H3Cアクセスコントローラ

WLANローミング設定ガイド

New H3Cテクノロジーズ

http://www.h3c.com

ドキュメントバージョン:6W104-20210413製品バージョン:R5426P02

はじめに

アクセスコントローラのマニュアルセットでは、アクセスコントローラのソフトウェア機能について説明し、ソフトウェア設定手順をガイドします。また、さまざまなネットワークシナリオにソフトウェア機能を適用する際に役立つ設定例も提供します。

『WLAN Roaming Configuration Guide』では、WLANローミング、WLANローミングセンター、および802.11rの設定について説明しています。

ここでは、マニュアルに関する次のトピックについて説明します。

- 対象ユーザー
- 表記規則
- マニュアルに関するフィードバック

対象ユーザー

このマニュアルは、次の読者を対象としています。

- ネットワークプランナー。
- フィールドテクニカルサポートおよびサービスエンジニア
- H3Cアクセスコントローラを使用するネットワーク管理者

表記規則

ここでは、本マニュアルで使用されている表記法について説明します。

コマンドの表記法

規約	説明
ボールド体	太字のテキストは、表示されているとおりに入力したコマンドおよびキーワードを表します。
イタリック	斜体テキストは、実際の値に置き換える引数を表します。
[]	角カッコは、オプションの構文選択(キーワードまたは引数)を囲みます。
{ x | y | ... }	中カッコは、必要な構文選択のセットを縦棒で区切って囲み、その中から1つを選択します。
[x | y | ...]	角カッコは、オプションの構文選択のセットを縦棒で区切って囲みます。この中から1つを選択するか、何も選択しません。
{ x | y | ... } *	中カッコで囲まれたアスタリスクは、必要な構文選択のセットを縦棒で区切って囲みます。この中から少なくとも1つを選択します。
[x | y | ...] *	アスタリスクでマークされた角カッコは、オプションの構文選択を縦棒で区切って囲みます。この中から、1つの選択、複数の選択、またはなしを選択できます。
&<1-n>	アンパサンド(&)記号の前の引数またはキーワードと引数の組み合わせは、1回からn回まで入力できます。
#	シャープ(#)記号で始まる行はコメントです。

GUIの表記法

規約	説明
ボールド体	ウィンドウ名、ボタン名、フィールド名、メニュー項目は太字で表示されます。 たとえば、**New User**ウィンドウが開きます。**OK**をクリックします。
>	複数レベルのメニューは、山括弧で区切られています。たとえば、**File** > **Create** >**Folder**.

記号

規約	説明
⚠警告!	重要な情報に注意を喚起する警告であり、理解または従わないと、人身事故につながる可能性があります。
△注意:	重要な情報に注意を喚起するアラート。この情報を理解しない、またはこの情報に従わないと、データの損失、データの破損、ハードウェアまたはソフトウェアの損傷につながる可能性があります。
ⓘ重要:	重要な情報への注意を喚起する警告。
注:	追加情報または補足情報を含むアラート。
ヒント:	有用な情報を提供するアラート。

ネットワークトポロジのアイコン

表記規則	説明
	ルータ、スイッチ、ファイアウォールなどの汎用ネットワークデバイスを表します。
	ルータやレイヤ3スイッチなどのルーティング対応デバイスを表します。
	レイヤ2またはレイヤ3スイッチなどの一般的なスイッチ、またはレイヤ2その他のレイヤ2機能をサポートするルータを表します。
	統合有線WLANスイッチ上のアクセスコントローラ、統合有線WLANモジュール、またはアクセスコントローラエンジンを表します。
	アクセスポイントを表します。
	ワイヤレスターミネータユニットを表します。
	ワイヤレスターミネータを表します。
	メッシュアクセスポイントを表します。
	全方向信号を表します。
	方向信号を表します。
	ファイアウォール、UTM、マルチサービスセキュリティゲートウェイ、ロードバランシングデバイスなどのセキュリティ製品を表します。

	ファイアウォール、ロードバランシング、NetStream、SSL VPN、IPS、ACGモジュールなどのセキュリティモジュールを表します。

本書で提供されている例

このドキュメントの例では、使用しているデバイスとハードウェアモデル、構成、またはソフトウェアバージョンが異なるデバイスを使用している場合があります。ポート番号、サンプル出力、スクリーンショット、および例のその他の情報が、使用しているデバイスのものと異なるのは正常です。

マニュアルに関するフィードバック

製品ドキュメントに関するご意見は、info@h3c.comまでEメールでお送りください。ご意見に感謝いたします。

内容

WLANローミングの設定

WLANローミングについて

WLANローミングを使用するとクライアントはESS内のAP間をシームレスにローミングできますが、ローミングプロセス中もIPアドレスと認証情報は保持されます。

用語

- **Inter Access Device Tunneling Protocol** - IADTPは、H3C独自のプロトコルであり、デバイスが相互に安全に通信するための汎用パケットのカプセル化と転送メカニズムを提供します。ローミングサービスを提供するデバイスは、相互にIADTPトンネルを確立して、制御メッセージとクライアント情報を交換します。
- **ホームAC**: HAは、無線クライアントが最初にアソシエートするAPを管理するACです。
- **Foreign AC**: FAは、AC間ローミング後にクライアントがアソシエートするACです。
- **モビリティグループ**: クライアントがローミングできる複数のメンバーデバイスを含むグループです。

IADTPトンネル開設

モビリティグループ内のデバイスは、接続要求を開始するクライアントとして動作することも、接続要求をリッスンして応答するサーバとして動作することもできます。

図1 IADTPトンネルの構築

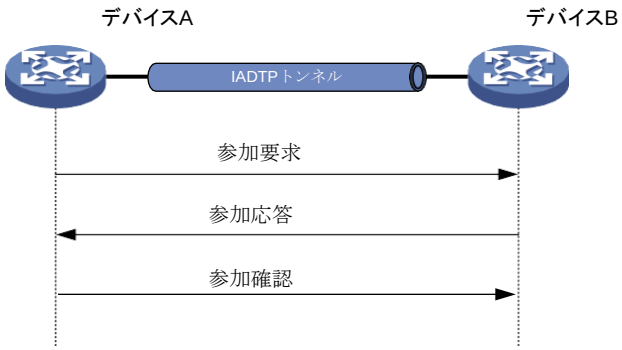


図1に示すように、次の手順を使用して2つのデバイスでIADTPトンネルを確立します。

1. デバイスAはデバイスBに参加要求を送信します。
2. 参加要求を受信すると、デバイスBはローカル設定とパケットコンテンツを使用して、デバイスAが同じモビリティグループに属しているかどうかを識別します。
   - デバイスBが同じモビリティグループに属している場合、デバイスBは成功を表す結果コードとともに参加応答を返します。
   - デバイスAが異なるモビリティグループに属している場合、デバイスAは失敗を表す結果コードとともに参加応答を返します。

3. 参加応答を受信すると、デバイスAIは応答の結果コードを検査します。
   - 結果コードが失敗を表す場合、デバイスAIはパケットを返しません。
   - 結果コードが成功を表す場合、デバイスAIはデバイスBに参加確認を送信します。
4. 参加確認を受信すると、デバイスBIはデバイスAIとIADTPトンネルを確立します。

WLANローミングメカニズム

クライアントは、同じモビリティグループ内のデバイス間でローミングできます。

AC内ローミング

AC内ローミングを使用すると、クライアントは同じACによって管理されているAP間で同じSSIDでローミングできます。

図2 AC内ローミング

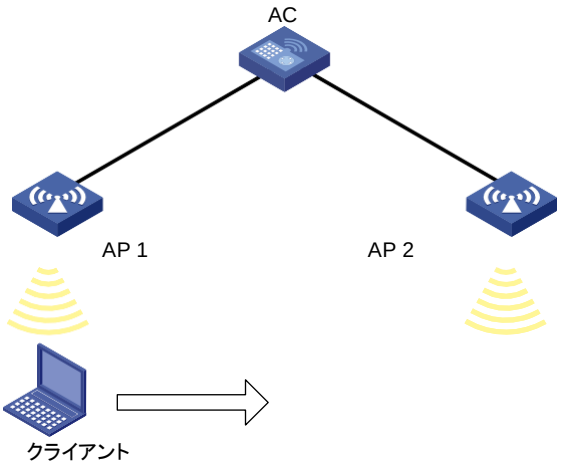


図2に示すように、AC内ローミングでは次の手順が使用されます。

1. クライアントはAP 1からオンラインになり、ACはクライアントのローミングエントリを作成します。
2. クライアントはAP 2にローミングします。ACはクライアントのローミングエントリを調べ、高速ローミングを実行するかどうかを決定します。

   クライアントがRSN + 802.1x認証を使用し、ACと同じPMKIDを伝送する場合、高速ローミングが使用され、クライアントは再認証なしでAP 2とアソシエートできます。そうでない場合、クライアントはAP 2とアソシエートする前に再認証をする必要があります。

AC間ローミング

AC間ローミングを使用すると、クライアントは異なるACによって管理されるAP間をローミングできます。これらのACは同じモビリティグループに属し、互いにIADTPトンネルを確立している必要があります。

図3 AC間ローミング

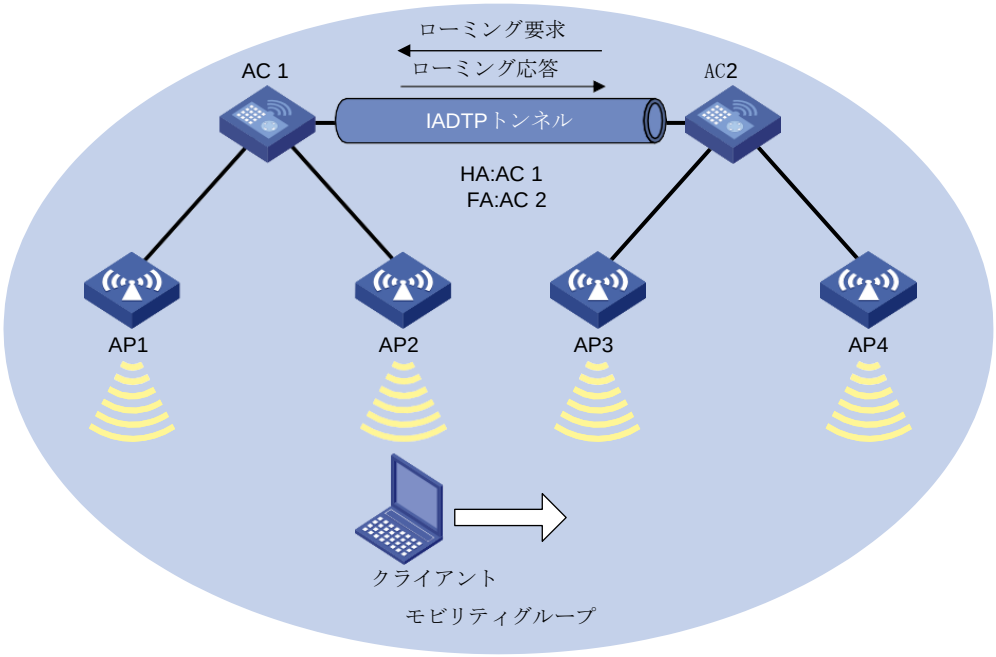


図3に示すように、AC間ローミングでは次の手順を使用します。

1. クライアントはAP 2からオンラインになります。AC 1はクライアントのローミングエントリを作成し、その情報をIADTPトンネル経由でAC 2に送信します。
2. クライアントはAP 3にローミングします。AC 2はクライアントのローミングエントリを調べ、高速ローミングを実行するかどうかを決定します。

   クライアントがRSN + 802.1x認証を使用し、ACと同じPMKIDを伝送する場合、高速ローミングが使用され、クライアントは再認証なしでAP 3とアソシエートできます。そうでない場合、クライアントはAP 3とアソシエートする前に再認証を行う必要があります。
3. クライアントはAP 3に関連付けられます。AC 2はAC 1にローミング要求を送信します。
4. AC 1はローミング要求を確認し、次のいずれかの操作を実行します。
   - 要求が無効な場合に、ローミング失敗を示すローミング応答をAC 2に送信します。AC 2はクライアントからログオフします。
   - ローミングトレースとローミングアウト情報を保存し、要求が有効な場合はローミング成功を示すローミング応答をAC 2に送信します。AC 2は、クライアントのローミングイン情報を保存します。

制約事項および注意事項:WLANローミング設定

APがクライアントオーセンティケータとして設定されているサービステンプレートの場合、WLANローミングはサポートされません。クライアント認証の詳細については、『User Access and Authentication Configuration Guide』を参照してください。

異なるVLANからのRSN+802.1Xクライアントがモビリティグループ内のデバイス間をローミングする場合は、メンバーデバイスのアップリンクインターフェイスがすべてのクライアントVLANを許可していることを確認します。

WLANローミングタスクの概要

WLANローミングを設定するには、次の作業を行います。

1. モビリティグループの作成
2. (任意)IADTP制御メッセージの認証モードの設定
3. IADTPトンネルのIPアドレスタイプの指定
4. IADTPトンネルを確立するための送信元IPアドレスの指定
5. (任意)IADTPキープアライブパケットのDSCP値の設定
6. モビリティグループメンバーの追加次のいずれかのタスクを実行します。
   - モビリティグループメンバーの手動での追加
   - グループメンバーの自動検出の有効化
7. (任意)デバイスのモビリティグループメンバーロールの指定
8. (任意)IADTPデータトンネルのディセーブル化
9. (任意)ローミングリレーのイネーブル化
10. モビリティグループのイネーブル化
11. (任意)モビリティグループのトンネル分離のイネーブル化
12. (任意)WLANローミングのSNMP通知のイネーブル化

モビリティグループの作成

制約事項とガイドライン

デバイス間ローミングが正常に動作するには、同じモビリティグループを作成し、モビリティグループ内の各デバイスにメンバーを追加します。

デバイス上に作成できるモビリティグループは1つだけです。

手順

1. システムビューを開始します。

   system-view
2. モビリティグループを作成し、そのビューを開始します。

   wlan mobility group *group-name*

IADTP制御メッセージの認証モードの設定

このタスクについて

この機能により、デバイスは、IADTPトンネルを介して送信される制御メッセージの整合性を検証できます。WLANローミングは、MD5アルゴリズムだけをサポートします。

手順

1. システムビューを開始します。
   system-view
2. モビリティグループビューを開始します。
   wlan mobility group *group-name*
3. IADTP制御メッセージの認証モードを設定します。
   authentication-mode *authentication-mode* { **cipher | simple** } *string*
   デフォルトでは、デバイスはIADTP制御メッセージの整合性を検証しません。

IADTPトンネルのIPアドレスタイプの指定

このタスクについて

モビリティグループを作成した後、IADTPトンネルのIPアドレスタイプを指定する必要があります。

手順

1. システムビューを開始します。
   system-view
2. モビリティグループビューを開始します。
   wlan mobility group *group-name*
3. IADTPトンネルのIPアドレスタイプを指定します。
   tunnel-type { ipv4| ipv6}
   デフォルトでは、IADTPトンネルのIPアドレスタイプはIPv4です。

IADTPトンネルを確立するための送信元IPアドレスの指定

このタスクについて

デバイスは、指定された送信元IPアドレスを使用して、同じモビリティグループ内の他のメンバーデバイスとIADTPトンネルを確立します。

制約事項とガイドライン

1つのIPv4アドレス、1つのIPv6アドレス、またはその両方を指定できますが、IADTPトンネルのIPアドレスタイプと同じIPアドレスタイプだけが有効になります。

IADTPトンネルを確立するための送信元IPアドレスを指定する前に、モビリティグループがディセーブルになっていることを確認します。

手順

1. システムビューを開始します。
   System-view
2. モビリティグループビューを開始します。
   wlan mobility group *group-name*
3. IADTPトンネルを確立するための送信元IPアドレスを指定します。
   Source {**ip** *ipv4-address* | **ipv6** *ipv6-address*}
   デフォルトでは、IADTPトンネルを確立するための送信元IPアドレスは指定されていません。

IADTPキープアライブパケットのDSCP値の設定

このタスクについて

IPパケットのDSCP値は、パケットのプライオリティレベルを指定し、パケットの送信プライオリティに影響を与えます。DSCP値が大きいほど、パケットプライオリティが高くなります。

制約事項とガイドライン

ベストプラクティスとして、IADTPキープアライブパケットのDSCP値を63に設定します。

手順

1. システムビューを開始します。
   system-view
2. モビリティグループビューを開始します。
   wlan mobility group *group-name*
3. IADTPキープアライブパケットのDSCP値を設定します。
   tunnel-dscp *dscp-value*
   デフォルト設定は0です。

モビリティグループメンバーの追加

モビリティグループメンバーの手動での追加

このタスクについて

モビリティグループのメンバーは、IADTPトンネルの確立に使用されるIPアドレスによって識別されます。

IPv4メンバーとIPv6メンバーの両方をモビリティグループに追加できます。IPアドレスタイプがIADTPトンネルのIPアドレスタイプと同じメンバーだけが有効になります。

メンバーにVLANを指定して、モビリティグループ内の他のメンバーが、指定されたVLANからメンバーのクライアントデータを直接転送できるようにすることができます。メンバーにVLANを指定しない場合、クライアントがそのメンバーにローミングしない限り、モビリティグループ内の他のメンバーからクライアントデータを直接転送することはできません。

制約事項とガイドライン

デバイスは1つのモビリティグループだけに属することができます。

モビリティグループには、最大31のIPv4メンバーと31のIPv6メンバーを追加できます。

モビリティグループメンバーにVLANを指定する場合は、次の制約事項および注意事項に従ってください。

- モビリティグループに複数のメンバーが存在する場合は、モビリティグループ内のメンバー間のIADTPトンネルにループが存在しないことを確認します。
- VLANがインターフェイスまたはサービスで使用されていないことを確認します。
- メンバーに指定されたVLANをインターフェイスまたはサービスに割り当てないでください。

手順

1. システムビューを開始します。

   system-view
2. モビリティグループビューを開始します。

   wlan mobility group *group-name*
3. モビリティグループメンバーを追加します。

   Member {**ip** *ipv4-address* | **ipv6** *ipv6-address* }[**vlan** *vlan-id-list*]

グループメンバーの自動検出の有効化

このタスクについて

モビリティグループのメンバーは、IADTPトンネルの確立に使用されるIPアドレスによって識別されます。モビリティグループには、IPv4メンバーとIPv6メンバーの両方を追加できます。IPアドレスタイプがIADTPトンネルのIPアドレスタイプと同じメンバーだけが有効になります。

この機能を使用すると、デバイスは、グループ内で送信元IPアドレスをブロードキャストすることによって、モビリティグループ内のメンバーデバイスを自動的に検出できます。IPアドレスを受信するグループ内のメンバーデバイスは、デバイスとのIADTPトンネルを自動的に確立します。デバイスは、他のすべてのメンバーとIADTPトンネルを確立した後、モビリティグループに加入します。

制約事項とガイドライン

デバイスは1つのモビリティグループだけに属することができます。

モビリティグループには、最大31のIPv4メンバーと31のIPv6メンバーを追加できます。最大数に達すると、デバイスは新たに検出されたデバイスとのIADTPトンネルの確立を停止します。

前提条件

sourceコマンドを実行して、IADTPトンネルの確立に使用される送信元IPアドレスを指定します。

手順

1. システムビューを開始します。
   system-view
2. モビリティグループビューを開始します。
   wlan mobility group *group-name*
3. グループメンバーの自動検出をイネーブルにします。
   member auto-discovery [**interval** *interval*]
   デフォルトでは、グループメンバーの自動検出はディセーブルです。

IADTPデータトンネルの無効化

このタスクについて

△注意:

データ損失を回避するために、クライアントVLAN用のデバイスでサービスポートが指定されていない場合は、IADTPデータトンネルをディセーブルにしないでください。

この機能を使用すると、IADTPデータトンネルを経由するのではなく、クライアントVLANのサービスポートから直接クライアントトラフィックを転送できます。これにより、IADTPデータトンネルから受信したブロードキャストパケットの処理に起因するデバイスのワークロードが軽減され、これらのトンネルを維持するためのリソースが節約されます。

制約事項とガイドライン

モビリティグループ内のすべてのデバイスでIADTPトンネルをイネーブルまたはディセーブルにする必要があります。この機能を設定できるのは、モビリティグループがディセーブルになっている場合だけです。

手順

1. システムビューを開始します。
   system-view
2. モビリティグループビューを開始します。
   wlan mobility group *group-name*
3. IADTPデータトンネルを無効にします。
   data-tunnel disable
   デフォルトでは、IADTPデータトンネルはイネーブルです。

ローミングリレーの有効化

このタスクについて

WLANでは、2つのデバイスがローミングエントリ交換のために互いにトンネルを確立する必要があるため、クライアントローミングによってWLANは徐々に完全なメッシュネットワークに変わります。大規模なネットワークでは、このようなトンネルを確立して維持すると、多くの帯

域幅リソースが消費され、ネットワークの複雑さが増し、可用性が低下する可能性があります。この問題を解決するために、ローミングリレーが導入されています。

この機能が設定されている場合、ローミングリレーがイネーブルになっているデバイスは、リレーデバイスとして動作して、各非リレーデバイスとIADTPトンネルを確立し、スタートポロジを形成します。非リレーデバイスは、相互にトンネルを確立する必要はありません。これらの非リレーデバイスは、ローミングエントリをリレーデバイスに同期させ、クライアントローミング時にリレーデバイスからクライアントエントリを要求します。

制約事項とガイドライン

この機能を設定する前に、モビリティグループがディセーブルになっていることを確認してください。

ローミングリレーを使用するには、デバイスでローミングリレーをイネーブルにし、そのデバイスを同じモビリティグループ内の他のデバイスの唯一のモビリティグループメンバーとして設定する必要があります。

ローミングリレーは、モビリティグループ内の1つのデバイスだけでイネーブルにできます。

クライアントが異なるVLANに属している場合は、リレーデバイスのトンネルインターフェイスがすべてのクライアントVLANからのパケットを許可していることを確認します。

手順

1. システムビューを開始します。

   System-view
2. モビリティグループビューを開始します。

   wlan mobility group *group-name*
3. ローミングリレーを有効にします。

   roam-relay enable

   デフォルトでは、ローミングリレーはディセーブルです。

モビリティグループの有効化

このタスクについて

この機能により、デバイスはIADTPトンネルを確立し、ローミングエントリをメンバーデバイスと同期化できます。

手順

1. システムビューを開始します。

   system-view
2. モビリティグループビューを開始します。

   wlan mobility group *group-name*
3. モビリティグループをイネーブルにします。

   group enable

   デフォルトでは、モビリティグループはディセーブルです。

モビリティグループのトンネル分離の有効化

このタスクについて

トンネル分離は、デバイスがモビリティグループ内のトンネル間でパケットを転送するのを防ぎ、モビリティグループ内のデバイス間にループが存在する場合のブロードキャストストームを回避します。

手順

1. システムビューを開始します。

   system-view
2. モビリティグループのトンネル分離をイネーブルにします。

   wlan mobility-group-isolation enable

   デフォルトでは、モビリティグループのトンネルグループに対してイネーブルです。

WLANローミングのSNMP通知の有効化

このタスクについて

重要なWLANローミングイベントをNMSに報告するには、WLANローミングのSNMP通知を有効にします。WLANローミングイベント通知を正しく送信するには、デバイスでSNMPも設定する必要があります。SNMP設定の詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

手順

1. システムビューを開始します。

   system-view
2. WLANローミングのSNMP通知をイネーブルにします。

   snmp-agent trap enable wlan mobility

   デフォルトでは、WLANローミングのSNMP通知はディセーブルです。

WLANローミングの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行します。

タスク	コマンド
デバイスとの間でローミングしたクライアントに関する情報を表示します。Roam-in, roam-outの情報は180秒保持されます。	**display wlan mobility** { **roam-in** | **roam-out**}[**member**{ **ip** *ipv4-address*|**ipv6** *ipv6-address* }]
モビリティグループ情報を表示します。	display wlan mobility group
HA上のクライアントのローミングトラック情報を表示します。	**display wlan mobility roam-track mac-address***mac-address*

WLANローミングの設定例

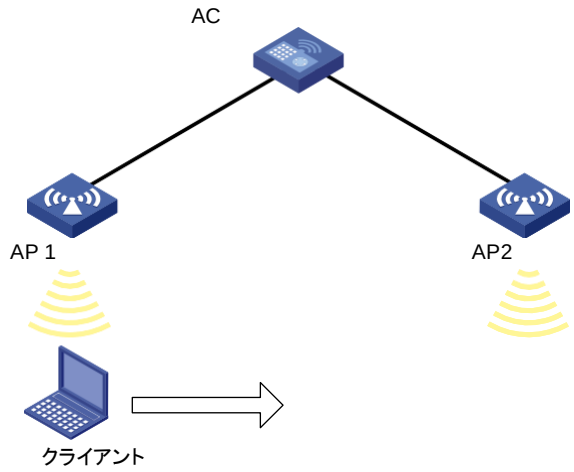
このドキュメントに記載されているAPモデルおよびシリアル番号は、あくまでも例です。APモデルおよびシリアル番号のサポートは、ACモデルによって異なります。

例:AC内ローミングの設定

ネットワーク構成

図4に示すように、クライアントがAP 1からAP 2の同じSSIDにローミングできるようにAC内ローミングを設定します。2つのAPは同じACによって管理されます。

図4:ネットワーク図



手順

#**service**という名前のサービステンプレートを作成し、SSIDを1に設定して、サービステンプレートをイネーブルにします。

<AC>system-view

[AC]wlan service-template service

[AC-wlan-st-service]ssid 1

[AC-wlan-st-service]service-template enable

[AC-wlan-st-service]quit

#**ap1**という名前の手動APを作成し、APのモデルとシリアルIDを指定します。

[AC]wlan ap ap1 model WA4320i-ACN

[AC-wlan-ap-ap1]serial-id 219801A0CNC13C004126

#サービステンプレートをAP 1の無線1にバインドします。

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] radio enable

[AC-wlan-ap-ap1-radio-1] service-template service

[AC-wlan-ap-ap1-radio-1] quit

[AC-wlan-ap-ap1] quit

#**ap2**という名前の手動APを作成し、APのモデルとシリアルIDを指定します。

[AC] wlan ap ap2 model WA4320i-ACN

[AC-wlan-ap-ap2] serial-id 219801A0CNC125002216

#サービステンプレートをAP 2の無線1にバインドします。

[AC-wlan-ap-ap2] radio 1

[AC-wlan-ap-ap2-radio-1] radio enable

[AC-wlan-ap-ap2-radio-1] service-template service

[AC-wlan-ap-ap2-radio-1] quit

[AC-wlan-ap-ap2] quit

設定の確認

#クライアントがAP 1からオンラインになるようにします(詳細は表示されません)。

#クライアントがAP 1に関連付けられており、ローミングステータスがN/Aであることを確認します。これは、クライアントがローミングを実行していないことを示します。

[AC] display wlan client verbose

Total number of clients: 1

MAC address : 9cd3-6d9e-6778

IPv4 address : 10.1.1.114

IPv6 address : N/A

Username : N/A

AID : 1

AP ID : 1

AP name : ap1

Radio ID : 1

SSID : 1

BSSID : 000f-e200-4444

VLAN ID : 1

Sleep count : 242

Wireless mode : 802.11ac

Channel bandwidth : 80MHz

SM power save : Enabled

SM power save mode : Dynamic

Short GI for 20MHz : Supported

Short GI for 40MHz : Supported

Short GI for 80MHz :

Supported Short GI for 160/80+80MHz :

Not supportedSTBC RX capability :

Not supported

STBC TX capability : Not supported

LDPC RX capability : Not supported

SU beamformee capability : Not supported

MU beamformee capability : Not supported

Beamformee STS capability : N/A

Block Ack : TID 0 In

Supported VHT-MCS set : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8

NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8

Supported HT MCS set : 0, 1, 2, 3, 4, 5, 6, 7,
8, 9, 10, 11, 12, 13, 14,
15, 16, 17, 18, 19, 20,
21, 22, 23

Supported rates : 6, 9, 12, 18, 24, 36,
48, 54 Mbps

QoS mode : WMM
Listen interval : 10
RSSI : 62
Rx/Tx rate : 130/11
Authentication method : Open system
Security mode : PRE-RSNA
AKM mode : Not configured
Cipher suite : N/A
User authentication mode : Bypass
Authorization ACL ID : 3001(Not effective)
Authorization user profile : N/A
Roam status : N/A
Key derivation : SHA1
PMF status : Enabled
Forward policy name : Not configured
Online time : 0days 0hours 1minutes 13seconds
FT status : Inactive

#ACにクライアント用のローミングエントリがあることを確認します。

[AC] display wlan mobility roam-track mac-address 9cd3-6d9e-6778

Total entries : 1
Current entries: 1
BSSID Created at Online time

AC IP address RID AP name 000f-e200-4444 2016-06-14 11:12:28 00hr 01min 16sec
127.0.0.1 1 ap1

#クライアントがAP 2にローミングできるようにします(詳細は省略)。

#クライアントがAP 2に関連付けられており、ローミングステータスがIntra-AC roamであることを確認します。

[AC] display wlan client

verboseTotal number of
clients: 1

MAC address : 9cd3-6d9e-6778
IPv4 address : 10.1.1.114
IPv6 address : N/A
Username : N/A
AID : 1
AP ID : 2
AP name : ap2
Radio ID : 1

SSID	: 1
BSSID	: 000f-e203-7777
VLAN ID	: 1
Sleep count	: 242
Wireless mode	: 802.11ac
Channel bandwidth	: 80MHz
SM power save	: Enabled
SM power save mode	: Dynamic
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
Short GI for 80MHz	: Supported
Short GI for 160/80+80MHz	: Not supported
STBC RX capability	: Not supported
STBC TX capability	: Not supported
LDPC RX capability	: Not supported
SU beamformee capability	: Not supported
MU beamformee capability	: Not supported
Beamformee STS capability	: N/A
Block Ack	: TID 0 In
Supported VHT-MCS set	: NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8 NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set	: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23
Supported rates	: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
QoS mode	: WMM
Listen interval	: 10
RSSI	: 62
Rx/Tx rate	: 130/11
Authentication method	: Open system
Security mode	: PRE-RSNA
AKM mode	: Not configured
Cipher suite	: N/A
User authentication mode	: Bypass
Authorization ACL ID	: 3001(Not effective)
Authorization user profile	: N/A
Roam status	: Intra-AC roam
Key derivation	: SHA1
PMF status	: Enabled
Forward policy name	: Not configured
Online time	: 0days 0hours 5minutes 13seconds
FT status	: Inactive

#ACがクライアントのローミングエントリを更新したことを確認します。

[AC] display wlan mobility roam-track mac-address 9cd3-6d9e-6778

Total entries : 2
Current entries: 2

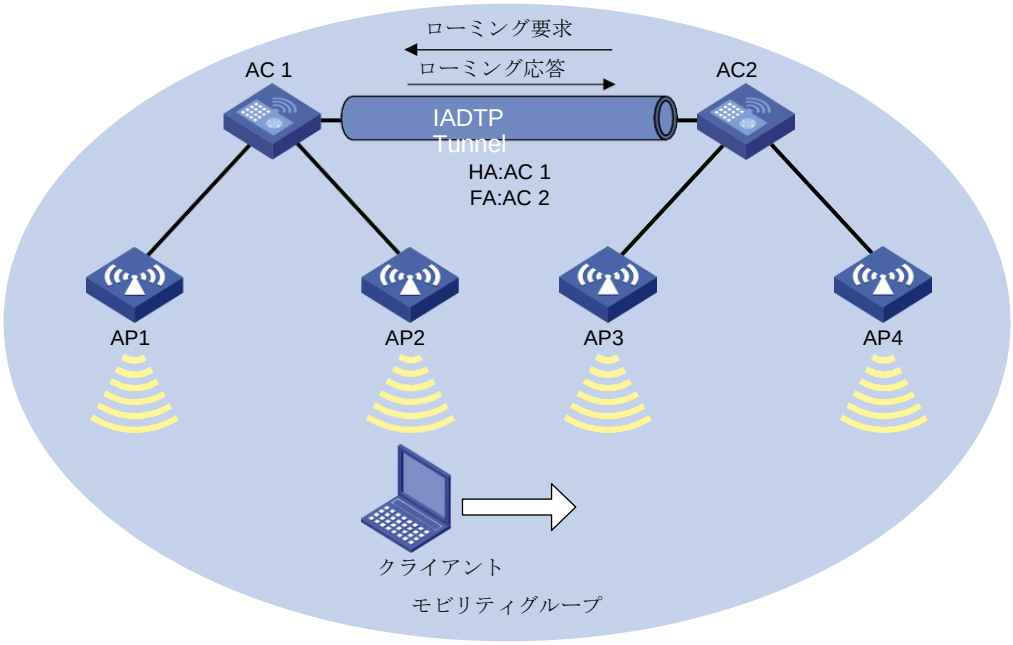
BSSID	Created at	Online time	AC IP address		
RID AP name000f-e203-7777	2016-06-14 11:12:28	00hr 01min 02sec	127.0.0.1	1	ap2
000f-e200-4444	2016-06-14 11:12:04	00hr 03min 51sec	127.0.0.1 1 ap1		

例:AC間ローミングの設定

ネットワーク構成

図5に示すように、AC間ローミングを設定して、クライアントが異なるACによって管理されているAP 2からAP 3にローミングできるようにします。

図5ネットワーク図



手順

1. AC 1を設定します。

   #serviceという名前のサービステンプレートを作成し、SSIDをofficeに設定して、サービステンプレートをイネーブルにします。

   <AC1> system-view

   [AC1] wlan service-template service

   [AC1-wlan-st-test] ssid office

   [AC1-wlan-st-test] service-template enable

   [AC1-wlan-st-test] quit

   #ap1という名前の手動APを作成し、APのモデルとシリアルIDを指定します。

   [AC1] wlan ap ap1 model WA4320i-ACN

   [AC1-wlan-ap-ap1] serial-id 219801A0CNC138011454

#サービステンプレートをAP 1の無線1にバインドします。

[AC1-wlan-ap-ap1] radio 1

[AC1-wlan-ap-ap1-radio-1] radio enable

[AC1-wlan-ap-ap1-radio-1] service-template service

[AC1-wlan-ap-ap1-radio-1] quit

[AC1-wlan-ap-ap1] quit

#ap2という名前の手動APを作成し、APのモデルとシリアルIDを指定します。

[AC1]wlan ap ap2 model WA4320i-ACN

[AC1-wlan-ap-ap2]serial-id 219801A0CNC138011445

#サービステンプレートをAP 2の無線1にバインドします。

[AC1-wlan-ap-ap2] radio 1

[AC1-wlan-ap-ap2-radio-1] radio enable

[AC1-wlan-ap-ap2-radio-1] service-template service

[AC1-wlan-ap-ap2-radio-1] quit

[AC1-wlan-ap-ap2] quit

#officeという名前のモビリティグループを作成します。

[AC1] wlan mobility group office

#IADTPトンネルのIPアドレスタイプをIPv4として指定します。

[AC1-wlan-mg-office] tunnel-type ipv4

#IADTPトンネルを確立するための送信元IPアドレスを10.1.4.22として指定します。

[AC1-wlan-mg-office] source ip 10.1.4.22

#AC 2をモビリティグループに追加します。

[AC1-wlan-mg-office] member ip 10.1.4.23

#モビリティグループを有効にします。

[AC1-wlan-mg-office] group enable

[AC1-wlan-mg-office]quit

2. AC 2を設定します。

#serviceという名前のサービステンプレートを作成し、SSIDをofficeと指定して、サービステンプレートをイネーブルにします。

<AC2> system-view

[AC2] wlan service-template service

[AC2-wlan-st-service] ssid office

[AC2-wlan-st-service] service-template enable

[AC2-wlan-st-service] quit

#ap3という名前の手動APを作成し、APのモデルとシリアルIDを指定します。

[AC2] wlan ap ap3 model WA4320i-ACN

[AC2-wlan-ap-ap3] serial-id 219801A0CNC138011439

#サービステンプレートをAP 3の無線1にバインドします。

[AC2-wlan-ap-ap3] radio 1

[AC2-wlan-ap-ap3-radio-1] radio enable

[AC2-wlan-ap-ap3-radio-1] service-template service

[AC2-wlan-ap-ap3-radio-1] quit

[AC2-wlan-ap-ap3] quit

#ap4という名前の手動APを作成し、APのモデルとシリアルIDを指定します。

[AC2] wlan ap ap4 model WA4320i-CAN

[AC2-wlan-ap-ap4] serial-id 219801A0CNC138011448

#サービステンプレートをAP 4の無線1にバインドします。

[AC2-wlan-ap-ap4] radio 1

[AC2-wlan-ap-ap4-radio-1] radio enable

[AC2-wlan-ap-ap4-radio-1] service-template service

[AC2-wlan-ap-ap4-radio-1] quit

[AC2-wlan-ap-ap4] quit

#officeという名前のモビリティグループを作成します。

[AC2] wlan mobility group office

#IADTPトンネルのIPアドレスタイプをIPv4として指定します。

[AC2-wlan-mg-office] tunnel-type ipv4

#IADTPトンネルを確立するための送信元IPアドレスを10.1.4.23として指定します。

[AC2-wlan-mg-office] source ip 10.1.4.23

#AC 2をモビリティグループに追加します。

[AC2-wlan-mg-office] member ip 10.1.4.22

#モビリティグループを有効にします。

[AC2-wlan-mg-office]group enable

[AC2-wlan-mg-office]quit

設定の確認

#AC 1にモビリティグループが作成されていることを確認します。

[AC1] display wlan mobility group

Mobility group name: office

Tunnel type: IPv4 Source IPv4: 10.1.4.22

Source IPv6: Not configured Authentication method: Not configuredMobility group status: Enabled

Member entries: 1

IP address	State	Online time
10.1.4.23	Up	00hr 00min 12sec

#AC 2上にモビリティグループが作成されていることを確認します。

[AC2] display wlan mobility group

Mobility group name: office

Tunnel type: IPv4 Source IPv4: 10.1.4.23

Source IPv6: Not configured Authentication method: Not configuredMobility group status: Enabled

Member entries: 1

IP address	State	Online time
10.1.4.22	Up	00hr 00min 05sec

#AP 2でクライアントをオンラインにしてから、クライアントをAP 3にローミングさせます(詳細は省略)。

#AC 1のクライアントローミング情報を表示して、クライアントがAP 2からオンラインになり、AP 3にローミングしたことを確認します。

[AC1] display wlan mobility roam-track

mac-address 9cd3-6d9e-6778Total entries : 2

Current entries: 2

BSSID	Created at	Online time	AC IP address	RID	APname
000f-e203-8889	2016-06-14 11:12:28	00hr 06min 56sec	10.1.4.23	1	ap3
000f-e203-7777	2016-06-14 11:11:28	00hr 03min 30sec	127.0.0.1	1	ap2

#AC 1で、クライアントがAC 2にローミングしたことを確認します。Roam-in, roam-outの情報は180秒保持されます。

<AC1>display wlan mobility roam-out

Total numbers of entry:1

MAC address BSSID VLAN ID online time FA IP address

9cd3-6d9e-6778 000f-e203-8889 10 0hour 01minitue 59S 10.1.4.23

#AC 2で、クライアントがAP 3に関連付けられており、ローミングステータスがInter-AC roamであることを確認します。

<AC1> display wlan mobility roam-out

Total entries: 1

MAC address BSSID VLAN ID Online time FA IP address9cd3-6d9e-

6778 000f-e203-8889 1 00hr 01min 59sec 10.1.4.23

On AC 2, verify that the client has associated with AP 3, and the roaming status is **Inter-AC roam**.

<AC2> display wlan client verbose

Total number of clients: 1

MAC address : 9cd3-6d9e-6778

IPv4 address : 10.1.1.114

IPv6 address : N/A

Username : N/A

AID : 1

AP ID : 3

AP name : ap3

Radio ID : 1

SSID : 1

BSSID : 000f-e203-8889

VLAN ID : 1

Sleep count : 242

Wireless mode : 802.11ac

Channel bandwidth : 80MHz

SM power save : Enabled

SM power save mode : Dynamic

Short GI for 20MHz : Supported

Short GI for 40MHz : Supported

Short GI for 80MHz : Supported

Short GI for 160/80+80MHz : Not supported

STBC RX capability : Not supported

STBC TX capability : Not supported

LDPC RX capability : Not supported

SU beamformee capability : Not supported

MU beamformee capability : Not supported
Beamformee STS capability : N/A
Block Ack : TID 0 In
Supported VHT-MCS set : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23
Supported rates : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
QoS mode : WMM
Listen interval : 10
RSSI : 62
Rx/Tx rate : 130/11
Authentication method : Open system
Security mode : PRE-RSNA
AKM mode : Not configured
Cipher suite : N/A
User authentication mode : Bypass
Authorization ACL ID : 3001(Not effective)
Authorization user profile : N/A
Roam status : Inter-AC roam
Key derivation : SHA1
PMF status : Enabled
Forward policy name : Not configured
Online time : 0days 0hours 5minutes 13seconds
FT status : Inactive

Verify that the client has roamed from AC 1 to AC 2.

<AC2> display wlan mobility
roam-inTotal entries: 1
MAC address BSSID VLAN ID
HA IP address9cd3-6d9e-6778 000f-e203-8889 1 10.1.4.22

内容

802.11rの設定

802.11r

802.11r fast BSS Transition(FT)は、クライアントが同じESS内でBSSから別のBSSにローミングするときの遅延を最小限に抑えます。802.11r FT中、クライアントはターゲットAPとメッセージを交換する必要があります。

802.11r操作機構

FTには、次のメッセージ交換方式が用意されています。

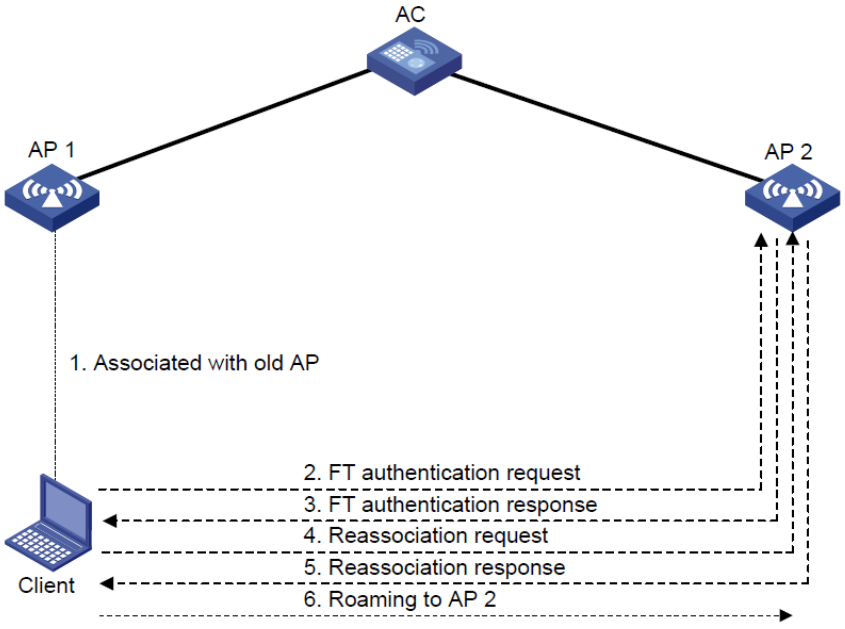
- **Over-the-air**:クライアントは、ローミング前の認証のためにターゲットAPと直接通信します。
- **Over-the-DS**:クライアントは現在のAPを介してターゲットAPと通信し、事前ローミング認証を行います。

Over-the-air FTを介したAC内ローミング

図1に示すように、クライアントはAP 1に関連付けられています。無線FTによるAC内ローミングでは、次のプロセスが使用されます。

1. クライアントはFT認証要求をAP 2に送信します。
2. AP 2はFT認証応答をクライアントに送信します。
3. クライアントは再アソシエーション要求をAP 2に送信します。
4. AP 2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。
5. クライアントはAP 2にローミングします。

図1 Over-the-air FTを介したAC内ローミング

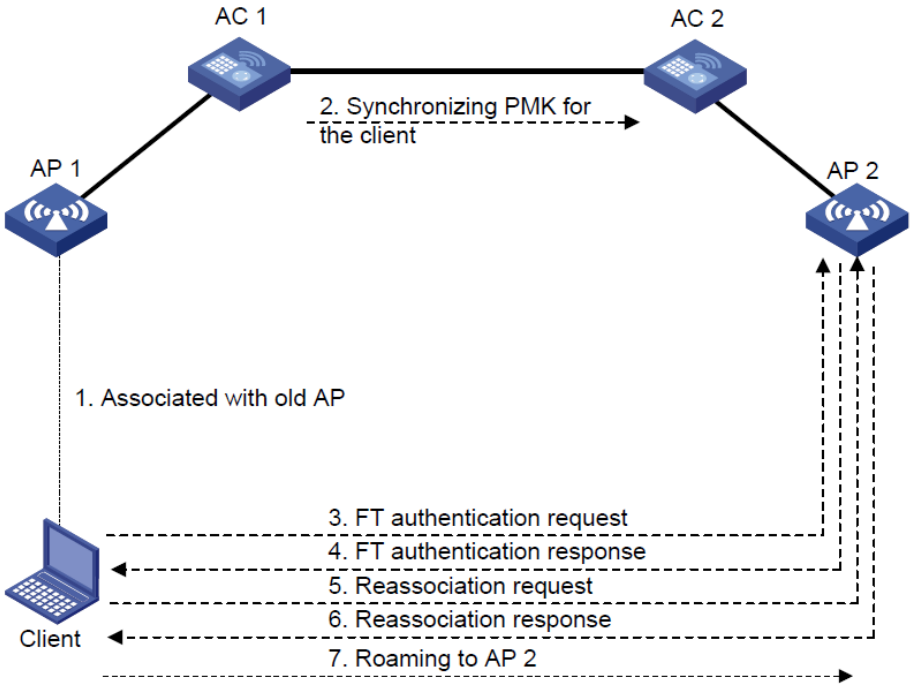


Over-the-air FTを介したAC間ローミング

図2に示すように、クライアントはAP 1に関連付けられています。無線FTによるAC間ローミングでは、次のプロセスが使用されます。

1. クライアントがオンラインになると、AC 1はクライアントのローミング情報をAC 2に送信します。ローミング情報には、PMKとクライアントVLANが含まれます。
2. クライアントはFT認証要求をAP 2に送信します。
3. AP 2はFT認証応答をクライアントに送信します。
4. クライアントは再関連付け要求をAP 2に送信します。
5. AP 2は再関連付け応答をクライアントに送信します。
6. クライアントはAP 2にローミングします。

図2 Over-the-air FTを介したAC間ローミング

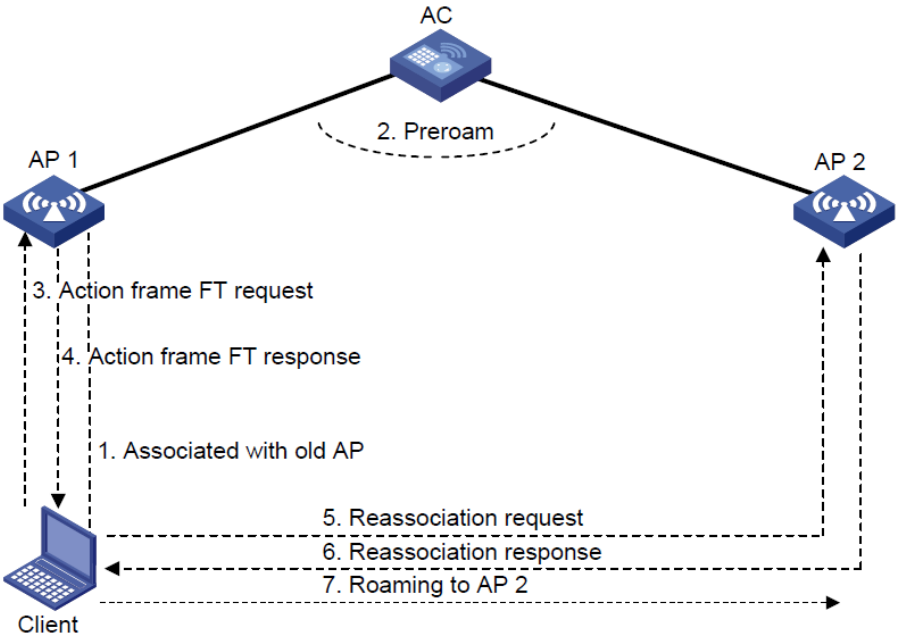


over-the-DS FTによるAC内ローミング

図3に示すように、クライアントはAP 1に関連付けられています。over-the-DS FTによるAC内ローミングでは、次のプロセスが使用されます。

1. クライアントがオンラインになると、ACはローミングエントリを作成し、それをクライアント用に保存します。
2. クライアントはFT認証要求をAP 1に送信します。
3. AP 1はFT認証応答をクライアントに送信します。
4. クライアントは再関連付け要求をAP 2に送信します。
5. AP 2は再関連付け応答をクライアントに送信します。
6. クライアントはAP 2にローミングします。

図 3 over-the-DS FTを介したAC内ローミング

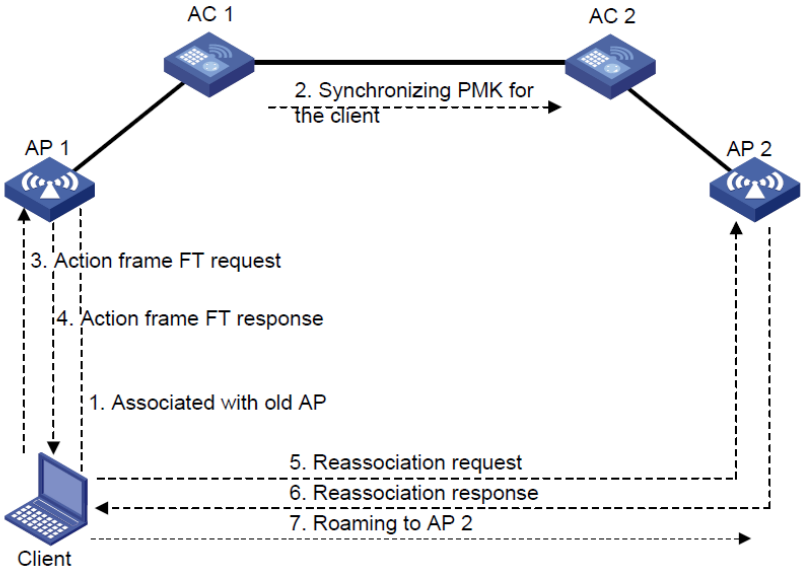


over-the-DS FTによるAC間ローミング

図4に示すように、クライアントはAP 1に関連付けられています。over-the-DS FTを介したAC間ローミングでは、次のプロセスを使用します。

1. クライアントがオンラインになると、AC 1はクライアントのローミング情報をAC 2に送信します。ローミング情報には、PMKとクライアントVLANが含まれます。
2. クライアントはFT認証要求をAP 1に送信します。
3. AP 1はFT認証応答をクライアントに送信します。
4. クライアントは再関連付け要求をAP 2に送信します。
5. AP 2は再関連付け応答をクライアントに送信します。
6. クライアントはAP 2にローミングします。

図4 over-the-DS FTを介したAC間ローミング



プロトコルと標準

802.11r IEEEシステム間の電気通信および情報交換、ローカルエリアネットワークとメトロポリタンエリアネットワーク、特定要件

制約事項および注意事項:802.11r設定

802.11rを設定する場合は、次の制約事項および注意事項に従ってください。

- FTをサポートしていないクライアントがWLANにアクセスできるようにするには、同じSSIDを使用して2つのサービステンプレートを作成します。1つはFTを有効にし、もう1つは無効にします。
- 定期的再認証タイマーが期限切れになるたびにクライアントがオンラインにならないようにするには、同じサービステンプレートに対してFTと802.1Xの定期的再認証をイネーブルにしないでください。802.1Xの定期的再認証の詳細については、『User Access and Authentication Configuration Guide』を参照してください。
- FTを介してWLANに関連付けられているクライアントでは、PTKアップデートはサポートされません。PTKアップデートの詳細については、『WLAN Security Configuration Guide』を参照してください。

802.11rの設定

1. システムビューを開始します。

   system-view
2. サービステンプレートビューを開始します。

   wlan service-template *service-template-name*
3. FTを有効にします。

   ft enable

   デフォルトでは、FTはディセーブルです。
4. (任意)FT方式を設定します。

   ft method { over-the-air | over-the-ds }

   デフォルトでは、FT方式は無線です。
5. (任意)再アソシエーションタイムアウトタイマーを設定します。

   ft reassociation-timeout *timeout*

   デフォルトでは、アソシエーションタイムアウトタイマーは20秒です。

   タイムアウトタイマーが満了する前にクライアントが再アソシエーション要求を送信しない場合、ローミングプロセスは終了します。

802.11rの設定例(内部AC)

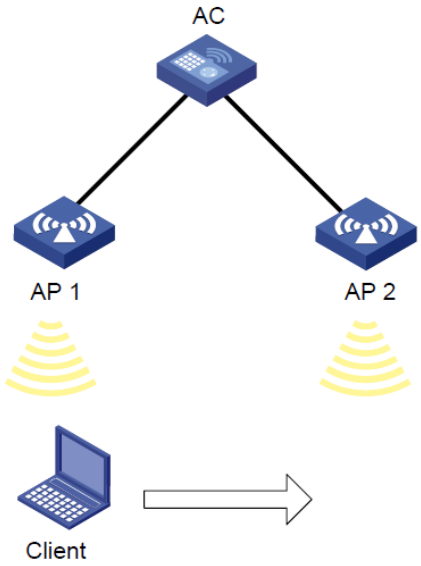
このドキュメントに記載されているAPモデルおよびシリアル番号は、あくまでも例です。APモデルおよびシリアル番号のサポートは、ACモデルによって異なります。

例:over-the-DS FTおよびPSK認証の設定

ネットワーク構成

図5に示すように、クライアントがAP 1とAP 2の間をローミングできるように、over-the-DS FTを介したAC内ローミングを設定します。認証およびキー管理モードとしてPSKを設定します。

図5 ネットワーク図



手順

#サービステンプレート**acstname**を作成します。

<AC> system-view

[AC] wlan service-template acstname

#SSIDを**service**に設定します。

[AC-wlan-st-acstname] ssid service

#認証およびキー管理モードを**PSK**に設定し、単純な文字列**12345678**を設定します。PSKと同じです。

[AC-wlan-st-acstname] akm mode psk

[AC-wlan-st-acstname] preshared-key pass-phrase simple 12345678

#CCMP暗号スイートを設定し、ビーコン応答とプローブ応答でRSN IEを有効にします。

[AC-wlan-st-acstname] cipher-suite ccmp

[AC-wlan-st-acstname] security-ie rsn

Enable FT.

[AC-wlan-st-acstname] ft enable

#再アソシエーションタイムアウトタイマーを50秒に設定します。

[AC-wlan-st-acstname] ft reassociation-timeout 50

#FTメソッドを**over-the-DS**に設定します。

[AC-wlan-st-acstname] ft method over-the-ds

#サービステンプレートを有効にします。

[AC-wlan-st-acstname] service-template enable

[AC-wlan-st-acstname] quit

#AP 1を作成し、サービステンプレート**acstname**をAPの無線1にバインドします。

[AC] wlan ap 1 model WA4320i-ACN
[AC-wlan-ap-1] serial-id 210235A1BSC12300005

[AC-wlan-ap-1] radio 1

[AC-wlan-ap-1-radio-1] service-template acstname

[AC-wlan-ap-1-radio-1] radio enable

[AC-wlan-ap-1-radio-1] quit

[AC-wlan-ap-1] quit

#AP 2を作成し、サービステンプレート**acstname**をAPの無線1にバインドします。

[AC] wlan ap 2 model WA4320i-ACN

[AC-wlan-ap-2] serial-id 210235A1BSC123000055

[AC-wlan-ap-2] radio 1

[AC-wlan-ap-2-radio-1] service-template acstname

[AC-wlan-ap-2-radio-1] radio enable

[AC-wlan-ap-2-radio-1] quit

[AC-wlan-ap-2] quit

設定の確認

#サービステンプレートが正しく設定されていることを確認します。

[AC]display wlan service-template acstname verbose

Service template name: acstname

Description: Not configured
SSID: service
SSID-hide: Disabled

User-isolation: Disabled Service

template status: Enabled Maximum

clients per BSS: Not configured

Frame format: Dot3

Seamless-roam status:

Disabled Seamless-roam

RSSI threshold : 50

Seamless-roam RSSI gap: 20

VLAN ID: 1

```
AKM mode                        : PSK
Security IE                     : RSN
Cipher suite                    : CCMP
```

TKIP countermeasure time: 0
sec PTK lifetime: 43200 sec
GTK rekey: Enabled
GTK rekey method: Time-based
GTK rekey time: 86400 sec
GTK rekey client-offline:
Disabled User authentication
mode: Bypass Intrusion
protection: Disabled
Intrusion protection mode: Temporary-
block Temporary block time: 180 sec
Temporary service stop time : 20 sec

Fail VLAN ID: Not configured
802.1X handshake: Disabled 802.1X
handshake secure: Disabled 802.1X
domain: Not configured
MAC-auth domain: Not configured
Max 802.1X users: 4096
Max MAC-auth users: 4096
802.1X re-authenticate:
Disabled Authorization fail
mode: Online Accounting fail
mode: Online
Authorization: Permitted
Key derivation: SHA1
PMF status: Disabled Hotspot policy
number: Not configured Forwarding
policy status: Disabled Forwarding
policy name: Not configured
Forwarder: AC

FT Status: Enable
```
FT Method: over-the-ds
```

FT Reassociation Deadline:
50 sec QoS trust: Port
QoS priority: 0

#ローミングステータスが**N/A**で、FTステータスが**Active**であることを確認します。

[AC] display wlan

client verbose Total

number of clients: 1

MAC address: fc25-3f03-8361

IPv4 address: 10.1.1.114
IPv6 address: N/A
Username: N/A

AID: 1
AP ID: 1

```
AP name: 1
```

Radio ID	:	1
SSID	:	service
BSSID	:	000f-e266-7788
VLAN ID	:	1
Sleep count	:	242
Wireless mode	:	802.11ac
Channel bandwidth	:	80MHz
SM power save	:	Enabled
SM power save mode	:	Dynamic
Short GI for 20MHz	:	Supported
Short GI for 40MHz	:	Supported
Short GI for 80MHz	:	Supported
Short GI for 160/80+80MHz	:	Not supported
STBC RX capability	:	Not supported
STBC TX capability	:	Not supported
LDPC RX capability	:	Not supported
SU beamformee capability	:	Not supported
MU beamformee capability	:	Not supported
Beamformee STS capability	:	N/A
Block Ack	:	TID 0 In
Supported VHT-MCS set:		NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8 NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23		

Supported rates: 6, 9, 12, 18, 24, 36,48, 54 Mbps

QoS mode: WMM
Listen interval: 10

RSSI: 62
Rx/Tx rate: 130/11

Authentication method : Open system

Security mode : RSN

AKM mode : PSK

Encryption cipher : CCMP

User authentication mode: Bypass
Authorization ACL ID: 3001(Not effective)
Authorization user profile: N/A

Roam status: N/A

Key derivation: SHA1

PMF status: Enabled

Forward policy name: Not configured

Online time: 0days 0hours 1minutes 13seconds

FT status: Active

#クライアントをAP 2のカバレッジに移動します(詳細は省略)。

#認証方式が**FT**で、ローミングステータスが**Intra-AC**ローミングであることを確認します。

[AC] display wlan client

verbose Total number of

clients: 1

MAC address: fc25-3f03-8361
IPv4 address: 10.1.1.114

IPv6 address: N/A
Username: N/A
AID: 1

AP ID: 2

AP name: 2

Radio ID: 1

SSID: service
BSSID: 000f-e211-2233

VLAN ID: 1

Sleep count: 242
Wireless mode: 802.11ac
Channel bandwidth: 80MHz

SM power save: Enabled
SM power save mode: Dynamic
Short GI for 20MHz: Supported

Short GI for 40MHz: Supported

Short GI for 80MHz: Supported Short GI for

160/80+80MHz: Not supported STBC RX

capability: Not supported

STBC TX capability: Not supported
LDPC RX capability: Not supported

SU beamformee capability: Not supported

MU beamformee capability: Not supported

Beamformee STS capability: N/A

Block Ack: TID 0 In
Supported VHT-MCS set: NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set: 0, 1, 2, 3, 4, 5, 6, 7,
8, 9, 10, 11, 12, 13, 14,
15, 16, 17, 18, 19, 20,
21, 22, 23
Supported rates: 6, 9, 12, 18, 24, 36,
48, 54 Mbps

QoS mode: WMM
Listen interval: 10

RSSI: 62
Rx/Tx rate: 130/11

```
Authentication method                : FT
Security mode                        : RSN
AKM mode                             : PSK
Encryption cipher                    : CCMP
```

User authentication mode: Bypass

Authorization ACL ID: 3001(Not effective)
Authorization user profile: N/A

```
Roam status: Intra-AC roam
```

Key derivation: SHA1

PMF status: Enabled

Forward policy name: Not configured

Online time: 0days 0hours 5minutes 13seconds

```
FT status: Active
```

例:無線FT認証およびPSK認証の設定

ネットワーク構成

図5に示すように、クライアントがAP 1とAP 2の間をローミングできるように、無線FTを介したAC内ローミングを設定します。認証およびキー管理モードとしてPSKを設定します。

手順

#サービステンプレート**acstname**を作成します。

<AC> system-view

[AC] wlan service-template acstname

#SSIDを**service**に設定します。

[AC-wlan-st-acstname] ssid service

#認証およびキー管理モードを**PSK**に設定し、単純な文字列**12345678**を設定します。PSKと同じです。

[AC-wlan-st-acstname] akm mode psk
[AC-wlan-st-acstname] preshared-key pass-phrase simple 12345678

#ビーコン応答およびプローブ応答でRSN IEを有効にします。

[AC-wlan-st-acstname] cipher-suite ccmp

[AC-wlan-st-acstname] security-ie rsn

#FTを有効にします。

[AC-wlan-st-acstname] ft enable

#再アソシエーションタイムアウトタイマーを50秒に設定します。

[AC-wlan-st-acstname] ft reassociation-timeout 50

#サービステンプレートを有効にします。

[AC-wlan-st-acstname] service-template enable

[AC-wlan-st-acstname] quit

#AP 1を作成し、サービステンプレートacstnameをAPの無線1にバインドします。

[AC] wlan ap 1 model WA4320i-ACN

[AC-wlan-ap-1] serial-id 210235A1BSC123000050

[AC-wlan-ap-1] radio 1

[AC-wlan-ap-1-radio-1] service-template acstname

[AC-wlan-ap-1-radio-1] radio enable

[AC-wlan-ap-1-radio-1] quit

[AC-wlan-ap-1] quit

#AP 2を作成し、サービステンプレートacstnameをAPの無線1にバインドします。

[AC] wlan ap 2 model WA4320i-ACN

[AC-wlan-ap-2] serial-id 210235A1BSC123000055

[AC-wlan-ap-2] radio 1

[AC-wlan-ap-2-radio-1] service-template acstname

[AC-wlan-ap-2-radio-1] radio enable

[AC-wlan-ap-2-radio-1] quit

[AC-wlan-ap-2] quit

設定の確認

#次の情報を確認します。

- RSN IEがイネーブルになっている。
- AKMモードは**PSK**です。
- 暗号スイートは**CCMP**です。
- FTステータスは**Active**です。

[AC] display wlan client

verbose Total number of

clients: 1

MAC address: fc25-3f03-8361

IPv4 address: 10.1.1.114
IPv6 address: N/A

Username: N/A

AID: 1

AP ID: 1

```
AP name: 1
```

Radio ID: 1
SSID: service
BSSID: 000f-e266-7788

VLAN ID: 1

Sleep count: 242
Wireless mode: 802.11ac

Channel bandwidth: 80MHz

SM power save: Enabled

SM power save mode: Dynamic
Short GI for 20MHz: Supported

Short GI for 40MHz: Supported
Short GI for 80MHz: Supported Short GI for

160/80+80MHz: Not supported STBC RX

capability: Not supported

STBC TX capability: Not supported

LDPC RX capability: Not supported

SU beamformee capability: Not supported

MU beamformee capability: Not supported
Beamformee STS capability: N/A

Block Ack: TID 0 In

Supported	VHT-MCS set:	NSS1 0, 1, 2, 3, 4, 5, 6,	7, 8
		NSS2 0, 1, 2, 3, 4, 5, 6,	7, 8
supported	HT MCS set:	0, 1, 2, 3, 4, 5, 6, 7,	
		8, 9, 10, 11, 12, 13, 14,	
		15, 16, 17, 18, 19, 20,	

21, 22, 23

Supported rates: 6, 9, 12, 18, 24, 36, 48, 54 Mbps

QoS mode: WMM
Listen interval: 10

RSSI: 62

Rx/Tx rate: 130/11

Authentication method	:	Open system
Security mode	:	RSN
AKM mode	:	PSK
Encryption cipher	:	CCMP

User authentication mode: Bypass

Authorization ACL ID: 3001(Not effective)
Authorization user profile: N/A

```
Roam status: N/A
```

Key derivation: SHA1
PMF status: Enabled
Forward policy name: Not configured

Online time: 0days 0hours 1minutes 13seconds

```
FT status: Active
```

クライアントをAP 2のカバレッジに移動します(詳細は省略)。

#認証方式が**FT**で、ローミングステータスが**Intra-AC**ローミングであることを確認します。

[AC] display wlan client verbose

Total number of clients: 1

MAC address: fc25-3f03-8361
IPv4 address: 10.1.1.114
IPv6 address: N/A

Username: N/A

AID: 1

AP ID: 2

```
AP name: 2
```

Radio ID	:	1
SSID	:	service
BSSID	:	000f-e211-2233
VLAN ID	:	1
Sleep count	:	242
Wireless mode	:	802.11ac
Channel bandwidth	:	80MHz

SM power save : Enabled
SM power save mode : Dynamic
Short GI for 20MHz : Supported
Short GI for 40MHz : Supported
Short GI for 80MHz : Supported
Short GI for 160/80+80MHz : Not supported
STBC RX capability : Not supported
STBC TX capability : Not supported
LDPC RX capability : Not supported
SU beamformee capability : Not supported
MU beamformee capability : Not supported
Beamformee STS capability : N/A
Block Ack : TID 0 In
Supported VHT-MCS set: NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set : 0, 1, 2, 3, 4, 5, 6, 7,
8, 9, 10, 11, 12, 13, 14,
15, 16, 17, 18, 19, 20,
21, 22, 23
Supported rates : 6, 9, 12, 18, 24, 36,
48, 54 Mbps
QoS mode : WMM
Listen interval : 10
RSSI : 62
Rx/Tx rate : 130/11

Authentication method : FT
Security mode : RSN
AKM mode : PSK
Encryption cipher : CCMP

User authentication mode: Bypass
Authorization ACL ID: 3001(Not effective)
Authorization user profile: N/A

```
Roam status: Intra-AC roam
```

Key derivation: SHA1
PMF status: Enabled
Forward policy name: Not configured
Online time: 0days 0hours 5minutes 13seconds

```
FT status: Active
```

例:over-the-DS FTおよび802.1X認証の設定

ネットワーク構成

図5に示すように、クライアントがAP 1とAP 2の間をローミングできるように、over-the-DS FTを介したAC内ローミングを設定します。認証およびキー管理モードとして802.1Xを設定します。

手順

#サービステンプレート**acstname**を作成します。

<AC> system-view

[AC] wlan service-template acstname

#SSIDを**service**に設定します。

[AC-wlan-st-acstname] ssid service

#AKMモードを**802.1X**に設定します。

[AC-wlan-st-acstname] akm mode dot1x

#ビーコン応答およびプローブ応答でRSN IEを有効にします。

[AC-wlan-st-acstname] cipher-suite ccmp

[AC-wlan-st-acstname] security-ie rsn

#クライアントの認証モードを802.1Xに設定します。

[AC-wlan-st-acstname] client-security authentication-mode dot1x

[AC-wlan-st-acstname] dot1x domain imc

#FTを有効にします。

[AC-wlan-st-acstname] ft enable

#FTメソッドを**over-the-DS**に設定します。

[AC-wlan-st-acstname] ft method over-the-ds

#サービステンプレートを有効にします。

[AC-wlan-st-acstname] service-template enable

[AC-wlan-st-acstname] quit

#802.1X認証モードをEAPに設定します。

[AC] dot1x authentication-method eap

#RADIUSスキームimccを作成します。

[AC] radius scheme imcc

#プライマリ認証サーバおよびアカウンティングサーバのIPアドレスを**10.1.1.3**に設定します。

[AC-radius-imcc] primary authentication 10.1.1.3

[AC-radius-imcc] primary accounting 10.1.1.3

#ACが認証サーバおよびアカウンティングサーバとパケットを交換するための共有キーを**12345678**に設定します。

[AC-radius-imcc] key authentication simple 12345678

[AC-radius-imcc] key accounting simple 12345678

#RADIUSサーバに送信されるユーザ名からISPドメイン名を削除するようにACを設定します。

[AC-radius-imcc] user-name-format without-domain

[AC-radius-imcc] quit

#ISPドメイン**imc**を作成し、認証、認可、アカウンティングにRADIUSスキームimccを使用するようにドメインを設定します。

[AC] domain imc

[AC-isp-imc] authentication lan-access radius-scheme imcc

[AC-isp-imc] authorization lan-access radius-scheme imcc

[AC-isp-imc] accounting lan-access radius-scheme imcc

[AC-isp-imc] quit

#AP 1を作成し、サービステンプレート**acstname**をAPの無線1にバインドします。

[AC] wlan ap 1 model WA4320i-ACN

[AC-wlan-ap-1] serial-id 210235A1BSC123000050

[AC-wlan-ap-1] radio 1

[AC-wlan-ap-1-radio-1] service-template acstname

[AC-wlan-ap-1-radio-1] radio enable

[AC-wlan-ap-1-radio-1] qui

[AC-wlan-ap-1] quit

#AP 2を作成し、サービステンプレート**acstname**をAPの無線1にバインドします。

[AC] wlan ap 2 model WA4320i-ACN

[AC-wlan-ap-2] serial-id 210235A1BSC123000055

[AC-wlan-ap-2] radio 1

[AC-wlan-ap-2-radio-1] service-template acstname

[AC-wlan-ap-2-radio-1] radio enable

[AC-wlan-ap-2-radio-1] quit

[AC-wlan-ap-2] quit

設定の確認

#サービステンプレートが正しく設定されていることを確認します。

[AC]display wlan service-template acstname verbose

Service template name:acstname

Description: Not configured

SSID: service
SSID-hide: Disabled

User-isolation: Disabled Service

template status: Enabled Maximum

clients per BSS: Not configured Frame

format: Dot3

Seamless-roam status: Disabled

Seamless-roam RSSI threshold :

50 Seamless-roam RSSI gap:

20

VLAN ID: 1

```
AKM mode                          : 802.1X
Security IE                       : RSN
Cipher suite                      : CCMP
```

TKIP countermeasure time: 0 sec

PTK lifetime: 43200 sec

GTK rekey: Enabled
GTK rekey method: Time-based
GTK rekey time: 86400 sec GTK

rekey client-offline: Disabled User

authentication mode: 802.1X

Intrusion protection: Disabled

Intrusion protection mode: Temporary-block

Temporary block time: 180 sec

Temporary service stop time :

20 sec

Fail VLAN ID: Not configured

802.1X handshake: Disabled

802.1X handshake secure:

Disabled

```
802.1X domain: imc
```

MAC-auth domain: Not configured

Max 802.1X users: 4096
Max MAC-auth users: 4096

802.1X re-authenticate: Disabled

Authorization fail mode: Online

Accounting fail mode: Online

Authorization: Permitted

Key derivation: SHA1
PMF status: Disabled Hotspot policy

number: Not configured Forwarding

policy status: Disabled Forwarding

policy name: Not configured Forwarder:

AC

FT Status: Enable

```
FT Method: over-the-ds
```

FT Reassociation Deadline:

20 sec QoS trust: Port

QoS priority: 0

#ローミングステータスがN/Aで、**FT**ステータスがActiveであることを確認します。

[AC] display wlan client

verbose Total number of

clients: 1

MAC address: fc25-3f03-8361
IPv4 address: 10.1.1.114

IPv6 address: N/A

Username: N/A

AID: 1
AP ID: 1

```
AP name: 1
```

Radio ID: 1

SSID: service

BSSID: 000f-e266-7788

VLAN ID: 1
Sleep count: 242

Wireless mode: 802.11ac
Channel bandwidth: 80MHz
SM power save: Enabled

SM power save mode: Dynamic
Short GI for 20MHz: Supported

Short GI for 40MHz: Supported

Short GI for 80MHz: Supported Short GI for

160/80+80MHz: Not supported

STBC RX capability: Not supported

STBC TX capability: Not supported

LDPC RX capability: Not supported
SU beamformee capability: Not supported

MU beamformee capability: Not supported
Beamformee STS capability: N/A
Block Ack: TID 0 In

Supported	VHT-MCS set:	NSS1 0, 1, 2, 3, 4, 5, 6,	7, 8
		NSS2 0, 1, 2, 3, 4, 5, 6,	7, 8
Supported	HT MCS set:	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23	
Supported	rates:	6, 9, 12, 18, 24, 36, 48, 54 Mbps	

QoS mode: WMM

Listen interval: 10

RSSI: 62
Rx/Tx rate: 130/11

Authentication method	:	Open system
Security mode	:	RSN
AKM mode	:	802.1X
Encryption cipher	:	CCMP

User authentication mode: 802.1X Authorization

ACL ID: 3001(Not effective)

Authorization user profile: N/A

```
Roam status: N/A
```

Key derivation: SHA1

PMF status: Enabled
Forward policy name: Not configured

Online time: 0days 0hours 1minutes 13seconds

```
FT status: Active
```

#クライアントをAP 2のカバレッジに移動します(詳細は表示されません)。

#認証方式が**FT**で、ローミングステータスが**Intra-AC**ローミングであることを確認します。

[AC] display wlan client

verbose Total number of

clients: 1

MAC address: fc25-3f03-8361

IPv4 address: 10.1.1.114
IPv6 address: N/A
Username: N/A

AID: 1
AP ID: 2

```
AP name: 2
```

Radio ID: 1
SSID: service
BSSID: 000f-e211-2233

VLAN ID: 1

Sleep count: 242

Wireless mode: 802.11ac

Channel bandwidth: 80MHz
SM power save: Enabled

SM power save mode: Dynamic
Short GI for 20MHz: Supported

Short GI for 40MHz: Supported

Short GI for 80MHz: Supported Short GI for

160/80+80MHz: Not supported STBC RX

capability: Not supported

STBC TX capability: Not supported
LDPC RX capability: Not supported

SU beamformee capability: Not supported

MU beamformee capability: Not supported

Beamformee STS capability: N/A
Block Ack: TID 0 In

Supported	VHT-MCS set:	NSS1 0, 1, 2, 3, 4, 5, 6,	7, 8
		NSS2 0, 1, 2, 3, 4, 5, 6,	7, 8
Supported	HT MCS set:	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23	
Supported	rates:	6, 9, 12, 18, 24, 36, 48, 54 Mbps	

QoS mode: WMM

Listen interval: 10
RSSI: 62

Rx/Tx rate: 130/11

```
Authentication method                : FT
Security mode                        : RSN
AKM mode                             : 802.1X
Encryption cipher                    : CCMP
```

User authentication mode: 802.1X Authorization ACL

ID: 3001(Not effective)

Authorization user profile: N/A

```
Roam status: Intra-AC roam
```

Key derivation: SHA1

PMF status: Enabled
Forward policy name: Not configured

Online time: 0days 0hours 5minutes 13seconds

```
FT status: Active
```

例:無線FTおよび802.1X認証の設定

ネットワーク構成

図5に示すように、クライアントがAP 1とAP 2の間をローミングできるように、無線FTを介したAC内ローミングを設定します。認証およびキー管理モードとして802.1X

を設定します。

手順

#サービステンプレート**acstname**を作成します。

<AC> system-view

[AC] wlan service-template acstname

#SSIDをserviceに設定します。

[AC-wlan-st-acstname] ssid service

#AKMモードを**802.1X**に設定します。

[AC-wlan-st-acstname] akm mode dot1x

#ビーコン応答およびプローブ応答でRSN IEを有効にします。

[AC-wlan-st-acstname] cipher-suite ccmp

[AC-wlan-st-acstname] security-ie rsn

#クライアントの認証モードを802.1Xに設定します。

[AC-wlan-st-acstname] client-security authentication-mode dot1x

[AC-wlan-st-acstname] dot1x domain imc

#FTを有効にします。

[AC-wlan-st-acstname] ft enable

#サービステンプレートを有効にします。

[AC-wlan-st-acstname] service-template enable

[AC-wlan-st-acstname] quit

#802.1X認証モードをEAPに設定します。

[AC] dot1x authentication-method eap

#RADIUSスキームimccを作成します。

[AC] radius scheme imcc

#プライマリ認証サーバおよびアカウンティングサーバのIPアドレスを**10.1.1.3**に設定します。

[AC-radius-imcc] primary authentication 10.1.1.3

[AC-radius-imcc] primary accounting 10.1.1.3

#ACが認証サーバおよびアカウンティングサーバとパケットを交換するための共有キーを**12345678**に設定します。

[AC-radius-imcc] key authentication simple 12345678

[AC-radius-imcc] key accounting simple 12345678

#RADIUSサーバに送信されるユーザ名からISPドメイン名を削除するようにACを設定します。

[AC-radius-imcc] user-name-format without-domain

[AC-radius-imcc] quit

#ISPドメイン**imc**を作成し、認証、認可、アカウンティングにRADIUSスキーム**imcc**を使用するようにドメインを設定します。

[AC] domain imc

[AC-isp-imc] authentication lan-access radius-scheme imcc

[AC-isp-imc] authorization lan-access radius-scheme imcc

[AC-isp-imc] accounting lan-access radius-scheme imcc

[AC-isp-imc] quit

#AP 1を作成し、サービステンプレート**acstname**をAPの無線1にバインドします。

[AC] wlan ap 1 model WA4320i-ACN
[AC-wlan-ap-1] serial-id 210235A1BSC123000050

[AC-wlan-ap-1] radio 1

[AC-wlan-ap-1-radio-1] service-template acstname

[AC-wlan-ap-1-radio-1] radio enable

[AC-wlan-ap-1-radio-1] quit

[AC-wlan-ap-1] quit

#AP 2を作成し、サービステンプレート**acstname**をAPの無線1にバインドします。

[AC]wlan ap 2 model WA4320i-ACN

[AC-wlan-ap-2] serial-id 210235A1BSC123000055

[AC-wlan-ap-2] radio 1

[AC-wlan-ap-2-radio-1] service-template acstname

[AC-wlan-ap-2-radio-1] radio enable

[AC-wlan-ap-2-radio-1] quit [AC-wlan-ap-2] quit

設定の確認

#次の情報を確認します。

- RSN IE is enabled.
- The AKM mode is **802.1X**.
- The cipher suite is **CCMP**.
- The FT status is **Active**.

[AC] display wlan

client verbose Total

number of clients: 1

MAC address: fc25-3f03-8361

IPv4 address: 10.1.1.114
IPv6 address: N/A

Username: N/A
AID: 1
AP ID: 1

```
AP name: 1
```

Radio ID: 1

SSID: service

BSSID: 000f-e266-7788

VLAN ID: 1
Sleep count: 242

Wireless mode: 802.11ac
Channel bandwidth: 80MHz
SM power save: Enabled

SM power save mode: Dynamic
Short GI for 20MHz: Supported

Short GI for 40MHz: Supported

Short GI for 80MHz: Supported Short GI

for 160/80+80MHz: Not supported STBC

RX capability: Not supported

STBC TX capability: Not supported
LDPC RX capability: Not supported
SU beamformee capability: Not supported

MU beamformee capability: Not supported
Beamformee STS capability: N/A
Block Ack: TID 0 In

Supported VHT-MCS set:	NSS1 0, 1, 2, 3, 4, 5, 6,	7, 8
	NSS2 0, 1, 2, 3, 4, 5, 6,	7, 8
Supported HT MCS set:	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23	
Supported rates:	6, 9, 12, 18, 24, 36, 48, 54 Mbps	

QoS mode: WMM
Listen interval: 10

RSSI: 62
Rx/Tx rate: 130/11

Authentication method	:	Open system
Security mode	:	RSN
AKM mode	:	802.1X
Encryption cipher	:	CCMP

User authentication mode: 802.1X Authorization

ACL ID: 3001(Not effective)

Authorization user profile: N/A

Roam status: N/A

Key derivation: SHA1

PMF status: Enabled

Forward policy name: Not configured

Online time: 0days 0hours 1minutes 13seconds

```
FT status: Active
```

#クライアントをAP 2のカバレッジに移動します(詳細は省略)。

#認証方式が**FT**で、ローミングステータスが**Intra-AC**ローミングであることを確認します。

[AC] display wlan client verbose Total number of clients: 1

MAC address: fc25-3f03-8361
IPv4 address: 10.1.1.114

IPv6 address: N/A
Username: N/A
AID: 1

AP ID: 2

```
AP name: 2
```

Radio ID: 1

SSID: service
BSSID: 000f-e211-2233

VLAN ID: 1

Sleep count: 242
Wireless mode: 802.11ac
Channel bandwidth: 80MHz

SM power save: Enabled
SM power save mode: Dynamic
Short GI for 20MHz: Supported

Short GI for 40MHz: Supported

Short GI for 80MHz:	Supported	
Short GI for 160/80+80MHz:	Not supported	
STBC RX capability:	Not supported	
STBC TX capability:	Not supported	
LDPC RX capability:	Not supported	
SU beamformee capability:	Not supported	
MU beamformee capability:	Not supported	
Beamformee STS capability:	N/A	
Block Ack:	TID 0 In	
Supported VHT-MCS set:	NSS1 0, 1, 2, 3, 4, 5, 6,	7, 8
	NSS2 0, 1, 2, 3, 4, 5, 6,	7, 8
Supported HT MCS set:	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23	
Supported rates:	6, 9, 12, 18, 24, 36, 48, 54 Mbps	

QoS mode: WMM
Listen interval: 10
RSSI: 62
Rx/Tx rate: 130/11
Security mode: RSN
AKM mode: 802.1X
Encryption cipher: CCMP
User authentication mode: 802.1X Authorization
ACL ID: 3001(Not effective)
Authorization user profile: N/A

```
Roam status: Intra-AC roam
```

Key derivation: SHA1
PMF status: Enabled
Forward policy name: Not configured
Online time: 0days 0hours 5minutes 13seconds

```
FT status: Active
```