CHAPTER 15

その他の設定作業

その他の設定作業

この章では、Cisco IOS Mobile Wireless Home Agent ソフトウェアの次の機能について、その概念と設定手順を詳しく説明します。

トンネル インターフェイスでの ACL のサポート

シスコのトンネル テンプレート機能を使用すると、作成済みのスタティック トンネルの ACL 設定を Home Agent（HA）で起動されたダイナミック トンネルに適用できます。トンネル テンプレートは、HA と PDSN/Foreign Agent（FA; 外部エージェント）の間のトンネルに定義され、適用されます。

Mobile IP トンネル テンプレート機能の設定

Mobile IP トンネル テンプレート機能をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface tunnel 10` `ip access-group 150`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 **tunnel** インターフェイスは仮想インターフェイスです。番号は、作成または設定を行うトンネル インターフェイスの番号です。作成するインターフェイスの数に制限はありません。
ステップ 2	`Router(config)# access-list 150 deny any 10.10.0.0 0.255.255.255` `access-list permit any any`	プロトコル タイプまたはベンダー コードによってフレームをフィルタリングするアクセス リスト メカニズムを設定します。
ステップ 3	`Router(config)# ip mobile home-agent template tunnel 10 address 10.0.0.1`	HA がテンプレート トンネルを使用するように設定します。

テンプレート トンネル機能を使用して一部のトラフィックをブロックする設定例を示します。

```
interface tunnel 10
ip access-group 150 in -------> apply access-list 150
access-list 150 deny any  10.10.0.0 0.255.255.255
access-list permit any any------> permit all but traffic to 10.10.0.0 network
ip mobile home-agent template tunnel 10 address 10.0.0.1
```

（注）　Mobile IP トンネル テンプレート機能をイネーブルにしていて、設定からトンネル インターフェイスを削除する場合は、対応する **mobileip tunnel template** コマンドも手動で削除する必要があります。必要な場合は、新しいトンネル インターフェイスを設定してから、**mobileip tunnel template** コマンドを再度設定できます。

制約事項

PMIP と Session Redundancy を使用して、タイムスタンプに msec オプションを選択し（**ip mobile foreign-service revocation timeout** 5 **retransmit** 4 **timestamp msec**）、PDSN SR セットアップで PMIP フローを開いた場合、**cdma redundancy** デバッグ出力で、アクティブとスタンバイの PDSN の「revocation timestamp」値が同じになります。

スイッチオーバーを実行すると、スタンバイ PDSN がアクティブとして動作を引き継ぎます。PMIP フローを閉じようとした場合、タイムスタンプが一致しないため、PDSN から HA に送信された失効メッセージは無視されます。そのため、数回の再試行後、PDSN は Ack 保留中の失効エントリを削除し、HA 上のバインディングは削除されません。

この制約は、アトリビュートの同期には関係ありませんが、ルータの動作時間に関係します。**msec** オプションは timestamp フィールドに動作時間を入力しますが、スタンバイ ルータの動作時間はそれより小さい値になると考えられるます。デフォルトの **seconds** ベースのオプション（timestamp に UTC で入力）を使用する場合は、このような問題は発生しないと考えられます。さらに、**msec** は 49+ days のラップ アラウンドにも問題があるので、always-on セットアップでは使用できません。

AAA アトリビュート MN-HA-SPI および MN-HA SHARED KEY のサポート

Cisco HA は、次の 3GPP2 標準アトリビュートをサポートしています。

MN-HA-SPI（26/57）

MN-HA-SHARED-KEY（26/58）

このサポートの手順は次のとおりです。

ステップ 1　HA が PDSN/FA から RRQ を受信します。

ステップ 2　HA が AAA に Access Request を送信します。HA は RRQ の MHAE SPI を MN-HA-SPI（26/57）アトリビュートとして Access Request に追加します。

ステップ 3　AAA サーバは MN-HA-SPI（26/57）を対応する MN-HA-SHARED-KEY（26/58）と照合します。

ステップ 4　AAA サーバは、その MN-HA-SHARED-KEY（26/58）を Access Reply に含めます。

ステップ 5　HA はダウンロードされた共有鍵 MN-HA-SHARED-KEY（26/58）を使用して RRQ の MHAE を認証します。

ユーザ プロファイル

HA は、各 NAI のプロファイルを維持します。このプロファイルには、次のパラメータが含まれています。

- ユーザ ID — NAI
- ユーザ ID — IP アドレス
- セキュリティ アソシエーション
- リバース トンネル ID このパラメータは、Mobile IP サービスによるユーザ データ転送に必要とされるリバース トンネリングのスタイルを指定します。
- 再送保護のタイムスタンプ ウィンドウ
- 要求されて与えられたすべての Registration Request フラグ（S|B|D|M|G|V フラグなど）の状態情報が維持されます。

  このプロファイルは、NAI で識別され、ローカルに設定することも、AAA サーバから取得することもできます。

さらに HA は、セッション確立レートを最適化し、セッション確立にかかる時間を最小にするインテリジェントなセキュリティ アソシエーション キャッシング メカニズムをサポートしています。

HA は最大 200000 のユーザ プロファイルのローカル設定をサポートしています。SAMI では、HA は 6 × 200000 のユーザ プロファイルをサポートします。ユーザ プロファイルは、NAI で識別され、ローカルに設定することも、AAA サーバから取得することもできます。

モビリティ バインディング アソシエーション

HA は、モビリティ バインディングを次の方法で識別します。

- スタティック IP アドレス割り当ての場合は、NAI + IP
- ダイナミック IP アドレス割り当ての場合は、NAI

- **show ip mobile binding** コマンドを使用すると、各ユーザのモビリティ バインディング情報が表示されます。

バインディング アソシエーションには、次の情報が含まれています。

- 気付アドレス
- ホーム アドレス
- アソシエーションのライフタイム
- Signalling identification フィールド

アップストリーム パスでの MS トラフィック リダイレクション

この機能を使用すると、モバイル ノードから受信したトラフィックをアップストリーム パスのネクストホップ アドレスにリダイレクトできます。モバイル ノード間のトラフィックは、HA の外部で送信され、外部デバイスからルーティングされて戻ってきます。この機能はレルム単位で設定できるので、各レルムに異なるネクストホップ アドレスを設定できます。したがって、この機能を使用できるのは NAI ベースのホストだけです。IP ベースのホストではリダイレクションはサポートされません。冗長構成の場合も、この機能を使用できます。

外部エージェント別アクセス タイプ サポート

この機能を使用すると、HA は外部エージェントの IP アドレスに基づいて外部エージェント別にサポートするアクセス タイプを認識できます。外部エージェントのアクセス タイプは、**3gpp2** または **WiMAX** ですが、両方を指定することはできません。指定されたアクセス タイプに応じて、その外部エージェント下にある全モバイル ノードに関して HA から AAA サーバに送信されるすべての認証およびアカウンティング レコードに、3gpp2 または WiMAX のアトリビュートが含まれます。ただし、両方のアトリビュートが含まれることはありません。HA は、Access-Accept を受信すると、指定されたアクセス タイプに基づいてアトリビュートを処理します。特定の外部エージェント アドレスにアクセス タイプが指定されていないと、その外部エージェント下のモバイル ノードすべてにデフォルトのアクセス タイプである **3gpp2** が使用されます。デフォルトのアクセス タイプを **3gpp2** から **WiMAX** に変更することもできます。

外部エージェント アクセス タイプ サポートの設定

外部エージェント アクセス タイプのサポートを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router# ip mobile home-agent foreign-agent { default |{ip-address mask} } access-type {3gpp2 | wimax}`	要求が通過してくる外部エージェントの IP アドレスに基づいて、登録者に **3gpp2** または **wimax** のアクセス タイプを選択します。

（注）　該当するアクセス タイプが RADIUS で設定されていない場合（認証では **radius vsa send authentication 3gpp2/wimax**、アカウンティングでは **radius vsa send accounting 3gpp2/wimax**）、この設定は考慮されません。

HA バインディングのアップデート

モバイル ノードの初回のパケット データ サービス登録時には、その PDSN で PPP セッションおよび関連づけられている Mobile IP フローが確立されます。PDSN 間のハンドオフが発生すると、ターゲット PDSN で別の PPP セッションが確立され、そのモバイル ノードは新しい PDSN/FS を使用して HA に登録します。PDSN 仮想テンプレートに PPP アイドル タイムアウトが設定されている場合は、そのモバイル ノードにアドバタイズされる最大 Mobile IP ライフタイムは、アイドル タイムアウトよりも 1 秒短くなります。

PDSN/Foreign Agent にアイドル状態または未使用の PPP セッションがあると、貴重なリソースが消費されます。Cisco PDSN/Foreign Agent と HA はこのようなアイドル状態の PPP セッションに Binding Update と Binding Acknowledge のメッセージをできる限り早く送信します。PDSN 間ハンドオフと Mobile IP 登録が発生すると、HA はそのモバイル ノードのモビリティ バインディング情報を新しい PDSN/FA の Care-of Address（CoA; 気付アドレス）でアップデートします。

同時バインディングがイネーブルになっていない場合、HA は Binding Update メッセージの形で、前の PDSN/FA に通知を送信します。前の PDSN/FA は Binding Acknowledge で確認応答し、必要に応じて、その Mobile IP セッションのビジター リスト エントリを削除します。前の PDSN/FA は、そのモバイル ステーションにアクティブ フローがなくなると、PPP セッションの解放を開始します。

（注）　HA が Binding Update メッセージをグローバルベースで送信するように設定することもできます。

（注）　この機能は、ボックスでバインド アップデートがイネーブルになっている Cisco FA で機能します。FA と HA の間のセキュリティ アソシエーションは、この機能がイネーブルに設定されている両方のボックスで設定される必要があります。

選択的なモバイル ブロッキング

前払いの割り当て分が終了した場合や、請求の支払いがないためサービスが無効になっている場合など、特定のモバイル ノードに対してアクセスをブロックしたい場合もあります。そのような場合は、AAA サーバのユーザ プロファイルに “mobileip:prohibited” cisco-avpair アトリビュートを追加します。mobileip:prohibited アトリビュートが Access Accept で HA に戻ってきた場合の動作は次のようになります。

- AAA サーバが Access Accept で mobileip:prohibited=1 を返した場合、およびそのモバイル ノードの MN-HA セキュリティ アソシエーションが AAA サーバ上に設定されていて、それが Access Accept で HA に戻った場合には、HA はその MN に、エラー コード 129（管理者による禁止）と登録要求（エラー）を送信します。
- AAA サーバが Access Accept で mobileip:prohibited=0 を返した場合、または Access Accept でアトリビュートが HA に戻らない場合、HA は登録要求の通常の処理を実行します。

（注）　mobileip:prohibited アトリビュートは 0 と 1 以外の値に設定することはできません。

MEID のサポート

Mobile Equipment Identifier（MEID; 移動体識別番号）は、IS-835D で導入された新しいアトリビュートで、最終的には ESN に置き換わると考えられます。MEID は、モバイル ステーション機器の物理部分を識別するためのグローバルに一意な 56 ビット識別番号です。暫定期間中は、HA で両方のアトリビュートをサポートする必要があります。

MEID NVSE は、PDSN ノードによって Mobile IP RRQ に付加されます。HA が MEID NVSE を受信し、**ip mobile cdma ha-chap send attribute A3** コマンドが設定されていると、その MEID 値が HA-CHAP アクセス要求に含まれます。

コール アドミッション制御（CAC）のサポート

現在、HA-SLB のロード バランシングの計算に使用されるのは、バインディングの数とメモリ利用量です。既存の Dynamic Feedback Protocol（DFP）重み計算式を変更して、各実サーバ（HA）上の CPS（1 秒当たりのコール）頻度とスループットのパラメータが考慮されるようにすることも可能です。

HA 上の CPS は毎分計算可能で、Usage CPS と呼ばれています。さらに、HA が処理可能な最大値（Available CPS）に設定することもできます。Usage CPS が Available CPS と同じ値であれば、HA 実サーバは SLB に軽い重みを返します。

ルータ上のスループットの計算は難しく、パケット処理のための CPU 割り込み使用率で解決されています。

上記の 2 つのパラメータによる式は、次のようになります。

```
dfp_weight = (Maxbindings - NumberofBindings)*(cpu+mem)*
(Available cps - Usage cps) *dftp_max_weight / (Maxbindings*32*Available cps)
```

最大バインディングのサポート

最大バインディングをサポートするために使用できる機能は次のとおりです。

- 許可バインディングの最大数を指定するコマンド
- バインディング数が最大数に到達した場合の NM への SNMP アラートの発行

バインディングの最大数を設定すると、バインディングの数が指定値に制限されます。システムは、バインディングの最大数を受け入れると、その後は着信登録要求をすべて拒否し、NM に SNMP アラートを発行します。バインディングの数がしきい値を下回ると、アラートはクリアされます。

SNMP トラップをクリアする下限しきい値は、最大バインディング値の 90% です。バインディングの数が最大バインディング数の 90% に減少すると、HA は SNMP トラップをクリアします。

トラップ アクティビティが溢れないようにするには、トラップを調整する必要があります。HA は、バインディング数が最大バインディングを超えると通知を送信しますが、トラップを確実に調整するため、いったんバインディング数がしきい値を下回り、その後また最大バインディングに達するまではアラートを再生成しません。

最大バインディングのサポートを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent max-binding` *max-binding-value*	HA で許可される最大 dfp 重み値をイネーブルにします。デフォルトの最大 dfp 重み値は 24 です。

この機能はデフォルトではディセーブルに設定され、HA に設定できるバインディングの最大数はプラットフォームよって異なります。

HA での CAC の設定

HA で許可される最大バインディング数を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent max-binding` *max-binding-value*	HA で許可される最大 dfp 重み値をイネーブルにします。デフォルトの最大 dfp 重み値は 24 です。
ステップ 2	`Router(config)# ip mobile home-agent max-cps` *max-cps-value*	HA で許可される最大 cps をイネーブルにします。アカウンティングをサポートする場合のデフォルトの最大 cps 値は 160 cps です。

MIP/LAC（PPP 再生成）のサポート

この機能を使用すると、HA は設定に基づいて VPDN トンネル 内の PPP セッションに MIP コールをマッピングできます。

多くの場合、企業ネットワークや LNS（L2TP ネットワーク サービス）には、すでにインターネットやインターネット サービス プロバイダーへの Virtual Private Dialup Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）接続があり、着信ダイヤルアップ接続を処理しています。これらの接続方法では、公衆ネットワークを介したセキュリティが確保されています。これらの VPDN 接続のほとんどは、L2TP トンネルを通じて着信し、L2TP トンネル内で PPP を使用して着信パケットをカプセル化しています。

HA 技術を使用すると、MN（モバイル ノード）から発信され FA に接続されるユーザ データ トラフィックを、HA を通じて会社のネットワークに配信できます。さらに、HA は、従来のダイアルアップ方法で LNS にデータ トラフィックを配信することもできます。

MN は、通常の MIP トンネルを使用して、FA を通じて HA に接続されます。イネーブルに設定されていると、HA は企業 LNS への L2TP トンネルをセットアップし、L2TP トンネル内で MIP セッションを PPP セッションにマッピングできます。その後 MN は使用可能なインフラストラクチャを使用して、企業ネットワークに戻って接続されます。

（注）　企業 LNS へのデータ トラフィックを伝送する HA の機能は、MIP-LAC 機能と呼ばれています。この機能によって、HA は MIP セッションを終了し、さらに L2TP トンネル内で MIP セッション用の新しい PPP セッションを再生成します。

MIP セッションに対して、MIP-LAC 機能がイネーブルに設定されている場合、MN が RRQ を送信してから RRP 応答を受信するまでの一連のイベントのコール フローは次のようになります。

（注）　次に示すのは、最も一般的なシナリオ（AAA から VPDN パラメータを取得する場合）のコール フローであり、可能なすべてのシナリオを網羅しているわけではありません。

発生するイベントは次のとおりです。

1. MN が FA から、FA-CHAP チャレンジとともに Mobile IP アドバタイズメントを受信します。
2. MN は FA に、FA-CHAP エクステンションとともに RRQ を送信します。
3. FA はその MN を認証するために Access-Request を Visiting AAA（VAAA）に送信します。VAAA は MN の認証のためにさらに Home AAA（H/SP AAA）と接触する場合もあります。

4. FA は、AAA サーバから Access-Accept を受信すると、HA に RRQ（MN から最初に送信されたもの）を転送します。
5. HA は HAAA サーバの支援を受けて このメッセージを認証します。HA は AAA に Access-Request を送信し、AAA から Access-Accept を受信します。
6. HA は Access-Accept メッセージで受信したアトリビュートをスキャンします。メッセージ内で VPDN トンネル セットアップ パラメータが特定されれば、HA は LNS への VPDN トンネルを開始します。
7. L2TP トンネル セットアップの一部として、PPP の LCP および IPCP フェーズ中にトンネル パラメータのネゴシエーションが行われます。
8. L2TP トンネル セットアップの完了後、FA を通じて MN に RRP が送信されます。

HA と LNS の間の L2TP トンネルのセットアップ後、HA はエージェントとして機能し、L2TP トンネルとの間で Mobile IP データ トラフィックの送受信を行います。

ユーザの MIP-LAC がイネーブルになっていて、HA が認証 / 認可用の AAA に到達できない場合は、ローカル設定で VPDN パラメータが確認されます。

MIP LAC の設定

VPDN 設定をローカルにイネーブルにする手順は次のとおりです。

	コマンド	目的

ステップ 1	`Router(config)#ip mobile host nai @xyz.com address pool ?`
	`  dhcp-pool  Use local DHCP pools`
	`  dhcp-proxy-client  Use DHCP proxy client feature`
	`  local  Use local address pool`
	`  vpdn-tunnel  Use VPDN tunnel feature`
	
	`Router(config)#ip mobile host nai @xyz.com address pool vpdn-tunnel ?`
	`  interface  Home link is on this interface`
	`  virtual-network  Home link is on this virtual network`
		アドレス プール タイプを **vpdn-tunnel**（新規オプション）に指定します。
		
		既存の **ip mobile host** コマンドに、新たに **vpdn-tunnel** オプションが追加されました。これを使用すると、MIP LAC 機能を使用して LNS から Mobile IP クライアントを取得する必要があることを指示できます。

ステップ 2	`router# ip mobile realm` *`@xyz.com`* `vrf` *`vrf-name`* `ha-addr` *`ip-address`* `[aaa-group [accounting` *`aaa-acct-group`* `| authentication` *`aaa-auth-group`*`]] [dns dynamic-update method` *`word`*`] [dns server` *`primary dns server address secondary dns server address`* `[assign]] [hotline] | [`**`vpdn-tunnel`**`virtual-template` *`number`* `[setup-time` *`number`*`]]`	ユーザに対して MIP-LAC 機能をイネーブルにします。

既存の **ip mobile realm** コマンドに、特定ユーザの MIP-LAC 機能をイネーブルにする新規オプション **vpdn-tunnel virtual-template** *number* が追加されています。**vpdn-tunnel** 設定の **setup-time** は省略してもかまいません。**setup-time** の値の範囲は、5 ～ 300 秒です。setup-time のデフォルト値は 60 秒です。**setup-time** オプションを明示的に指定しない場合は、デフォルト値が使用されます。

setup-time の設定値は、PPP IDB 作成時を起点とした最大許容時間です。この時間内に、再生成された PPP セッションが完全に起動される必要があります。この期間が経過しても L2TP トンネルが起動していない場合、Mobile IP モジュールはこのセッションの L2TP セッション（PPP IDB とモバイル ノードのバインディング）を破棄します。また、**tunnel vtemplate** *number* の *number* オプションは、対応する **interface virtual-template** コマンドで設定される数値と一致していなければなりません。この点にも注意してください。

ステップ 3

```
Router(config)# interface virtual-template
number
Router(config-if)# ip address negotiated
Router(config-if)# no peer neighbor-route
Router(config-if)# encapsulation ppp
```

HA に PPP 仮想テンプレート インターフェイスを設定します。

（注）　**interface virtual-template** *number* は、対応する **vpdn-tunnel vtemplate** コマンドで設定される数値と一致していなければなりません。

また、**virtual-template** に、**ip address negotiated** と **no peer neighbor-route** を設定することも必要です。Cisco IOS ソフトウェアはデフォルトで自動的に近接ルートを生成するので、PPP IPCP ネゴシエーション完了時にポイントツーポイント インターフェイス（LNS サーバに接続する HA インターフェイス）上のピア アドレスへのルートを自動的に確立します。このデフォルトの動作をディセーブルにするには、**no peer neighbor-route** コマンドを使用します。このインターフェイスには、認証方式は設定しません。認証方式を設定すると、HA/LAC が LNS を認証しますが、これは必要ありません。LNS は HA/LAC を認証しますが、HA/LAC は LNS の認証は行いません。

ステップ 4

```
aaa new-model
aaa authentication ppp default local
!
username lac password 7 192840824D76
username lns password 7 320985235A35
```

ローカルに設定された LAC に AAA パラメータを追加します。

これらのコマンドは、トンネル認証を完了するためにローカル設定を使用するように HA に指示します。

ステップ 5

```
vpdn enable
vpdn search-order domain
```

VPDN と VPDN 検索順序をイネーブルにします。

HA の VPDN 機能をイネーブルにするには、これらのコマンドを設定する必要があります。**vpdn search-order domain** コマンドは、ドメイン照合に基づいた VPDN 設定の検索方法を HA に伝えます。このコマンドを使用すると、HA は接続している MN の **domain** を検索され、VPDN グループ内で一致するものを探します。

ステップ 6

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain xyz.com
 initiate-to ip 1.1.1.1
 local name lac
```

新しいグループを作成し、必要な VPDN パラメータをそのグループに関連付けることによって、VPDN トンネル認証のアトリビュートをローカルに設定します。

vpdn-group に設定されている **domain** は、**ip mobile realm** に設定されている **realm** から @ 文字を除いた値と一致する必要があります。VPDN パラーメータが設定され、その値がトンネルのセットアップに不十分であると、その設定は無効とみなされ、トンネルは廃棄されます。

ステップ 7

```
vpdn-group 1
 request-dialin
  protocol l2tp
  domain xyz.com
 initiate-to ip 1.1.1.1
 initiate-to ip 2.2.2.2
 initiate-to ip 3.3.3.3
 local name lac
```

ローカル設定に基づく LNS ロード バランシングを設定します。

VPDN グループ コンフィギュレーション モードで **initiate-to ip** コマンドの複数のインスタンスを設定すると、ローカルのセッション ロード バランシング機能が設定されます。

ステップ 8

```
ip vrf moip-vrf-comp4
 rd 100:4
!
ip mobile realm @xyz.com vrf
moip-vrf-comp4 ha-addr 13.1.1.119
```

ローカル設定に基づく VRF を設定します。

HA に VRF が設定されていて、特定の MIP-LAC トンネルを HA の特定の VRF インスタンス用にするには、HA にこれらのコマンドを設定する必要があります。

ユーザに対して MIP-LAC がイネーブルに設定されていて、AAA から Access-Accept メッセージで VPDN パラメータが受信された場合、AAA からダウンロードされた VPDN 設定が使用されます。AAA からダウンロードされた VPDN パラメータには、常に高い優先順位が与えられます。ダウンロードされた VPDN パラーメータが、トンネルのセットアップに不十分である場合、その設定は無効とみなされ、トンネルは廃棄されます。

ステップ 9	`radius host 6.6.6.6 auth-port 1645 acct-port 1646` `radius-server key cisco`	VPDN アトリビュートをダウンロードするように RADIUS サーバを設定します。

VPDN パラメータの **domain** は、**ip mobile realm** に設定されている **realm** から @ 文字を除いた値と一致する必要があります。設定された VPDN パラーメータが、トンネルのセットアップに不十分である場合、その設定は無効とみなされ、トンネルは廃棄されます。

AAA サーバ設定に基づく LNS のロード バランシング

2 つ以上の LNS の間でラウンドロビン方式のロード シェアリングが実行されるように LAC を設定できます。これを実行するために必要なのは、宛先 LNS に複数の IP アドレス（または DNS ホスト名）をカンマ区切り方式で定義することだけです。たとえば、上記の例を、2 つの LNS をサポートするように変更すると、次のようになります。

```
Cisco-avpair = "vpdn:ip-addresses=1.1.1.1, 2.2.2.2, 3.3.3.3"
```

この LNS ロード バランシング機能は、IOS に組み込まれています。MIP-LAC トンネル確立中に、AAA サーバが複数の LNS アドレスを返した場合、現在 IOS に実装されているラウンドロビン アルゴリズムに基づいて LNS アドレスが選択されます。

LNS の設定

（注）　HA/LAC からのダイヤルイン接続を受け入れる LNS の設定例を示します。ただし、このマニュアルでは、設定例についての細かい説明は省略します。

```
version 12.0
service timestamps debug datetime msec
service timestamps log uptime
service password-encryption
hostname lns
aaa new-model
aaa authentication login default local
aaa authentication ppp default local
aaa authentication ppp vpdn radius
aaa authorization network default radius
aaa accounting network default start-stop radius
!
username lac password 7 104D000A0618
username lns password 7 060506324F41
!
vpdn enable
!
vpdn-group 1
 accept dialin
 protocol l2tp
 virtual-template 1
 local name lns
 l2tp tunnel password 7 02347324D3
 source-ip 4.4.4.4
!
async-bootp dns-server 1.1.1.1 2.2.2.2
async-bootp nbns-server 8.8.8.8 9.9.9.9
!
!
interface FastEthernet0/0
ip address 172.22.66.25 255.255.255.192
no ip directed-broadcast
no ip mroute-cache
interface Virtual-Template1
ip unnumbered FastEthernet0/0
no ip directed-broadcast
peer default ip address pool default
ppp authentication chap vpdn
ppp multilink
!
ip local pool default 10.1.1.1 10.1.1.16
...
!
radius-server host 172.22.66.16 auth-port 1645 acct-port 1646
radius-server key cisco
end
```

AAA の設定

「cisco.com」ドメインの対応する RADIUS サーバ上のユーザ ファイルに、次の設定を含める必要があります。

```
Password = "cisco",
Service-Type = Outbound-User,
Cisco-avpair = "vpdn:tunnel-id=nas",
Cisco-avpair = "vpdn:tunnel-type=l2tp",
Cisco-avpair = "vpdn:ip-addresses=1.1.1.1",
Cisco-avpair = "vpdn:l2tp-tunnel-password=lab"
Cisco-avpair = "outbound:send-auth=2"
Cisco-avpair = "outbound:send-name=dgudimet"
Cisco-avpair = "outbound:send-secret=password"
Cisco-avpair = "mobileip-vrf-ha-addr=13.1.1.121"
Cisco-avpair = "ip:ip-vrf#0=moip-vrf-comp4"
```

これらのパラメータは、AAA サーバからの Access-Accept メッセージの一部として HA/LAC にダウンロードされます。

AAA サーバの設定に基づく VRF の設定

HA に VRF が設定されていて、特定の MIP-LAC トンネルを HA の特定の VRF インスタンス用にするには、次のコマンドを設定する必要があります。

```
ip vrf moip-vrf-comp4
 rd 100:4
```

さらに、ドメインが *cisco.com* の対応 RADIUS サーバ上のユーザ ファイルに、次の設定を含める必要があります。

```
Cisco-avpair = "mobileip-vrf-ha-addr=13.1.1.121"
Cisco-avpair = "ip:ip-vrf#0=moip-vrf-comp4"
```

設定の確認

MIP LAC の設定を確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	`router# show ip mobile binding`	特定の IP モバイル セッション用に MIP-LAC セッションが確立された場合、L2TP トンネルについての追加情報を表示します。**setup-time** は L2TP セッション確立の最大セットアップ時間です。 このコマンドでは、アクティブな L2TP/PPP 再生成セッションの数も表示されます。セッションの合計数には、MIP-LAC セッション（VPDN トンネルが確立されたもの）の合計数が含まれます。
ステップ 2	`router# ip mobile binding summary`	アクティブな L2TP/PPP 再生成セッションの合計数を表示します。セッションの合計数には、MIP-LAC セッション（VPDN トンネルが確立されたもの）の合計数が含まれます。
ステップ 3	`router# show ip mobile traffic`	MIP-LAC 関連の追加カウンタを表示します。

例を示します。

```
Router# show ip mobile binding
Mobility Binding List:
Total 15000
Total VPDN Tunneled 20
MIP-USER12573@ispxyz.com (Bindings 1):
    Home Addr 193.1.1.28
    Care-of Addr 7.0.0.85, Src Addr 7.0.0.85
    Lifetime granted INFINITE
    Flags sbdmg-T-, Identification C9ED9187.10000
    Tunnel3 src 73.0.0.42 dest 7.0.0.85 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Service Options:
        Dynamic HA assignment
    VPDN Tunnel (setup-time 30)
    Acct-Session-Id: 1677265
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
```

ip mobile binding summary コマンドの例を示します。

```
ha#show ip mobile binding summary
Mobility Binding List:
Total 15000
Total VPDN Tunneled 20
```

show ip mobile traffic コマンドの例を示します。

```
HA#show ip mobile traffic
IP Mobility traffic:
Time since last cleared: 00:05:59
UDP:
    Port: 434 (Mobile IP) input drops: 0
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register requests rcvd 2, denied 1, ignored 0, dropped 0, replied 2
    Register requests accepted 1, No simultaneous bindings 0
    Register requests rcvd initial 2, re-register 0, de-register 0
    Register requests accepted initial 1, re-register 0, de-register 0
    Register requests replied 2, de-register 0
    Register requests denied initial 1, re-register 0, de-register 0
    Register requests ignored initial 0, re-register 0, de-register 0
    Registration Request Errors:
      Unspecified 0, Unknown HA 0, NAI check failures 0
      Administrative prohibited 0, No resource 0
      Authentication failed MN 0, FA 0, active HA 0
      Bad identification 1, Bad request form 0
      Unavailable encap 0, reverse tunnel 0
      Reverse tunnel mandatory 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by MN to HA 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by FA to HA 0
    Binding Updates received 0, sent 1 total 1 fail 0
    Binding Update acks received 1 sent 0
    Binding info requests received 0, sent 0 total 0 fail 0
    Binding info reply received 0 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 0
    Binding Delete Req received 0, sent 0 total 0 fail 0
    Binding Delete acks received 0 sent 0
    Binding Sync Req received 0, sent 0 total 0 fail 0
    Binding Sync acks received 0 sent 0
    Gratuitous 3, Proxy 0 ARPs sent
    Route Optimization Binding Updates sent 0, acks received 0 neg acks received 0
    Registration Revocation msg sent 0 rcvd 0 ignored 0
    Registration Revocation acks sent 0 rcvd 0 ignored 0
    Total incoming registration requests using NAT detect 0
    Total VPDN Tunnel sessions attempted: 1 success: 1 fail: 0 pending: 0
                                PPP IDBs: 1 no resource: 0 deleted: 0
Foreign Agent Registrations:
    Register requests rcvd 0, valid 0, forwarded 0, denied 0, ignored 0
    Register requests valid initial 0, re-register 0, de-register 0
    Register requests forwarded initial 0, re-register 0, de-register 0
    Register requests denied initial 0, re-register 0, de-register 0
    Register requests ignored initial 0, re-register 0,  de-register 0
    Register replies rcvd 0, forwarded 0, bad 0, ignored 0
    Register replies rcvd initial 0, re-register 0, de-register 0
    Register replies forwarded initial 0, re-register 0, de-register 0
    Registration Errors:
      Unspecified 0, HA unreachable 0
      Administrative prohibited 0, No resource 0
      Bad lifetime 0, Bad request form 0
      Unavailable encapsulation 0
      Unavailable reverse tunnel 0, Reverse tunnel mandatory 0
      Authentication failed MN 0, HA 0
      Received challenge/gen. authentication extension, feature not enabled 0
      Unknown challenge 0, Missing challenge 0, Stale challenge 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by MN to FA 0
      Unrecognized VendorID or CVSE-Type in CVSE sent by HA to FA 0
    Route Optimization Binding Updates received 0, acks sent 0 neg acks sent 0
    Registration Revocation msg sent 0 rcvd 0 ignored 0
    Registration Revocation acks sent 0 rcvd 0 ignored 0
```

新しい MIP-LAC 機能に関連して追加されたカウンタは次のとおりです。

```
Total VPDN Tunnel sessions attempted: 34 success: 33 fail: 1 pending: 0
                           PPP IDBs: 34 no resource: 6 deleted: 34
```

これらの新しいカウンタについて説明します。

- **attempted —** Mobile IP 登録要求の照合によって試行された MIP-LAC セッションの総数
- **success —** 全試行のうち、成功した MIP-LAC セッションの総数
- **fail —** 全試行のうち、失敗した MIP-LAC セッションの総数
- **pending —** 全試行のうち、保留状態（in-progress 状態）の MIP-LAC セッションの総数
- **PPP IDBs —** MIP-LAC セッションを起動するために作成された PPP IDB の総数
- **No resource —** リソース不足（IP アドレスやメモリを使用できない場合など）で完了できなかったセッションの総数
- **Deleted —** セッションの正常な確立後に停止された（管理者が手動で停止、またはエラーによる停止）セッションの総数

制約事項

この機能にはソフトウェア設定上の制約事項があります。次の点に留意してください。

- HA が LNS に接続するインターフェイスに VRF を設定した場合、MIP-LAC 機能は正常に機能しません。

Framed-Pool 基準

Framed-Pool は、指定アドレス プールの名前を含む AAA アトリビュートで、HA 上のユーザへのアドレス割り当てに使用されます。HA3.1 では、Cisco VSA でこの機能がサポートされています。

HAAA は、ダイナミック / スタティック アドレスの割り当てに使用できるように、これらのアトリビュートを Access-Accept メッセージで HA に送信します。HA が、Access-Accept で両方のアトリビュートを受信した場合、HA が受け入れることができるのは、HA に事前設定されている方のアトリビュートです。

Framed-Pool 基準機能を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`router# ip mobile home-agent aaa attribute framed-Pool`	HA による Framed-Pool アトリビュートの使用をイネーブルにします。RADIUS サーバからの Access-Accept の一部にローカル プール名が含まれます。

例を示します。

```
ip mobile home-agent aaa attribute Framed-Pool
ip local pool haPool 70.1.1.1 70.1.1.254
ip mobile home-agent
ip mobile virtual-network 70.1.1.0 255.255.255.0
ip mobile host nai @cisco.com interface FastEthernet1/0 aaa load-sa
```

ローカル プールのプライオリティ メトリック

モバイル クライアントに IP アドレスを割り当てるために、HA は IP アドレス範囲で指定されたローカル プールを使用します。HA は、登録要求を受信すると必ず、MN の認証を行い、IP アドレスを割り当てるためのプール名を取得します。HA は、ローカル設定からプール名を取得するか、あるいは Cisco VSA または Framed-Pool アトリビュートを通じて RADIUS サーバからプール名を取得します。

IP ローカル プールの設定時に、複数のグループを指定し、各グループ内に複数のプールを入れ、各プール内には複数の IP アドレス範囲を含めることができます。ただし、1 つのグループ内では IP アドレス範囲を重複させることはできません。1 つのグループ内では、すべてのアドレスが重複しないようにする必要があります。

デフォルトでは、IP アドレス要求には、プール名（必須）、スタティック IP アドレス（任意）、関連付けられているユーザ名（任意）が含まれます。最初はすべての IP アドレスがフリー プールに入り、各アドレスはそこから割り当てられます。IP アドレスの指定時には必ず、IP アドレスを特定のユーザ名に関連づける必要があります。

アドレスにプライオリティを追加し、新規要求の場合、プールから望ましい IP アドレス範囲を選択することもできます。すべての登録者が新しいアドレッシング スキームに移行すると、以前のアドレッシング スキーム（プライオリティの低い範囲）はシステムから削除されます。

一般的に、IP アドレスが予約されると、その IP アドレスはそのユーザに関連付けられます（userid によって）。そのユーザの接続が切断され、再接続された場合、同じアドレスが使用されていなければ、そのユーザに同じアドレスが与えられます。このようなユーザと IP アドレスの関連付けは、プール設定とキャッシュ制限によって制御されます。したがって、アドレッシング スキームのプライオリティを変更したり、高プライオリティのアドレッシング スキームがフリー アドレスで使用可能であったりすると、HA は以前予約された IP アドレスではなく、新しいアドレッシング スキームから新しい IP アドレスを割り当てます。プライオリティに変更がなければ、HA は以前の IP アドレスを割り当てようとします。

Network Manager からアクセスし、SNMP MIBS を通じてプライオリティ値を設定し、取得することも可能です。“cIpLocalPoolConfigEntry” テーブルにプライオリティ用の新しい MIB オブめくとが追加され、プライオリティ値にアクセスできます。新しい MIB オブジェクトを使用すると、既存のローカル プールのプライオリティを変更できます。

ローカル プールのプライオリティ メトリックの設定

ローカル プール機能のプライオリティ メトリックを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	router# Router(config)#**ip local pool {default** | *poolname*} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**priority** *1-255*] [**theshold** *low-threshold high-threshold*]	リモート ピアがポインツーポイント インターフェイスに接続した場合に使用される IP アドレスのローカル プールを設定します。このプールの利用率が上限または下限のしきい値（パーセンテージ）に達すると、トラップが生成されます。 新しいオプション、**priority** *1-255* を使用すると、新たに作成されたプールにプライオリティを指定し、そのプライオリティを IP アドレスの割り当てに使用できます。
ステップ 2	Router(config)#**no ip local pool** vsa-pool 1.0.0.201 priority 180	プールの設定を解除します。

例を示します。

この例では、HA は、プライオリティがデフォルト値の 1（最も低いプライオリティ）であるローカル プールを作成します。

```
R1(config)#ip local pool ha-pool 10.0.0.1 10.0.0.255
```

次の例では、HA はプライオリティ値が 100 のローカル プールを作成します。

```
R1(config)#ip local pool ha-pool 10.0.0.1 10.0.0.255 priority 100
```

設定の確認

設定の確認手順は次のとおりです。

	コマンド	目的
ステップ 1	`Router#show running-config | include pool`	ローカル プールの設定を表示します。プライオリティ値が表示されるのは、プライオリティ値が 1（デフォルトで設定される最低値）でない場合だけです。

例を示します。

```
Router# show running-config | include pool
ip local pool frmd-pool 1.0.0.191 priority 20
ip local pool vsa-pool 1.0.0.201 priority 180
ip local pool vsa-pool 1.0.0.211 1.0.0.219
ip local pool vsa-pool 1.0.0.202 1.0.0.209 priority 100


router# show ip local pool

 Pool          Begin         End           Free  In use  Priority
 frmd-pool     1.0.0.191     1.0.0.191        1       0        20
 vsa-pool      1.0.0.201     1.0.0.201        1       0       180
               1.0.0.211     1.0.0.219        9       0         1
               1.0.0.202     1.0.0.209        8       0       100
```

Mobile IPv4 ホスト設定エクステンション（RFC4332）

ここでは、IOS に実装されている、Mobile IP ホスト設定エクステンションについて説明します。

IP デバイスが通信できるようにするには、基本的なホスト設定が必要です。たとえば、通常は IP アドレスと DNS サーバのアドレスが必要となります。この情報はスタティックに設定されるか、あるいは DHCP または PPP/IPCP を使用してダイナミックに取得されます。ただし、DHCP と PPP/IPCP は両方ともアクセス ネットワークに基づいてホスト設定を提供します。Mobile IPv4 では、アクセス ネットワーク（外部ネットワークとも言います）のモバイル ノードは登録プロセスによって起動されます。ホストの設定に使用される情報はホーム ネットワークに基づいたものでなければなりません。外部ネットワークのモバイル ノードは、ネットワーク インターフェイスの起動時に、IP アドレス、ホーム サブネット プレフィクス、デフォルト ゲートウェイ、ホーム ネットワークの DNS サーバを取得する必要があります。

モバイル ノードがホストの設定を取得する必要がある場合、Host Configuration Request VSE が Registration Request に付加されます。この VSE は、すべてのまたは選択されたホスト設定 VSE を Registration Reply に付加する必要があることを HA に指示します。HA が プロキシ DHCP モードで DHCP サーバから情報を取得すると、DHCP クライアント ID と DHCP サーバ エクステンションが Registration Reply に付加されます。これらの DHCP 関連のエクステンションには、HA と DHCP サーバの間で交換された DHCP メッセージで使用された値が保存されます。VSE は、Mobile IP に定義されているいずれかの認証メカニズムを使用して、登録メッセージの一部として認証されます。

次に示すシスコのベンダー固有エクステンションは、モバイル ノードにホスト設定を提供します。Host Configuration Request エクステンションが許可されるのは、Registration Request 内だけです。

そのほかのエクステンションは Registration Reply に付加されます。

- Host Configuration Request：モバイル ノードから HA へのホスト設定情報の要求
- Home Network Prefix Length：ホーム ネットワーク上のサブネット プレフィクスの長さ
- Default Gateway：ホーム ネットワーク上のデフォルト ゲートウェイの IP アドレス
- DNS Server：ホーム ネットワーク内の DNS サーバの IP アドレス
- DNS Suffix：ホーム ネットワーク内のホスト名解決用の DNS サフィクス
- DHCP Client ID：IP アドレスの取得に使用される DHCP クライアント ID。モバイル ノードがホームに戻り、それ自身のアドレスの管理を実行する場合、この情報は Client identifier オプションにマッピングされます。
- DHCP Server：ホーム ネットワーク内の DHCP サーバの IP アドレス
- Configuration URL：サーバから設定パラメータをダウンロードするモバイル ノードの URL

WiMAX AAA アトリビュート

Cisco Home Agent Release 4.0 には、AAA Authorization and Accounting アトリビュートが追加されています。ここでは、アトリビュートの概要と、特定のアトリビュートのサポートに関する情報を説明します。

WiMAX 用の HA-AAA Authorization アトリビュートのサポート

WiMAX のサポートを拡張するために、次の HA-AAA アトリビュートが追加されます。

- Framed IP Address : Framed IP Address : **ip mobile home-agent send-mn-address** コマンドが設定されている場合、Mobile IP RRQ で受信されたホーム アドレスは Access-Request メッセージの Framed-IP-Address アトリビュートの値として送信されます。
- WiMAX Capability : このアトリビュートが HAAA に送信される Access-Request メッセージ内にある場合、受信された Access-Accept メッセージにもこのアトリビュートが含まれている可能性があります。HA が受信する Access-Accept メッセージ内にある場合、このアトリビュートに含まれるのは Accounting Capabilities sub-TLV だけです。これは、そのセッションに対してサーバが選択したアカウンティング機能を示します。Access-Accept で HAAA が返したアカウンティング機能は Access-Request で HA が指定した値と一致すると予想されます。HA は現在のところ、Access-Request で受信した WiMAX Capability VSA をまったく処理せず、アカウンティング機能が一致しているかどうかの確認を実行しません。
- HA-IP-MIP4：HA からのすべての Access-Request メッセージに含まれます。既存のバインディングでは（つまり再登録および削除に対応する Access-Request）、値はそのバインディングの HA アドレスに設定されます。新しいバインディングの Access-Requests では、このアトリビュートの値は、**ip mobile home-agent address** または **ip mobile home agent redundancy** コマンドを使用して設定された HA IP アドレスになります。
- RRQ-HA-IP：HA がこのアトリビュートを Access-Request メッセージに含めるのは、Mobile IP RRQ の HA フィールド内の IP アドレスが HA の IP アドレスとは異なる場合だけです。その場合、値は Mobile IP RRQ 内の HA IP アドレスに設定されます。
- MN-HA-MIP4-KEY：このアトリビュートは、MIP4 手順に使用される MN-HA キーを識別します。このアトリビュートは Access-Accept メッセージに含まれ、MN-HA-SHARED-KEY に類似しています。HA は、WiMAX 登録者用の MN-HA MIP4 キーに基づいて、MN-HA Authentication エクステンションを計算します。
- MN-HA-MIP4-SPI：このアトリビュートは、MIP4 手順に使用される MN-HA SPI キーを識別します。このアトリビュートは Access-Request メッセージに含まれ、MN-HA-SPI と類似しています。

表 15-1 に、HA の WiMAX AAA Authorization アトリビュートを示します。

表 15-1　WiMAX AAA Authorization アトリビュート

アトリビュート名	タイプ	説明	Access Request	Access Chall.	Access Accept	Access Reject	HA 4.0 でのサポート
Message-Authenticator	80	AAA メッセージの整合性保護のためのメッセージ オーセンティケータ	1	0	1	0	あり
WiMAX Capability	26/1	HA がサポートする WiMAX 機能を特定します。RADIUS サーバによって選択された機能を示します。	1	0	0-1	0	あり
CUI（Chargeable User Identity）	89	課金ユーザの ID。支払いユーザの固有の一時的ハンドル	0-1	0	0-1	0	あり
AAA-Session-ID	26/4	このセッションに対するホーム レルムでの固有の識別子（HAAA で設定）	0-1	0	1	0	あり
HA-IP-MIP4	26/6	この要求を作成している HA の IP アドレス	0-1	0	0	0	あり
RRQ-HA-IP	26/18	Registration Request または Binding Update に含まれる HA-IP	0-1	0	0	0	あり
MN-HA-MIP4-KEY	26/10	MIP4 手順に使用される MN-HA キー	0	0	1	0	あり
MN-HA-MIP4-SPI	26/11	MN-HA-MIP4-KEY に関連付けられた SPI	1	0	1	0	あり
RRQ-MN-HA-KEY	26/19	RRQ-HA-IP アトリビュートで報告される HA-IP アドレスとバウンドされる MN-HA-KEY	0	0	0-1		あり
RRQ-MN-HA-SPI	26/20	RRQ-MN-HA-KEY と関連付けられた SPI	1	0	1	0	あり
HA-RK-Key-Requested	26/58	HA-RK-KEY アトリビュートが Access-Accept に含まれる必要があることを示します。	1	0	0	0	あり
HA-RK-KEY	26/15	FA-HA キーの生成に使用される HA-RK キー	0	0	0-1	0	あり
HA-RK-SPI	26/16	HA-RK と関連付けられた SPI	0-1	0	0-1	0	あり
HA-RK-Lifetime	26/17	MIP4 操作用の FA-HA キーの生成に使用される HA-RK キー	0	0	0-1	0	あり
Acct-Interim-Interval	85	この特定のセッションの暫定アップデート間の秒数を示します。	0	0	0-1	0	あり

HA からの Access-Request に、値 **1** の HA-RK-Key-Request VSA が含まれていた場合、HAA は Access-Accept で HA_RK-KEY, HA-RK-SPI と HA_RK-Lifetime のアトリビュートを返します。これらのアトリビュートのいずれかがある場合は、すべてがなければなりません。そうでなければ、HA は Access-Accept を廃棄します。このアトリビュートは、あらゆる Accounting（Start/Stop/Interim）メッセージに含まれます。

HAAA は、各 HA にランダムな 160 ビットの HA-RK キーを作成します。HA-RK は、特定の EAP 認証の結果として生成された MIP-RK に基づくものではありません。したがって、個別のユーザまたは認証セッションではなく、オーセンティケータと HAAA のペアにバインドされます。

HA と FA（オーセンティケータと共存している可能性が高い）は、HA-RK からの FA-HA キーを次のように計算します。

FA-HA = H(HA-RK, “FA-HA” | HA-IPv4 | FA-CoAv4 | SPI)

上記で

H は、HMAC-SHA1（RFC 2104「HMAC: Keyed-Hashing for Message Authentication」に指定されているもの）です。

HA-Ipv4 は、FA が認識し、Mobile メッセージで報告される HA の IP アドレスです。32 ビット値で表現されます。

FA-CoAv4 は、HA が認識する FA のアドレスです。32 ビット値で表現されます。

FA から受信した MobileIP RRQ に FHAE エクステンションが含まれている場合、このエクステンションの検証には FA-HA キーと SPI が使用されます。

HMAC-SHA1 は 20 バイトの出力を生成します。現在の HA 実装で FHAE 用にサポートされているのは、HMAC および HMAC-MD5 アルゴリズムであり、必要とされるのは 16 バイトのキーだけです。HA 4.0 は最初の 16 バイトの HMAC-SHA1 出力を FHAE 検証用のキーとして使用します。

HA は MHAE で受信した SPI を MN-HA-MIP4-SPI アトリビュートとして Access-Request に含めます。Mobile IP RRQ 内の MHAE の検証には、MN-HA-MIP4-SPI アトリビュート内の SPI 値に対応する AAA からダウンロードされた MN-HA-MIP4-KEY アトリビュート値が使用されます。**ip mobile secure host** コマンドを使用して、MHAE 検証にローカルに使用できる SPI とキーを設定することも可能です。

HA が受信した MobileIP RRQ に FHAE エクステンションが含まれていた場合、HA は HAAA への Access-Request に HA-RK-Key-Requested アトリビュートを入れて、Access-Accept での HA-RK-KEY アトリビュートの受信を求めます。Access-Request には HA-RK-SPI アトリビュートも含まれ、その値は FHAE で受信された SPI に設定されます。HA は、FHAE 検証用の FA-HA キーを生成するために、HA-RK-SPI アトリビュート内の SPI 値に対応する AAA からダウンロードされた HA-RK-KEY アトリビュート値を使用します。FA-HA キーは、WiMAX Forum Stage 3 仕様（R1.0.0, Section 4.3.5.1）に指定されている HA-RK-KEY から生成されます。**ip mobile secure foreign-agent** コマンドを使用して、FHAE 検証にローカルに使用できる SPI とキーを設定することも可能です。

CLI を使用して WiMAX AAA アトリビュートの機能をイネーブルにした場合、HA は HAAA サーバに送信される Accounting Start/Stop メッセージ に WiMAX AAA アトリビュートを含めます。

WiMAX 用の HA-AAA Accounting アトリビュートのサポート

AAA Accounting アトリビュートの現在の機能は次のとおりです。

- HA は、モバイル ノードの最初のバインディングの作成時に Accounting Start レコードを送信します。
- HA は、モバイル ノードの最後のバインディングの削除時に Accounting Stop レコードを送信します。
- HA はハンドオフ発生時に Accounting Update を送信します。

表 15-2 に、Cisco HA の WiMAX AAA Accounting アトリビュートを示します。

表 15-2　WiMAX AAA Accounting アトリビュート

名前	タイプ	説明	Start	Int	Stop
Session-Continue	26/21	True の場合、停止後すぐに開始されます。このアトリビュートがないか、FALSE の場合は、最終的な停止です。	0	0	0-1
Beginning of Session	26/22	True : 新しいフローが開始されます。False またはこのアトリビュートがない場合は、これまでのフローが継続されます。	0-1	0	0
Hotline-Indicator	26/24	フローがホットラインであることを示します。	0-1	0-1	0-1
Calling-Station-Id	31	MS の MAC アドレス	1	1	1
HA-IP-MIP4	26/6	HA の IP アドレス	1	1	1
Event-Timestamp	55	イベント発生時刻	1	1	1
Control-Packets-In	26/31	IPv4 および IPv6 の着信 Mobile IP、DHCP、ICMP メッセージのパケット カウント	0	0-1	0-1
Acct-Input-Packets-Gigaword	26/48	アトリビュート 47 オーバーフロー時に増分されます。	0	0-1	0-1
Acct-Output-Packets-Gigaword	26/49	アトリビュート 48 オーバーフロー時に増分されます。	0	0-1	0-1
Control Octets In	26/32	着信 Mobile Ipv4、DHCP、ICMP メッセージなどのオクテット カウント	0	0-1	0-1
Control Packets Out	26/33	発信 Mobile Ipv4、DHCP、ICMP メッセージなどのパケット カウント	0	0-1	0-1
Control Octets Out	26/34	発信 Mobile Ipv4、DHCP、ICMP メッセージなどのオクテット カウント	0	0-1	0-1

WiMAX サポートの設定

HA で WiMAX AAA サポートをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# radius-server vsa send authentication wimax`	WiMAX VSA が RADIUS メッセージに含まれるように設定します。このコマンドがイネーブルに設定されていると、HA が生成する Access-Request メッセージに次の RADIUS アトリビュートが含まれます。 • Acct-Interim-Interval (85) • Message-Authenticator(80) • Chargeable-User-Identity(89) • WiMAX Capability (26/1) • HA-IP-MIP4 (26/2) • RRQ-HA-IP (26/18) • MN-HA-MIP4-SPI (26/11) • RRQ-MN-HA-SPI (26/20)
ステップ 2	`Router# radius-server vsa send accounting wimax`	WiMAX VSA が RADIUS メッセージに含まれるように設定します。このコマンドがイネーブルに設定されていると、HA が生成する Accounting メッセージに次の RADIUS アトリビュートが含まれます。 • Acct-Terminate-Cause (49) • Acct-Multi-Session-Id (50) • Acct-Session-Time (46) • Chargeable-User-Identity(89) • Acct-Input-Gigawords (52) • Acct-Output-Gigawords (53) • HA-IP-MIP4 (26/2) • GMT-Time-Zone-Offset (26/3)
ステップ 3	`Router# ip mobile home-agent send-mn-address`	標準 IETF アトリビュート が RADIUS メッセージに含まれるように設定します。設定すると、Mobile IP RRQ で受信されたホーム アドレスが Access-Request メッセージの Framed-IP-Address アトリビュート値として送信されます。
ステップ 4	`Router# radius-server attribute 55 access-request include`	Access-Request に Event-Timestamp（55）アトリビュートを含めます。
ステップ 5	`Router# radius-server attribute 55 include-in-acct-req`	Accounting メッセージに Event-Timestamp（55）アトリビュートを含めます。

設定の確認

WiMAX サポートがイネーブルになっていることを確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# show ip mob bind`	登録者の認証中に WiMAX 機能のネゴシエーションが実行された場合を示します。

例を示します。

```
Router# show ip mob bind
Mobility Binding List:
Total 15000
MIP-USER12573@ispxyz.com (Bindings 1):
    Home Addr 193.1.1.28
    Care-of Addr 7.0.0.85, Src Addr 7.0.0.85
    Lifetime granted INFINITE
    Flags sbdmg-T-, Identification C9ED9187.10000
    Tunnel3 src 73.0.0.42 dest 7.0.0.85 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Service Options:
        Dynamic HA assignment
    Acct-Session-Id: 1677265
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
```

AAA サーバの設定

ここでは、AAA サーバに対する AAA Authentication および Accounting アトリビュートの設定について説明します。ここで説明するのは一般的な設定です。

表 15-3　AAA サーバの AAA Authentication および Accounting アトリビュート

RSIM アトリビュート	説明
アトリビュート 4 *vsa string*	このセッションに対するホーム レルムでの固有の識別子（HAAA で設定）
アトリビュート 6 *ip address as string*	MIP4 の場合の HA の IPv4 アドレス。要求を作成している HA の IP アドレスです。
アトリビュート 10 *ascii* または *hex corresponding string*	RADIUS サーバが ASN（PMIP の場合）に送信する MN-HA-KEY、または MIP4（MIP または PMIP）の場合は RADIUS サーバが HA に送信する MN-HA-KEY。PMIP4 中、ASN が MN-HAAE の計算に使用します。 HA に送信されて、MIP バージョン（MIP4 または MIP6）および SPI に基づく MN-HA-AE（MIP4）の検証、および MIP4 Registration Response または MIP6 Binding Answer の AUTH の完了に使用されます。
アトリビュート 11 *spi hex value* 16 進値 100 ～ FFFFFFFF の範囲	MN-HA-MIP4-KEY に関連付けられた SPI
アトリビュート 15 *ascii* または *hex corresponding string*	RADIUS サーバによる EAP 認証中に決定され、EAP 認証成功の場合は NAS に渡される HA-RK-KEY。NAS はこのキーを FA-HA キーの生成に使用します。
アトリビュート 16 *spi hex value* 16 進値 100 ～ FFFFFFFF の範囲	HA-RK に使用された SPI
アトリビュート 17 *vsa value*	HA-RK および抽出されたキーのライフタイム
アトリビュート 19 *ascii* または *hex corresponding string*	HAAA が HA に送信し、Mobile IP Registration Request の MN-HA-AE の検証に使用される MN-HA キー
アトリビュート 20 *spi hex value* 16 進値 100 ～ FFFFFFFF の範囲	HAAA が HA に送信し、Mobile IP Registration Request の MN-HA-AE の検証に使用される MN-HA キー

アップストリームでの MS トラフィック リダイレクション

この機能を使用すると、モバイル ノードから受信した IP トラフィックをアップストリーム パスのネクストホップ IP アドレスにリダイレクトできます。ネクストホップ IP アドレスは、レルム単位で設定されます。これをサポートしているのは、NAI ベースのモバイル ノードだけです。冗長構成の場合は、アクティブとスタンバイの両方の HA に同じ設定が必要です。

アップストリーム トラフィックでの MS トラフィック リダイレクションの設定

これまでの設定に加えて、次の作業を実行します。

	コマンド	目的
ステップ 1	Router(config)# **ip mobile realm** *realm* **any-traffic next-hop** *next-hop-ipadress*	そのレルムのネクストホップ アドレスを設定します。 ***any-traffic*** は、そのモバイル ノードからのアップストリームのすべてのトラフィックがリダイレクトされるように指示します。 ***next-hop*** はネクストホップ機能を指定します。 *next-hop-ip-address* は、ネクストホップの IP アドレスです。パケットはこのアドレスにリダイレクトされます。

設定の確認

MS トラフィックがリダイレクトされることを確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **show ip mobile binding**	バインディングの変更、およびそのモバイル ノードに設定されているネクストホップ アドレスが表示されます。

例を示します。

```
Router#sh ip mobile binding
Mobility Binding List:
Total 1
Total VPDN Tunnel'ed 0
xyz1@xyz.com (Bindings 1):
    Home Addr 11.110.1.1
    Care-of Addr 13.1.1.112, Src Addr 13.1.1.112
    Lifetime granted 00:30:00 (1800), remaining 00:29:52
    Flags sbdmg-T-, Identification CAF62BE1.1
    Tunnel0 src 13.1.254.254 dest 13.1.1.112 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Acct-Session-Id: 0x00000002
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Hotline status Active
    Radius Disconnect Enabled

    Next-hop set for any-traffic to 14.1.1.201
```