポイントをリロードすると dot11 無線サブシステムが初期化されます。アクセス ポイントと WDS は無線クライアントに直接アソシエートします。このモードの場合 WDS では、20 個の無線クライアント アソシエーションに加え、30 個のインフラストラクチャ アクセス ポイントと 600 のクライアントがサポートされます。

WDS 情報の表示

Web ブラウザのインターフェイスでは、Wireless Services Summary ページを参照して WDS ステータスの概要を表示します。

特権 EXEC モードの CLI では、次のコマンドを使って、現在の WDS デバイスと CCKM に参加している他のアクセス ポイントについて情報を表示します。

コマンド	説明
show wlccp ap	CCKM に参加する任意のアクセス ポイント上で、このコマンドを使用して、WDS デバイスの MAC アドレス、WDS デバイスの IP アドレス、アクセス ポイントの状態（認証中、認証済み、登録済み）、インフラストラクチャ認証サーバの IP アドレス、クライアント デバイス（MN）認証サーバの IP アドレスを表示することができます。
show wlccp wds { **ap** | **mn** } [**detail**] [**mac-addr** *mac-address*]	WDS デバイスでのみ、このコマンドを使って、アクセス ポイントとクライアント デバイスに関するキャッシュ情報を表示できます。 • **ap**：このオプションを使用して、CCKM に参加するアクセス ポイントを表示します。このコマンドは、各アクセス ポイントの MAC アドレス、IP アドレス、状態（認証中、認証済み、または登録済み）、有効期間（アクセス ポイントが再認証を必要とするまでの秒数）を表示します。**mac-addr** オプションを利用して、特定のアクセス ポイントに関する情報を表示します。 • **mn**：このオプションを使用して、クライアント デバイスや呼び出されたモバイル ノードに関するキャッシュ情報を表示します。このコマンドによって、各クライアントの MAC アドレス、IP アドレス、クライアントがアソシエートされているアクセス ポイント（cur-AP）、および状態（認証中、認証済み、または登録済み）が表示されます。**detail** オプションを使用して、クライアントの有効期間（アクセス ポイントが再認証を必要とするまでの残りの秒数）、SSID、VLAN ID を表示します。**mac-addr** オプションを使用して、特定のクライアント デバイスに関する情報を表示します。 コマンド **show wlccp wds** のみを入力した場合は、アクセス ポイントの IP アドレス、MAC アドレス、優先順位、インターフェイス ステート（管理上スタンドアロン、アクティブ、バックアップ、候補、または WDS 専用）が表示されます。 状態がバックアップの場合、コマンドは現在の WDS デバイスの IP アドレス、MAC アドレス、および優先順位も表示します。 ステートが WDS 専用の場合は、コマンドによってデバイスの MAC アドレス、IP アドレス、インターフェイス ステート、アクセス ポイント数、モバイル ノード数が表示されます。

デバッグ メッセージの使用

特権 EXEC モードでは、デバッグ コマンドを使用して、WDS デバイスと対話するデバイス用のデバッグ メッセージの表示を制御します。

コマンド	説明
debug wlccp ap {**mn** | **wds-discovery** | **state**}	このコマンドを使用して、クライアント デバイス（**mn**）、WDS 検出プロセス、WDS デバイス（**state**）に対するアクセス ポイントの認証に関連するデバッグ メッセージの表示をオンにします。
debug wlccp dump	このコマンドを使用して、バイナリ形式で送受信された WLCCP パケットのダンプを実行します。
debug wlccp packet	このコマンドを使用して、WDS デバイスとやり取りするパケットの表示をオンにします。
debug wlccp wds [**aggregator** | **authenticator** | **nm** | **state** | **statistics**]	このコマンドとそのオプションを使用して、WDS デバック メッセージの表示をオンにします。**statistics** オプションを使って、障害統計情報の表示をオンにします。
debug wlccp wds authenticator {**all** | **dispatcher** | **mac-authen** | **process** | **rxdata** | **state-machine** | **txdata**}	このコマンドとそのオプションを使用して、認証に関連する WDS デバック メッセージの表示をオンにします。

高速安全ローミングの設定

WDS を設定すると、CCKM 用に設定したアクセス ポイントは、アソシエートされたクライアント デバイスに高速安全ローミングを提供できます。この項では、高速で安全なローミングを無線 LAN 上で設定する方法を説明します。この項の構成は、次のとおりです。

- 高速安全ローミングの要件
- 高速安全ローミングをサポートするアクセス ポイントの設定

高速安全ローミングの要件

高速安全ローミングを設定するには、無線 LAN で次の 3 つの項目が必要となります。

- WDS デバイスとして設定される 1 つ以上のアクセス ポイント、ISR、または WLSM を備えたスイッチ
- WDS に参加するように設定されたアクセス ポイント
- 高速安全ローミング用に設定されたアクセス ポイント
- 認証サーバ（またはローカル認証サーバとして設定されたアクセス ポイント、ISR、またはスイッチ）
- Cisco Aironet クライアント デバイス、または、Cisco Compatible Extensions（CCX）のバージョン 2 以降と互換性のあるシスコ互換のクライアント デバイス

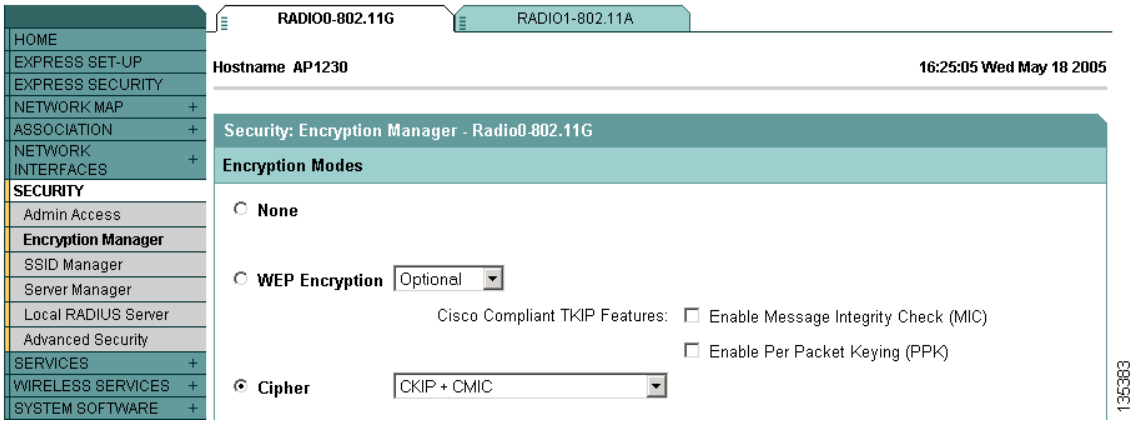
WDS の設定方法については、「WDS の設定」の項（P.12-9）を参照してください。

高速安全ローミングをサポートするアクセス ポイントの設定

高速安全ローミングをサポートするには、WDS に参加するように無線 LAN 上のアクセス ポイントを設定し、アクセス ポイントで少なくとも 1 つの SSID に対して CCKM 認証キー管理を許可する必要があります。SSID に CCKM を設定する手順は、次のとおりです。

ステップ 1　アクセス ポイント GUI で、Encryption Manager ページを表示します。図 12-14 は、Encryption Manager ページの上部を示しています。

図 12-14　Encryption Manager ページ



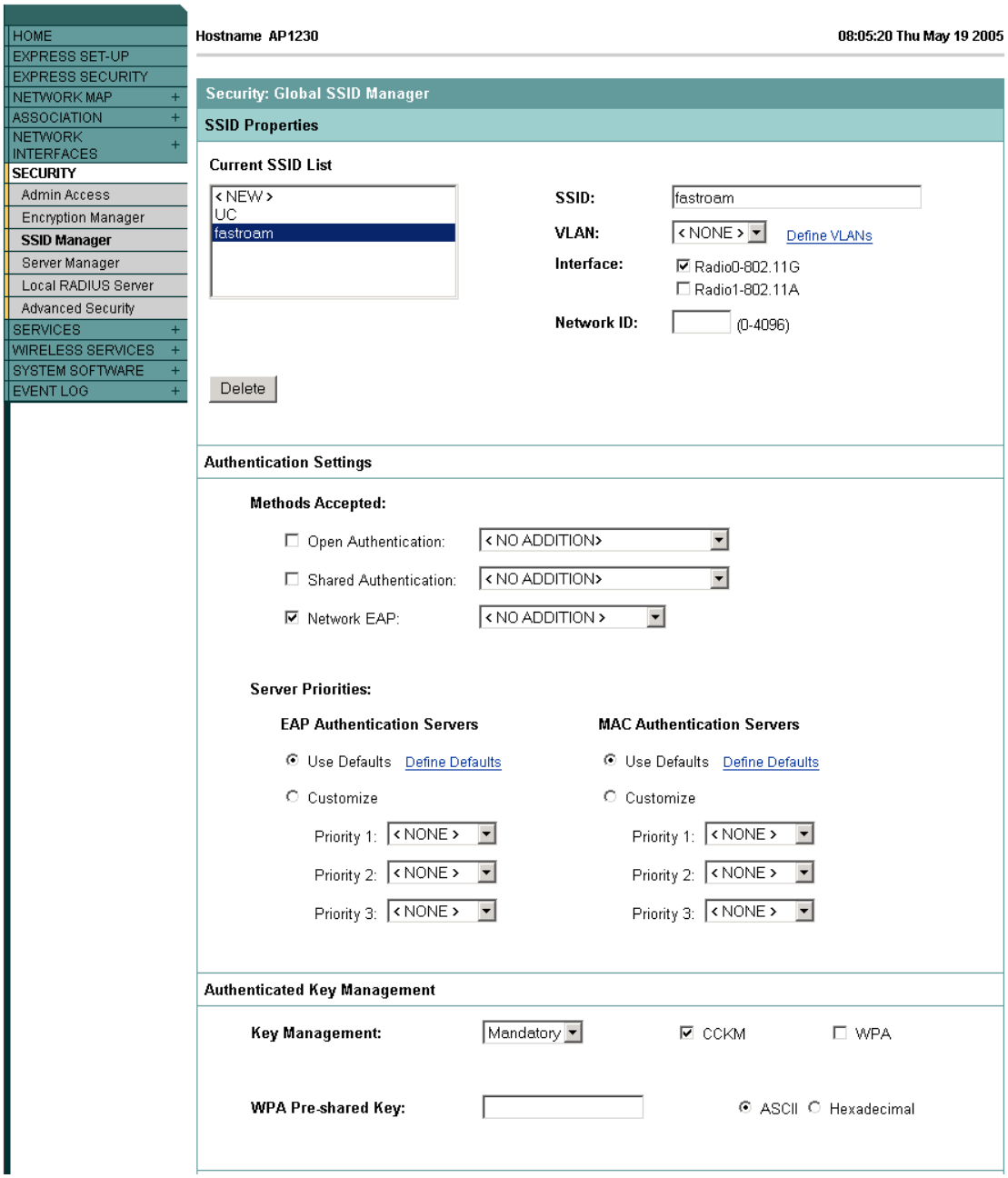
ステップ 2　**Cipher** ボタンをクリックします。

ステップ 3　Cipher ドロップダウン メニューから、**CKIP + CMIC** を選択します。

ステップ 4　**Apply** をクリックします。

ステップ 5　Global SSID Manager ページを表示します。図 12-15 は、Global SSID Manager ページの上部を示しています。

図 12-15　Global SSID Manager ページ



ステップ 6　CCKM をサポートする SSID で、次の設定を選択します。

a. アクセス ポイントに複数の無線インターフェイスが含まれている場合は、SSID が適用されるインターフェイスを選択します。

b. Authentication Settings で、**Network EAP** を選択します。CCKM を有効にする際は、認証タイプとして Network EAP を有効にする必要があります。

c. Authenticated Key Management で、**Mandatory** または **Optional** を選択します。**Mandatory** を選択した場合は、CCKM をサポートするクライアントだけが、SSID を使用してアソシエートできます。Optional を選択した場合は、CCKM クライアントと CCKM をサポートしないクライアントの両方が、SSID を使用してアソシエートできます。

d. **CCKM** チェックボックスをオンにします。

ステップ 7　**Apply** をクリックします。

CLI の設定例

次の例は、「高速安全ローミングをサポートするアクセス ポイントの設定」の項（P.12-24）に記載された手順と同じ機能を果たす CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# dot11 ssid fastroam
AP(config-ssid)# authentication network-eap eap_methods
AP(config-ssid)# authentication key-management cckm
AP(config-ssid)# exit
AP(config)# interface dot11radio0
AP(config-if)# encryption mode ciphers ckip-cmic
AP(config-if)# ssid fastroam
AP(config-if)# exit
AP(config)# end
```

次の例では、SSID *fastroam* は Network EAP と CCKM をサポートするように設定されています。2.4GHz 無線インターフェイス上で CKIP-CMIC 暗号スイートが有効になっています。また、2.4GHz 無線インターフェイス上で、SSID *fastroam* が有効になっています。

この例で使用されているコマンドの詳細は、『Cisco Aironet アクセス ポイント / ブリッジ Cisco IOS コマンド リファレンス』を参照してください。

管理フレーム保護の設定

管理フレーム保護の稼動には WDS が必要で、この保護は 32MB プラットフォーム（s : 1130、1240 シリーズ アクセス ポイント、および AP モードの 1300 シリーズ アクセス ポイント）でのみ利用できます。MFP は WLSE で設定されますが、アクセス ポイントおよび WDS では MFP を手動で設定できます。

（注）　WLSE が存在しないと MFP では検出した侵入をレポートできないため、有効性が限定されます。WLSE が存在する場合は、WLSE から設定を実行します。

完全に保護するには、MFP アクセス ポイントで Simple Network Transfer Protocol（SNTP）を設定します。

管理フレーム保護

管理フレーム保護は、アクセス ポイントとクライアント ステーション間で転送される管理メッセージにセキュリティ機能を提供します。MFP は、インフラストラクチャ MFP とクライアント MFP の 2 つの機能コンポーネントで構成されます。

インフラストラクチャ MFP はインフラストラクチャ サポートを提供します。インフラストラクチャ MFP は、不正デバイスおよびサービス拒否攻撃の検出に有益なブロードキャストおよび誘導された管理フレームに対する Message Integrity Check （MIC; メッセージ完全性チェック）を利用します。クライアント MFP はクライアント サポートを提供します。クライアント MFP は、WLAN に対する一般的な攻撃の多くを無力化することによって、認証されたクライアントをスプーフィング フレームから保護します。

管理フレーム保護の稼動には WDS が必要で、この保護は 32MB プラットフォーム（1130、1240 シリーズ アクセス ポイント、および AP モードの 1300 シリーズ アクセス ポイント）でのみ利用できます。MFP は WLSE で設定されますが、アクセス ポイントおよび WDS では MFP を手動で設定できます。

（注）　WLSE が存在しないと MFP では検出した侵入をレポートできないため、有効性が限定されます。WLSE が存在する場合は、WLSE から設定を実行します。

完全に保護するには、MFP アクセス ポイントで Simple Network Transfer Protocol （SNTP）を設定します。

概要

クライアント MFP は、アクセス ポイントと CCXv5 対応クライアント ステーション間で送信されるクラス 3 の管理フレームを暗号化し、スプーフィングされた クラス 3 の管理フレーム（AP と認証およびアソシエートされたクライアント ステーション間で送信される管理フレーム）を廃棄することによって AP とクライアントの両方が予防措置を実行できるようにします。クライアント MFP は、IEEE 802.11i に規定されたセキュリティ メカニズムを使用して、クラス 3 ユニキャスト管理フレームを保護します。再アソシエーション要求の RSNIE で Spanning Tree Alogorithm（STA; スパニング ツリー アルゴリズム）によって決定されたユニキャスト暗号スイートによって、ユニキャスト データとクラス 3 管理フレームの両方が保護されます。ワークグループ ブリッジ、リピータ、または非ルート ブリッジモードのアクセス ポイントでクライアント MFP を使用するには、TKIP または AES-CCMP のいずれかのネゴシエーションが必要です。

ユニキャスト管理フレームの保護

ユニキャスト クラス 3 管理フレームは、すでにデータ フレームに使用されている方法と同様にして AES-CCMP と TKIP のいずれかを適用することによって保護されます。クライアント MFP は、暗号化が AES-CCMP または TKIP で、キー管理 WPA バージョン 2 の場合に限り、Autonomous アクセス ポイントで有効化されます。

ブロードキャスト管理フレームの保護

ブロードキャスト フレームを使用した攻撃を防ぐため、CCXv5 をサポートするアクセス ポイントではブロードキャスト クラス 3 管理フレームを送信しません。クライアント MFP が有効化されている場合、ワークグループ ブリッジ、リピータ、または非ルート ブリッジモードのアクセス ポイントでは、ブロードキャスト クラス 3 の管理フレームが廃棄されます。

クライアント MFP は、暗号化が AES-CCMP または TKIP で、キー管理 WPA バージョン 2 の場合に限り、Autonomous アクセス ポイントで有効化されます。

ルート モードのアクセス ポイントのクライアント MFP

ルート モードの Autonomous アクセス ポイントでは、混合モードのクライアントがサポートされます。CCXv5 に対応し、WPAv2 の暗号スイート AES または TKIP が決定されているクライアントは、クライアント MFP が有効です。CCXv5 に対応していないクライアントでは、クライアント MFP が無効です。デフォルトの場合、クライアント MFP はアクセス ポイント上の特定の SSID に対するオプションで、SSID 設定モードで CLI を使用して有効と無効を切り替えることができます。

個別の SSID ごとに、クライアント MFP を必須とするか、オプションとするかを設定できます。クライアント MFP を必須とする設定を行うには、キー管理 WPA バージョン 2 を必須に設定する必要があります。キー管理が WPAv2 必須に設定されていない場合、エラー メッセージが表示され CLI コマンドが拒否されます。クライアント MFP を必須として設定したキー管理およびキー管理 WPAv2 を変更しようとすると、エラー メッセージが表示され、CLI コマンドが拒否されます。オプションとして設定されている場合、クライアント MFP は SSID で WPAv2 に対応している場合にのみ有効化され、これに対応していない場合は MFP が無効化されます。

クライアント MFP の設定

次の CLI コマンドは、ルート モードのアクセス ポイントでクライアント MFP を設定する際に使用されます。

ids mfp client required

この SSID 設定コマンドは、特定の SSID でクライアント MFP を必須として有効化します。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。また、このコマンドでは、SSID が WPA バージョン 2 が必須として設定されていることが要求されます。SSID で WPAv2 が必須として設定されていない場合、エラー メッセージが表示され、コマンドが拒否されます。

no ids mfp client

この SSID 設定コマンドは、特定の SSID でクライアント MFP を無効にします。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。

ids mfp client optional

この SSID 設定コマンドは、特定の SSID でクライアント MFP をオプションとして有効化します。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。この SSID が WPAv2 に対応している場合は、SSID でクライアント MFP が有効になりますが、対応していない場合はクライアント MFP が無効になります。

show dot11 ids mfp client statistics

このコマンドを使用すると、Dot11Radio インターフェイスのアクセス ポイント コンソールにクライアント MFP 統計が表示されます。

clear dot11 ids mfp client statistics

このコマンドを使用すると、クライアント MFP 統計がクリアされます。

authentication key management wpa version {1|2}

このコマンドを使用すると、特定の SSID の WPA キー管理に使用される WPA バージョンが明示的に指定されます。

	コマンド	説明
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 ids mfp generator**	アクセス ポイントを MFP ジェネレータとして設定します。有効にすると、アクセス ポイントは Message Integrity Check Information Element （MIC IE; メッセージ完全性チェック情報エレメント）を追加して送信する管理フレームを保護します。フレームのコピー、改変、およびリプレイなどの攻撃が仕掛けられた場合、MIC が無効にされ、MFP フレームを検出（検証）するように設定された受信アクセス ポイントのすべてで不一致がレポートされます。アクセス ポイントは、WDS のメンバーである必要があります。
ステップ 3	**dot11 ids mfp detector**	アクセス ポイントを MFP ディテクタとして設定します。有効にすると、アクセス ポイントで他のアクセス ポイントから受信した管理フレームが検証されます。有効な要求 MIC IE が含まれないフレームを受信すると、WDS に不一致がレポートされます。アクセス ポイントは、WDS のメンバーである必要があります。
ステップ 4	**sntp server** *server IP address*	SNTP サーバの名前または IP アドレスを入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（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。

特権 EXEC モードから、次の手順に従って WDS を設定します。

	コマンド	説明
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 ids mfp distributor**	WDS を MFP ディストリビュータとして設定します。有効にすると、WDS では署名キーが管理されます。このキーは MIC IE の作成に使用され、ジェネレータとディテクタ間に安全に転送されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（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。

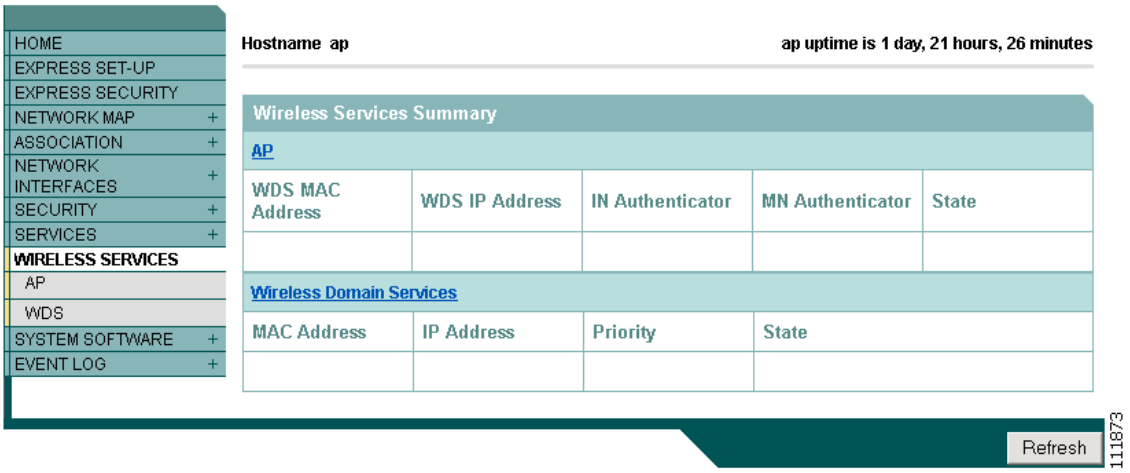
無線管理の設定

* 無線 LAN 上のアクセス ポイントで WDS の使用を設定すると、このアクセス ポイントは WDS デバイスとの対話時に自動的に無線管理における役割を実行します。無線管理の設定を行うには、ネットワーク上の WLSE デバイスと対話するように WDS デバイスを設定します。

WDS デバイスとして設定されたアクセス ポイント上の無線管理を有効にする手順は、次のとおりです。

ステップ 1　Wireless Services Summary ページを表示します。図 12-16 は、Wireless Services Summary ページを示しています。

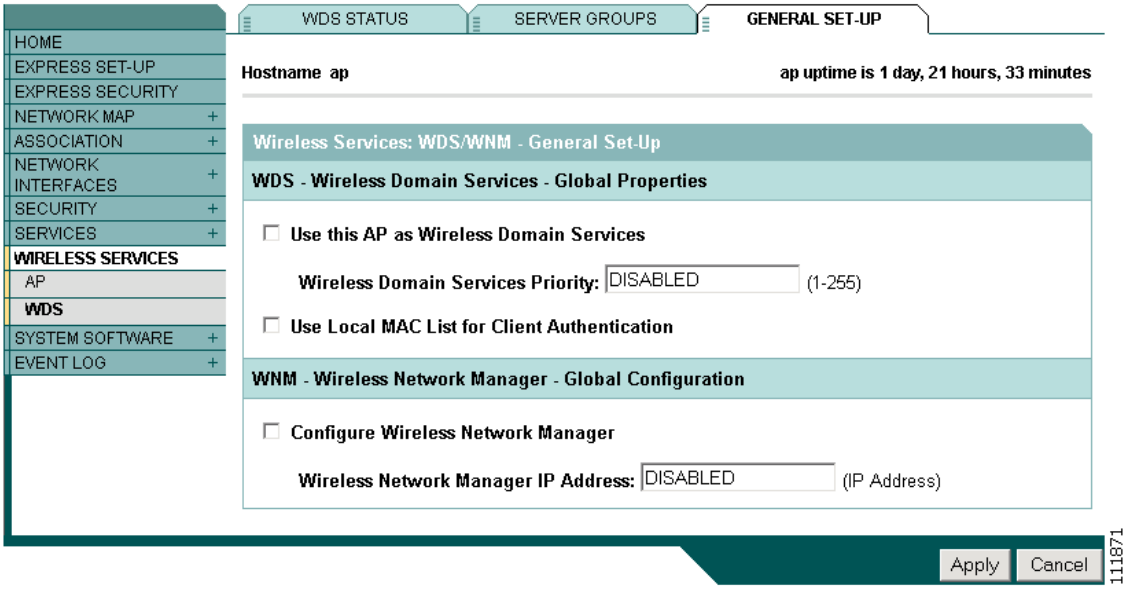
図 12-16　Wireless Services Summary ページ



ステップ 2　**WDS** をクリックして General Setup ページを表示します。

ステップ 3　WDS/WNM Summary ページで、**Settings** をクリックして General Setup ページを表示します。図 12-17 は、General Setup ページを示しています。

図 12-17　WDS/WNM General Setup ページ



ステップ 4　*Configure Wireless Network Manager* チェックボックスをオンにします。

ステップ 5　*Wireless Network Manager IP Address* フィールドに、ネットワーク上の WLSE デバイスの IP アドレスを入力します。

ステップ 6　**Apply** をクリックします。WDS アクセス ポイントが WLSE デバイスと対話するように設定されます。

CLI の設定例

次の例は、「無線管理の設定」の項（P.12-31）に記載された手順と同じ機能を果たす CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# wlccp wnm ip address 192.250.0.5
AP(config)# end
```

この例では、WDS アクセス ポイントは、IP アドレスが 192.250.0.5 の WLSE デバイスと対話できるようになります。

この例で使用されているコマンドの詳細は、『Cisco Aironet アクセス ポイント / ブリッジ Cisco IOS コマンド リファレンス』を参照してください。

アクセスポイントの WIDS 参加の設定

WIDS に参加するには、アクセス ポイントで WDS と無線管理への参加を設定する必要があります。アクセス ポイントの WDS および無線管理への参加を設定するには、「アクセス ポイントを WDS デバイスを使用するように設定する」の項（P.12-15）および「無線管理の設定」の項（P.12-31）の手順を実行します。

アクセス ポイントをスキャナ モードに設定する

スキャナ モードの場合、アクセス ポイントは無線活動のチャネルをすべてスキャンし、その活動をネットワーク上の WDS デバイスに報告します。スキャナ アクセス ポイントは、クライアント アソシエーションを受け付けません。

特権 EXEC モードから、次の手順に従ってアクセス ポイントに無線ネットワークの役割をスキャナに設定します。

	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 dot11radio { 0 | 1 }**	無線インターフェイスのインターフェイス設定モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。
ステップ 3	**station role scanner**	アクセス ポイントの役割をスキャナに設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

アクセス ポイントをモニタ モードに設定する

アクセス ポイントをスキャナとして設定すると、モニタ モードでフレームのキャプチャも可能になります。モニタ モードでは、アクセス ポイントは 802.11 フレームをキャプチャし、これをネットワーク上で WIDS エンジンに転送します。アクセス ポイントは、転送するすべての 802.11 フレームに 28 バイトのキャプチャ ヘッダーを追加します。ネットワーク上の WIDS エンジンは、このヘッダー情報を分析に使用します。アクセス ポイントは、キャプチャしたフレームの転送に User Datagram Protocol（UDP; ユーザ データグラム プロトコル）パケットを使用します。ネットワーク帯域幅を節約するため、複数のキャプチャしたフレームを 1 つの UDP パケットに結合できます。

スキャナ モードでは、アクセス ポイントは無線活動のすべてのチャネルをスキャンします。ただし、モニタ モードの場合、アクセス ポイントは、アクセス ポイント無線が設定されているチャネルだけを監視します。

（注） アクセス ポイントに 2 つ無線が含まれている場合、インターフェイス上でモニタ モードを設定するには、無線が両方ともスキャナ モードに設定されている必要があります。

特権 EXEC モードから、次の手順に従って 802.11 フレームをキャプチャして転送するようにアクセス ポイントを設定します。

	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 dot11radio** {**0** | **1**}	無線インターフェイスのインターフェイス設定モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。
ステップ 3	**monitor frames endpoint ip address** *IP-address* **port** *UDP-port* [**truncate** *truncation-length*]	モニタ モードに無線を設定するネットワーク上の WIDS エンジン上で、IP アドレスと UDP ポートを入力します。 • （オプション）転送したフレームごとに、バイト単位で最大長を設定します。アクセス ポイントは、この値より長いフレームを切り捨てます。デフォルトの長さは 128 バイトです。
ステップ 4	**end**	特権 EXEC モードに戻ります。

モニタ モード統計の表示

show wlccp ap rm monitor statistics グローバル設定コマンドを使用して、キャプチャしたフレームの統計を表示します。

コマンドの出力結果は、次のようになります。

```
ap# show wlccp ap rm monitor statistics

Dot11Radio 0
====================
WLAN Monitoring           : Enabled
Endpoint IP address       : 10.91.107.19
Endpoint port             : 2000
Frame Truncation Length   : 535 bytes

Dot11Radio 1
====================
WLAN Monitoring           : Disabled

WLAN Monitor Statistics
=========================
Total No. of frames rx by DOT11 driver      : 58475
Total No. of Dot11 no buffers               : 361
Total No. of Frames Q Failed                : 0
Current No. of frames in SCAN Q             : 0

Total No. of frames captured                : 0
Total No. of data frames captured           : 425
Total No. of control frames captured        : 1957
Total No. of Mgmt frames captured           : 20287
Total No. of CRC errored frames captured: 0

Total No. of captured frames forwarded      : 23179
Total No. of captured frames forward failed : 0
```

clear wlccp ap rm statistics コマンドを使用して、モニタ モード統計を消去します。

モニタ モード制限の設定

モニタ モードでアクセス ポイントが使用するしきい値を設定できます。しきい値を超えると、アクセス ポイントは、情報をログに記録するかまたは警告を送信します。

認証失敗制限の設定

認証失敗制限を設定すると、*EAPOL フラッディング*と呼ばれるサービス拒否攻撃からネットワークを保護できます。クライアントとアクセス ポイントとの間で発生する 802.1X 認証により、アクセス ポイント、認証者、および EAPOL メッセージングを使用する認証サーバの間に、一連のメッセージが表示されます。通常、RADIUS サーバである認証サーバは、過度に認証が試みられるとすぐに負荷に耐えられなくなります。規制されていない場合、1 台のクライアントからネットワークに影響を与えるほどの認証要求が発生する可能性があります。

モニタ モードでは、アクセス ポイントは 802.1X クライアントがアクセス ポイントを通じて認証を試みる割合をトラッキングします。過度な認証の試みによってネットワークが攻撃される場合、アクセス ポイントは、認証しきい値が超えると警告を発します。

これらの制限はアクセス ポイント上で設定できます。

- アクセス ポイントからの 802.1X の試みの回数
- アクセス ポイント上の秒単位での EAPOL フラッドの期間

アクセス ポイントは、過度の認証の試みを検出すると、この情報を示すための MIB 変数を設定します。

- EAPOL フラッドが検出されました。
- 認証の試みの回数
- 認証の試みの回数が最も多いクライアントの MAC アドレス

特権 EXEC モードから、次の手順に従って、アクセス ポイント上の失敗をトリガする認証制限を設定します。

	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 ids eap attempts** *number* **period** *seconds*	認証の試みの回数と、アクセス ポイント上で失敗をトリガする EAPOL フラッドの秒数を設定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

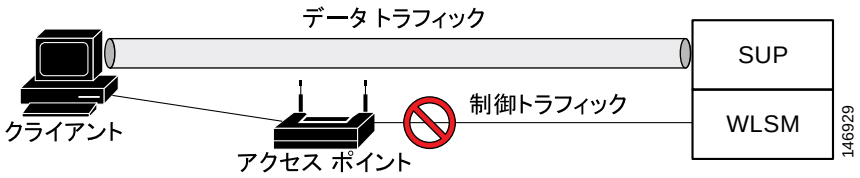
WLSM フェールオーバーの設定

WLSM 障害時にホットスタンバイに類似の機能を確保するため、WLSM バージョン 2.13 リリースでは、復元トンネル リカバリ、およびアクティブとスタンバイの WLSM がサポートされます。

復元トンネル リカバリ

単一シャーシ シナリオ（1 つのシャーシに 1 つの WLSM）では、WLSM ソフトウェアに障害が発生した場合も、SUP に接続されている既存のアクセス ポイント クライアントがその SUP への接続を継続し、サービスの中断が認識されません。アクセス ポイントが WLSM 障害を検出したときに、アクティブなトンネルは破壊されずクライアントと SUP 間のデータ トラフィックの通信が保持されます。しかし WLSM 障害が原因で、アクセス ポイントと WLSM 間で送信される制御トラフィックは中断され（図 12-18 参照）、アクセス ポイントでは WLSM ソフトウェアがオンラインに復旧するまで新規のクライアント接続を承認できません。復元トンネル リカバリは自動実行され、特別な設定は必要ありません。

図 12-18　復元トンネル リカバリ



アクティブ / スタンバイ WLSM のフェールオーバー

WLSM では、復元トンネル リカバリのほかにアクティブ WLSM とスタンバイ WLSM の 2 つの WLSM を 1 つのシャーシに展開できるようにすることで、回復機能のサポートがさらに強化されています。アクティブ WLSM に障害が発生すると、スタンバイ WLSM がアクティブになり、データ トラフィックを中断することなく、既存および新しいアクセス ポイント クライアントのトラフィックの制御を行います。復元トンネル リカバリにこの機能を加えることによって、WLSM 障害時にホットスタンバイに類似の機能が提供されます。