CHAPTER 25

WDS、高速セキュア ローミング、および無線管理の設定

このマニュアルでは、アクセス ポイントに Wireless Domain Services（WDS）、クライアント デバイスの高速セキュア ローミング、および無線管理を設定する方法について説明します。具体的な内容は次のとおりです。

- 「WDS の概要」（P.25-1）
- 「高速セキュア ローミングの概要」（P.25-2）
- 「無線管理の概要」（P.25-4）
- 「WDS および高速セキュア ローミングの設定」（P.25-4）
- 「デバッグ メッセージの使用方法」（P.25-13）

WDS の概要

以降の各項では、WDS について説明するとともに、Cisco Wireless Mobile Interface Card（WMIC）がアクセス ポイントとして設定されている場合でも WDS サーバとして設定できることを説明します。アクセス ポイントとして設定された WMIC は、WDS サーバを使用して、WDS オーセンティケータ（クライアント）として機能できます。

WDS を実行するようにアクセス ポイントが設定されているときは、無線 LAN 上の他のアクセス ポイント（アクセス ポイントとして設定された WMIC など）は、この WDS アクセス ポイントを使用して、クライアント デバイスの高速セキュア ローミングを行うとともに、無線管理に参加します。

高速セキュア ローミングは、クライアント デバイスがアクセス ポイント間で移動するときの再認証を短時間で実行し、音声やその他の時間依存アプリケーションの遅延を防止します。

無線管理に参加するアクセス ポイントは、無線環境に関する情報（不正アクセス ポイントの可能性があるものや、クライアントのアソシエーションとアソシエーション解除など）を WDS アクセス ポイントに転送します。WDS アクセス ポイントはこの情報を集計して、ネットワーク上の Wireless LAN Solution Engine（WLSE）デバイスに転送します。

WDS アクセス ポイントの役割

WDS アクセス ポイントは無線 LAN で次の作業を実行します。

- 自身の WDS 機能をアドバタイズし、無線 LAN のための最適な WDS アクセス ポイントの選定に参加します。無線 LAN に WDS を設定する場合は、1 つのアクセス ポイントをメインの WDS アクセス ポイント候補として設定し、1 つまたは複数の別のアクセス ポイントをバックアップの WDS アクセス ポイント候補として設定します。
- サブネット内のすべてのアクセス ポイントを認証し、それぞれとのセキュアな通信チャネルを確立します。
- サブネット内のアクセス ポイントから無線データを収集し、データを集計して、ネットワーク上の WLSE デバイスに転送します。
- サブネット内のすべてのクライアント デバイスを登録し、これらのセッション キーを設定して、セキュリティ クレデンシャルをキャッシュに格納します。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と、WDS アクセス ポイント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。

WDS アクセス ポイントを使用するアクセス ポイントの役割

無線 LAN 上のアクセス ポイントは、次のアクティビティに関して WDS アクセス ポイントと相互作用します。

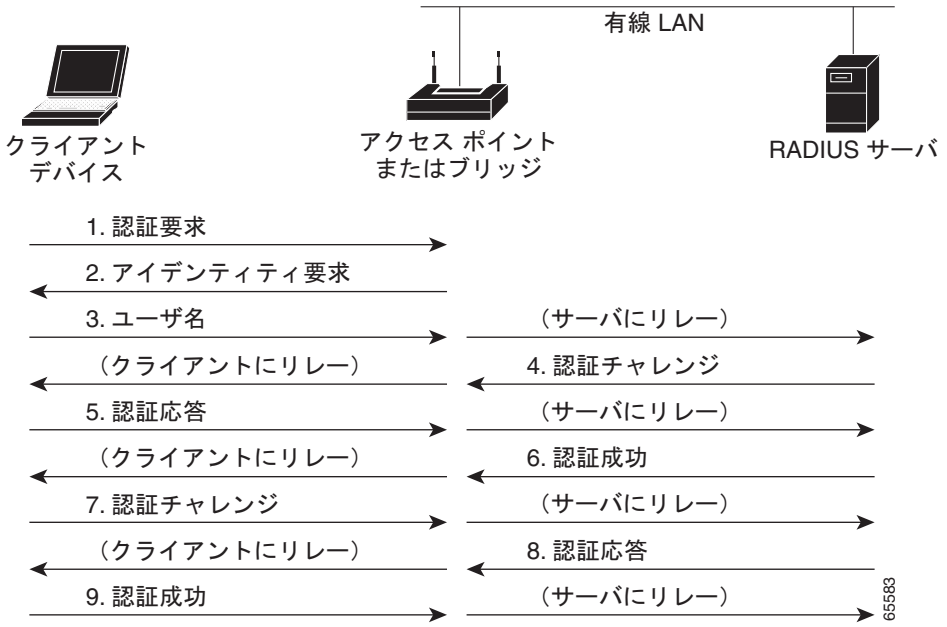
- 現在の WDS アクセス ポイントを検出して追跡し、WDS アドバタイズを無線 LAN にリレーします。
- WDS アクセス ポイントに対する認証を行い、WDS アクセス ポイントへのセキュアな通信チャネルを確立します。
- アソシエートしたクライアント デバイスを WDS アクセス ポイントに登録します。
- 無線データを WDS アクセス ポイントに報告します。

高速セキュア ローミングの概要

通常、無線 LAN 内のアクセス ポイントは、設置されたアクセス ポイント間でローミングを行うモバイル クライアント デバイスを処理します。クライアント デバイスで稼動するアプリケーションの中には、別のアクセス ポイントにローミングするときに、再アソシエーションを短時間で行わなければならないものもあります。たとえば、音声アプリケーションでは会話の遅延や途切れを防止するために、ローミングをシームレスに行う必要があります。

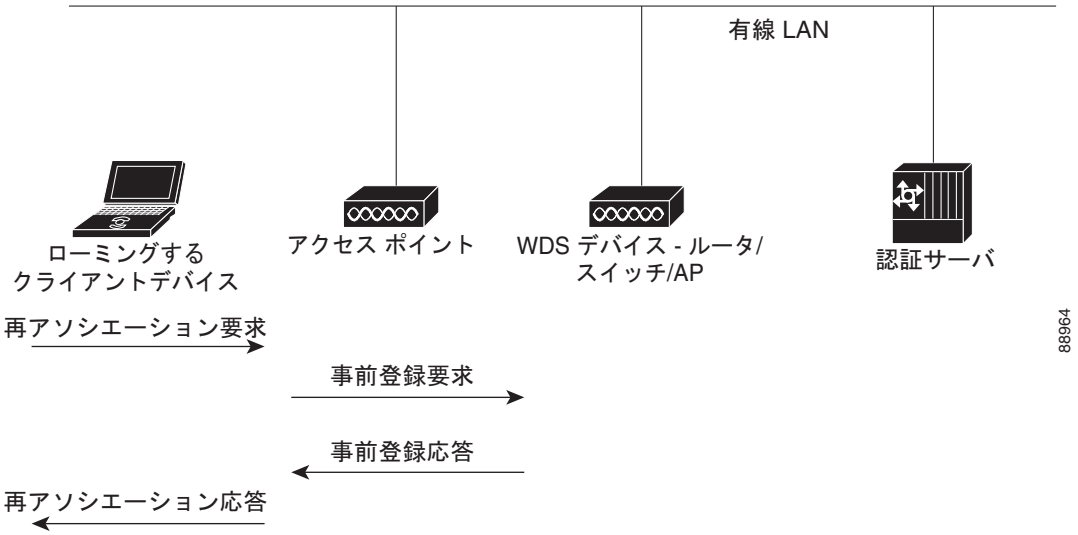
通常動作時は、LEAP 対応クライアント デバイスと新しいアクセス ポイントとが相互認証を行うときに、完全な LEAP 認証が実行されます。これには、メイン RADIUS サーバとの通信も含まれます（図 25-1 を参照）。

図 25-1　RADIUS サーバを使用したクライアント認証



ただし、無線 LAN に高速セキュア ローミングを設定すると、LEAP 対応クライアント デバイスがアクセス ポイント間でローミングするときに、メイン サーバの関与は不要になります。Cisco Centralized Key Management（CCKM）を使用すると、WDS を実行するように設定されたアクセス ポイントが RADIUS サーバに代わってクライアントを短時間で認証することができるので、音声などの遅延に敏感なアプリケーションにおいて認識可能な遅延が生じることはなくなります。図 25-2 に、CCKM を使用したクライアント認証を示します。

図 25-2　CCKM および WDS アクセス ポイントを使用したクライアント再アソシエーション



WDS アクセス ポイントは、無線 LAN 上にある CCKM 対応クライアント デバイスのクレデンシャルのキャッシュを維持します。アクセス ポイント間でローミングした CCKM 対応クライアントは、再アソシエーション要求を新しいアクセス ポイントに送信します。新しいアクセス ポイントは、この要求を WDS アクセス ポイントにリレーします。WDS アクセス ポイントは、クライアントのクレデンシャルを新しいアクセス ポイントに転送し、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 ポイントの間で受け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所要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使用して、ユニキャスト キーも生成します。

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、無線環境を調べて、無線情報に関するレポートを WDS アクセス ポイントに送信します。報告される情報には、不正アクセス ポイントの可能性があるもの、アソシエートしているクライアント、クライアント信号強度、他のアクセス ポイントからの無線信号などがあります。WDS アクセス ポイントは、集計され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、無線 LAN の自己修復機能も支援します。これは、近隣のアクセス ポイントに障害が発生した場合にカバレッジを提供するように設定を自動調整する機能です。

WDS および高速セキュア ローミングの設定

ここでは、無線 LAN に WDS および高速セキュア ローミングを設定する手順について説明します。ここでは、次の内容について説明します。

- 「WDS に関する注意事項」（P.25-4）
- 「WDS および高速セキュア ローミングの要件」（P.25-5）
- 「WDS アクセス ポイントを使用するように WMIC を設定する方法」（P.25-5）
- 「高速セキュア ローミングをサポートするように認証サーバを設定する方法」（P.25-6）
- 「CLI コマンドを使用して WDS サーバをイネーブルにする方法」（P.25-10）
- 「CLI コマンドを使用してルート デバイスをイネーブルにする方法」（P.25-11）
- 「デバッグ メッセージの使用方法」（P.25-13）

WDS に関する注意事項

WDS の設定を行うときは、次の注意事項に従ってください。

- WDS アクセス ポイントがクライアント デバイスの処理も行う場合は、参加するアクセス ポイントを最大 30 台サポートしますが、WDS アクセス ポイントの無線が無効になっている場合は、参加するアクセス ポイントを最大 60 台サポートできます。
- WDS 専用モードでは、WDS によってサポートされるインフラストラクチャ アクセス ポイントは最大 60 台、クライアント数は最大 1200 です。
- 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 の候補として設定しないでください。また、イーサネットの障害時に WDS アクセス ポイントをリピータ モードに戻す（フォールバックする）ようには設定しないでください。

WDS および高速セキュア ローミングの要件

WMIC が配置された無線 LAN は、次の要件を満たす必要があります。

- 中央の Wireless Domain Services（WDS）サーバが特定のゾーンの処理を行っている（詳細は第 25 章「WDS、高速セキュア ローミング、および無線管理の設定」を参照）。
- ルート デバイスがそのゾーンの中央 WDS サーバと通信するように設定されている。
- サブネット / ゾーン境界上のルート デバイスが、ホーム エージェントへの未認証トラフィックだけを許可するように設定されている。
- 外部エージェント モードの Modem over IP（MoIP）。
- シスコ互換のクライアント デバイス。Cisco Compatible eXtensions（CCX）バージョン 2 以降に準拠していること。

WDS アクセス ポイントを使用するように WMIC を設定する方法

WDS を使用するように WMIC を設定するには、まずアクセス ポイントとして設定する必要があります。WDS アクセス ポイントを通して認証を行い、CCKM に参加するように、WMIC を設定します。

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

この例では、WMIC は WDS アクセス ポイントと相互作用できるように設定され、認証サーバに対する認証にはユーザ名 *APWestWing* およびパスワード *wes7win8* が使用されます。アクセス ポイントを認証サーバのクライアントとして設定する場合は、同じユーザ名およびパスワードのペアを設定する必要があります。

同様に、WDS アクセス ポイントを使用するようにアクセス ポイントを設定するには、アクセス ポイントに暗号方式および認証方式を設定する必要があります。次に例を示します。

```
encryption mode ciphers ckip-cmic
 !
 ssid kin_leap
    authentication network-eap eap_methods
    authentication key-management cckm
```

詳細については、「認証タイプ」を参照してください。

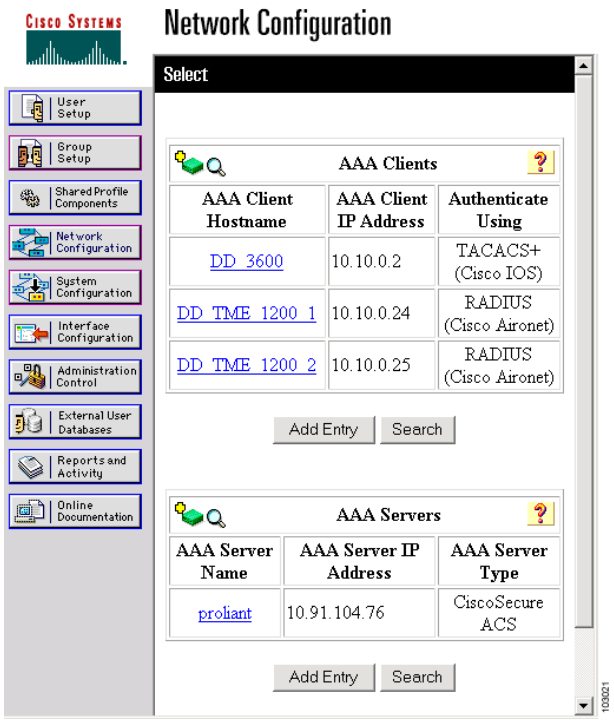
高速セキュア ローミングをサポートするように認証サーバを設定する方法

CCKM に参加している WDS アクセス ポイントおよびすべてのアクセス 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 ポイントのユーザ名とパスワード、および WDS アクセス ポイントのユーザ名とパスワードを設定する必要があります。

サーバにアクセス ポイントを設定する手順は、次のとおりです。

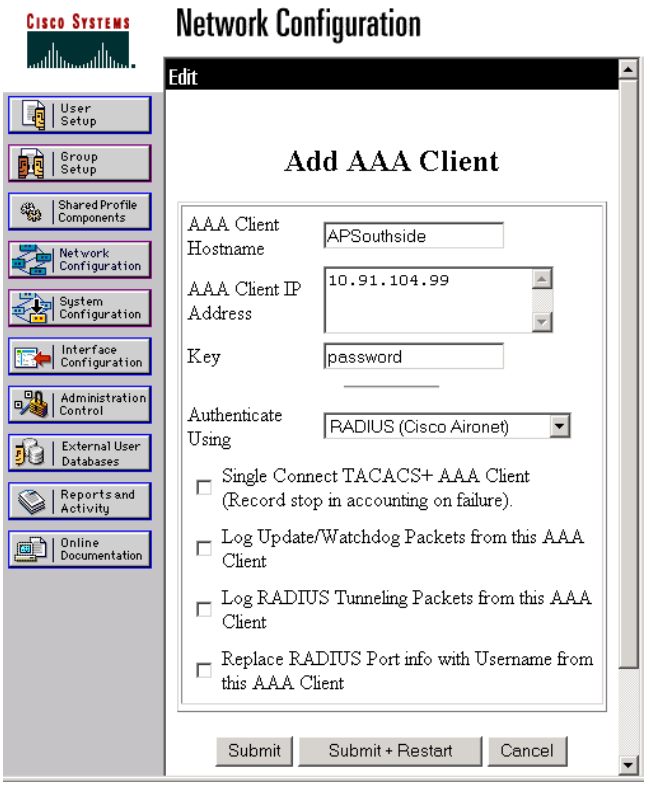
ステップ 1　Cisco Secure ACS にログインし、[Network Configuration] をクリックして [Network Configuration] ページを表示します。この [Network Configuration] ページを使用して、WDS アクセス ポイントのエントリを作成する必要があります。図 25-3 に、[Network Configuration] ページを示します。

図 25-3　[Network Configuration] ページ



ステップ 2　[AAA Clients] テーブルの下の [Add Entry] をクリックします。[Add AAA Client] ページが表示されます。図 25-4 に、[Add AAA Client] ページを示します。

図 25-4　[Add AAA Client] ページ



ステップ 3　[AAA Client Hostname] フィールドに、WDS アクセス ポイント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 アクセス ポイントの IP アドレスを入力します。

ステップ 5　[Key] フィールドに、WDS アクセス ポイントに設定されたパスワードとまったく同じパスワードを入力します。

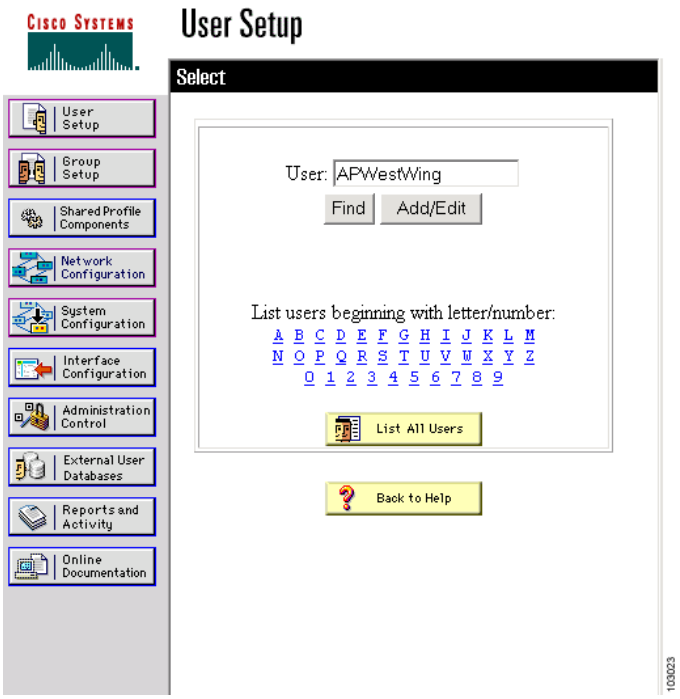
ステップ 6　[Authenticate Using] ドロップダウン メニューで、[RADIUS] を選択します。

ステップ 7　[Submit] をクリックします。

ステップ 8　WDS アクセス ポイントの候補ごとに、ステップ 2 ～ ステップ 7 を繰り返します。

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。この [User Setup] ページを使用して、WDS アクセス ポイントを使用するアクセス ポイントのエントリを作成する必要があります。図 25-5 に、[User Setup] ページを示します。

図 25-5　[User Setup] ページ

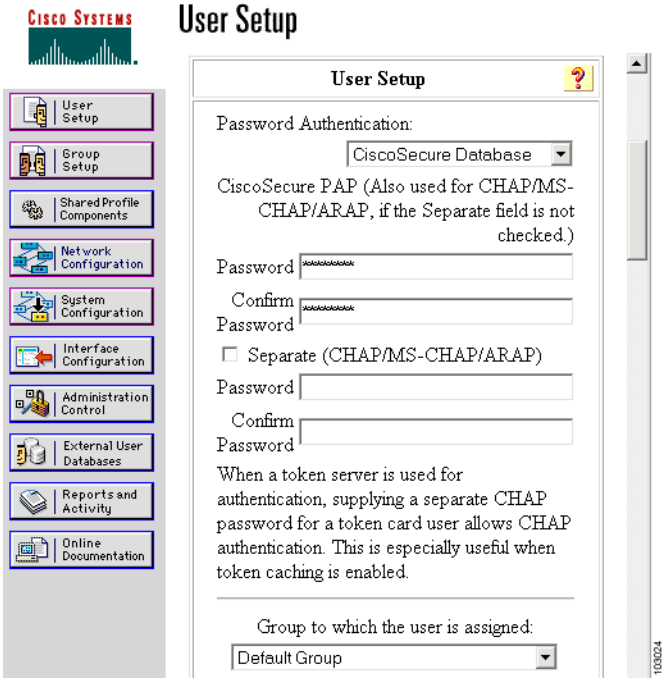


ステップ 10　[User] フィールドにアクセス ポイントの名前を入力します。

ステップ 11　[Add/Edit] をクリックします。

ステップ 12　下の [User Setup] ボックスまでスクロールします。図 25-6 に、[User Setup] ボックスを示します。

図 25-6　　ACS の [User Setup] ボックス



ステップ 13　[Password Authentication] ドロップダウン メニューで [CiscoSecure Database] を選択します。

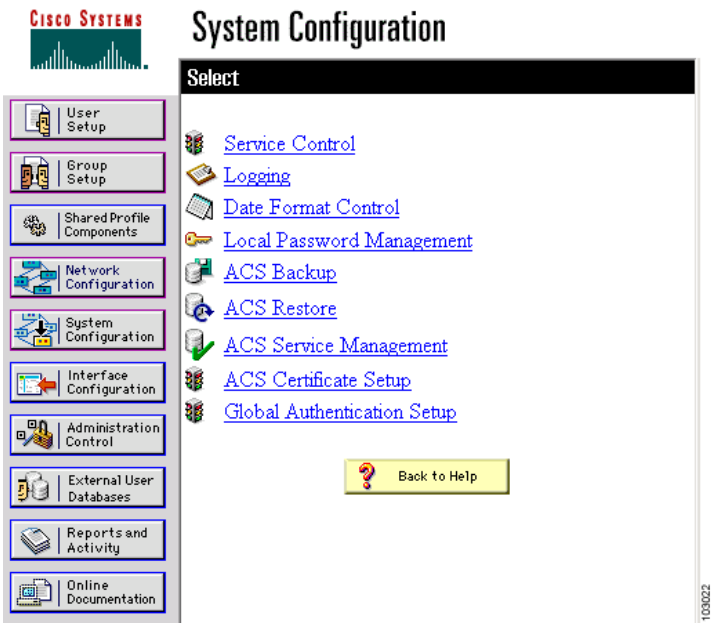
ステップ 14　[Password] および [Confirm Password] フィールドに、[Wireless Services AP] ページで入力したアクセス ポイントのパスワードとまったく同じパスワードを入力します。

ステップ 15　[Submit] をクリックします。

ステップ 16　WDS アクセス ポイントを使用するアクセス ポイントごとに、ステップ 10 ～ステップ 15 を繰り返します。

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を適用します。図 25-7 に、[System Configuration] ページを示します。

図 25-7　ACS の [System Configuration] ページ



CLI コマンドを使用して WDS サーバをイネーブルにする方法

次に示す CLI（コマンドライン インターフェイス）コマンドは、WDS サーバをイネーブルにするために必要です。コマンドの **no** 形式は、WDS サーバをディセーブルにするときに使用します。同じ設定が、中央 WDS サーバとサブネットごとの WDS サーバに適用されます。同じ設定が WMIC に適用されます。

```
[no] wlccp wds priority <1-255> interface BVI1
[no] wlccp authentication-server infrastructure <method_infra>
where <method_infra> is <authentication server list name>
[no] wlccp authentication-server client [any | eap | leap | mac] <method_client>
where <method_ client > is <authentication server list name>
[no] aaa group server radius infra
    [no] server <IP address of RADIUS server> auth-port <Port number> acct-port <Port
    number>
[no] aaa group server radius client
    [no] server <IP address of RADIUS server> auth-port <Port number> acct-port <Port
    number>
[no] aaa authentication login <method_infra> group infra
where <method_infra> is <named authentication list>

[no] aaa authentication login <method_client> group client
where <method_ client > is <named authentication list>
```

CLI コマンドを使用してルート デバイスをイネーブルにする方法

次に示す CLI コマンドは、ルート デバイスと中央 WDS サーバが通信できるようにするために必要です。**no** 形式は、WDS サーバをディセーブルにするときに使用します。この設定を行うと、中央 WDS サーバが停止した場合にルート デバイスがサブネットごとの WDS サーバを使用して認証を行うことも可能になります。

```
[no] wlccp ap wds ip address <IP address of the WDS>
[no] wlccp ap username <WLCCP user name> password 0 <The UNENCRYPTED (cleartext) LEAP
password>
[no] interface Dot11Radio0
    [no] encryption mode ciphers [aes-ccm | tkip | wep128 | wep40]
    [no] ssid <radio Service Set ID>
[no] authentication network-eap <eap_methods>
                where <eap_methods> is <leap list name>
[no] authentication key-management cckm
[no] aaa group server radius rad_eap
    [no] server <IP address of RADIUS server> auth-port <Port number> acct-port <Port
    number>
[no] aaa authentication login <eap_methods> group rad_eap
where <eap_methods> is <named authentication list>
```

authentication network-eap <eap_methods> コマンドを実行すると、ルート デバイスによるクライアントの認証実行中にそのクライアントとの間でトラフィックを送受信できるようになります。このコマンドは、ゾーン境界内に存在するすべてのルート デバイスに対して、およびすべてのクライアントに対して実行してください。

```
authentication network-eap <eap_methods> <non-blocking>
```

<non-blocking> を指定すると、ルート デバイスによるクライアントの認証実行中に、そのクライアントがトラフィックを送受信できるようになります。

認証実行中のクライアント トラフィックのブロックをイネーブルにするには、このコマンドを **non-blocking** キーワードを指定せずに実行します。

```
authentication network-eap <eap_methods>
```

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ibm_r1/ib1_a1g.pdf には、クライアントからホーム エージェントへのトラフィック送信だけを許可するようにアクセス ポイント上のアクセス コントロール リストを設定する方法の詳しい説明があります。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/iprmb_r/ip4bookg.pdf には、モバイル IP 設定コマンドの詳しい説明があります。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtfamoip.htm には、*外部エージェント ローカル ルーティング*機能とその設定方法の詳しい説明があります。

WDS 情報の表示

CCKM に現在参加している WDS アクセス ポイントおよびその他のアクセス ポイントに関する情報を表示するには、イネーブル EXEC モードの CLI で次のコマンドを使用します。

コマンド	説明
show wlccp ap	CCKM に参加しているアクセス ポイントに対してこのコマンドを実行すると、WDS アクセス ポイントの MAC（メディア アクセス制御）アドレス、WDS アクセス ポイントの IP アドレス、アクセス ポイントのステート（認証中、認証済み、または登録済み）、インフラストラクチャ オーセンティケータの IP アドレス、クライアント デバイス（MN）オーセンティケータの IP アドレスが表示されます。
show wlccp wds { **ap** | **mn** } [**detail**] [**mac-addr** *mac-address*]	WDS アクセス ポイント専用です。アクセス ポイントおよびクライアント デバイスに関するキャッシュ内情報を表示する場合に使用します。 • **ap**：CCKM に参加しているアクセス ポイントを表示する場合に使用します。各アクセス ポイントの MAC アドレス、IP アドレス、ステート（認証中、認証済み、または登録済み）およびライフタイム（アクセス ポイントの再認証が必要になるまでの秒数）が表示されます。特定のアクセス ポイントに関する情報を表示するには、**mac-addr** オプションを使用します。 • **mn**：クライアント デバイス（別名モバイル ノード）に関するキャッシュ内情報を表示する場合に使用します。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しているアクセス ポイント（cur-AP）、およびステート（認証中、認証済み、または登録済み）が表示されます。**detail** オプションを指定すると、クライアントのライフタイム（クライアントの再認証が必要になるまでの秒数）、SSID、および VLAN ID が表示されます。特定のクライアント デバイスに関する情報を表示するには、**mac-addr** オプションを使用します。 **show wlccp wds** だけを入力した場合は、アクセス ポイントの IP アドレス、MAC アドレス、プライオリティ、およびインターフェイス ステート（管理上のスタンドアロン、アクティブ、バックアップ、または候補）が表示されます。ステートが「バックアップ」の場合は、現在の WDS アクセス ポイントの IP アドレス、MAC アドレス、およびプライオリティも表示されます。

デバッグ メッセージの使用方法

WDS アクセス ポイントと相互作用するデバイスに関するデバッグ メッセージ出力を制御するには、イネーブル EXEC モードで次の debug コマンドを使用します。

コマンド	説明
debug wlccp ap { **mn** | **mobility** | **rm** | **state** |**wds-discovery** }	クライアント デバイス（**mn**）、WDS 検出プロセス、および WDS アクセス ポイントに対するアクセス ポイント認証（**state**）に関連するデバッグ メッセージ出力を有効にする場合に使用します。
debug wlccp leap-client	LEAP 対応クライアント デバイスに関連するデバッグ メッセージ出力を有効にする場合に使用します。
debug wlccp packet	WDS アクセス ポイントとの間で送受信されるパケットを表示する場合に使用します。
debug wlccp wds [**state** | **statistics**]	WDS デバッグおよびステートに関するメッセージ出力を有効にする場合は、このコマンドに **state** オプションを使用します。障害に関する統計情報出力を有効にする場合は、**statistics** オプションを使用します。

CLI コマンドを使用してローミングをイネーブルにする方法

次の CLI コマンドは、ローミングをイネーブルにするときに使用します。

- **mobile station period <1-1000> threshold <1-100> mode <1-2>**
- **mobile station scan <channel / frequency list>**

Cisco 3205 5.0 GHz 無線では、クライアントはチャネル上にトラフィックがあることをリスニングによって確認してから、プローブ要求を送信します。このプロセスのため、WMIC が新しい AP に再アソシエートするには最大 3 秒かかります。ネットワークのチャネルが 1 つだけの場合は、mode コマンドの指定に従って Cisco 3205 無線のアクティブ スキャンが実行されます。このコマンドのデフォルト値は 2 です。このときは、WMIC はリスニングと送信をすべての使用可能なチャネルに対して行います。この値が 1 に設定されている場合は、WMIC はアクティブ スキャンを現在のアクティブ チャネルに対して実行します。WMIC が新しい AP にアソシエートされない場合は、WMIC は残りのチャネルに対するリスニングと送信を行って新しい AP を特定します。

mobile station scan <channel / frequency list> CLI コマンドを実行すると、「クライアント」モードの WMIC が「ルート」デバイスを見つけるためのスキャン対象のチャネル数を制限することができます。このようにすると、ローミング時間が短縮されます。