CHAPTER 14

モビリティ グループの設定

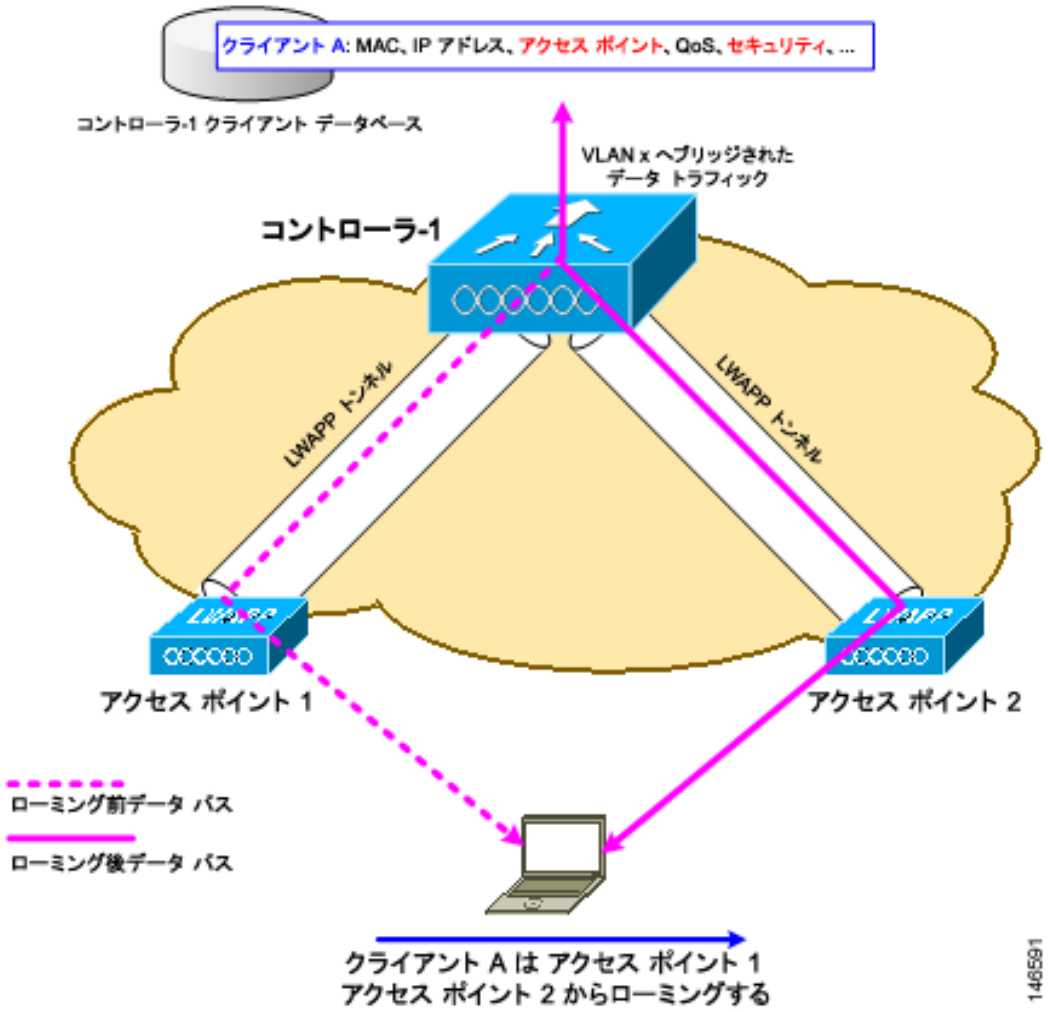
この章の内容は、次のとおりです。

モビリティについて

モビリティ（ローミング）は、できるだけ遅れることなく、確実かつスムーズに、あるアクセス ポイントから別のアクセス ポイントへアソシエーションを維持する無線 LAN クライアントの機能です。この項では、コントローラが無線ネットワークに存在する場合のモビリティの動作について説明します。

あるワイヤレス クライアントがアクセス ポイントにアソシエートして認証すると、アクセス ポイントのコントローラは、クライアント データベースにそのクライアントに対するエントリを設定します。このエントリには、クライアントの MAC アドレス、IP アドレス、セキュリティ コンテキストおよびアソシエーション、Quality of Service（QoS）コンテキスト、WLAN、およびアソシエートされたアクセス ポイントが含まれます。コントローラはこの情報を使用してフレームを転送し、ワイヤレス クライアントで送受信されるトラフィックを管理します。図 14-1 に、2 つのアクセス ポイントが同一のコントローラに join している場合の両アクセス ポイント間におけるワイヤレス クライアント ローミングの様子を示します。

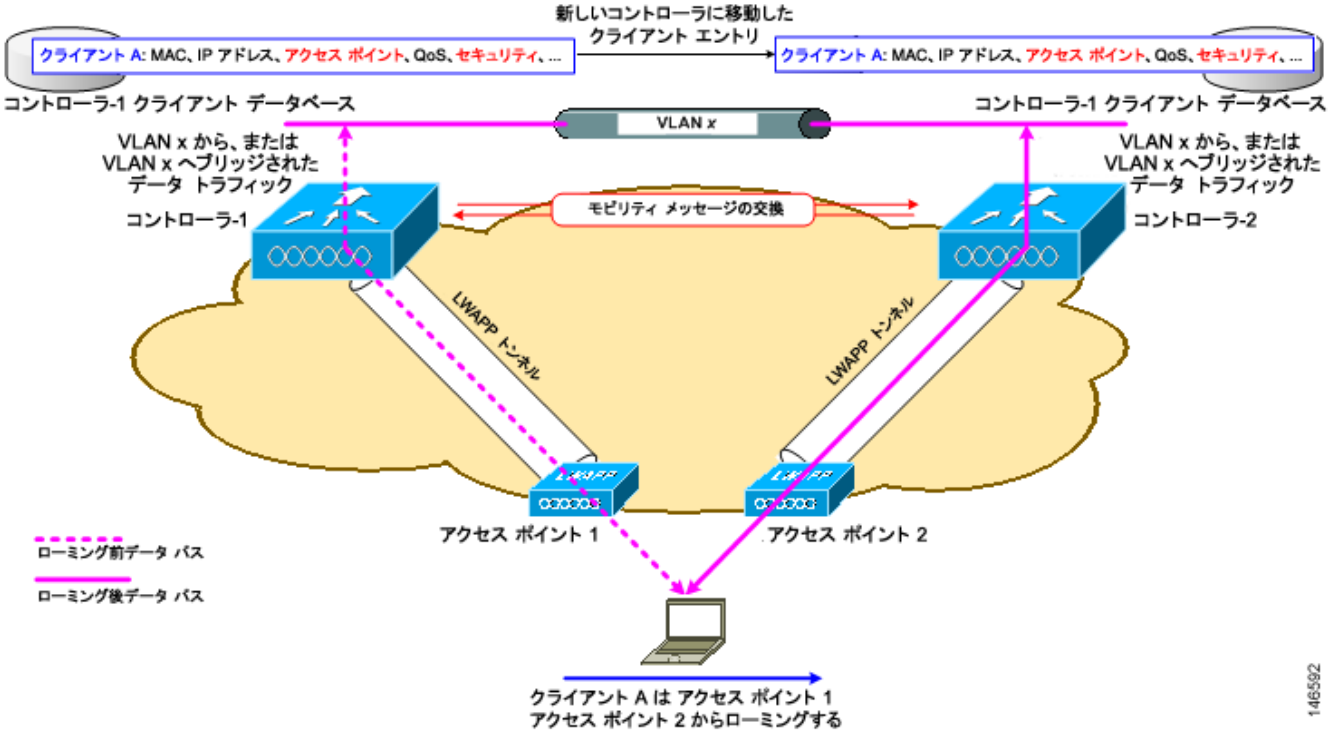
図 14-1　コントローラ内ローミング



ワイヤレス クライアントがそのアソシエーションをあるアクセス ポイントから別のアクセス ポイントへ移動する場合、コントローラはクライアントのデータベースを新たにアソシエートするアクセス ポイントでアップデートするだけです。必要に応じて、新たなセキュリティ コンテキストとアソシエーションも確立されます。

しかし、クライアントが 1 つのコントローラに join されたアクセス ポイントから別のコントローラに join されたアクセス ポイントにローミングする際には、プロセスはより複雑になります。また、同一のサブネット上でこれらのコントローラが動作しているかどうかによっても異なります。図 14-2 に、コントローラの無線 LAN インターフェイスが同じ IP サブネット上に存在する場合に発生するコントローラ間ローミングを示します。

図 14-2　コントローラ間ローミング

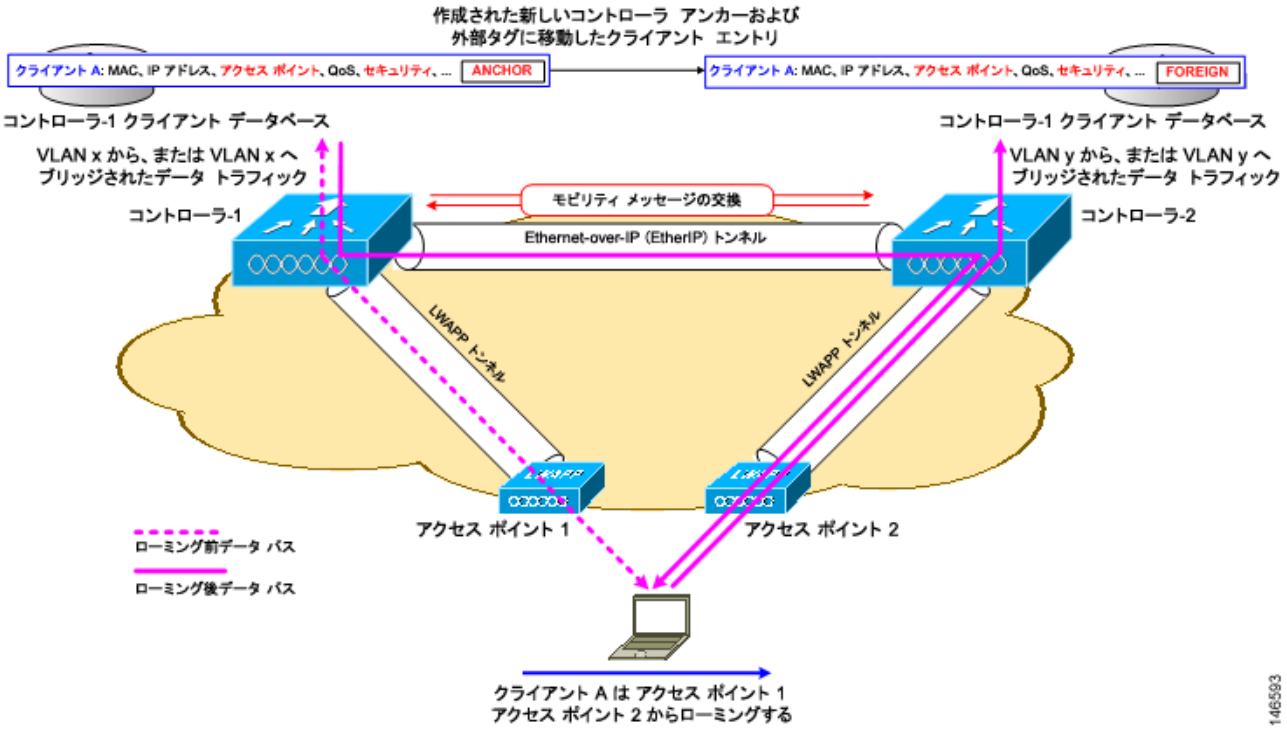


クライアントが新たなコントローラに join されたアクセス ポイントへアソシエートする場合、新たなコントローラはモビリティ メッセージを元のコントローラと交換し、クライアントのデータベース エントリは新たなコントローラに移動されます。新たなセキュリティ コンテキストとアソシエーションが必要に応じて確立され、クライアントのデータベース エントリは新たなアクセス ポイントに対してアップデートされます。このプロセスは、ユーザには透過的に行われます。

（注）　802.1X/Wi-Fi Protected Access（WPA）セキュリティで設定したすべてのクライアントは、IEEE 標準に準拠するために完全な認証を行います。

図 14-3 に、コントローラの無線 LAN インターフェイスが異なる IP サブネット上に存在する場合に発生するサブネット間ローミングを示します。

図 14-3　サブネット間ローミング



サブネット間ローミングは、コントローラがクライアントのローミングに関するモビリティ メッセージを交換する点でコントローラ間ローミングと似ています。ただし、クライアントのデータベース エントリを新しいコントローラに移動するのではなく、元のコントローラのクライアント データベース内で該当クライアントに「アンカー」エントリのマークが付けられます。このデータベース エントリが新しいコントローラのクライアント データベースにコピーされ、新しいコントローラ内で「外部」エントリのマークが付けられます。ローミングはワイヤレス クライアントには透過的なまま行われ、クライアントは元の IP アドレスを保持します。

サブネット間ローミングでは、アンカーと外部の両コントローラの WLAN に同一のネットワーク アクセス権限を設定し、ソースベースのルーティングやソースベースのファイアウォールを設定しないでおく必要があります。そのようにしない場合、ハンドオフ後クライアントにネットワーク接続上の問題が発生することがあります。

（注）　クライアントが Web 認証状態でローミングする場合、クライアントはモバイル クライアントして見なされるのではなく、別のコントローラ上の新しいクライアントとして見なされます。

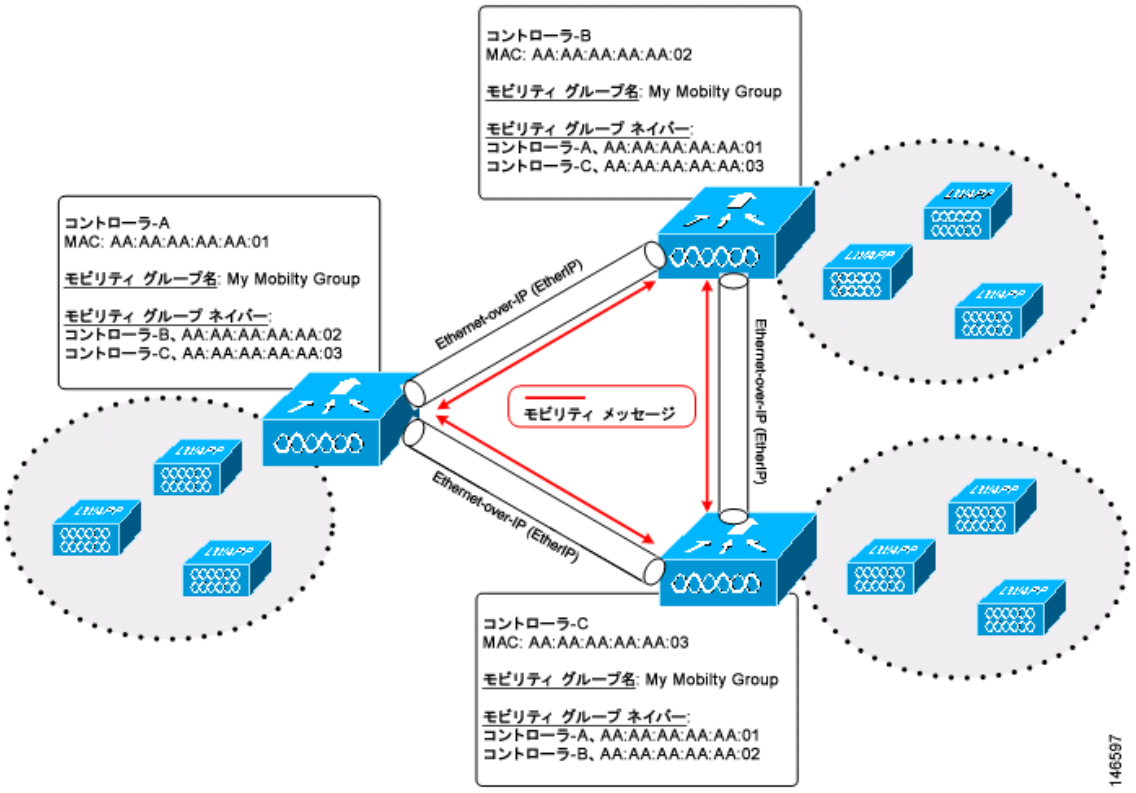
（注）　インターフェイスがタグ付けされていない場合、シームレス モビリティはネイティブ IPv6 クライアントではサポートされません。

モビリティ グループについて

モビリティ グループは、同じモビリティ グループ名で定義されるコントローラのセットで、ワイヤレス クライアントのローミングをシームレスに行う範囲を定義します。モビリティ グループを作成すると、ネットワーク内で複数のコントローラを有効化して、コントローラ間またはサブネット間のローミングが発生した際に、動的に情報を共有してデータ トラフィックを転送できるようになります。同じモビリティ グループ内のコントローラは、相互のアクセス ポイントを不正なデバイスとして認識しないように、クライアント デバイスのコンテキストと状態およびアクセス ポイントのリストを共有できます。この情報を使用して、ネットワークはコントローラ間無線 LAN ローミングとコントローラの冗長性をサポートできます。図 14-4 には、モビリティ グループの例が示されています。

（注） 1 つのモビリティ グループのメンバとなるコントローラは、同じモデルである必要はありません。モビリティ グループは、コントローラ プラットフォームの任意の組み合わせで構成できます。

図 14-4　　シングル モビリティ グループ



図示したように、各コントローラはモビリティ グループの別メンバーのリストを使用して設定されています。新しいクライアントがコントローラに join すると、コントローラはユニキャスト メッセージ（またはモビリティ キャストが設定されている場合はマルチキャスト メッセージ）をそのモビリティ グループの全コントローラに送信します。クライアントが以前に接続されていたコントローラは、クライアントのステータスを送信します。

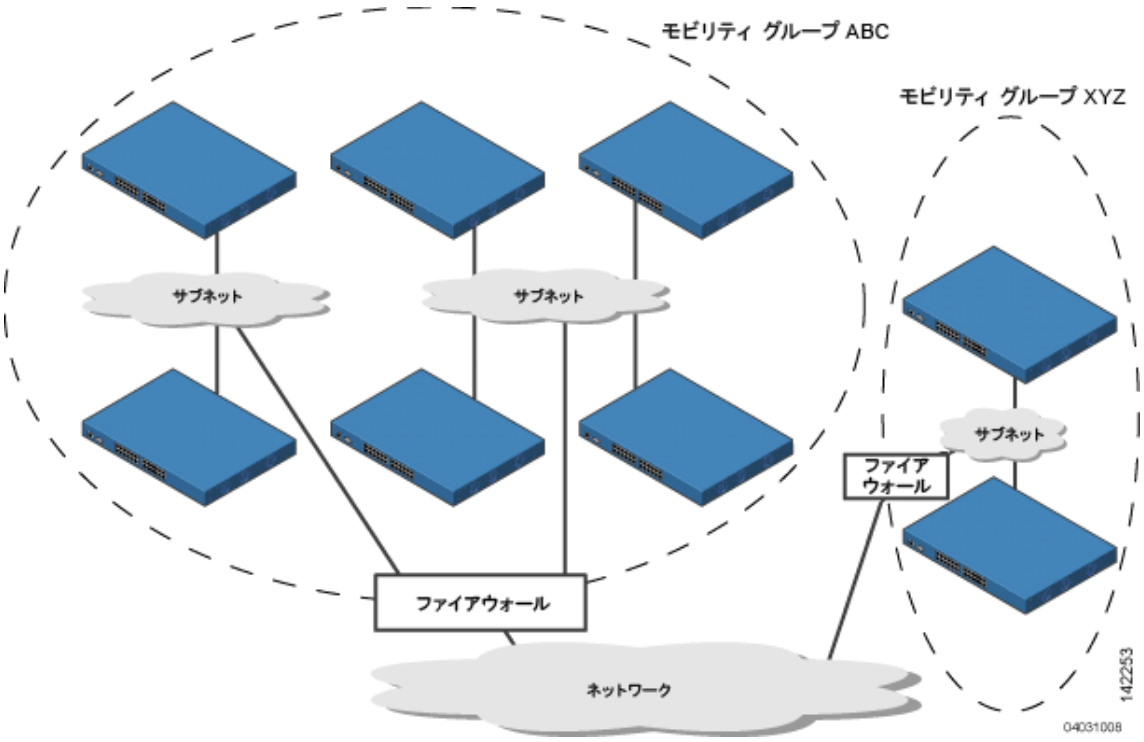
（注）　コントローラ ソフトウェア リリース 5.1 以降では、1 つのモビリティ グループにつき最大 24 台のコントローラがサポートされます。モビリティ グループでサポートされるアクセス ポイントの数は、そのグループのコントローラの数とタイプによって決まります。

例：

1. 4404-100 コントローラは、最大 100 台のアクセス ポイントをサポートします。したがって、24 台の 4404-100 コントローラで構成されているモビリティ グループは、最大 2400 台のアクセス ポイント（24 * 100 = 2400 アクセス ポイント）をサポートします。
2. 4402-25 コントローラは最大 25 台のアクセス ポイントをサポートし、4402-50 コントローラは最大 50 台のアクセス ポイントをサポートします。したがって、12 台の 4402-25 コントローラと 12 台の 4402-50 コントローラで構成されたモビリティ グループは最大 900 台のアクセス ポイント（12 * 25 + 12 * 50 = 300 + 600 = 900 アクセス ポイント）をサポートします。

異なるモビリティ グループ名を同じ無線ネットワーク内の異なるコントローラに割り当てると、モビリティ グループによって、1 つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限できます。図 14-5 には、2 つのコントローラ グループに異なるモビリティ グループ名を作成した結果が示されています。

図 14-5　　2 つのモビリティ グループ



ABC モビリティ グループのコントローラは、アクセス ポイントとクライアント情報を相互に共有します。ABC モビリティ グループのコントローラは、異なるモビリティ グループのアクセス ポイントまたは XYZ コントローラのクライアント情報を共有しません。同様に、XYZ モビリティ グループ内のコントローラは、ABC モビリティ グループのアクセスポイントまたはコントローラのクライアント情報を共有しません。この機能により、ネットワークでのモビリティ グループの切り離しが確実に行われます。

各コントローラは、モビリティ リスト内のピア コントローラに関する情報を保持します。コントローラ同士が相互のモビリティ リストに含まれている場合は、モビリティ グループ間のコントローラで通信を行うことができ、クライアントは異なるモビリティ グループのアクセス ポイント間でローミングを行うことができます。次の例のコントローラ 1 はコントローラ 2 または 3 と通信できますが、コントローラ 2 およびコントローラ 3 はコントローラ 1 だけと通信し、相互には通信できません。クライアントは同様に、コントローラ 1 とコントローラ 2 の間またはコントローラ 1 とコントローラ 3 の間はローミングを行うことができますが、コントローラ 2 とコントローラ 3 の間でローミングを行うことはできません。

例：

```
Controller 1                    Controller 2                    Controller 3
Mobility group: A               Mobility group: A               Mobility group: C
Mobility list:                  Mobility list:                  Mobility list:
    Controller 1 (group A)          Controller 1 (group A)          Controller 1 (group A)
    Controller 2 (group A)          Controller 2 (group A)          Controller 3 (group C)
    Controller 3 (group C)
```

（注） コントローラ ソフトウェア リリース 5.1 以降では、1 つのコントローラのモビリティ リストで最大 72 台のコントローラがサポートされます。1 つのモビリティ グループにつき 24 台のコントローラがサポートされるのはすべてのリリースで同じです。

コントローラでは、複数のモビリティ グループ間でのシームレスなローミングがサポートされています。シームレスなローミングでは、クライアントは異なるモビリティ グループでも同じ IP アドレスを維持します。ただし、Cisco Centralized Key Management（CCKM）および Public Key Cryptography（PKC）は、モビリティ グループ間ローミングの場合だけ、サポートされています。ローミング中にモビリティ グループの境界を越える場合、クライアントは完全に認証されますが、IP アドレスは維持され、レイヤ 3 ローミングのモビリティ トンネルが開始されます。

（注） コントローラ ソフトウェア リリース 5.0 リリースでは、1 つのモビリティ リストで最大 48 台のコントローラがサポートされます。

モビリティ グループにコントローラを追加するタイミングの判断

ネットワーク内のワイヤレス クライアントが、あるコントローラに join したアクセス ポイントから、別のコントローラに join したアクセス ポイントへローミングできますが、どちらのコントローラも同じモビリティ グループに属している必要があります。

モビリティ グループ間のメッセージング

コントローラでは、モビリティ メッセージを他のメンバ コントローラに送信することにより、クライアントにサブネット間モビリティが提供されます。コントローラ ソフトウェア リリース 5.0 以降のリリースでは、モビリティ メッセージングに対して 2 つの改良が行われました。どちらも、モビリティ メンバの全リストにメッセージを送信する場合に役立ちます。

- Mobile Announce メッセージを、まず同じグループ内に送信してから、リスト内の他のグループに送信する
- コントローラは、新しいクライアントがアソシエートされるたびに、モビリティ リスト内のメンバに Mobile Announce メッセージを送信します。5.0 より前のコントローラ ソフトウェア リリースでは、コントローラは所属グループに関係なく、このメッセージをリスト内のすべてのメンバに

送信します。しかし、コントローラ ソフトウェア リリース 5.0 以降のリリースでは、コントローラは自分と同じグループ（ローカル グループ）に属するメンバに対してのみメッセージを送信し、その後、再試行を送信する際に他のメンバをすべて加えます。

- ユニキャストではなくマルチキャストを使用して Mobile Annouce メッセージを送信する

  5.0 より前のコントローラ ソフトウェア リリースでは、コントローラはユニキャスト モードを使用して、すべてのモビリティ メッセージを送信しますが、これには、すべてのモビリティ メンバにメッセージのコピーを送信する必要があります。多くのメッセージ（Mobile Announce、PMK Update、AP List Update、IDS Shun など）はグループ内のすべてのメンバに向けられたものなので、この動作は効率的ではありません。コントローラ ソフトウェア リリース 5.0 以降のリリースでは、マルチキャストを使用して Mobile Announce メッセージを送信するようにコントローラを設定できます。これにより、コントローラからネットワークに送られるメッセージは 1 コピーのみになります。このコピーはモビリティ メンバすべてを含むマルチキャスト グループに宛てて送られます。マルチキャスト メッセージングを最大限生かすには、グループ メンバすべてに対してこの機能を有効化することを推奨します。

NAT デバイスでのモビリティ グループの使用

4.2 より前のコントローラ ソフトウェア リリースでは、同じモビリティ グループ内のコントローラ間のモビリティは、コントローラのいずれかがネットワーク アドレス変換（NAT）デバイスの背後にある場合には機能しません。この動作により、1 台のコントローラがファイアウォールの外側にあると考えられるゲストのアンカー機能では、問題が発生します。

モビリティ メッセージのペイロードは、ソース コントローラに関する IP アドレス情報を伝達します。この IP アドレスは、IP ヘッダーのソース IP アドレスで検証されます。この動作は、NAT デバイスがネットワークに導入される際に問題となります。これは、IP ヘッダー内でソース IP アドレスが変更されるためです。ゲスト WLAN 機能では、NAT デバイス経由でルーティングされているモビリティ パケットは、IP アドレスの不一致によりドロップされます。

コントローラ ソフトウェア リリース 4.2 以降のリリースでは、ソース コントローラの MAC アドレスを使用するようにモビリティ グループの検索が変更されています。NAT デバイスのマッピングに従ってソース IP アドレスが変更されるため、要求元のコントローラの IP アドレスを取得するために応答が送信される前に、モビリティ グループのデータベースが検索されます。このプロセスは、要求元のコントローラの MAC アドレスを使用して実行されます。

NAT が有効になっているネットワークのモビリティ グループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。さらに、PIX などのファイアウォールを使用している場合には、ファイアウォールで次のポートが開いていることを確認します。

- UDP 16666：トンネル コントロール トラフィック用
- IP プロトコル 97：ユーザのデータ トラフィック用
- UDP 161 および 162：SNMP

（注） コントローラ間のクライアント モビリティは、自動アンカー モビリティ（ゲスト トンネリングとも呼ばれる）またはシンメトリック モビリティ トンネリングが有効になっている場合にのみ機能します。アシンメトリック トンネリングは、モビリティ コントローラが NAT デバイスの背後にある場合にはサポートされません。これらのモビリティ オプションの詳細については、「自動アンカー モビリティの設定」および「シンメトリック モビリティ トンネリングの使用」の項を参照してください。

図 14-6 は、NAT デバイスを使用したモビリティ グループの設定例を示しています。この例では、すべてのパケットが NAT デバイスを通過します（つまり、送信元から宛先、およびその逆方向に送信されるパケット）。図 14-7 は、2 台の NAT デバイスを使用したモビリティ グループの設定例を示しています。この例では、送信元とゲートウェイとの間に 1 台の NAT デバイスを使用し、宛先とゲートウェイとの間にもう 1 台の NAT デバイスを使用しています。

図 14-6　　1 台の NAT デバイスを使用したモビリティ グループの設定

図 14-7　　2 台の NAT デバイスを使用したモビリティ グループの設定

モビリティ グループの設定

この項では、GUI または CLI を使用してコントローラのモビリティ グループを設定する方法について説明します。

（注） Cisco Wireless Control System（WCS）を使用してモビリティ グループを設定することもできます。手順については、『*Cisco Wireless Control System Configuration Guide*』を参照してください。

モビリティ グループを設定するための前提条件

コントローラをモビリティ グループに追加する前に、グループに追加するコントローラすべてについて、次の要件が満たされていることを確認する必要があります。

- すべてのコントローラの管理インターフェイス間に IP 接続が存在する必要があります。

（注） コントローラに対し Ping することで、IP 接続を確認できます。

（注） モビリティ制御パケットは、ルーティング テーブルに基づいて、任意のインターフェイス アドレスをソースとして使用できます。モビリティ グループのすべてのコントローラには、同一のサブネットの管理インターフェイスを必ず備えることを推奨します。1 つのコントローラの管理インターフェイスと他のコントローラの動的インターフェイスが同じサブネット上にあるトポロジは、シームレス モビリティには推奨しません。

- すべてのコントローラは、同じモビリティ グループ名で設定する必要があります。

（注） 通常、モビリティ グループ名は展開時にスタートアップ ウィザードを使用して設定されます。ただし、必要に応じて、[Controller] > [General] ページの [Default Mobility Domain Name] テキスト ボックスで変更できます。モビリティ グループ名では、大文字と小文字が区別されます。

（注） Cisco WiSM の場合、300 のアクセス ポイント間のルーティングをシームレスにするために両方のコントローラを同じモビリティ グループ名で設定してください。

（注） モビリティ グループの 1 つのコントローラが優先コール設定に設定されている場合、モビリティ グループの他のコントローラも同じ優先コール設定に設定する必要があります。

- モビリティ リスト内のコントローラが異なるソフトウェア バージョンを使用している場合、レイヤ 2 またはレイヤ 3 のクライアントのローミング サポートは制限されます。レイヤ 2 またはレイヤ 3 クライアント ローミングは、同じバージョンを使用する、またはバージョン 4.2.X、6.0.X、および 7.0.X を実行するコントローラ間でのみサポートされます。コントロール間のモビリティ サポートの詳細については、表 14-2 を参照してください。

（注） ソフトウェア リリース 5.2 以降のリリースが実行されているコントローラに別のソフトウェア リリース（4.2、5.0、5.1 など）が実行されているフェールオーバー コントローラを誤って設定すると、アクセス ポイントがフェールオーバー コントローラに接続するのに長い時間がかかることがあります。アクセス ポイントが検出プロセスを CAPWAP で開始してから、LWAPP 検出に変更するからです。

- すべてのコントローラは、同じ仮想インターフェイス IP アドレスで設定する必要があります。

（注）　必要に応じて、仮想インターフェイス IP アドレスを変更するには、[Controller] > [Interfaces] ページで仮想インターフェイス名を編集します。コントローラの仮想インターフェイスの詳細については、第 3 章「ポートとインターフェイスの設定」を参照してください。

（注）　モビリティ グループ内のすべてのコントローラが同じ仮想インターフェイスを使用していない場合、コントローラ間ローミングが動作しているように見えても、ハンドオフが完了せず、クライアントの接続はしばらくの間切断されます。

- モビリティ グループに追加するコントローラごとに、MAC アドレスと IP アドレスを収集しておく必要があります。この情報が必要となるのは、他の全モビリティ グループ メンバの MAC アドレスと IP アドレスを使用してすべてのコントローラを設定するからです。

（注）　モビリティ グループに追加する他のコントローラの MAC アドレスと IP アドレスは、各コントローラの GUI の [Controller] > [Mobility Groups] ページにあります。

- サード パーティのファイアウォール、たとえば、Cisco PIX または Cisco ASA を使用してモビリティ グループを設定する際は、ポート 16666 および IP プロトコル 97 を開く必要があります。
- コントローラ間 CAPWAP データおよびリリース 5.0、6.0、および 7.0 のコントロール トラフィックでは、ポート 5247 および 5246 を開く必要があります。
- コントローラ間 LWAPP データおよび 5.0 以前のリリースのトラフィックでは、ポート 12222 および 12223 を開かないでください。

表 14-1 に、管理および操作目的で使用する必要があるプロトコルおよびポート番号を示します。

表 14-1　プロトコル/サービスとポート番号

プロトコル/サービス	ポート番号
SSH/Telnet	TCP ポート 22 または 29
TFTP	UDP ポート 69
NTP	UDP ポート 123
SNMP	取得および設定では UDP ポート 161、トラップでは UDP ポート 162。
HTTPS/HTTP	HTTPS では TCP ポート 443、HTTP ではポート 80。
Syslog	TCP ポート 514
Radius 認証/アカウント	UDP ポート 1812 および 1813

（注）　ファイアウォール上ではポート アドレス変換（PAT）は実行できません。1 対 1 のネットワーク アドレス変換（NAT）を設定する必要があります。

表 14-2 に、異なるソフトウェア バージョンのコントローラ間でのモビリティのサポートについて説明します。

表 14-2　コントローラ バージョン間のモビリティのサポート

CUWN サービス	4.2.X.X	5.0.X.X	5.1.X.X	6.0.X.X	7.0.X.X
レイヤ 2 およびレイヤ 3 ローミング	X	–	–	X	X
ゲスト アクセス/ターミネーション	X	X	X	X	X
不正の検出	X	–	–	X	X
モビリティ グループ内のファスト ローミング（CCKM）	X	–	–	X	X
ロケーション サービス	X	–	–	X	X
Radio Resource Management（RRM）	X	–	–	X	X
Management Frame Protection（MFP）	X	–	–	X	X
AP フェールオーバー	X	–	–	X	X

モビリティ グループの設定（GUI）

ステップ 1　[Controller] > [Mobility Management] > [Mobility Groups] の順に選択して、[Static Mobility Group Members] ページを開きます。

図 14-8　[Static Mobility Group Members] ページ

このページでは、[Default Mobility Group] テキスト ボックスにモビリティ グループ名が表示され、現在モビリティ グループのメンバである各コントローラの MAC アドレスと IP アドレスが示されます。最初のエントリはローカル コントローラで、これを削除することはできません。

（注）　モビリティ グループからいずれかのリモート コントローラを削除するには、そのコントローラの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

ステップ 2　次のいずれかを実行して、コントローラをモビリティ グループに追加します。

- コントローラを 1 つだけ追加する場合、または別々に複数のコントローラを追加する場合、[New] をクリックして進みます。

  または

- 複数のコントローラを追加する場合、それらを一括で追加するには、[EditAll] をクリックしてへ進みます。

（注）　[EditAll] オプションを使用すると、現在のモビリティ グループ メンバのすべての MAC アドレスと IP アドレスを入力した後で、すべてのエントリをモビリティ グループの 1 つのコントローラから別のコントローラにコピーして貼り付けることができます。

ステップ 3　[New] をクリックして、[Mobility Group Member > New] ページを開きます。

ステップ 4　次の手順でコントローラをモビリティ グループに追加します。

a. [Member IP Address] テキスト ボックスに、追加するコントローラの管理インターフェイスの IP アドレスを入力します。

（注）　ネットワーク アドレス変換（NAT）が有効になっているネットワークのモビリティ グループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティ グループ内のコントローラ間でモビリティが失敗します。

b. [Member MAC Address] テキスト ボックスに、追加するコントローラの MAC アドレスを入力します。

c. [Group Name] テキスト ボックスに、モビリティ グループ名を入力します。

（注）　モビリティ グループ名では、大文字と小文字が区別されます。

d. [Apply] をクリックして、変更を確定します。新しいコントローラが、[Static Mobility Group Members] ページのモビリティ グループ メンバのリストに追加されます。

e. [Save Configuration] をクリックして、変更を保存します。

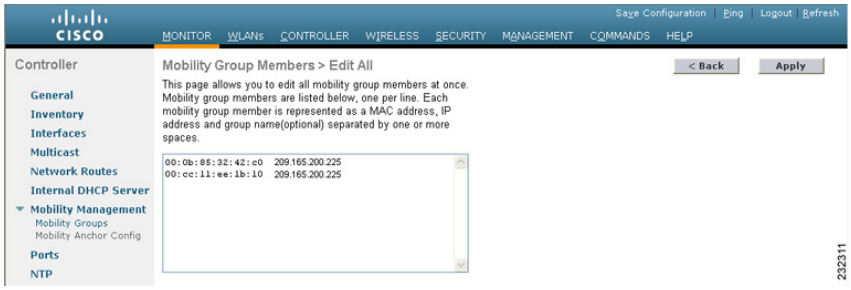
f. ステップ a ～ステップ e を繰り返して、すべてのコントローラをモビリティ グループに追加します。

g. モビリティ グループに追加するすべてのコントローラごとに、この手順を繰り返します。モビリティ グループ内のすべてのコントローラでは、他のすべてのモビリティ グループ メンバの MAC アドレスと IP アドレスを設定する必要があります。

[Mobility Group Members > Edit All] ページ（図 14-9 を参照）に現在モビリティ グループにあるすべてのコントローラの MAC アドレス、IP アドレス、およびモビリティ グループ名（オプション）が表示されます。コントローラのリストは、先頭にローカルのコントローラが表示され、1 行に 1 つずつ表示されます。

（注）　必要に応じて、リストのコントローラを編集または削除できます。

図 14-9　[Mobility Group Member > Edit All] ページ



ステップ 5　次の手順で、さらにコントローラをモビリティ グループに追加します。

a. 編集ボックス内をクリックして、新たな行を開始します。

b. MAC アドレス、管理インターフェイスの IP アドレス、および追加するコントローラのモビリティ グループ名を入力します。

（注） これらの値は 1 行に入力し、1 つまたは 2 つのスペースで区切ってください。

（注） モビリティ グループ名では、大文字と小文字が区別されます。

c. モビリティ グループに追加するコントローラごとに、ステップ a およびステップ b を繰り返します。

d. 編集ボックス内のエントリ全体を強調表示して、コピーします。

e. [Apply] をクリックして、変更を確定します。新しいコントローラが、[Static Mobility Group Members] ページのモビリティ グループ メンバのリストに追加されます。

f. [Save Configuration] をクリックして、変更を保存します。

g. リストをモビリティ グループ内の他のすべてのコントローラの [Mobility Group Members > Edit All] ページにあるテキスト ボックスに貼り付けて、[Apply] と [Save Configuration] をクリックします。

ステップ 6　[Multicast Messaging] を選択して、[Mobility Multicast Messaging] ページを開きます。

図 14-10　[Mobility Multicast Messaging] ページ

現在、設定されているモビリティ グループすべての名前がページの中央に表示されます。

ステップ 7　[Mobility Multicast Messaging] ページで、[Enable Multicast Messaging] チェックボックスをオンにすると、Mobile Announce メッセージをモビリティ メンバに送信するために、コントローラでマルチキャスト モードを使用できるようになります。このチェックボックスをオフにしておくと、Mobile Announce メッセージはユニキャスト モードで送信されます。デフォルト値ではオフになっています。

ステップ 8　前の手順でマルチキャスト メッセージングを有効化した場合は、[Local Group Multicast IP Address] テキスト ボックスに、ローカル モビリティ グループのマルチキャスト グループ IP アドレスを入力します。このアドレスは、マルチキャスト モビリティ メッセージングに使用されます。

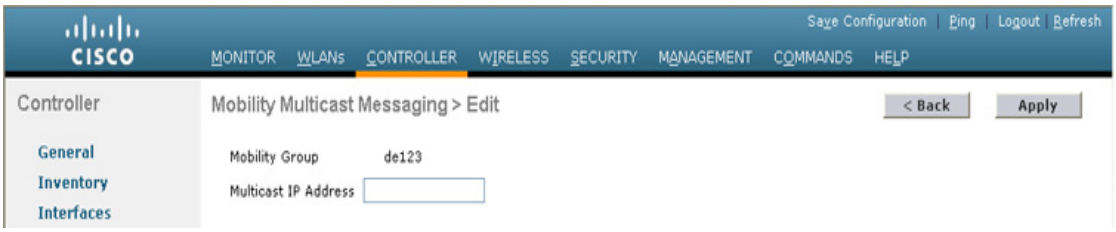
（注）　マルチキャスト メッセージングを使用するには、ローカル モビリティ グループの IP アドレスを設定する必要があります。

ステップ 9　[Apply] をクリックして、変更を確定します。

ステップ 10　必要に応じて、モビリティ リスト内にあるローカル以外のグループのマルチキャスト グループ IP アドレスを設定することもできます。このためには、ローカル以外のモビリティ グループの名前をクリックして、[Mobility Multicast Messaging > Edit] ページ（図 14-11 を参照）を開き、[Multicast IP Address] テキスト ボックスにローカル以外のモビリティ グループのマルチキャスト グループ IP アドレスを入力します。

（注）　ローカル以外のグループにマルチキャスト IP アドレスが設定されていない場合、コントローラはこのグループのメンバに対して、ユニキャスト モードでモビリティ メッセージを送信します。

図 14-11　[Mobility Multicast Messaging > Edit] ページ



ステップ 11　[Apply] をクリックして、変更を確定します。

ステップ 12　[Save Configuration] をクリックして、変更を保存します。

モビリティ グループの設定（CLI）

ステップ 1　このコマンドを入力して現在のモビリティ設定を確認します。

show mobility summary

以下に類似した情報が表示されます。

```
Symmetric Mobility Tunneling (current) .......... Enabled
Symmetric Mobility Tunneling (after reboot) ..... Enabled
Mobility Protocol Port........................... 16666
Mobility Security Mode........................... Disabled
Default Mobility Domain.......................... snmp_gui
Multicast Mode .................................. Disabled
```

```
Mobility Domain ID for 802.11r..................... 0x66bd
Mobility Keepalive Interval....................... 10
Mobility Keepalive Count.......................... 3
Mobility Group Members Configured................. 3
Mobility Control Message DSCP Value.............. 0

Controllers configured in the Mobility Group
 MAC Address        IP Address       Group Name Multicast IP Status
 00:0b:85:32:42:c0 1.100.163.24     snmp_gui     0.0.0.0     Up
 00:cc:11:ee:1b:10 10.100.100.1    VoWLAN        0.0.0.0     Control and Data Path Down
 11:22:11:33:11:44 1.2.3.4         test          0.0.0.0     Control and Data Path Down
```

ステップ 2　モビリティ グループを作成するには、次のコマンドを入力します。

config mobility group domain *domain_name*

（注）　グループ名には、最大 31 文字の ASCII 文字列を使用できます。大文字と小文字が区別されます。モビリティ グループ名には、スペースは使用できません。

ステップ 3　グループ メンバを追加するには、次のコマンドを入力します。

config mobility group member add *mac_address ip_address*

（注）　ネットワーク アドレス変換（NAT）が有効になっているネットワークのモビリティ グループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティ グループ内のコントローラ間でモビリティが失敗します。

（注）　グループ メンバを削除するには、**config mobility group member delete** *mac_address* コマンドを入力します。

ステップ 4　マルチキャスト モビリティ モードを有効または無効にするには、次のコマンドを入力します。

config mobility multicast-mode {**enable** | **disable**} *local_group_multicast_address*

ここで、*local_group_multicast_address* は、ローカル モビリティ グループのマルチキャスト グループ IP アドレスです。このアドレスは、マルチキャスト モビリティ メッセージングに使用されます。

マルチキャスト モビリティ モードを有効にした場合、Mobile Announce メッセージはマルチキャスト モードでローカル グループに送信されます。マルチキャスト モビリティ モードを無効にした場合、Mobile Announce メッセージはユニキャスト モードでローカル グループに送信されます。デフォルト値では無効になっています。

ステップ 5　（オプション）モビリティ リスト内で、非ローカル グループのマルチキャスト グループ IP アドレスを設定することもできます。そのためには、次のコマンドを入力します。

config mobility group multicast-address *group_name IP_address*

ローカル以外のグループにマルチキャスト IP アドレスが設定されていない場合、コントローラはこのグループのメンバに対して、ユニキャスト モードでモビリティ メッセージを送信します。

ステップ 6　モビリティ設定を確認するには、次のコマンドを入力します。

show mobility summary

ステップ 7　次のコマンドを入力して、変更を保存します。

save config

ステップ 8　モビリティ グループに追加するすべてのコントローラごとに、この手順を繰り返します。モビリティ グループ内のすべてのコントローラでは、他のすべてのモビリティ グループ メンバの MAC アドレスと IP アドレスを設定する必要があります。

ステップ 9　モビリティ メッセージのマルチキャスト使用のデバッグを有効または無効にするには、次のコマンドを入力します。

debug mobility multicast {**enable** | **disable**}

モビリティ グループの統計の表示

コントローラの GUI から次の 3 種類のモビリティ グループの統計を表示できます。

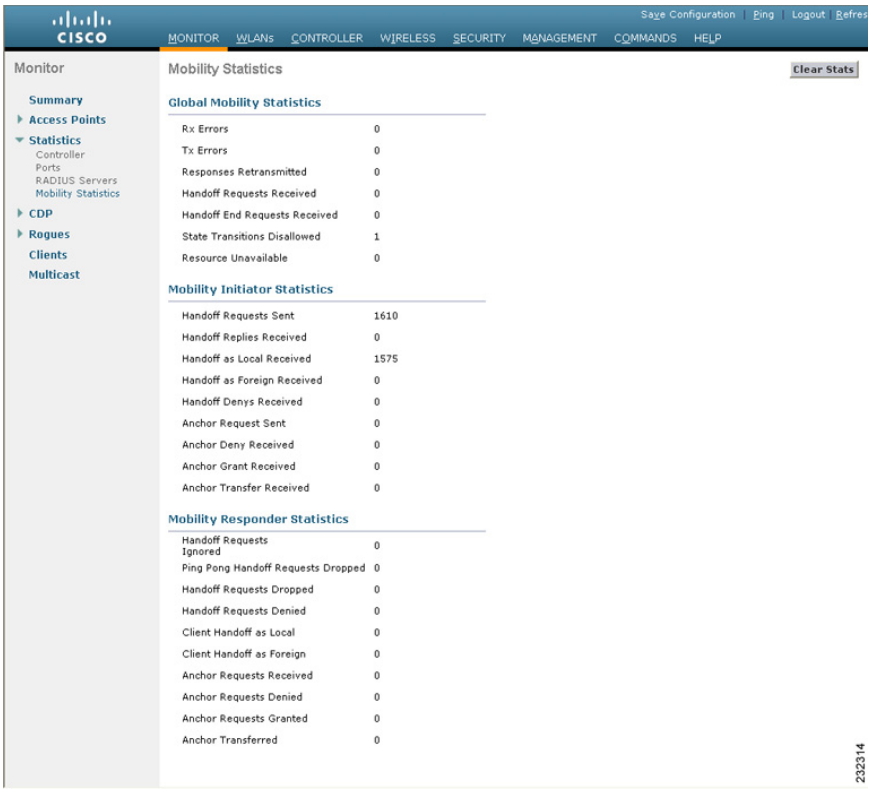
- Global Mobility Statistics：すべてのモビリティ トランザクションに影響します。
- Mobility Initiator Statistics：モビリティ イベントを開始するコントローラによって生成されます。
- Mobility Responder Statistics：モビリティ イベントに応答するコントローラによって生成されます。

コントローラの GUI または CLI を使用して、モビリティ グループの統計を表示できます。

モビリティ グループの統計の表示（GUI）

ステップ 1　[Monitor] > [Statistics] > [Mobility Statistics] の順に選択して、[Mobility Statistics] ページを開きます。

図 14-12　[Mobility Statistics] ページ



ここでは、次の内容について説明します。

- Global Mobility Statistics
  - [Rx Errors]：短すぎるパケットや不正な形式などの、一般的なプロトコル パケット受信エラー。
  - [Tx Errors]：パケット送信失敗など、一般的なプロトコル パケット送信エラー。
  - [Responses Retransmitted]：モビリティ プロトコルで UDP が使用されているときに応答が受信されない場合には、複数回にわたって要求が再送信されます。ネットワークの遅延または処理の遅延のため、応答側が最初に要求に応答した後に、1 回以上の再試行要求を受信する場合があります。このテキスト ボックスには、応答が再送信された回数が表示されます。
  - [Handoff Requests Received]：ハンドオフ要求が受信、無視または応答された合計回数。
  - [Handoff End Requests Received]：ハンドオフ終了要求が受信された合計回数。これらの要求は、クライアント セッションの終了について通知するために、アンカー コントローラまたは外部コントローラによって送信されます。

- [State Transitions Disallowed]：ポリシー施行モジュール（PEM）がクライアントの状態の遷移を拒否しました。通常、その結果としてハンドオフが中断されます。
- [Resource Unavailable]：バッファなどの必要なリソースが使用できませんでした。その結果としてハンドオフが中断されます。

- Mobility Initiator Statistics
  - [Handoff Requests Sent]：コントローラにアソシエートされ、モビリティ グループに通知されているクライアントの数。
  - [Handoff Replies Received]：送信された要求に応答して受信されている、ハンドオフ応答の数。
  - [Handoff as Local Received]：クライアント セッション全体が転送されているハンドオフの数。
  - [Handoff as Foreign Received]：クライアント セッションが別の場所でアンカーされたハンドオフの数。
  - [Handoff Denys Received]：拒否されたハンドオフの数。
  - [Anchor Request Sent]：スリーパーティ（外部から外部）ハンドオフ用に送信されたアンカー要求の数。ハンドオフが別の外部コントローラから受信され、新しいコントローラがクライアントを移動させるためのアンカーを要求しています。
  - [Anchor Deny Received]：現在のアンカーによって拒否されたアンカー要求の数。
  - [Anchor Grant Received]：現在のアンカーによって許可されたアンカー要求の数。
  - [Anchor Transfer Received]：現在のアンカー上でセッションを閉じ、要求元にアンカーを送り返したアンカー要求の数。
- Mobility Responder Statistics
  - [Handoff Requests Ignored]：コントローラにクライアントが認識されていなかったために無視された、ハンドオフ要求またはクライアント通知の数。
  - [Ping Pong Handoff Requests Dropped]：ハンドオフ期間が短すぎた（3 秒）ために拒否されたハンドオフ要求の数。
  - [Handoff Requests Dropped]：クライアントについての認識が不完全であるか、パケットの問題が原因でドロップされたハンドオフ要求の数。
  - [Handoff Requests Denied]：拒否されたハンドオフ要求の数。
  - [Client Handoff as Local]：クライアントがローカル ロールにある間に送信されたハンドオフ応答の数。
  - [Client Handoff as Foreign]：クライアントが外部ロールにある間に送信されたハンドオフ応答の数。
  - [Anchor Requests Received]：受信したアンカー要求の数。
  - [Anchor Requests Denied]：拒否されたハンドオフ要求の数。
  - [Anchor Requests Granted]：許可されたアンカー要求の数。
  - [Anchor Transferred]：クライアントが外部コントローラから現在のアンカーとして同じサブネット上のコントローラに移動したために、転送されたアンカーの数。

ステップ 2　現在のモビリティ統計をクリアする場合は、[Clear Stats] をクリックします。

モビリティ グループの統計の表示（CLI）

- モビリティ グループの統計情報を表示するには、**show mobility statistics** コマンドを入力します。
- 現在のモビリティ統計をクリアするには、**clear stats mobility** コマンドを入力します。

自動アンカー モビリティの設定

この項では、次のトピックを扱います。

自動アンカー モビリティについて

無線 LAN 上でローミング クライアントのロード バランシングとセキュリティを向上させるために、自動アンカー モビリティ（ゲスト トンネリングとも呼ばれる）を使用できます。通常のローミング状態では、クライアント デバイスは無線 LAN に接続され、最初に接触するコントローラにアンカーされます。クライアントが異なるサブネットにローミングする場合、クライアントのローミング先のコントローラは、クライアント用にアンカー コントローラとの外部セッションを設定します。ただし、自動アンカー モビリティ機能を使用している場合は、無線 LAN 上のクライアントのアンカー ポイントとしてコントローラまたはコントローラのセットを指定できます。

自動アンカー モビリティ モードでは、モビリティ グループのサブセットは WLAN のアンカー コントローラとして指定されます。クライアントのネットワークへのエントリ ポイントに関係なく、この機能を使用して WLAN を単一のサブネットに制限できます。それにより、クライアントは企業全体にわたりゲスト WLAN にアクセスできますが、引き続き特定のサブネットに制限されます。WLAN は建物の特定のセクション（ロビー、レストランなど）を表すことができるため、自動アンカー モビリティで地理的ロード バランシングも提供でき、WLAN のホーム コントローラのセットを効果的に作成できます。モバイル クライアントがたまたま最初に接触するコントローラにアンカーされるのではなく、特定の圏内にあるアクセス ポイントを制御するコントローラにモバイル クライアントをアンカーできます。

クライアントが WLAN のモビリティ アンカーとして事前設定されているモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、クライアントのローカル セッションが作成されます。クライアントは、WLAN の事前設定されたアンカー コントローラにのみアンカーできます。指定された WLAN の場合、モビリティ グループのすべてのコントローラ上で同じセットのアンカー コントローラを設定する必要があります。

クライアントが WLAN のモビリティ アンカーとして設定されていないモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、クライアントのローカル セッションが作成され、そのクライアントがモビリティ リスト内の別のコントローラに通知されます。その通知に対する回答がない場合、コントローラは WLAN に設定されたいずれかのアンカー コントローラに接触して、ローカルスイッチ上のクライアントに対する外部セッションを作成します。クライアントからのパケットは EtherIP を使用してモビリティ トンネルを介してカプセル化され、アンカー コントローラに送信されます。ここでカプセルを解除されて有線ネットワークへ配信されます。クライアントへのパケットは、アンカー コントローラで受信され、EtherIP を使用してモビリティ トンネルを介して外部コントローラへ転送されます。外部コントローラはパケットのカプセルを解除し、クライアントへ転送します。

外部コントローラ上の特定の WLAN に複数のコントローラがモビリティ アンカーとして追加されている場合、外部コントローラは IP アドレスでコントローラを内部的にソートします。最も低い IP アドレスを持つコントローラが最初のアンカーになります。たとえば、標準的な順序付きリストが 172.16.7.25、172.16.7.28、192.168.5.15 であるとします。最初のクライアントを外部コントローラのアンカーされた WLAN にアソシエートされると、クライアント データベース エントリがリストの最初のアンカー コントローラに、2 番目のクライアントがリストの 2 番目のコントローラに、というように、アンカー リストの最後に達するまで送信されます。プロセスは最初のアンカー コントローラから始まり、繰り返されます。いずれかのアンカー コントローラがダウンしていることが検出された場合、そのコントローラにアンカーされているクライアントが認証解除され、クライアントはアンカー リスト内の残りのコントローラについてラウンドロビン方式で認証/アンカー プロセスを処理します。この機能は、モビリティ フェールオーバーによって通常のモビリティ クライアントにも使用されます。この機能によって、モビリティ グループのメンバは到着不能なメンバを検出してクライアントを再ルーティングできます。

ガイドラインと制限事項

- 4.1 より前のコントローラ ソフトウェア リリースでは、モビリティ グループ内に到着不能になったコントローラがあるかどうか自動で判断する方法はありませんでした。そのため、到着不能なアンカー コントローラに外部コントローラが新たなクライアント要求を送信し続け、セッションがタイムアウトするまでクライアントがこの到着不能なコントローラに接続し続けることがありました。コントローラ ソフトウェア リリース 4.1 以降のリリースでは、モビリティ リストのメンバ同士が ping 要求をお互いに送信し合い、データを確認してそのデータのパスを管理することで、到着不能なメンバがいないかを調べてクライアントを再ルーティングできます。それぞれのアンカー コントローラに送信する ping 要求の数と間隔は、設定可能です。この機能には、ゲスト トンネリングのほか、通常のモビリティでモビリティ フェールオーバーを実行できるよう、ゲスト N+1 冗長性が備わっています。
- Cisco 2100 シリーズ コントローラは、WLAN のアンカーとして指定できません。ただし、Cisco 2100 シリーズ コントローラ上に作成された WLAN に Cisco 4400 シリーズ コントローラをアンカーとして指定できます。
- IPsec および L2TP レイヤ 3 セキュリティ ポリシーは、モビリティ アンカーで設定された WLAN には使用できません。
- コントローラを WLAN のモビリティ アンカーとして指定するには、そのコントローラをモビリティ グループ メンバ リストに追加する必要があります。
- WLAN のモビリティ アンカーとして、複数のコントローラを設定できます。
- WLAN のモビリティ アンカーを設定する前に、WLAN を無効にする必要があります。
- 自動アンカー モビリティは、Web 認可をサポートしていますが、その他のレイヤ 3 セキュリティ タイプをサポートしていません。
- 外部コントローラ上の WLAN とアンカー コントローラ上の WLAN は、両方ともモビリティ アンカーを使用して設定する必要があります。アンカー コントローラ上で、アンカー コントローラ自体をモビリティ アンカーとして設定します。外部コントローラ上で、アンカーをモビリティ アンカーとして設定します。
- 自動アンカー モビリティは、DHCP オプション 82 と共には使用できません。
- ゲスト N+1 冗長性とモビリティ フェールオーバー機能にファイアウォールを組み合わせて使用する場合は、次のポートに空きがあることを確認してください。
  - UDP 16666：トンネル コントロール トラフィック用
  - IP プロトコル 97：ユーザのデータ トラフィック用
  - UDP 161 および 162：SNMP

自動アンカー モビリティの設定（GUI）

ステップ 1　モビリティ グループ内に到達不能なアンカー コントローラがないかを検出するには、次の手順でコントローラを設定してください。

a. [Controller] > [Mobility Management] > [Mobility Anchor Config] の順に選択して、[Mobility Anchor Config] ページを開きます。

b. [Keep Alive Count] テキスト ボックスに、そのアンカーが到着不能と判断するまでにアンカー コントローラに ping 要求を送信する回数を入力します。有効な範囲は 3 ～ 20 で、デフォルト値は 3 です。

c. [Keep Alive Interval] テキスト ボックスには、アンカー コントローラに送信する各 ping 要求の間隔を秒単位で入力します。有効な範囲は 1 ～ 30 秒で、デフォルト値は 10 秒です。

d. [DSCP Value] テキスト ボックスに、DSCP の値を入力します。デフォルトは 0 です。

e. [Apply] をクリックして、変更を確定します。

ステップ 2　[WLANs] を選択して、[WLANs] ページを開きます。

ステップ 3　目的の WLAN または有線ゲスト LAN の青いドロップダウン矢印をクリックして、[Mobility Anchors] を選択します。[Mobility Anchors] ページが表示されます。

このページには、すでにモビリティ アンカーとして設定されているコントローラが一覧表示されるほか、そのデータと管理パスの現状が表示されます。モビリティ グループ内のコントローラは、well-known UDP ポート上でお互いに通信し合い、Ethernet-over-IP（EoIP）トンネルを通じてデータ トラフィックを交換します。mping を送信して、モビリティ制御パケットの到着可能性を管理インターフェイスのモビリティ UDP ポート 16666 によってテストします。また、eping を送信して、モビリティ データ トラフィックを管理インターフェイスの EoIP ポート 97 によってテストします。[Control Path] テキスト ボックスは、mping が成功した（up）か失敗した（down）かを表示します。[Data Path] テキスト ボックスは、eping が成功した（up）か失敗した（down）かを表示します。[Data Path] テキスト ボックスまたは [Control Path] テキスト ボックスに「down」が表示された場合は、モビリティ アンカーが到着できず、接続できないと考えられます。

ステップ 4　モビリティ アンカーに指定されたコントローラの IP アドレスを、[Switch IP Address (Anchor)] ドロップダウン リストで選択します。

ステップ 5　[Mobility Anchor Create] をクリックします。選択したコントローラが、この WLAN または有線ゲスト LAN のアンカーになります。

（注）　WLAN または有線ゲスト LAN のモビリティ アンカーを削除するには、アンカーの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

ステップ 6　[Save Configuration] をクリックして、変更を保存します。

ステップ 7　ステップ 4 およびステップ 6 を繰り返し、他のコントローラをこの WLAN または有線ゲスト LAN のモビリティ アンカーとして設定します。

ステップ 8　モビリティ グループのすべてのコントローラに同じセットのモビリティ アンカーを設定します。

自動アンカー モビリティの設定（CLI）

- コントローラは、到着不能なモビリティ リスト メンバを常に検出するようにプログラムされます。モビリティ メンバ間で ping を交換するためのパラメータを変更するには、次のコマンドを入力します。
  - **config mobility group keepalive count** *count*：そのメンバが到着不能と判断されるまでにモビリティ リスト メンバに送信する ping 要求の回数。有効な範囲は 3 ～ 20 で、デフォルト値は 3 です。
  - **config mobility group keepalive interval** *seconds*：モビリティ リスト メンバに送信する各 ping 要求の間隔（秒単位）。有効な範囲は 1 ～ 30 秒で、デフォルト値は 10 秒です。
- モビリティ アンカーを設定している WLAN または有線ゲスト LAN を無効にするには、次のコマンドを入力します。

  config {wlan | guest-lan} disable {*wlan_id* | *guest_lan_id*}
- WLAN または有線ゲスト LAN の新たなモビリティ アンカーを作成するには、次のコマンドのいずれかを入力します。
  - **config mobility group anchor add** {**wlan | guest-lan**} {*wlan_id* | *guest_lan_id*} *anchor_controller_ip_address*
  - **config** {**wlan | guest-lan**} **mobility anchor add** {*wlan_id* | *guest_lan_id*} *anchor_controller_ip_address*

  （注） *wlan_id* または *guest_lan_id* は、存在しているが無効になっており、*anchor_controller_ip_address* は、デフォルトのモビリティ グループのメンバである必要があります。

  （注） 1 つ目のモビリティ アンカーを設定するときに、WLAN または有線ゲスト LAN で自動アンカー モビリティを有効にします。
- WLAN または有線ゲスト LAN のモビリティ アンカーを削除するには、次のコマンドのいずれかを入力します。
  - **config mobility group anchor delete {wlan | guest-lan} {wlan_id | guest_lan_id}** *anchor_controller_ip_address*
  - **config {wlan | guest-lan} mobility anchor delete {wlan_id | guest_lan_id}** *anchor_controller_ip_address*

  （注） *wlan_id* または *guest_lan_id* は必ず指定し、無効にする必要があります。

  （注） 最後のアンカーを削除すると、自動アンカー モビリティ機能は無効になり、新しいアソシエーションに対しては標準のモビリティが再度使用されるようになります。
- 次のコマンドを入力して、設定を保存します。

  save config
- 特定の WLAN または有線ゲスト LAN のモビリティ アンカーとして設定されたコントローラのリストとステータスを表示するには、次のコマンドを入力します。

show mobility anchor {**wlan** | *guest-lan*} {*wlan_id* | *guest_lan_id*}

（注）　*wlan_id* パラメータと *guest_lan_id* パラメータはオプションであり、リストを特定の WLAN またはゲスト LAN のアンカーに制限します。システムのすべてのモビリティ アンカーを表示するには、**show mobility anchor** コマンドを入力します。

以下に類似した情報が表示されます。

```
Mobility Anchor Export List
WLAN ID    IP Address     Status
    1      10.50.234.2    UP
    1      10.50.234.6    UP
    2      10.50.234.2    UP
    2      10.50.234.3    CNTRL_DATA_PATH_DOWN

GLAN ID    IP Address     Status
    1      10.20.100.2    UP
    2      10.20.100.3    UP
```

[Status] テキスト ボックスには、次のうちいずれかの値が表示されます。

- UP：コントローラはアクセス可能で、データを渡すことができます。
- CNTRL_PATH_DOWN：mpings に失敗しました。コントロール パス経由でコントローラにアクセスできないため、エラーが発生したと見なされます。
- DATA_PATH_DOWN：epings に失敗しました。コントローラにアクセスできないため、エラーが発生したと見なされます。
- CNTRL_DATA_PATH_DOWN：mpings および epings の両方に失敗しました。コントローラにアクセスできないため、エラーが発生したと見なされます。

- すべてのモビリティ グループ メンバのステータスを確認するには、次のコマンドを入力します。

  show mobility summary

  以下に類似した情報が表示されます。

```
Mobility Keepalive interval..................... 10
Mobility Keepalive count........................ 3
Mobility Group members configured............... 3

Controllers configured in the mobility group
MAC Address        IP Address     Group Name     Status
00:0b:85:32:b1:80  10.10.1.1      local          Up
00:0b:85:33:a1:70  10.1.1.2       local          Data Path Down
00:0b:85:23:b2:30  10.20.1.2      local          Up
```

- モビリティの問題のトラブルシューティングを行うには、次のコマンドを入力します。
  - **debug mobility handoff** {**enable** | **disable**}：モビリティのハンドオフの問題をデバッグします。
  - **debug mobility keep-alive** {**enable** | **disable**} **all**：すべてのモビリティ アンカーの keepalive パケットをダンプします。
  - **debug mobility keep-alive** {**enable** | **disable**} *IP_address*：特定のモビリティ アンカーの keepalive パケットをダンプします。

WLAN モビリティ セキュリティの値の検証

WLAN モビリティ セキュリティの値について

すべてのアンカーまたはモビリティのイベントでは、各コントローラの WLAN セキュリティ ポリシーの値は一致する必要があります。これらの値はコントローラのデバッグで検証することができます。表 14-3 に、WLAN モビリティ セキュリティの値およびそれらに対応するセキュリティ ポリシーのリストを示します。

表 14-3　WLAN モビリティ セキュリティの値

セキュリティの 16 進数値	セキュリティ ポリシー
0x00000000	Security_None
0x00000001	Security_WEP
0x00000002	Security_802_1X
0x00000004	Security_IPSec*
0x00000008	Security_IPSec_Passthrough*
0x00000010	Security_Web
0x00000020	Security_PPTP*
0x00000040	Security_DHCP_Required
0x00000080	Security_WPA_NotUsed
0x00000100	Security_Cranite_Passthrough*
0x00000200	Security_Fortress_Passthrough*
0x00000400	Security_L2TP_IPSec*
0x00000800	Security_802_11i_NotUsed **（注）** ソフトウェア リリース 6.0 以降を実行しているコントローラは、このセキュリティ ポリシーをサポートしていません。
0x00001000	Security_Web_Passthrough

シンメトリック モビリティ トンネリングの使用

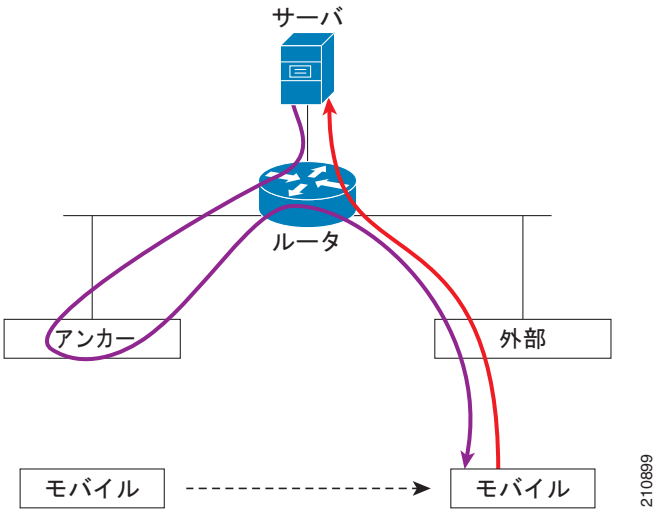
この項では、次のトピックを扱います。

- 「シンメトリック モビリティ トンネリングについて」（P.14-25）
- 「ガイドラインと制限事項」（P.14-27）

シンメトリック モビリティ トンネリングについて

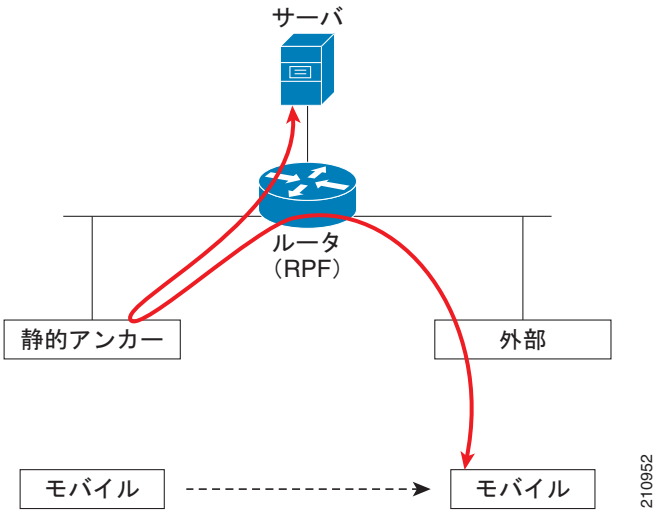
アシンメトリック トンネリングでは、図 14-13 に示すとおり、有線ネットワークへのクライアント トラフィックは外部コントローラから直接ルーティングされます。

図 14-13　アシンメトリック トンネリングまたは単一指向性トンネリング



アシンメトリック トンネリングは、上流のルータに Reverse Path Filtering（RPF; 逆方向パス転送）が有効に設定されている場合、切断されます。この場合、RPF チェックによって、ソース アドレスに戻るパスとパケットの着信先パスを一致させるため、クライアント トラフィックがルータでドロップされます。シンメトリック モビリティ トンネリングを有効に設定すると、図 14-14 に示すように、すべてのクライアント トラフィックがアンカー コントローラに送信され、RPF チェックを正常に通過します。

図 14-14　シンメトリック モビリティ トンネリングまたは双方向トンネリング



シンメトリック モビリティ トンネリングは、次の場合にも便利です。

- 送信元 IP アドレスがパケットの受信先サブネットと一致しないため、クライアント パケット パス内のファイアウォールでパケットがドロップされる場合。
- アンカー コントローラ上のアクセス ポイント グループ VLAN が、外部コントローラ上の WLAN インターフェイス VLAN とは異なる場合。この場合、モビリティ イベント中に、クライアント トラフィックが誤った VLAN に送信される可能性があります。

ガイドラインと制限事項

- コントローラ ソフトウェア リリース 4.1 ～ 5.1 は、アシンメトリック モビリティ トンネリングとシンメトリック モビリティ トンネリングの両方をサポートしています。コントローラ ソフトウェア リリース 5.2 以降のリリースは、シンメトリック モビリティ トンネリングのみをサポートしており、デフォルトでは常に有効です。
- 自動アンカー モビリティを使用中の場合、Cisco 2100 シリーズ コントローラは WLAN のアンカーとして指定できませんが、シンメトリック モビリティ トンネリングではアンカーとして指定して、外部コントローラからトンネリングされている上流のクライアント データ トラフィックを処理して転送できます。

シンメトリック モビリティ トンネリングの確認

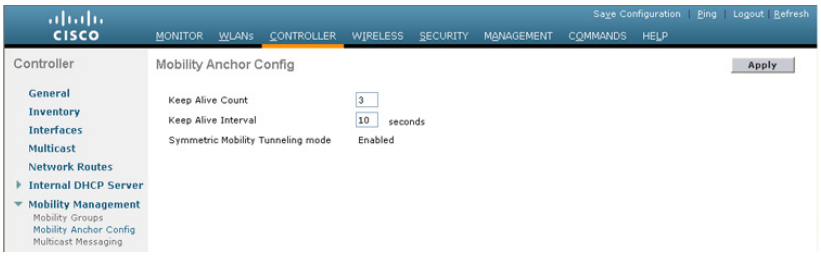
この項では、次のトピックを扱います。

- 「シンメトリック モビリティ トンネリングの確認（GUI）」（P.14-27）
- 「シンメトリック モビリティ トンネリングが有効な場合の確認（CLI）」（P.14-27）

シンメトリック モビリティ トンネリングの確認（GUI）

ステップ 1　[Controller] > [Mobility Management] > [Mobility Anchor Config] の順に選択して、[Mobility Anchor Config] ページを開きます。[Symmetric Mobility Tunneling Mode] テキスト ボックスに [Enabled] と表示されます。

図 14-15　[Mobility Anchor Config] ページ



シンメトリック モビリティ トンネリングが有効な場合の確認（CLI）

コントローラ CLI を使用して、シンメトリック モビリティ トンネリングが有効であることを検証するには、次のコマンドを入力します。

show mobility summary

以下に類似した情報が表示されます。

```
Symmetric Mobility Tunneling (current) .......... Enabled
Symmetric Mobility Tunneling (after reboot) ..... Enabled
Mobility Protocol Port........................... 16666
Mobility Security Mode........................... Disabled
Default Mobility Domain.......................... User1
Mobility Keepalive interval...................... 10
Mobility Keepalive count......................... 3
Mobility Group members configured................ 7

Controllers configured in the Mobility Group
MAC Address         IP Address    Group Name      Status
00:0b:85:32:b0:80    10.28.8.30       User1        Up
00:0b:85:47:f6:00    10.28.16.10      User1        Up
00:16:9d:ca:d8:e0    10.28.32.10      User1        Up
00:18:73:34:a9:60    10.28.24.10      <local>      Up
00:18:73:36:55:00    10.28.8.10       User1        Up
00:1a:a1:c1:7c:e0    10.28.32.30      User1        Up
00:d0:2b:fc:90:20   10.28.32.61     User1        Control and Data Path Down
```

モビリティ ping テストの実行

この項では、次のトピックを扱います。

モビリティ ping テストについて

1 つのモビリティ リスト内のコントローラは、well-known UDP ポート上で情報を制御し、Ethernet-over-IP（EoIP）トンネルを通じてデータ トラフィックを交換することにより、お互いに通信します。UDP と EoIP は信頼できる転送メカニズムではないため、モビリティ コントロール パケットまたはデータ パケットがモビリティ ピアに配信される保証はありません。ファイアウォールによる UDP ポートや EoIP パケットのフィルタリング、あるいはルーティングの問題のために、モビリティ パケットが転送中に消失する可能性があります。

ガイドラインと制限事項

コントローラ ソフトウェア リリース 4.0 以降のリリースを使用すると、モビリティ ping テストを実行することにより、モビリティ通信環境をテストできます。これらのテストを使用して、モビリティ グループ（ゲスト コントローラを含む）のメンバ間の接続を検証できます。次の 2 つの ping テストが利用できます。

- UDP でのモビリティ ping：このテストは、モビリティ UDP ポート 16666 上で実行されます。このテストでは、管理インターフェイスを介してモビリティ制御パケットが到達できるかどうかを確認します。
- EoIP でのモビリティ ping：このテストは EoIP 上で実行されます。管理インターフェイス上で、モビリティ データ トラフィックをテストします。

各コントローラにつき、実行できるモビリティ ping テストは 1 度に 1 回だけです。

（注）　これらの ping テストは、インターネット制御メッセージ プロトコル（ICMP）ベースではありません。「PING」という用語は、エコー要求とエコー応答メッセージを示すために使用されます。

（注）　ICMP パケットが 1280 バイトより大きい場合は、常に応答には 1280 バイトに切り詰められたパケットが使用されます。たとえば、ホストから管理インターフェイスに 1280 バイトを超えるパケットを使用して ping すると、常に 1280 バイトに切り詰められたパケットが使用されます。

モビリティ ping テストの実行（CLI）

- 2 つのコントローラ間でモビリティ UDP コントロール パケット通信をテストするには、次のコマンドを入力します。

  mping *mobility_peer_IP_address*

  mobility_peer_IP_address パラメータは、モビリティ リストに属するコントローラの IP アドレスにする必要があります。

- 2 つのコントローラ間でモビリティ EoIP データ パケット通信をテストするには、次のコマンドを入力します。

  eping *mobility_peer_IP_address*

  mobility_peer_IP_address パラメータは、モビリティ リストに属するコントローラの IP アドレスにする必要があります。

- モビリティ ping に対するコントローラのトラブルシューティングを行うには、次のコマンドを入力します。

  config logging buffered debugging

  show logging

  UDP でのモビリティ ping に対するコントローラのトラブルシューティングを行うには、次のコマンドを入力します。

  debug mobility handoff enable

  （注）　トラブルシューティングを行う際には、Ethereal トレース キャプチャを使用することをお勧めします。

スタティック IP アドレスを使用したクライアントのダイナミック アンカーの設定

この項では、次のトピックを扱います。

スタティック IP を使用したクライアントのダイナミック アンカーについて

ワイヤレス クライアントのスタティック IP アドレスを設定する場合があります。これらのワイヤレス クライアントをネットワーク内で移動するときは、他のコントローラへのアソシエートを試みることができました。クライアントがスタティック IP と同じサブネットをサポートしていないコントローラとのアソシエートを試みた場合、クライアントはネットワークへの接続に失敗します。今ではクライアントのダイナミック トンネリングをスタティック IP で有効にできるようになりました。

スタティック IP アドレスを使用したスタティック IP クライアントのダイナミック アンカーは、クライアントのサブネットが同じモビリティ グループ内の別のコントローラへのトラフィックをトンネリングすることによってサポートされている、他のコントローラにアソシエートすることができます。この機能により、クライアントがスタティック IP アドレスを使用していてもネットワークが処理されるように WLAN を設定できます。

スタティック IP クライアントのダイナミック アンカーの機能

スタティック IP アドレスを持つクライアントがコントローラへのアソシエートを試みると、次の一連の手順が行われます。

1. クライアントがコントローラ、たとえば WLC-1 にアソシエートすると、モビリティ アナウンスを行います。モビリティ グループ内のコントローラが応答した場合（たとえば WLC-2）、クライアント トラフィックがコントローラ WLC-2 にトンネリングされます。結果として、コントローラ WLC 1 が外部コントローラとなり、WLC-2 がアンカー コントローラとなります。
2. 応答するコントローラがない場合、クライアントはローカル クライアントとして扱われ、認証が実行されます。クライアントの IP アドレスは孤立したパケットの処理または ARP 要求の処理のいずれかによって更新されます。クライアントの IP サブネットがコントローラ（WLC-1）でサポートされていない場合、WLC-1 は別のスタティック IP モバイル アナウンスを送信し、クライアントのサブネットをサポートするコントローラ（たとえば WLC-3）がそのアナウンスに応答した場合、クライアントのトラフィックはそのコントローラ WLC-3 にトンネリングされます。結果として、コントローラ WLC 1 がエクスポート外部コントローラとなり、WLC-2 がエクスポート アンカー コントローラとなります。
3. 応答が受信されると、クライアント トラフィックはアンカーとコントローラ（WLC-1）との間でトンネリングされます。

（注） WLAN をインターフェイス グループで設定し、インターフェイス グループ内のいずれかのインターフェイスがスタティック IP クライアント サブネットをサポートしている場合、クライアントはそのインターフェイスに割り当てられます。この状況は、ローカルまたはリモート（スタティック IP アンカー）で発生します。

（注） セキュリティ レベル 2 認証は、ローカル（スタティック IP 外部）コントローラでのみ実行されます。これは、エクスポート外部コントローラとも呼ばれます。

ガイドラインと制限事項

- スタティック IP トンネリングの AAA を実行する際は、上書きされたインターフェイスを設定しないでください。これは、上書きされたインターフェイスがクライアントのサブネットをサポートしていない場合、トラフィックがクライアントに対して遮断される可能性があるためです。これは、上書きするインターフェイス グループがクライアントをサポートしている極端な場合に発生する可能性があります。
- ローカル コントローラは、このクライアント エントリが存在する正しい AAA サーバに設定する必要があります。

次の制限事項は、同じ WLAN でスタティック IP トンネリングに他の機能を設定する場合に適用されます。

- 自動アンカー モビリティ（ゲスト トンネリング）は同じ WLAN に設定できません。
- FlexConnect ローカル認証は同じ WLAN に設定できません。
- DHCP Required オプションは、同じ WLAN に設定できません。
- スタティック IP クライアントのダイナミック アンカーを FlexConnect ローカル スイッチングで設定できません。

スタティック IP クライアントのダイナミック アンカー（GUI）

ステップ 1　[WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2　IP クライアントのダイナミック アンカーを有効にする WLAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。

ステップ 3　[Advanced] タブを選択して、[WLANs > Edit]（[Advanced]）ページを開きます。

ステップ 4　[Static IP Tunneling] チェックボックスを選択し、スタティック IP クライアントのダイナミック アンカーを有効にします。

ステップ 5　[Apply] をクリックして、変更を確定します。

スタティック IP クライアントのダイナミック アンカーの設定（CLI）

config wlan static-ip tunneling {enable | disable} *wlan_id* : 指定した WLAN 上でスタティック IP クライアントのダイナミック アンカーを有効または無効にします。

スタティック IP を使用したクライアントのコントローラをモニタし、トラブルシューティングを行うには、次のコマンドを使用します。

- **show wlan** *wlan_id* : スタティック IP クライアント機能のステータスを表示できるようにします。

```
.............
Static IP client tunneling..... Enabled
.............
```

- **debug client** *client-mac*
- **debug dot11 mobile** enable
- **debug mobility handoff** enable

外部マッピングの設定

この項では、次のトピックを扱います。

外部マッピングについて

Auto-Anchor モビリティ（外部マッピングとも呼ばれます）により、異なる外部コントローラ上のユーザがサブネットまたはサブネットのグループから IP アドレスを取得するように設定できます。

外部コントローラ MAC マッピングの設定（GUI）

ステップ 1　[WLANs] タブを選択して、[WLANs] ページを選択します。

[WLANs] ページが表示され、使用可能な WLAN のリストが示されます。

ステップ 2　目的の WLAN の青いドロップダウン矢印をクリックして、[Foreign-Maps] を選択します。

外部マッピングのページが表示されます。このページには、モビリティ グループ内およびインターフェイス グループ内の外部コントローラの MAC アドレスもリスト表示されます。

ステップ 3　目的の外部コントローラ MAC、およびマッピングする必要があるインターフェイスまたはインターフェイス グループを選択し、[Add Mapping] をクリックします。

外部コントローラ MAC マッピングの設定（CLI）

config wlan mobility foreign-map add *wlan-id foreign_ctlr_mac interface/interface_grp name*

外部マッピングを設定するには、次のコマンドを使用します。

config wlan mobility foreign-map add *wlan_id interface*