Cisco Mobile Wireless Home Agent リリース 5.2 for Cisco IOS リリース 12.4(22)YD2

Cisco Mobile Wireless Home Agent Release 5.2 for Cisco IOS Release 12.4(22)YD2

12.4(22)YD2
2009 年 11 月 13 日

Text Part Number: OL-21460-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Mobile Wireless Home Agent リリース 5.2 for Cisco IOS リリース 12.4(22)YD2

CONTENTS

CHAPTER 1

Cisco Mobile Wireless Home Agent の概要

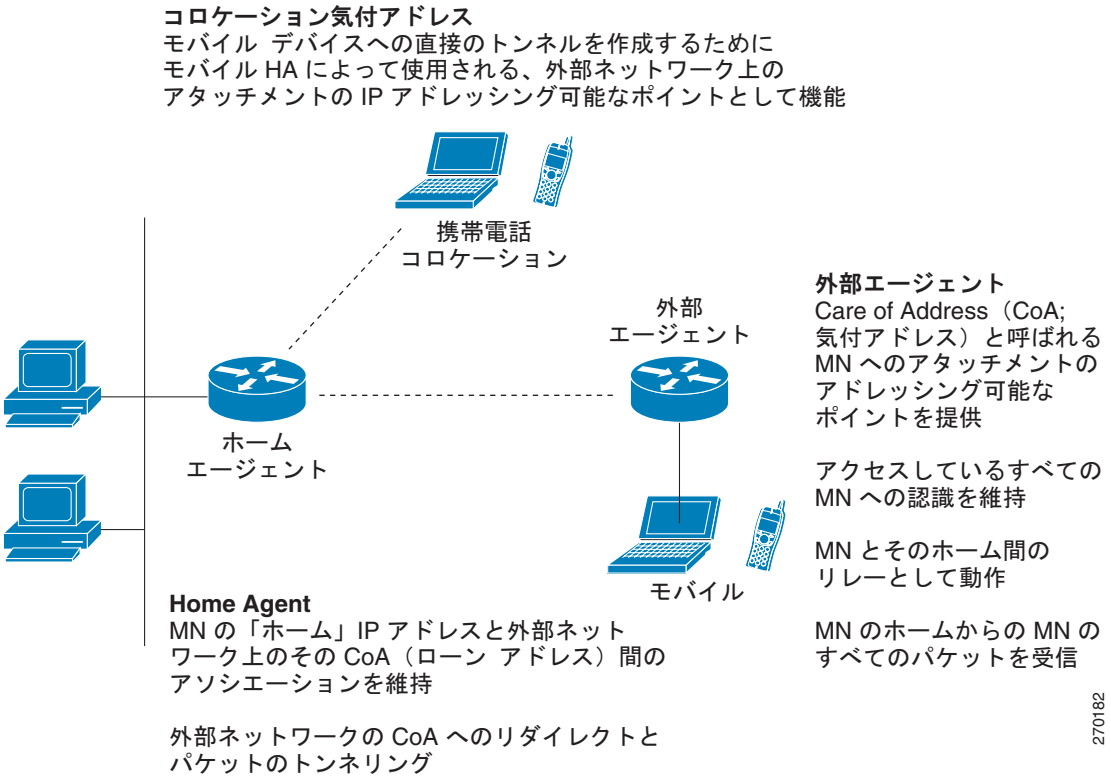
この章では、一般的なモバイル IP パケット データ システムにおける機能要素、このソリューションをサポートする販売中のシスコ製品、さらに Cisco IOS Mobile Wireless Home Agent ソフトウェアでの実装について説明します。

この章は、次の内容で構成されています。

機能の概要

Cisco Mobile Wireless Home Agent は、サブスクライバのアンカー ポイントとなり、使いやすくて安全なローミング機能とともに、Quality of Service （QoS）機能を提供して、モバイル ユーザのサービス利用を最適化します。Cisco Mobile Wireless Home Agent（HA）は、Foreign Agent（FA）およびモバイル ノードと連動して、効率的なモバイル IP ソリューションを実現します。図 1-1 に、基本的なトポロジを示します。

図 1-1　モバイル IP のトポロジ



Cisco Mobile Wireless Home Agent は、外部エージェントを通じて、またはコロケーション モード（Colocated Care-of Address（CCOA; コロケーション気付アドレス））でモバイル ユーザ登録を維持し、モバイル デバイス宛てのパケットを外部エージェントにトンネリングします。リバース トンネリングをサポートし、IP Security（IPSec）を使用して外部エージェントにパケットを安全確実にトンネリングできます。Cisco Mobile Wireless Home Agent はさらに、パブリック アドレスとプライベート アドレスの両方について、モバイル デバイスへのダイナミックおよびスタティック ホーム アドレス割り当てをサポートします。ホーム アドレスの割り当ては、ローカルでまたは Differentiated Services Code Point（DHCP; DiffServ コード ポイント）サーバ アクセスによってリモートで設定されたアドレス プール、Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）サーバから、または On-Demand Address Pool（ODAP）から行われます。

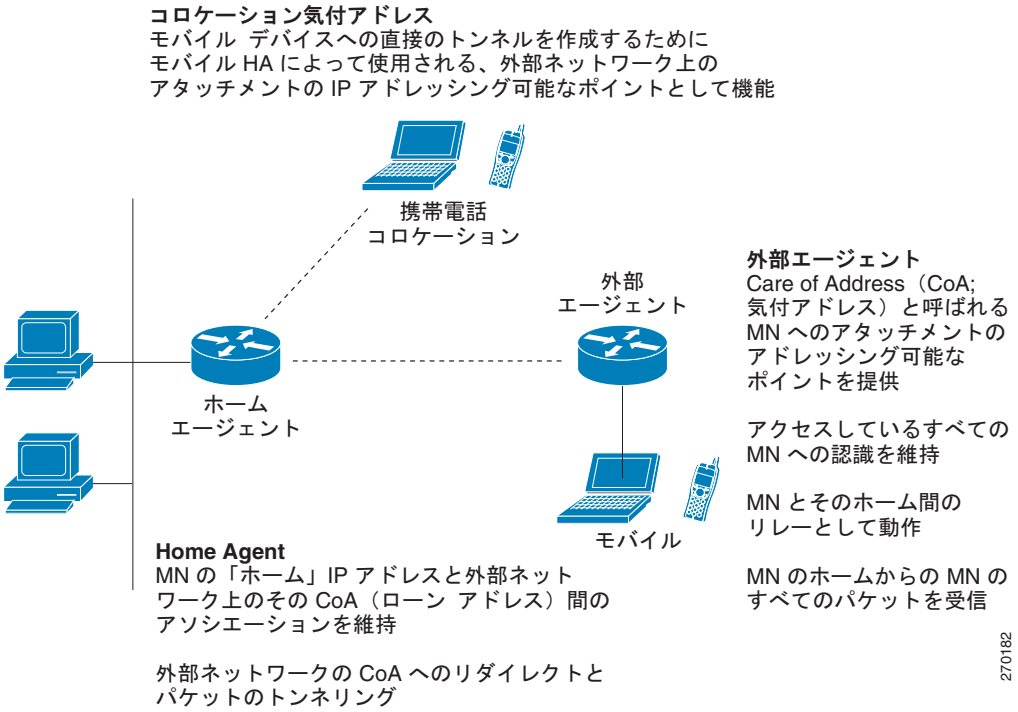
Cisco Mobile Wireless Home Agent は、モバイル端末のアンカー ポイントであり、そこからモバイル端末にモバイル サービスまたはプロキシ モバイル サービスが提供されます。端末に送信されたトラフィックは、Home Agent を使用してルーティングされます。リバース トンネリングによって、端末からのトラフィックも Cisco Mobile Wireless Home Agent 経由でルーティングされます。Home Agent 冗長性、ロード バランシングなどの独自機能が、高度な可用性と信頼性をもたらし、アカウンティングの整合性を維持しながら、地理的分散を可能にします。もう 1 つの独自機能である Network Address Translation（NAT; ネットワーク アドレス変換）トラバーサルによって、さまざまなアクセス テクノロジーにまたがるアンカー ポイントとして Cisco HA を使用できます。したがってユーザは、さまざまなアクセス ネットワークを透過的に移動しながら、固定接続とアドレッシング能力を維持できます。

Code Division Multiple Access（CDMA）環境における Cisco Mobile Wireless Home Agent

CDA2000 は第三世代（3G）の無線ソリューションであり、すでに Code Division Multiple Access（CDMA）テクノロジーを採用しているモバイル無線事業者はパケット データ サービスを提供できるようになります。Cisco CDMA 2000 Packet Data Services ソリューションは、3G セルラー データ サービスに移行するモバイル無線業界のニーズに応える設計です。Cisco Mobile Wireless Home Agent は、このソリューションの重要な構成要素です。Cisco CDMA2000 Packet Data Services ソリューションには、外部エージェント機能を備えた Cisco Packet Data Serving Node（PDSN）、CDMA2000 ベースの Cisco Mobile Wireless Home Agent、Cisco Network Registrar®、Cisco Access Registrar® サーバ、およびその他のセキュリティ製品および機能が含まれます。図 1-2 に、一般的な Cisco CDMA2000 Packet Data Services システムの機能要素を示します。

Cisco Mobile Wireless Home Agent は、国際無線規格に準拠し、モバイル性の拡大を実現し、モバイル IP およびプロキシ モバイル IP を使用していつでもアドレッシング可能であり、アクセス可能な Cisco Systems® ソリューションに含まれています。Cisco Mobile Wireless Home Agent を Cisco Packet Data Serving Node（PDSN）Foreign Agent と組み合わせることによって、モバイル IP クライアント機能を備えたモバイル ステーションは、モバイル IP ベースのサービス アクセスを使用して、インターネットまたは企業イントラネットにアクセスできます。モバイル IP は、ユーザのモバイル能力をカバー エリアよりさらに拡げ、ローミング機能を提供します。CDMA2000 環境では、別の Cisco PDSN がコールに割り当てられると（ハンドオフ後）、新しい Cisco PDSN が Cisco Mobile Wireless Home Agent へのモバイル IP 登録を行います。これは、モバイル クライアントに、最初のセッション確立時に割り当てられたものと同じホーム アドレスを割り当てるうえで有効です。トラフィックは Cisco Mobile Wireless Home Agent を介してルーティングされ、HA もプロキシ Address Resolution Protocol（ARP; アドレス解決プロトコル）サービスを提供します。リバース トンネリング使用時は、端末からのトラフィックもホーム エージェント経由でルーティングされます。モバイル IP クライアント機能のないクライアントでも、プロキシ モバイル IP またはクライアント モバイル IP 機能を使用することによって、これらのサービスを利用できます。図 1-2 に、Cisco Mobile Wireless Home Agent およびパケット データ サービスに必要なその他のコンポーネントからなる CDMA2000 ネットワークを示します。

図 1-2　CDMA2000 ネットワーク



図のように、モバイル ステーションは無線タワーおよび Base Transceiver Station（BTS; 無線基地局）に接続します。モバイル ステーションは、簡易 IP またはモバイル IP のどちらかをサポートする必要があります。BTS は Base Station Controller（BSC; 基地局コントローラ）に接続し、BSC には Packet Control Function（PCF; パケット制御機能）というコンポーネントが組み込まれています。PCF は A10/A11 インターフェイスを通じて、Cisco PDSN と通信します。A10 インターフェイスはユーザ データ用であり、A11 インターフェイスはコントロール メッセージ用です。このインターフェイスは Radio Access Network（RAN; 無線アクセス ネットワーク）-PDSN（R-P）インターフェイスともいいます。Cisco Home Agent Release 2.1 以上では、Cisco Service Application Module for IP（SAMI）プラットフォーム上で Giga Ethernet（GE; ギガ イーサネット）インターフェイスを使用する必要があります。

PDSN と外部データ ネットワーク間の IP ネットワーキングは、PDSN-イントラネット/インターネット（Pi）インターフェイスを介して行われます。Cisco HA の場合は、Pi インターフェイスとして Fast Ethernet（FE; ファスト イーサネット）インターフェイスまたは GE インターフェイスのどちらでも使用できます。

AAA サーバ接続などの「バック オフィス」接続に関して、インターフェイスはメディアに依存しません。

HA を PDSN および Foreign Agent と組み合わせることによって、モバイル IP クライアント機能を備えたモバイル ステーションは、モバイル IP ベースのサービス アクセスを使用して、インターネットまたは企業イントラネットにアクセスできます。モバイル IP はユーザのモバイル能力を現在の PDSN/Foreign Agent のカバー エリアよりさらに拡げます。別の PDSN がコールに割り当てられると（ハンドオフ後）、ターゲット PDSN が HA にモバイル IP 登録を行うので、モバイル ステーションに確実に同じホーム アドレスが割り当てられます。さらに、モバイル IP クライアント機能のないクライアントでも、PDSN のプロキシ モバイル IP 機能を使用することによって、これらのサービスを利用できます。

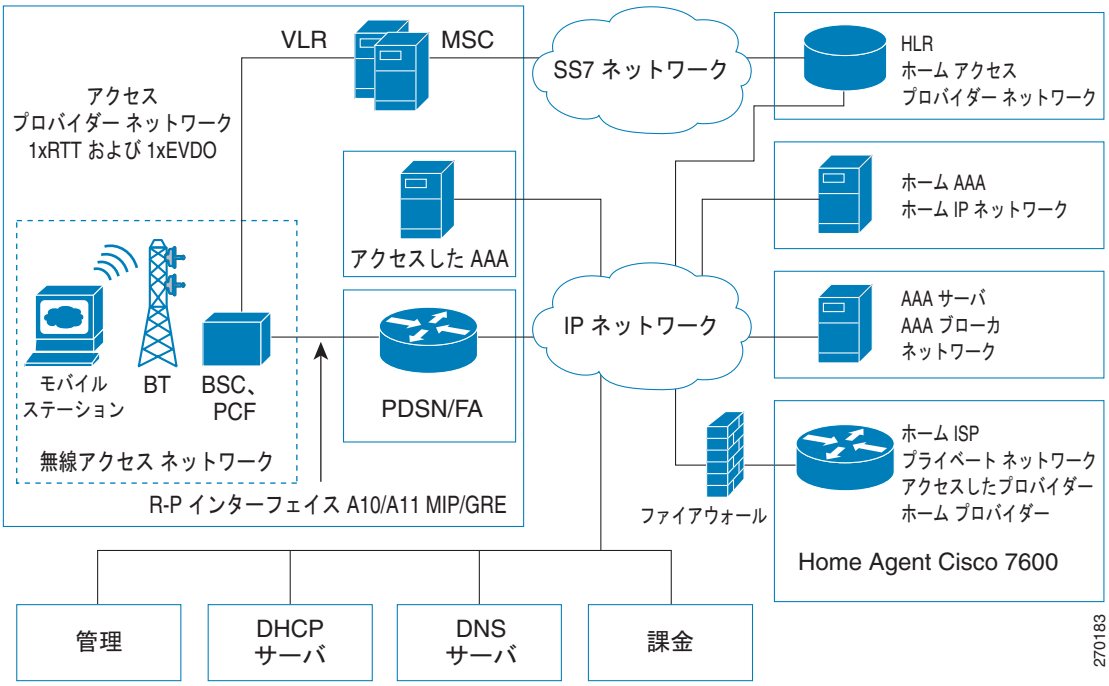
HA は、モバイル端末のアンカー ポイントであり、そこからモバイル端末にモバイル IP サービスまたはプロキシ モバイル IP サービスが提供されます。トラフィックは HA を介してルーティングされ、Home Agent もプロキシ ARP サービスを提供します。リバース トンネリングの場合は、端末からのトラフィックも HA 経由でルーティングされます。

Cisco Mobile Wireless Home Agent は、必要な規格をすべてサポートします。Third-Generation Partnership Project 2（3GPP2）Technical Specification Group P および X（TSG-P、TSG-X）Standard、CDMA2000 ネットワーク全体の構造を定義する Wireless IP Network Standard（別名 TIA/EIA/IS-835-D）などです。Cisco Mobile Wireless Home Agent には、拡張モバイル IP、セキュリティ、認証などの機能が組み込まれています。

Worldwide Interoperability for Microwave Access（WiMAX）環境における Cisco Mobile Wireless Home Agent

Worldwide Interoperability for Microwave Access（WiMAX）は、急成長中の新しい市場で先進的なブロードバンド無線サービスを提供する、IEEE 標準テクノロジーに基づいた第四世代（4G）の無線ソリューションです。WiMAX は数々の大きな利点をもたらしますが、中でも重要なのは、すべてデータ、すべて IP のアーキテクチャによる配備コストの削減、周波数域取得コストの削減、さらに IP ブロードバンド ドメインに由来する広範な IP 対応アプリケーションです。Cisco HA は、WiMAX エンドツーエンド リファレンス モデルのコア サービス ノードに含まれます。WiMAX エンドツーエンド リファレンス モデルを構成する論理エンティティは、Mobile Subscriber Station（MSS; モバイル サブスクライバ ステーション）、Access Service Network（ASN; アクセス サービス ネットワーク）、および Core Service Network（CSN; コア サービス ネットワーク）です。図 1-3 に、ASN の分解図を示します。Network Reference Model（NRM; ネットワーク リファレンス モデル）は、ネットワーク アーキテクチャの論理表現です。NRM では、機能エンティティを特定し、さらに機能エンティティ間の相互運用性を実現できるリファレンス ポイントを示します。

図 1-3　　WiMAX リファレンス モデル



アクセス サービス ネットワーク（ASN）

ASN は、WiMAX サブスクライバが無線アクセスできるようにする、一連のネットワーク機能として定義されます。ASN は、（1 つまたは複数のベース ステーション クラスタに含まれる）ベース ステーション（複数可）、ASN ゲートウェイ（複数可）などのネットワーク要素で構成されます。ASN は、複数の Connectivity Service Network（CSN; 接続サービス ネットワーク）間で共有することもあります。

接続サービス ネットワーク（CSN）

接続サービス ネットワーク（CSN）は、サービス レイヤに IP 接続機能を提供する一連のネットワーク要素です。AAA サーバ、DHCP サーバなどのプロビジョニング要素は、HA によって使用可能になる機能、マクロ モバイル アンカー ポイントとともに、CSN に配置されます。サービス レイヤは、豊富なサービス提供、サブスクライバ識別、およびポリシー実施を実現するためのベースになります。シスコでは、シスコの総合的な IP Next Generation Network（NGN）ビジョン、アーキテクチャ、およびネットワーキング ソリューションによって、サービス プロバイダーがネットワーク統合を発展させることができるように支援しています。WiMAX Forum Network Reference Model（この団体の Network Working Group による定義）は、ネットワーク、サービス コントロール、およびアプリケーション レイヤ統合の利用を提示しています。

ハードウェア プラットフォーム サポート

Cisco Mobile Wireless Home Agent は、Cisco 7600 シリーズに対応する Cisco Service Application Module for IP（SAMI）上で動作します。Cisco 7600 シリーズ プラットフォームでサポートされる物理インターフェイスは、ファスト イーサネットおよびギガビット イーサネットが中心であり、さらに FlexWAN（Asynchronous Transfer Mode（ATM; 非同期転送モード）、フレームリレー）、Shared Port Adaptor（SPA; 共有ポート アダプタ）および SPA Interface Processor（SIP; SPA インターフェイス プロセッサ）ラインカードの新シリーズがあります。物理メディアには依存しません。

スーパーバイザ サポート

HA Release 5.1 の機能は、次の SUP32、SUP720、および RSP720 バリアント上でサポートされます。必要なスーパーバイザの製品番号は次のとおりです。

- WS-SUP32-GE-3B(=)
- WS-SUP32-10GE-3B(=)
- WS-SUP720-3BXL(=)
- WS-SUP720-3B(=)
- WS-SUP720(=)
- RSP720-3C-GE(=)
- RSP720-3CXL-GE(=)
- RSP720-3CXL-10GE(=)

セッション冗長性インフラストラクチャ

Home Agent Release 5.0 以上では、HA は他の Cisco Mobile Service Exchange Framework（mSEF; モバイル サービス エクスチェンジ フレームワーク）製品に使用されているものと同じセッション冗長性インフラストラクチャを使用します。ただし、冗長性を実現するための外部動作が大幅に変更されます。Release 4.0 以前の HA 固有の冗長性スキームは、引き続きサポートされます。ただし、Session Redundancy（SR; セッション冗長性）インフラストラクチャベースのアプローチは、以前の HA 冗長性スキームとの互換性がありません。

5.0 以上の HA 冗長性スキームでは、アクティブ/スタンバイ ロール解決の手段および障害が発生したかどうかを判断するためのメカニズムとして、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を引き続き使用できます。

セッション冗長性の詳細については、「HA セッション冗長性のインフラストラクチャ」（P.6-2）を参照してください。

プラットフォームの利点

- HA SAMI サービス モジュールは、異なる配置シナリオにおけるさまざまなシャーシ構成が可能なキャリア クラスの Cisco 7600 シリーズ ルータを活用します。
- 拡張性の非常に高いソリューションにより、トラフィック負荷に合わせてサービス モジュールを追加し、迅速にシステムを拡張できます。
- モバイル空間で各種アプリケーションのサポートに使用されてきた、堅牢で実績のあるアプローチを利用できます。

パケット データ サービス

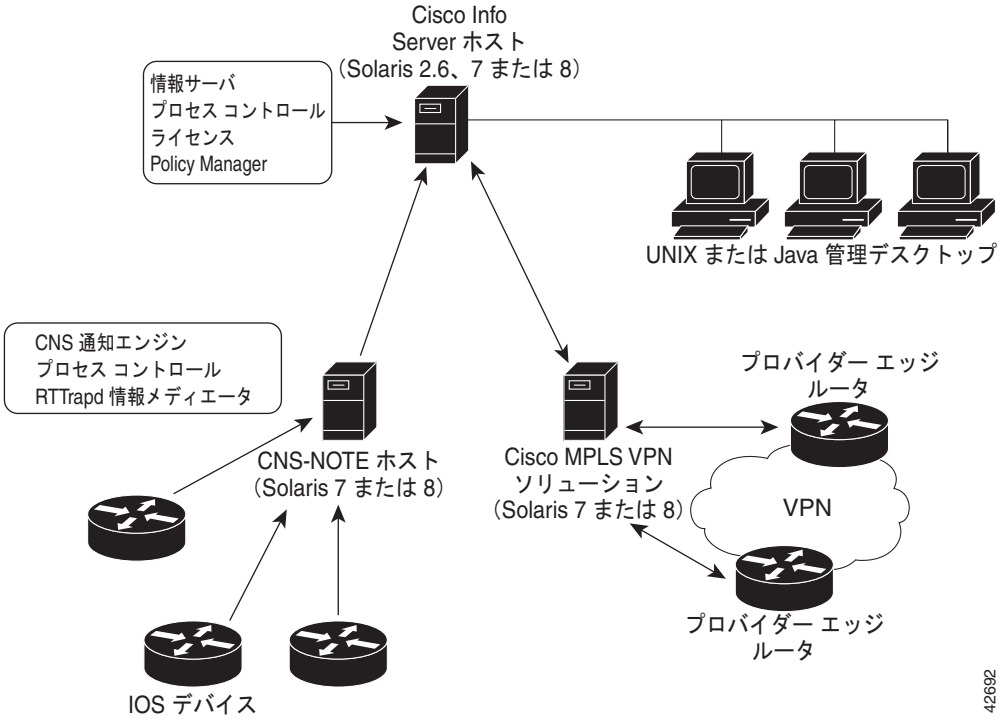
CDMA2000 ネットワークのコンテキストにおいて、Cisco HA は 2 種類のパケット データ サービスをサポートします。モバイル IP サービスおよびプロキシ モバイル IP サービスです。Cisco HA にとって、この 2 種類のサービスは同じです。

シスコのモバイル IP サービス

モバイル IP を使用する場合、モバイル ステーションは所定の PDSN のカバー エリアを越えて移動でき、なおかつ同じ IP アドレスとアプリケーション レベルの接続を維持できます。

図 4 に、モバイル IP シナリオにおける Cisco HA の配置を示します。

図 4　CDMA ネットワーク - モバイル IP シナリオ



通信プロセスの発生順は、次のとおりです。

1. モバイル ステーションが FA を通じて HA に登録します。CDMA 2000 ネットワークのコンテキストでは、FA は Cisco PDSN です。
2. Cisco HA は登録を受け付け、モバイル ステーションに IP アドレスを割り当て、FA へのトンネルを作成します。その結果、モバイル ステーションと FA（つまり PDSN）間に Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）リンク、FA と HA 間に IP-in-IP または Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネルが設定されます。

   登録処理の一部として、Cisco HA はバインディング テーブル エントリを作成して、モバイル ステーションのホーム アドレスと対応する *Care-of* Address（CoA; 気付アドレス）を関連付けます。

   （注）　ホームから離れている間（HA から見た場合）、モバイル ステーションは気付アドレスに関連付けられています。このアドレスは、現在のトポロジから見た、モバイル ステーションのインターネットへの接続ポイントを示し、このアドレスを使用して、モバイル ステーションにパケットがルーティングされます。Foreign Agent のアドレス、または特定のネットワーク上に存在している間、使用するためにモバイル ステーションが取得したアドレスが気付アドレスとして使用されます。Cisco HA の場合、気付アドレスは常に Foreign Agent のアドレスです。

3. HA はモバイル ステーションにネットワークへの到達可能性を通知し、現在の位置のモバイル ステーションにデータグラムをトンネリングします。
4. モバイル ステーションは、送信元 IP アドレスとしてホーム アドレスを指定してパケットを送信します。

5. モバイル ステーション宛てのパケットは HA を通過し、HA が PDSN にトンネリングします。PDSN からは、気付アドレス を使用して、モバイル ステーションに送信されます。このシナリオは、リバース トンネリングにも適用され、モバイルからネットワークに、HA をパススルーしてトラフィックを流すことができます。
6. PPP リンクが新しい PDSN に引き渡されるときに、リンクの再ネゴシエーションが行われ、モバイル IP 登録が更新されます。
7. HA は、新しい気付アドレスを使用して、バインディング テーブルをアップデートします。

（注）　モバイル IP の詳細については、Cisco IOS Release 12.4 のマニュアル『*Cisco IOS IP Mobility Configuration Guide*』Release 12.4 および『*Cisco IOS IP Mobility Command Reference*』Release 12.4 を参照してください。RFC 2002 で、詳細な仕様が規定されています。TIA/EIA/IS-835-B でも、HA でモバイル IP を実現する方法が定義されています。

シスコのプロキシ モバイル IP サービス

サービス プロバイダーによっては、モバイル IP クライアント ソフトウェアを販売していませんが、PPP は Internet Service Provider（ISP; インターネット サービス プロバイダー）との接続に広く使用されており、IP デバイスには必ず存在します。モバイル IP の代用として、シスコのプロキシ モバイル IP 機能を使用できます。Cisco PDSN のこの機能は PPP と統合されており、PDSN（Foreign Agent として動作）とモバイル IP クライアントが認証 PPP ユーザにモバイル能力を提供できるようにします。

通信プロセスの発生順は、次のとおりです。

1. Cisco PDSN（FA として動作）がモバイル ステーション認証情報（具体的には PPP 認証情報）を収集して、AAA サーバに送信します。
2. モバイル ステーションが Cisco PDSN プロキシ モバイル IP サービスの使用許可を受けると、AAA サーバが登録データおよび HA アドレスを返します。
3. FA はこの情報およびその他の情報を使用して、モバイル ステーションのために Registration Request（RRQ; 登録要求）を生成し、Cisco HA に送信します。
4. 登録に成功すると、Cisco HA が FA に、IP アドレスが指定された Registration Reply（RRP; 登録応答）を送信します。
5. FA が IP Control Protocol（IPCP; IP コントロール プロトコル）を使用して、モバイル ステーションに（RRP で受け取った）IP アドレスを割り当てます。
6. Cisco HA と FA、つまり PDSN 間にトンネルが設定されます。リバース トンネリングがイネーブルの場合、トンネルはモバイル ステーションに対して双方向でトラフィックを伝送します。

（注）　PDSN はプロキシ Mobile IP（MIP; モバイル IP）クライアントに代わって、あらゆるモバイル IP 再登録を引き受けます。

機能

IOS Release 12.4(22)YD2 の新機能

ここでは、Cisco IOS Release 12.4(22)YD2 対応の Home Agent Release 5.2 で追加または変更された機能について説明します。

- 「代替 MN ID のサポート」（P.16-18）
- 「コール アドミッション制御（CAC）のサポート」（P.16-19）
- 「使用済みの場合のフレーム化された IP の拒否」（P.16-32）
- 「非 VPN ルーティングおよびフォワーディング（VRF）環境での GRE 鍵 Critical Vendor-Specific Extension（CVSE）」（P.16-41）

次の機能は、Cisco IOS Release 12.4(22)YD2 以前で導入または修正されたものです。

- 「FA-HA IP-in-IP トンネルに対する一意の IP ID の保護」（P.16-16）
- 「Offset=0 による第 1 パケットのフラグメント サイズの設定」（P.16-14）
- 「Worldwide Interoperability for Microwave Access（WiMAX）ホットラインの CoA」（P.15-11）
- 「モニタリングでの DNS リダイレクション」（P.9-4）
- 「ローカル MN-HA SPI および Key を使用した NAI 認証」（P.5-4）
- 「ホットラインを適用していないユーザのための IP リダイレクト」（P.15-6）
- 「ネットワーク アクセス識別子（NAI）/ レルム単位の入力 / 出力 アクセス リスト」（P.10-3）
- 「HA：レルム ケース インセンシティブ オプション」（P.16-2）
- 「FA-HA 認証エクステンションの義務化」（P.16-3）
- 「NAI ごとの絶対タイムアウト」（P.16-8）
- 「"ip mobile host/realm" の AAA アトリビュート」（P.16-26）
- 「China Telecom アトリビュートの Vendor-Specific Extensions（VSE）サポート」（P.16-16）
- 「3GPP2 / WiMAX バインディングの OM メトリック」（P.16-38）
- 「MIP/ユーザ データグラム プロトコル（UDP）トンネルの単一インターフェイス記述ブロック（IDB）」（P.16-39）
- 「ホットラインの冗長性サポート」（P.15-4）
- 「再登録 / 登録解除に対する無認可」（P.5-5）
- 「SNMP によるトンネル統計情報」（P.17-2）
- 「Mobile-Home Authentication Extension（MHAE）を持たない 3GPP2 登録要求（RRQ）」（P.5-3）

ここでは、Cisco IOS Release 12.4(22)YD2 以前で導入された機能について説明します。

- 単一 IP インフラストラクチャ
  - 「MIP の単一インターフェイス」（P.3-3）
  - 「設定の単一インターフェイス」（P.3-3）
  - 「SNMP 管理の単一インターフェイス」（P.3-4）
  - 「トラブルシューティングおよびデバッグの単一インターフェイス」（P.3-4）
  - 「AAA の単一インターフェイス」（P.3-4）

  - 「MIP および AAA の単一インターフェイス」（P.3-5）
  - 「フェールオーバーの単一インターフェイス」（P.3-10）
  - 「AAA 無応答に対するトラップ生成」（P.3-11）
  - 「シャーシ間の設定同期」（P.3-14）
- 「HA セッション冗長性のインフラストラクチャ」（P.6-2）
- バインディングの最大数の制限の排除（「HA での CAC の設定」（P.16-20）時）
- 「輻輳制御機能」（P.16-20）
- 「外部エージェントの分類」（P.16-35）
- 「Show/Clear バインディング キーとしての MAC アドレス」（P.16-37）
- 「データ パス アイドル タイマー」（P.16-37）
- 「RFC 4917 のサポート」（P.16-42）
- 「アドレス割り当て機能」（P.4-1）
- 「Show/Clear バインディング キーとしての MAC アドレス」（P.16-37）
- 「中間アカウンティングの同期化」（P.12-4）
- 「単一 IP HA アカウンティングのサポート」（P.12-2）
- 「ドメイン単位のアカウンティング」（P.12-4）
- 「Acct-Terminate-Cause のサポート」（P.16-33）
- 「認証設定拡張機能」（P.5-2）

ここでは、Cisco IOS Release 12.4(15)XM1 以前で導入または修正された機能を示します。

- 「SAMI サポート」（P.2-1）

  Cisco HA 4.0 以上は、Cisco 7600 シリーズ ルータ シャーシに搭載された Cisco SAMI カードで動作します。7600 シャーシでは SUP720、SUP32、および RSP720 を使用します。また、負荷分散のための IOS Server Load Balancing（SLB; サーバ ロード バランシング）コンポーネントをホストします。

  1 つの Cisco 7600 シリーズ ルータ シャーシで、最大 9 台の SAMI カードをサポートできます。
- 「ホットライニング」（P.15-1）の機能拡張
- 「Home Agent（HA）の サービス品質（QoS）」（P.14-1）の機能拡張
- 「Framed-Pool 基準」（P.16-21）
- 「WiMAX AAA アトリビュート」（P.16-24）
- 「アップストリーム パスでのモバイル ステーション（MS）トラフィック リダイレクション」（P.16-13）
- 「外部エージェント別アクセス タイプ サポート」（P.16-33）
- 「コール アドミッション制御（CAC）のサポート」（P.16-19）
- 「ローカル プールのプライオリティ メトリック」（P.16-22）
- 「モバイル IPv4 ホスト設定エクステンション（RFC4332）」（P.16-24）

ここでは、Home Agent Release 4.0 以前で追加または変更された機能について説明します。

- 移動体識別番号（MEID）のサポート
- HA のアカウンティングの機能拡張
  - 冗長セットアップの HA アカウンティング

  - アカウンティング レコードのパケット カウントおよびバイト カウント
  - アカウンティング レコードで追加されたアトリビュート
  - 追加されたアカウンティング方式：中間アカウンティングのサポート
- RADIUS サーバ上の VRF マッピング
- 条件付きデバッグの機能拡張
- HA の冗長性の機能拡張
  - RADIUS ダウンロード プール名を使用した冗長性
- IP-LOCAL-POOL-MIB 用の CLI
- パケット フィルタリングでのモバイル ユーザ アクセス コントロール リスト（ACL）
- IP 到達可能性
- DNS サーバのアドレスの割り当て
- Home Agent のネットワーク管理、管理情報ベース（MIB）、および簡易ネットワーク管理プロトコル（SNMP）のモバイル IP MIB の拡張

ここでは、Cisco Mobile Wireless Home Agent の旧リリースで追加または変更された機能について説明します。

- 「モバイル IPv4 登録の失効」（P.8-1）
- 「HA サーバ ロード バランシング」（P.7-1）
- 「HA アカウンティングの概要」（P.12-1）
- 「MN-FA Challenge Extension（MFCE）による HA-CHAP の省略」（P.5-5）
- 「HA での VRF サポート」（P.13-1）
- 「Remote Authentication Dial-In User Service（RADIUS）切断」（P.8-4）
- 「条件付きデバッグ」（P.17-5）
- 「ホーム アドレス割り当て」（P.4-1）
- 「HA の冗長性」（P.6-1）
- 「仮想ネットワーク」（P.6-8）
- 「モバイル IP の IPSec」（P.11-1）
- 「トンネル インターフェイスでのアクセス制御リスト（ACL）のサポート」（P.16-11）
- 「AAA アトリビュート MN-HA-SPI および MN-HA SHARED KEY のサポート」（P.16-11）
- 「3 DES 暗号化」（P.11-1）
- 「ユーザ プロファイル」（P.16-12）
- 「モビリティ バインディング アソシエーション」（P.16-12）
- 「ユーザ認証および認可」（P.5-1）
- 「HA バインディングのアップデート」（P.16-13）
- 「ユーザ単位パケット フィルタリング」（P.10-1）
- 「セキュリティ」（P.11-1）

機能サポート

HA として設定された Cisco 7600 シリーズ ルータは、Cisco IOS のネットワーキング機能をサポートする以外に、HA に固有の次の機能をサポートします。

- スタティック IP アドレス割り当てのサポート
  - パブリック IP アドレス
  - プライベート IP アドレス
- ダイナミック IP アドレス割り当てのサポート
  - パブリック IP アドレス
  - プライベート IP アドレス
- スタティック アドレスまたはダイナミック アドレスを使用する、異なる Network Access Identifier（NAI; ネットワーク アクセス識別子）に対応するマルチフロー
- 異なるスタティック アドレスを使用する、同一 NAI に対するマルチフロー
- RFC 3012 - bis 03 で規定された Foreign Agent Challenge の機能拡張
  - モバイル IP エージェント アドバタイズ チャレンジの機能拡張
  - MN-FA チャレンジの機能拡張
  - 汎用モバイル IP 認証拡張機能（MN-AAA 認証拡張機能のフォーマットを指定）
- RFC 2002 で規定されたモバイル IP 拡張機能
  - MN-HA 認証拡張機能
  - FA-HA 認証拡張機能
- リバース トンネリング（RFC 2344）
- Mobile NAI Extension（モバイル NAI 拡張機能）、RFC 2794
- FA と HA 間の複数のトンネリング モード
  - IP-in-IP カプセル化（RFC 2003）
  - 総称ルート カプセル化（RFC 2784）
- 古いバインディングを管理するためのバインディング アップデート メッセージ
- HA 冗長性サポート
- RFC 3220 で規定されたモバイル IP 拡張機能
  - SPI セクション 3.2 を使用しなければならない認証
- パケット フィルタリングのサポート
  - 入力アクセス リスト
  - 出力アクセス リスト
- プロキシおよび gratuitous ARP のサポート
- タイムスタンプを使用するモバイル IP 登録再送保護。ナンスベースの再送保護はサポートされません。

利点

- スタティックおよびダイナミック IP アドレス割り当てをサポートします。
- Mobile Station（MS; モバイル ステーション）に配信するデータグラムを誘引、代行受信、およびトンネリングします。
- MS から（FA を介して）トンネリングされたデータグラムの受信、カプセル化解除、Corresponding Node（CN; 対応ノード）への配信を行います。

（注）　設定に応じて、MS がリバース トンネリングを使用する場合もあれば、使用しない場合もあります。また、HA がリバース トンネリングを受け付ける場合もあれば、受け付けない場合もあります。

- ネットワークに一意のルーティング可能アドレスを提示します。
- 入力および出力フィルタリングをサポートします。
- Care-of-Address（CoA; 気付アドレス）とホーム アドレス、NAI、およびセキュリティ キーとのアソシエーション、そのアソシエーションのライフタイムを含めた、各登録 MS に対応するバインディング情報を維持します。
- モバイル IP 登録 ライフタイム タイマーの範囲内での、（モバイル IP の場合、FA を介して）MS から、または（プロキシ モバイル IP の場合）FA から送信された登録更新要求を受信して処理します。
- （モバイル IP の場合、FA を介して）MS から、または（プロキシ モバイル IP の場合）FA から送信された登録解除要求を受信して処理します。
- ローカルに保管された、または外部ソースから取得したサブスクライバ データベースを維持します。
- 適切に設定されている場合、ハンドオフ条件下で送信元 PDSN にバインディング アップデートを送信します。
- ダイナミック HA 割り当てをサポートします。

サポートされなくなった機能

Home Agent Release 5.0 以上では、次の機能はサポートされません。

- MIP/L2TP Access Concentrator（LAC）（PPP 再生成）のサポート
- On-Demand Address Pool（ODAP）

HA

HA は、モバイル ユーザ登録を維持し、モバイル宛てのパケットを PDSN/FA にトンネリングします。HA はリバース トンネリングをサポートし、IPSec を使用して PDSN にパケットを安全確実にトンネリングできます。ブロードキャスト パケットはトンネリングされません。HA はさらに、モバイルへのダイナミック ホーム アドレス割り当てを実行します。ホーム アドレスは、ローカルに設定されたアドレス プールから割り当てることも、DHCP サーバ アクセスによって、または AAA サーバから割り当てることもできます。

Cisco Mobile Wireless HA は、プロキシ モバイル IP 機能をサポートし、Cisco 7600 シリーズ ルータ プラットフォーム上で利用できます。

Cisco 7600 シリーズ ルータを使用し、2 台の SAMI カードに 6 つのアクティブ HA イメージと 6 つのスタンバイ イメージを格納した Cisco HA は、上記の 6 倍の数字をサポートします。

HA の設定作業に関連するモバイル IP の詳細については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.htm

CHAPTER 2

Home Agent（HA）の設定プランニング

この章では、Cisco Mobile Wireless Home Agent を設定する前に理解しておく必要のあることがらについて説明します。

この章は、次の内容で構成されています。

サポート対象プラットフォーム

Cisco Home Agent（HA）は Cisco 7600 シリーズ ルータに搭載する、Cisco Service Application Module for IP（SAMI）プロセッサ ブレード上で使用できます。HA は、これらのプラットフォーム上のファスト イーサネットおよびギガビット イーサネット インターフェイスをサポートします。

SAMI サポート

Cisco Service Application Module for IP（SAMI）のインストールおよび設定方法については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/hw/modules/ps5510/products_installation_and_configuration_guide_book09186a0080875d19.html

前提条件

ここでは、Cisco Mobile Wireless Home Agent をネットワーク内で設定する前に、従うべき一般的な注意事項を示します。

7600 シリーズ ルータ上の HA

プラットフォームの詳細および 7600 シリーズ ルータ上でサポートされるインターフェイスをすべて網羅した一覧については、Cisco.com の次の URL にアクセスしてください。
http://www.cisco.com/en/US/products/hw/routers/ps368/index.html

7600 シリーズ スイッチ上の HA に関してサポートされる設定は、必要な容量、装備するインターフェイス タイプ、IPSec サポートの必要性によって異なります。

Cisco HA をインストールする前に、次の考慮事項を確認してください。

SAMI には、MSFC-3（WS-SUP720）/PFC-3（WS-F6K-PFC3BXL）を搭載した Supervisor Engine 32 または Supervisor Engine-720（WS-SUP720-3BXL）が必要です。詳細については、『Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers』の「Upgrading to a New Software Release」を参照してください。Sup32 および Sun720 には SRB1 以上が必要です。RSP720 には SRC が必要です。

HA 機能を実行するには、Cisco SAMI モジュールが必要です。SAMI モジュールごとに、6 つの HA イメージ（6 つの HA インスタンス）をサポートします。

IPSec をサポートするには、Catalyst プラットフォーム対応の IPSec VPN アクセラレータ（VPNSPA）が 7600 シャーシごとに 1 つずつ必要です。

設定作業

ここでは、Cisco HA の設定手順について説明します。プラットフォーム番号で各イメージを示します。

- c7svcsamifeature-mz HA イメージ

SAMI ソフトウェアのアップグレード

SAMI はオペレーティング システム ソフトウェアとともに、納品時にはすでにロードされています。しかし、新しいソフトウェア バージョンが利用可能になった時点で、新機能や不具合の修正を利用するために SAMI をアップグレードできます。

SAMI ソフトウェア（イメージ 名は c7svcsamifeature-mz）は、ベース カードおよびドーター カード コンポーネント用のイメージからなるイメージ バンドルです。

バンドル内のイメージごとに、専用のバージョン番号およびリリース番号が与えられています。特権 EXEC コマンド upgrade hw-module を使用してアップグレードを開始すると、バンドルのバージョンおよびリリース番号と現在動作しているバージョンが比較されます。バージョンが異なる場合は、イメージが自動的にアップグレードされます。

（注）　show module コマンドによって表示されるのは、LCP イメージのソフトウェア バージョンであり、SAMI バンドル全体のバージョンではありません。

SAMI イメージをアップグレードする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Sup> enable`	特権 EXEC モードを開始します。
ステップ 2	`Sup# upgrade hw-module slot slot_num software file` *url/file-name*	指定された URL からコンパクト フラッシュにバンドル イメージをコピーします。
ステップ 3	`Sup# hw-module module` *slot_num reset*	電源を切断してから再投入することによって、モジュールをリセットします。新しいイメージを使用して SAMI がリセットされます。
ステップ 4	`Sup# show upgrade software progress`	実行中のアップグレードの状況が表示されます。
ステップ 5	`Sup# show module` *slot_num*	リセット後に SAMI カードが正しくアップすることを確認します。SAMI のステータスは "OK" です。

次に、**show module** コマンドの例を示します。

```
sup#show module 2
Mod Ports Card Type Model Serial No.
--- ----- -------------------------------------- ------------------ -----------
2 1 SAMI Module (h2ik9s) WS-SVC-SAMI-BB-K9 SAD121202UK

Mod MAC addresses Hw Fw Sw Status
--- ---------------------------------- ------------ ----------- -------
2 001f.6c89.0dca to 001f.6c89.0dd1 2.2 8.7(0.22)FW1 12.4(2009020 Ok

Mod Sub-Module Model Serial Hw Status
---- --------------------------- ------------------ ----------- ------- -------
2 SAMI Daughterboard 1 SAMI-DC-BB SAD121204DZ 1.1 Ok
2 SAMI Daughterboard 2 SAMI-DC-BB SAD121204CL 1.1 Ok

Mod Online Diag Status
---- -------------------
2 Pass
```

設定例

Cisco 7600 シャーシのスロット 2 に搭載された SAMI のイメージをアップグレードする場合は、次のコマンドを入力します。

```
Sup>
Sup> enable
Sup# upgrade hw-module slot 2 software file
tftp://10.1.1.1/c7svcsami-h1is-ms
Loading c7svcsami-h1is-ms from <TFTP SERVER IPADDRESS> (via Vlan10):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 34940891 bytes]
Sup# hw-module module 2 reset
Proceed with reload of module?[confirm]
% reset issued for module 2
Sup#
Apr 18 17:53:16.149 EDT: SP: The PC in slot 2 is shutting down. Please wait ...
Apr 18 17:53:33.713 EDT: SP: PC shutdown completed for module 2
```

```
000151: Apr 18 17:53:33.713 EDT: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off
(Reset)
000152: Apr 18 17:57:52.033 EDT: %MLS_RATE-4-DISABLING: The Layer2 Rate Limiters have been
disabled.
000153: Apr 18 17:57:51.513 EDT: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimal
Diagnostics...
000154: Apr 18 17:57:51.537 EDT: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
000155: Apr 18 17:57:52.073 EDT: %OIR-SP-6-INSCARD: SAMI inserted in slot 2, interfaces
are now online
000156: Apr 18 17:57:59.589 EDT: %SVCLC-5-FWTRUNK: Firewalled VLANs configured on trunks
Sup#
```

ユーザの移行

Cisco 7200 および MWAM 上で HA ソフトウェアのサポートが終了したので、ここでは Cisco 7200 または MWAM 上の旧リリース（R3.1 以前）から SAMI プラットフォーム上の Home Agent Release 4.0 以降に移行するパスを示します。

複数の移行シナリオが可能です。

表 2-1　移行シナリオ

	HA R3.0 以前	HA R3.1 以前	HA R4.0 以降
プラットフォーム	NPE400/NPE-G1	MWAM	SAMI
シャーシ/電源モジュール、ファン トレイ	7200VXR	SUP 冗長構成 /Server Load Balancing（SLB; サーバ ロード バランシング）	SUP 冗長構成 /SLB
		SUP IOS SX ベース	SUP IOS SRB ベース
		SUP2/SUP720/SUP32	SUP720/RSP720
		6500/7600	7600

当然、さまざまな移行シナリオが存在します。通常、同じ（1 つまたは複数の）冗長または非冗長 HA を共有する外部エージェントが多数あります。モバイル IP フローは、スタティックに設定されたモバイル デバイス、FA のコンフィギュレーション、または authentication, authorization, and accounting（AAA; 認証、認可、アカウンティング）サーバで定義されたユーザ プロファイルから HA アドレスを取得します。HA SLB の場合は、SLB サーバが実 HA アドレスを提供します。

実際の移行パスは、カスタマーごとにエンドツーエンドの配置に基づいて決定する必要があります。したがって、移行をきちんと計画し、ネットワークを再設計（IP アドレス スキームの設計変更、ルーティング プロトコルの設定、FA と HA 間のネットワーク接続の設定、HA と AAA サーバ間のアプリケーション接続の設定、新しい SAMI HA でのルーティングの設定など）する機会が得られるようにする必要があります。移行は、メンテナンス ウィンドウで実行することを推奨します。たとえば、モバイル デバイスが HA の IP アドレスを使用してスタティックに設定されている場合、使用環境内で移行を十分テストする必要があります。MS/FA を認識するように HA の IP アドレスを変更するには、大がかりなネットワーク サービス プロビジョニングが必要です。

表 2-2 に、移行パスをいくつか示します。

表 2-2　Cisco SAMI ブレード上の Cisco Mobile Wireless Home Agent 移行シナリオ

シナリオ	移行元	移行先	説明
1	非冗長 非 SLB 7200VXR/NPE-G1 × 1	非冗長 非 SLB SUP720/SAMI × 1	ハードウェアとソフトウェアの両方で相当な設定変更
2	非冗長 非 SLB 複数の 7200VXR/NPE-G1	非冗長 SLB 対応 SUP720/SAMI × 1	ハードウェアとソフトウェアの両方で相当な設定変更
3	冗長 非 SLB 7200VXR/NPE-G1 × 2	冗長 非 SLB SUB720/冗長 SAMI × 2（単一シャーシ）	相当な設定変更（ハードウェアおよびソフトウェア）
4	7600/冗長 SUP2 HA-SLB 対応 冗長 MWAM （単一シャーシ）	7600/冗長 SUP720 HA-SLB 対応 冗長 SAMI （単一シャーシ）	ハードウェアとソフトウェアで大量の設定変更（SUP2 から SUP720、シャーシ全体のリセット）
5	7600/冗長 SUP720 HA-SLB 対応 冗長 MWAM（単一シャーシ） SUP IOS SXF	7600/冗長 SUP720 HA-SLB 対応 冗長 SAMI （同じ単一シャーシ） SUP IOS SRB	ハードウェアとソフトウェアで最小限の設定変更 SXF から SUP 用の SRB リリースに変更するには、シャーシのリセットが必要
6	7600/冗長 SUP720 HA-SLB 対応 冗長 MWAM（二重シャーシ） SUP IOS SXF	7600/冗長 SUP72 HA-SLB 対応 冗長 SAMI （二重シャーシ） SUP IOS SRB	ハードウェアとソフトウェアで最小限の設定変更

機能の互換性およびシームレスな移行

移行とは、単に MWAM モジュールを SAMI モジュールに置き換えるだけではありません。既存のモバイル サブスクライバのサービス接続に与える影響が最小限ですむように、きちんと考えて実行する必要があります。

HA リリース 4.0 以降上に冗長性の下位互換性がない場合、HA-SLB をイネーブルにして、サービス停止が回避されるように設定できますが、それには余分なネットワーク設定とプロビジョニングが必要です。HA R4.0 上に冗長性の下位互換性がある場合、ネットワーク設定とプロビジョニングは最小限になります。

表 2-3 に、SAMI プラットフォームへの移行に必要な手順を示します。使用できる移行シナリオのそれぞれについて検討します。

表 2-3　表 2-2 の移行シナリオに対応する移行手順

シナリオ	移行手順
1	• SAMI が搭載された Cisco 7600/SUP720 に HA をインストールして設定します。 • 新たに追加された SAMI ベースの HA を使用するように、MS および FA をプロビジョニングします。これは、きわめて大がかりな作業になる可能性があります。 • 大量のプロビジョニング作業の代わりに、SAMI HA は 7200 NPE-G1 ベースの HA IP アドレスおよびルーティング方式を再利用できます（メンテナンス ウィンドウで行い、サービスを中断することが前提）。
2	• SAMI および SLB 対応の Cisco 7600/SUP720 に HA をインストールして設定します。SUP720 SRB リリースで HA SLB をテストする必要があります。 • 新たに追加された SAMI ベースの HA を使用するように、MS および FA をプロビジョニングします。これは、きわめて大がかりなプロビジョニング作業になる可能性があります。
3	• SAMI が搭載された Cisco 7600/SUP720 に HA をインストールして設定し、7200 ベースの HA で設定したのと同じ HSRP 冗長グループに組み込みます。 • SAMI ベースの HA の方がプライオリティと HSRP プリエンプションが高くなるように設定します。 **（注）** SAMI HA R4.0 は冗長性に関して、下位互換性が得られない場合があります。 – HA R4.0 には、ルールベース ホットライニングなどのバインディング単位の機能、Quality of Service（QoS; サービス品質）、ホスト拡張アトリビュートがあります。バインディング単位の機能は、プロファイルベースのホットライニングにも適用可能です。R3.1 またはそれ以前のバインディング単位の情報に比べ、実質的にバインディング単位の情報が増えることになります。Release 3.x から R4.0 に、バインディングが同期するかどうかについては、まだテストされていません。これまでのところ、バインディング情報は、HA R3.x のアクティブ HA とスタンバイ HA 間で同期する唯一の情報です。 – HA R4.0 のハイ アベイラビリティが L2 HSRP ベースではなく、L3 ベースの場合、HA R3.x と HA R4.0 間で、ステートフルな冗長性の互換性はありません。その場合、この冗長性の設定は 2 つのリリース間でかなり大幅に異なります。 – HA R4.0 はバッチ モードで bulk-sync を行いますが、HA R3.x の同期はバインディング単位です。 • これが理想的です。また、メンテナンス ウィンドウで行う必要はありません。
4	• 単一シャーシの場合、SUP2 から SUP720 への変更はかなりの作業になります。シャーシ全体をリセットするので、すべてのサービス モジュール（MWAM、SAMI など）もリセットすることになります。 • この移行は、メンテナンス ウィンドウの間に実行する必要があります。そうしないと、サービスが停止します。 • HA-SLB の確認が必要です。

表 2-3　表 2-2 の移行シナリオに対応する移行手順 （続き）

シナリオ	移行手順
5	• 単一シャーシの場合、SUP720 SXF から SUP720 SRB への変更は、シャーシ全体のリセットを伴います。したがって、すべてのサービス モジュール（MWAM、SAMI など）もリセットされます。 • この移行は、メンテナンス ウィンドウの中で実行する必要があります。 • その後、同一シャーシの両方の SUP720 で SRB リリースを実行します。 • SAMI をサポートするように SUP720 を設定します。 **1.** MWAM のコンフィギュレーションが SUP720 のブートフラッシュに保存されていることを確認します。 **2.** SUP720 上で SAMI VLAN グループ用の VLAN を MWAM として設定します。 **3.** MWAM プロセッサ コンフィギュレーションから取得した SAMI PPC コンフィギュレーションが SUP720 ブートフラッシュの SAMI コンフィギュレーション ファイルのネーミング規則に従っているかどうかを確認します。 **4.** スタンバイ MWAM の電源を切り、引き出します。 **5.** 同じスロットに SAMI ブレードを挿入し、有効な HA R4.0 イメージでブートします。 **6.** MWAM HA の実行 IOS コンフィギュレーションは 5 つですが、SAMI には 6 つの PPC があります。したがって、SAMI 上の PPC の 1 つを未使用にするか、または単独で設定する必要があります。 **7.** SAMI PPC に適切なコンフィギュレーションが与えられていることを確認します。 **8.** HA のバインディング同期とステートフルな冗長性は、3 番のシナリオと同じ状況になります。 • アクティブ MWAM を切断して取り外し、第 2 SAMI ブレードを搭載します。 • HA-SLB が動作するかどうかを確認します。 HA の冗長性がリリースにまたがって機能しない場合は、（SAMI HSRP 上でさらに設定して）次の作業を実行します。 • 両方の SAMI を挿入し、冗長モードで設定して、インサービス モードで SLB サーバに追加します。 • SLB サーバ ファームで MWAM をアウトオブサービスにします。 • MWAM 上のすべての MS 接続が完了するまで待機します。 • MWAM をシャットダウンして取り外します。

表 2-3　表 2-2 の移行シナリオに対応する移行手順 （続き）

シナリオ	移行手順
6	• シャーシ 1 を SUP720 SXF から SUP720 SRB にアップグレードします。 • SAMI ブレードをサポートするようにシャーシ 1 を設定します。 – MWAM のコンフィギュレーションが SUP720 のブートフラッシュに保存されていることを確認します。 – SUP720 上で SAMI VLAN グループ用の VLAN を MWAM と同じに設定します。 – MWAM プロセッサ コンフィギュレーションから取得した SAMI PPC コンフィギュレーションが SUP720 ブートフラッシュの SAMI コンフィギュレーション ファイルのネーミング規則に従っているかどうかを確認します。 – シャーシ 1 の MWAM の電源を切り、引き出します。 – 同じスロットに SAMI を挿入し、有効な HA R4.0 イメージでブートします。 – MWAM HA では 5 つの IOS が実行しているので、コンフィギュレーションは 5 つですが、SAMI には 6 つの PPC があります。したがって、SAMI の PPC の 1 つを未使用にするか、または単独で設定する必要があります。 – SAMI PPC に適切なコンフィギュレーションが与えられていることを確認します。 – HA のバインディング同期とステートフルな冗長性は、3 番のシナリオと同じ状況になります。 HA の冗長性がリリースにまたがって機能しない場合は、次の作業を実行します（SAMI HSRP のコンフィギュレーションを変更する必要があります)。 • シャーシ 1 の SAMI HA をインサービス モードで SLB サーバに追加します。 • SLB サーバ ファームでシャーシ 2 の MWAM をアウトオブサービスにします。 • MWAM 上のすべての MS 接続が終了するまで待機し、シャーシ 2 の第 2 項を繰り返します。

SAMI の移行に関する警告および制約事項

- HA のステートフルな冗長性は、リリースにまたがって機能しない場合があります。たとえば、R3.0 リリースのバインディング情報は、R4.0 リリースで R3.0 ベースの機能だけが設定されている場合でも、R4.0 と同じではありません。
- 基本の HSRP がリリースによって異なる場合があります。
- 同じプラットフォームでもリリースが異なると、同じ状況で異なるシステム動作になる場合があります。したがって、一貫して同じ動作を確保するには、追加設定が必要です。
- 徹底的なテストを行わない場合、これらの手順は推奨できません。
- MWAM プラットフォームをサポートするのは、SUP IOS SRB リリースです。

必要な基本設定

HA を設定するには通常、3 方向でインターフェイスを定義する必要があります。PDSN/FA、ホーム ネットワーク、および AAA サーバです。HA の冗長性が必要な場合は、HA 間の HSRP バインディング アップデート用に、もう 1 つインターフェイスを設定する必要があります。SAMI 上で HA を動作させた場合、HA は Catalyst 7600 バックプレーンに接続する 1 つの GE ポートへのアクセスを調べます。必要なネットワーク アクセスごとにサブインターフェイスを用意し、トランク ポートとしてこのポートを設定できます。

次の各インターフェイスに対応する VLAN を定義できます。PDSN/FA、ホーム ネットワーク、および AAA です。同じ 7600 シャーシに複数の HA インスタンスが存在する場合、そのすべてに同じ VLAN を使用できます。

次に、Cisco Mobile Wireless Home Agent に必要な基本設定について説明します。

- 「SAMI モジュールに関するスーパーバイザの基本的な IOS コンフィギュレーション」（P.2-9）
- 「HA 環境における AAA の設定」（P.2-10）
- 「HA 環境における RADIUS の設定」（P.2-10）
- 「設定例」（P.2-11）

SAMI モジュールに関するスーパーバイザの基本的な IOS コンフィギュレーション

SAMI モジュールを認識するようにスーパーバイザ エンジンを設定し、バックプレーンとの物理接続を確立するには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	`sup-7602(config)#vlan 3`	イーサネット VLAN を追加します。VLAN コンフィギュレーション サブモードを開始します。
ステップ 2	`sup-7602(config-vlan)#exit`	VLAN データベースをアップデートし、管理ドメイン全域に伝達して、特権 EXEC モードに戻ります。
ステップ 3	`sup-7602(config)#interface vlan 3`	
ステップ 4	`sup-7602(config-if)# ip address 3.3.3.25 255.255.255.0`	
ステップ 5	`sup-7602(config)#vlan 30`	
ステップ 6	`sup-7602(config-vlan)#exit`	
ステップ 7	`sup-7602(config)#interface vlan 30`	
ステップ 8	`sup-7602(config-if)# ip address 30.0.0.25 255.0.0.0`	
ステップ 9	`sup-7602#svclc vlan-group 1 3`	
ステップ 10	`sup-7602#svclc vlan-group 2 30`	
ステップ 11	`sup-7602#svclc module 8 vlan-group 1,2`	

SAMI コンフィギュレーションの詳細については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/hw/modules/ps5510/products_installation_and_configuration_guide_book09186a0080875d19.html

（注）　SAMI モジュールは、スーパーバイザ エンジンのクロック タイマーに基づいて、タイミング機能を同期させます。個々の SAMI ではタイマーを設定しないでください。

HA 環境における AAA の設定

アクセス コントロールは、ネットワーク サーバへのアクセスをだれに許可し、どのサービスを使用させるかを管理する手段です。AAA ネットワーク セキュリティ サービスは、ルータまたはアクセス サーバ上でアクセス コントロールを設定するための基本的なフレームワークを提供します。AAA 設定オプションの詳細については、『*Cisco IOS Security Configuration Guide*』の「Configuring Authentication」および「Configuring Accounting」を参照してください。

HA 環境で AAA を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# aaa new model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 1	`Router(config)# aaa authentication ppp default group radius`	Remote Authentication Dial-In User Service（RADIUS）による PPP ユーザの認証をイネーブルにします。
ステップ 2	`Router(config)# aaa authorization network default group radius`	ユーザのネットワーク アクセスを制限します。ネットワークに関連するあらゆるサービス要求に認可を実行します。デフォルトの認可方式として、group radius 認可方式を使用します。

HA 環境における RADIUS の設定

RADIUS は、ネットワークでの AAA 情報の交換を定義する 1 つの方法です。シスコの実装では、RADIUS クライアントはシスコのルータ上で動作し、あらゆるユーザ認証およびネットワーク サービス アクセス情報が登録されている RADIUS サーバに、認証要求を送信します。RADIUS 設定オプションの詳細については、『*Cisco IOS Security Configuration Guide*』の「Configuring RADIUS」を参照してください。

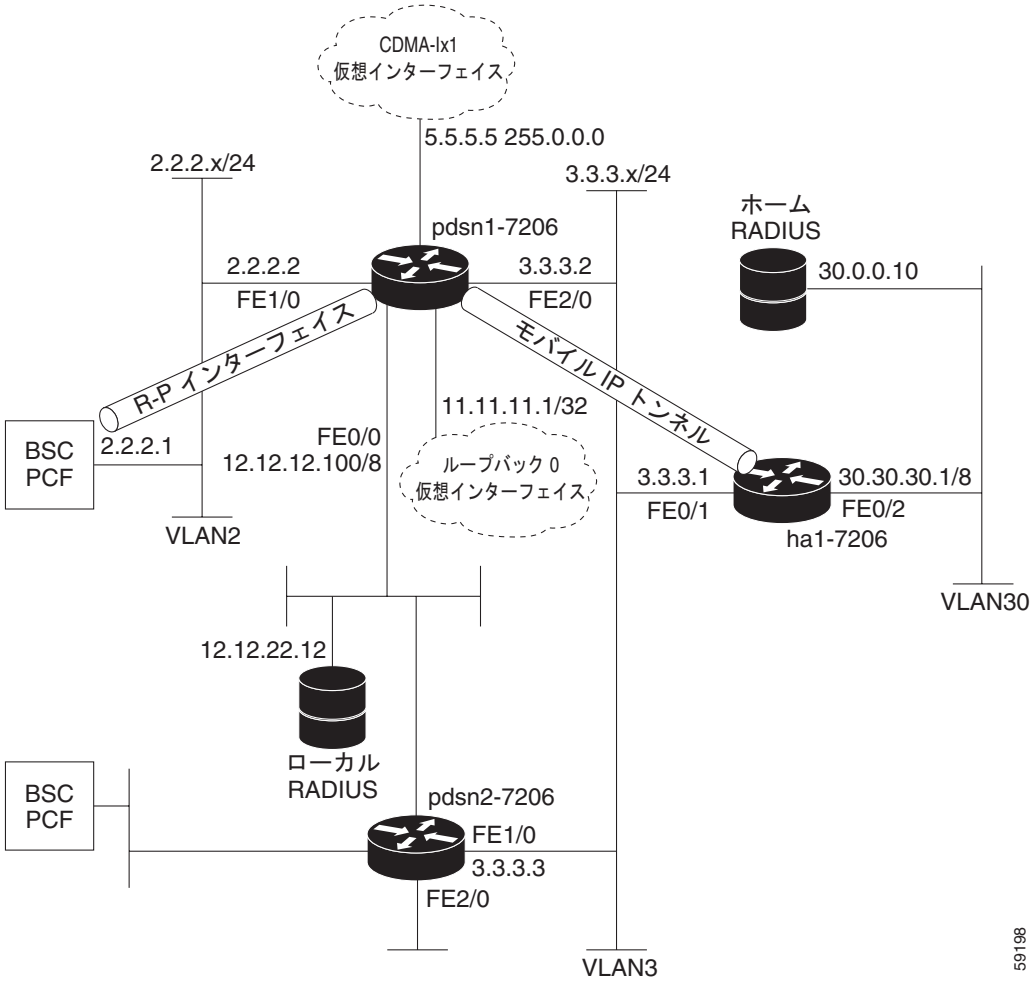
HA 環境で RADIUS を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# radius-server host` *ip-addr* `key` *sharedsecret*	RADIUS サーバ ホストの IP アドレスを指定し、ルータと RADIUS サーバ間で使用する共有秘密文字列を指定します。

設定例

図 1 およびそれに続く情報は、Cisco HA の配置と設定の例です。

図 1　　HA：ネットワーク マップ



例 1　　HA の設定

```
Cisco_HA#sh run
Building configuration...
Current configuration : 4532 bytes
!
version 12.2
no parser cache
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers
!
```

```
hostname ha1
!
aaa new-model
!
!
aaa authentication login default group radius
aaa authentication login CONSOLE none
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
username simulator password 0 cisco
username userc-moip password 0 cisco
username pdsn password 0 cisco
username userc password 0 cisco
username USER_PDSN
ip subnet-zero
ip cef
!
!
no ip domain-lookup
!
! !
!
interface GigabitEthernet0/0.3
description To FA/PDSN
encapsulation dot1Q 3
ip address 3.3.3.1 255.255.255.0
!
interface GigabitEthernet0/0.30
description To AAA
encapsulation dot1Q 30
ip address 30.30.30.1 255.255.255.0
!
router mobile
!
ip local pool ha-pool1 10.35.35.1 35.35.35.254
ip mobile home-agent broadcast
ip mobile virtual-network 10.35.35.0 255.255.255.0
ip mobile host nai @xyz.com address pool local ha-pool1 virtual-network 10.35.35.0
255.255.255.0 aaa load-sa lifetime 65535
!
radius-server host 30.0.0.10 auth-port 1645 acct-port 1646 key cisco
!
!
mgcp profile default
!
dial-peer cor custom
!
!
gatekeeper
shutdown
!
!

line con 0
exec-timeout 0 0
login authentication CONSOLE
```

制約事項

同時バインディング

Cisco HA は、同時バインディングをサポートしていません。同じ Network Access Identifier（NAI; ネットワーク アクセス識別子）に複数のフローが確立されると、各フローに異なる IP アドレスが割り当てられます。つまり、同時バインディングは不要です。同時バインディングは、同じ IP アドレスへの複数のフローを維持する場合に使用されるからです。

セキュリティ

HA は、IS-835-B の要件に基づいて、IPSec、IKE、IPSec Authentication Header（AH; 認証ヘッダー）、および IP Encapsulating Security Payload（ESP）をサポートしています。HA は、制御トラフィック用またはユーザ トラフィック用の個別のセキュリティはサポートしていません。両方のセキュリティを有効にするか無効にするかのどちらかです。

HA は、IS-835-B に定義されているダイナミックな鍵の割り当て、または共有秘密はサポートしていません。

サポート対象の規格、management information base（MIB; 管理情報ベース）、および Request For Comments（RFC; コメント要求）

RFC

Cisco IOS Mobile Wireless Home Agent Release 3.0 がサポートする RFC は、次のとおりです。

- IPv4 Mobility（IPv4 モバイル性）、RFC 2002
- IP Encapsulation within IP（IP 内 IP カプセル化）、RFC 2003
- Applicability Statement for IP Mobility Support（IP モバイル サポートの適用可能ステートメント）、RFC 2005
- The Definitions of Managed Objects for IP Mobility Support Using SMIv2（SMIv2 を使用する IP モバイル サポートの管理対象オブジェクト定義）、RFC 2006
- Reverse Tunneling for Mobile IP（モバイル IP のリバース トンネリング）、RFC 3024
- Mobile IPv4 Challenge/Response Extensions （モバイル IPv4 チャレンジ / レスポンス機能拡張）、RFC 3012
- Mobile NAI Extension（モバイル NAI 拡張機能）、RFC 2794
- Generic Routing Encapsulation（総称ルーティング カプセル化）、RFC 1701
- GRE Key and Sequence Number Extensions（GRE 鍵およびシーケンス番号機能拡張）、RFC 2890
- IP Mobility Support for IPv4（IPv4 の IP モバイル サポート）、RFC 3220、Section 3.2 認証
- The Network Access Identifier（ネットワーク アクセス識別子）、RFC 2486、1999 年 1 月
- An Ethernet Address Resolution Protocol（イーサネット アドレス解決プロトコル）、RFC 826、1982 年 11 月
- The Internet Key Exchange (IKE)（インターネット キー エクスチェンジ）、RFC 2409、1998 年 11 月
- Cisco Hot Standby Routing Protocol (HSRP)（Cisco ホット スタンバイ ルーティング プロトコル）、RFC 2281、1998 年 3 月

規格

Cisco IOS Mobile Wireless Home Agent Release 4.0 がサポートする規格は、次のとおりです。

- TIA/EIA/IS-835-B、TIA/EIA/IS-835-C、および TIA/EIA/IS-835-D

MIB

Cisco IOS Mobile Wireless Home Agent Release 4.0 がサポートする MIB は、次のとおりです。

- CISCO- MOBILE-IP-MIB：拡張管理機能を提供
- Radius MIB：RADIUS 認証クライアント MIB（RFC 2618、1999 年 6 月）で定義

HA はプロトコル スイート RFC 1901 ～ RFC 1908 で規定された SNMPv2 を実装します。HA は、SMIv2 を使用する IP モバイル サポートの管理対象オブジェクト定義（RFC 2006、1995 年 10 月）で定義された MIB をサポートします。

Cisco 7600 プラットフォームでサポートされる MIB の全リストは、Cisco Web にあります。次の URL にアクセスしてください。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

MIB で維持されるセッション カウンタは、SNMP または CLI ではリセットできません。HA CPU カウンタおよびメモリ使用率カウンタには、CISCO-PROCESS-MIB を使用してアクセスできます。

Release 3.0 の MIB では、さらに次のカウンタがサポートされます。

- FA/CoA のバインディング数
- FA/CoA 別の受信登録要求数
- FA/CoA 別障害カウンタ：HA R2.0 はグローバル障害カウンタをサポートします。FA/CoA 別カウンタは、これらのカウンタのそれぞれに追加されます。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 3

単一 IP インフラストラクチャ

この章では、サービス プロバイダーの Home Agent（HA）アプリケーションに対する単一 IP インフラストラクチャおよび管理性の要件に関連する概念について説明します。このアプリケーションは、Cisco 7600 スイッチの Service Application Module for IP（SAMI）サービス ブレードに常駐する、Mobile Services Exchange Framework（mSEF; モバイル サービス エクスチェンジ フレームワーク）製品ファミリの一部です。ここでは、この機能の設定方法についても説明します。

この章は、次の内容で構成されています。

単一 IP 機能の概要

現行の mSEF SAMI のゲートウェイ ソリューション（Cisco Mobile Wireless Home Agent、WiMax BWG、Cisco GGSN、および PDSN）はすべて multiple-routers-on-a-stick モデルを提供していますが、これには担当者の管理性および操作上の問題があります。HA の単一 IP のシステム設計では、ブレード単位で SAMI のゲートウェイを管理できます。これは、ブレードごとに 6 台のプロセッサを搭載する以前のモデルと比べると操作の複雑さが「6 分の 1 に減少」することになります。

単一 IP 機能では、それぞれがコントロール プレーン機能とトラフィック プレーン機能の両方を実行する独立した IOS プロセッサ 6 台を搭載する現行モデルから、IOS プロセッサ 1 台が Control Plane（CP; コントロール プレーン）プロセッサとして、残りの 5 台が Traffic Plane（TP; トラフィック プレーン）プロセッサとして指定されたモデルに、SAMI サービス ブレードの機能が割り当て直されています。

ここでは、シャーシ単位モデルで提供されるその他の対象機能サブセットを説明します。ブレード単位モデルは次の領域に適用されます。

- ネットワーク プロトコルへのアクセス
- 認証/認可の相互作用
- Management Information Base（MIB; 管理情報ベース）を取得するための Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を介したネットワーク管理の相互作用
- サブスクライバごとのダイナミック ゲートウェイ割り当てのベースとして、SNMP を介した「ロード パラメータ」の取得
- 設定、表示、およびデバッグ機能
- ブレードの障害検出とフェールオーバー
- AAA サーバの応答時間判別とアラーム表示

また、シャーシ単位モデルは次の対象機能に適用されます。

- さまざまな出力フィルタリング機能を備えた、シャーシ上のサブスクライバの表示
- シャーシ上の 1 人または複数のサブスクライバのセッション アクティビティの表示
- トラブルシューティングを行うための 1 人または複数の特定サブスクライバに対するサブスクライバのモニタリング（呼トレース）
- シャーシのバルク統計情報の照合、転送、および保存

外部システムによって認識される HA 機能の動作には変更はありません。ブレード上の単一 IP HA のルックアンドフィールは、単一プロセッサ上で実行する Home Agent 4.0 イメージと同じです。

単一 IP インターフェイス

次の機能はブレード単位の単一 IP によって管理されます。

MIP の単一インターフェイス

サービス ブレードは HA の IP アドレスである個別の IP アドレスを提供します。このアドレスは Home Agent Release 4.0 と同じように設定します。この同じ IP アドレスは、Foreign Agent（FA; 外部エージェント）Care-of-Address（CoA; 気付アドレス）かコロケーション CoA かに関係なく、HA と CoA 間のトンネルのエンドポイント アドレスにもなります。この IP アドレスは、コントロール プレーン プロセッサとトラフィック プレーン プロセッサの両方に設定されます。これにより、現行の 6 つではなく、Mobile Node（MN; モバイル ノード）-HA および FA-HA のそれぞれのブレードごとに 1 つのモバイル IP セキュリティ アソシエーションを設定できます。

HA の IP アドレスはループバック アドレスにする必要があり、この同じ IP アドレスが HA と気付アドレス（CoA）の間のトンネルのエンドポイント アドレスにもなります。

サービス ブレードは、ユーザ トラフィックのパケットが適切なトラフィック プレーン プロセッサに送信される、IXP ユーコードでのパケット配信機能を実装しています。コントロール プレーン トラフィックとして識別されたパケットは、コントロール プレーン プロセッサに送信されます。特定の識別情報と一致しないパケットは、コントロール プレーン プロセッサに送信されて処理されます。

設定の単一インターフェイス

サービス ブレードは、ブレード機能を設定する単一ポイントを提供します。つまり、Home Agent Release 4.0 で行っていたのと同じようにサービス ブレードにセッションを確立できます。セッションは、サービス ブレード上のコントロール プロセッサに確立されます。この単一セッションからサービス ブレードに、HA の機能に必要な各コマンドを 1 回実行して機能を設定できます。この設定は同じ設定が必要なすべてのプロセッサに適用され、追加設定作業を行う必要はありません。

IOS コンフィギュレーション コマンドのデフォルト処理では、設定がサービス ブレード上のすべての IOS プロセッサに適用されます。コンフィギュレーション セッションをホスティングするプロセッサ上でだけ実行されるコマンドのセットを定義できます。フィルタリングされたコンフィギュレーション コマンドの例には、Open Shortest Path First（OSPF）および Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）関連のコンフィギュレーション コマンドがあります。

SNMP 管理の単一インターフェイス

サービス ブレードは、SNMP 操作のターゲット アドレスである設定可能な個別 IP アドレスを提供します。この IP アドレスはコントロール プレーン プロセッサでホスティングされます。HA 機能に関連するサービス ブレード上のすべての MIB は、この IP アドレスを使用してアクセスできます。コントロール プレーン プロセッサ以外のプロセッサから必要な情報は、MIB ターゲットに応じてプッシュまたはプルです。

プロセッサ単位で情報を表示する、プロセッサのリソース使用量およびメモリ使用量に関連する MIB が 2 つあります。1 つのプロセッサ リソース MIB 結果が 6 つの個別エントリ（プロセッサごとに 1 つ）で返されます。メモリ使用量に対しても同様です。

トラブルシューティングおよびデバッグの単一インターフェイス

サービス ブレードは、**show** および **debug** コマンドを実行するための単一エントリ ポイント（コントロール プレーン プロセッサへのセッション）を提供します。デフォルトでは、**show** コマンドはコントロール プレーン プロセッサでだけ実行されます。1 つまたは複数のトラフィック プレーン プロセッサで実行する必要がある各コマンドが個別に装備されています。

トラフィック プレーン プロセッサからの追加情報が必要で、ユーザ（Network Access Identifier（NAI）または IP アドレス）ごとに認可されるコマンドの場合は、そのユーザをホスティングするトラフィック プレーン プロセッサが特定され、コマンドがそのプロセッサ上で実行されます。

各プロセッサからの結果は、コマンドに対して応答する前に 1 つの表示にまとめられます。

条件付きデバッグ コマンドでも同じアプローチが使用されます。シャーシ全体の「サブスクライバのデバッグ」機能をサポートするために、識別されたサブスクライバのモバイル IP バインディング登録要求を受信する前に、そのサブスクライバのトリガーを事前に設定しておく必要があります。登録要求を受信すると、要求を受信したプロセッサ以外のすべてのプロセッサの設定済みトリガーは削除できます。

AAA の単一インターフェイス

サービス ブレードは AAA 相互作用の単一 IP アドレスを提供します。Radius ベースと Diameter ベースの両方の相互作用に IP アドレスを 1 つ使用することも、各プロトコルに別個の IP アドレスを使用することもできます。

Radius ベースの認証および認可が実行されるのはコントロール プレーン プロセッサからだけです。

Radius ベースの Change of Authorization および Packet of Disconnect の交換はコントロール プレーンで行われ、その処理が該当するトラフィック プロセッサで開始されます。これらの機能は、Radius ベース アカウンティングのサポートとは関係なく提供されます。

ポリシーをサポートする Diameter ベース 相互作用もコントロール プレーン プロセッサ上に限り実行されます。これは Home Agent Release 5.0 の一部としてサポートされます。

Radius ベースおよび Diameter ベース アカウンティングは、HA のこのリリースの単一 IP ではサポートされません。サービス ブレードのパケット配信機能は、宛先 UDP ポートに基づいて特定のプロセッサに Radius トラフィックを転送しません。

MIP および AAA の単一インターフェイス

単一 IP ベースの HA では、CP は AAA サーバへのインターフェイスを終了します。すべてのサブスクライバの認証は CP によって行われます。ただし、認証だけが行われることに注意してください。

アクティブ/スタンバイ CP から TP への情報を更新するために、CP は IPC メカニズムを使用します。CP は、TP に対して更新を行いながらコントロール メッセージのプロセスを待機します。ここでは、各コントロール プレーン メッセージに対するアプローチについて説明します。

アクティブ HA での手順

次のコントロール メッセージは、アクティブな HA の CP によって処理されます。

- Registration Request（RRQ）：サブスクライバの登録、再登録、および登録解除
- Registration Revocation メッセージ
- Registration Revocation ACK メッセージ
- Change of Authorization（COA）
- Packet of Disconnect（POD; パケット オブ ディスコネクト）

アクティブ HA の CP 上の MN の Registration Request

1. アクティブ HA の CP は RRQ を受信し、MN の認可を行います。CP と AAA サーバの間のインターフェイスは HA 4.0 と同じです。
2. MN の認可が失敗した場合、CP はエラー コードを使用して Registration Reply を FA に送信します。
3. 認可が正常に行われると、バインディング用に IP アドレスが割り当てられます。IP アドレス割り当てのメカニズムは Home Agent 4.0 と同じです。CP はハッシュ テーブルを検索して、割り当てられた MN アドレスに基づいて TP ID を 1 つ取得します。
4. CP は、応答を待たずに IPC 高信頼性メカニズムを使用して対応する TP に対してバインディング情報を更新します。また、UDP/IP を介してスタンバイ HA の CP に対して更新情報を送信し、Registration Reply を使用して FA に応答します。
5. CP が TP からエラー コードなしで確認応答を受信した場合は、CP は何の処理も行いません。
6. タイムアウトや TP から受信した応答が無効なために障害が発生した場合、CP はバインディングを削除します。また、スタンバイ HA に "binddeleterequest" を開始し、HA で登録失効がイネーブルになっている場合は FA に Registration Revocation メッセージを送信します。

次の情報は、バインディング用に CP から TP に更新されます。

- RRQ ヘッダー：RFC 3344 準拠
- 拡張として Mobile-Home Authentication Extension（MHAE）の Security Parameter Index（SPI; セキュリティ パラメータ インデックス）
- NAI 拡張機能
- マルチパス Normal Vendor Specific Extension（NVSE）
- アドレス タイプ CVSE：MN の DHCP アドレス割り当てを示します。
- MR ダイナミック ネットワーク NVSE
- スタティック/ダイナミック プールの名前
- クラス アトリビュート：アカウンティング専用
- Chargeable User Identity（CUI）：アカウンティングおよび WiMAX サブスクライバ専用

- アカウンティング マルチ セッション ID、アカウンティング暫定インターバル：WiMAX サブスクライバ用
- VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）名および対応する HA IP アドレス（存在する場合）
- In ACL および Out ACL の名前
- ホットラインの基本情報
- ホットラインのアカウンティング表示
- NVSE としてホットライン ルール/プロファイル ベースのリスト

アクティブ HA での MN の登録解除

次のコール フローは、アクティブ HA での MN の登録解除を示します。

1. アクティブ HA の CP は登録解除の RRQ を受信し、MN の認可を行います。CP と AAA サーバ間のインターフェイスは HA Release 4.0 と同じです。
2. MN の認可が失敗した場合、CP はエラー コードを使用して Registration Reply を FA に送信します。
3. 認可が正常に行われると、CP は IPC 高信頼性メカニズムを使用して対応する TP にバインディング情報を送信して、バインディングを削除します。登録解除の間は CP は TP からの応答を待機しません。
4. CP は MN アドレスとエラー コード **0** を使用して Registration Reply を送信します。
5. アクティブ HA の CP はそのピアにバインディング削除要求を送信します。

次の情報は、バインディング用に CP から TP に更新されます。

- メッセージ タイプとエラー コード
- MN ホーム アドレス
- HA アドレス
- 気付アドレス

アクティブ HA の Registration Revocation メッセージ

次のコール フローは、アクティブ HA での登録失効の手順を示します。

1. アクティブ HA の CP は Registration Revocation メッセージを受信します。Foreign-Home Authentication Extension（FHAE）に関する解析失敗または認証失敗の場合、CP はエラー コードを使用して Registration Revocation ACK を FA に送信します。
2. CP は IPC 高信頼性メカニズムを使用して対応する TP にバインディング情報を送信して、バインディングを削除します。削除要求の間は CP は TP からの応答を待機しません。
3. アクティブ HA の CP はそのピアにバインディング削除要求を送信します。
4. CP は MN のバインディング情報を削除します。
5. CP は MN アドレスとエラー コード **0** を使用して Registration Revocation ACK を送信します。

次の情報は、バインディング用に CP から TP に更新されます。

- メッセージ タイプとエラー コード
- MN ホーム アドレス
- HA アドレス
- 気付アドレス

アクティブ HA の Registration Revocation ACK

アクティブ HA の CP は、アクティブ HA が送信した対応する Registration Revocation メッセージの Registration Revocation ACK を受信します。CP はバインディング情報を更新するための TP 更新処理は行いませんが、FHAE または 、IP Security（IPSec; IP セキュリティ）認証は完了します。

アクティブ HA で受信された COA

次のコール フローは、アクティブ HA で受信された COA の手順を示します。

1. アクティブ HA の CP は COA を受信し、MN の認可を行います。CP と AAA サーバ間のインターフェイスは、Home Agent Release 4.0 のインターフェイスと同じです。
2. MN の認可が失敗した場合、CP は COA NAK エラー コードを AAA サーバに送信します。
3. AAA サーバに対してホットライン情報を解析する間に障害が発生した場合、CP は COA NAK を送信します。CP は TP または スタンバイ HA に対して情報を更新しません。
4. CP は、応答を待たずに IPC 高信頼性メカニズムを使用して対応する TP に暫定更新情報を送信します。また、UDP/IP を介してスタンバイ HA の CP に暫定更新情報を送信し、COA ACK を使用して AAA に応答します。
5. CP が TP からエラー コードなしで確認応答を受信した場合は、CP はそれ以上の処理を行いません。
6. タイムアウトや TP から受信した応答が無効なために障害が発生した場合、CP はバインディングを削除し、スタンバイ HA に "binddeleterequest" を開始します。HA で登録失効がイネーブルになっている場合は、Registration Revocation メッセージが FA に送信されます。

次の情報は、バインディング用に CP から TP に更新されます。

- MN アドレス
- HA IP アドレス
- ホットラインの基本情報
- ホットラインのアカウンティング表示
- NVSE としてホットライン ルール/プロファイルのリスト

アクティブ HA で受信された POD

次のコール フローは、POD がアクティブ HA で受信されたときの手順を示します。

1. アクティブ HA の CP は POD を受信し、MN の認可を行います。CP と AAA サーバ間のインターフェイスは、Home Agent 4.0 のインターフェイスと同じです。
2. MN の認可が失敗した場合、CP は POD NAK エラー コードを AAA サーバに送信します。
3. CP は MN アドレスの Registration Revocation メッセージを作成し、対応する気付アドレスに送信します。
4. CP は IPC 高信頼性メカニズムを使用して対応する TP にバインディング情報を送信して、バインディングを削除します。削除要求の間は CP は TP からの応答を待機しません。
5. アクティブ HA の CP はそのピアにバインディング削除要求を送信します。
6. CP は MN のバインディング情報を削除します。
7. CP は、MN アドレスとエラー コード **0** を使用した Registration Revocation ACK を受信するまで待機します。応答を受信する前にタイムアウトになった場合は、HA は PDSN に対して Registration Revocation を使用して再試行します。

スタンバイ HA 上の手順

スタンバイ HA の CP は、アクティブ/スタンバイ同期の次の 2 つの場合にトラフィック プロセッサを更新します。

- ダイナミック同期
- バルク同期

ダイナミック同期中にスタンバイ HA の CP で受信された BindUpdateRequest

次のコール フローは、MN の登録/再登録用にアクティブ HA が送信する "BindUpdate Request" をスタンバイ HA が処理する方法を示します。

1. スタンバイ CP はアクティブ CP から "BindUpdateRequest" を受信し、MN の認可を行います。これにより、受信された "BindUpdateRequest" が検証されます。
2. アクティブ HA/スタンバイ HA 間で HHAE 認証が失敗した場合、スタンバイ CP は有限エラー コードを使用して "BindUpdate ACK" を送信します。
3. 認証が正常に行われると、CP は受信したホーム アドレスにバインディングを作成します。また、CP はハッシュ テーブルを検索して、割り当てられた MN アドレスに基づいて TP ID を 1 つ取得します。
4. CP は、応答を待たずに IPC 高信頼性メカニズムを使用して対応する TP に対してバインディング情報を更新します。CP は "bindudpate ack" を使用してアクティブ HA に確認応答します。
5. CP が TP からエラー コードなしで確認応答を受信した場合は、CP は何の処理も行いません。
6. タイムアウトや TP から受信した応答が無効なために障害が発生した場合、CP はスタンバイ HA のバインディングを削除します。スタンバイ HA でバインディングを削除する場合、アクティブ HA のバインディング情報を損なわないようにする必要があります。

次の情報は、バインディング用に CP から TP に更新されます。

- RRQ ヘッダー：RFC 3344 準拠
- 拡張として Mobile-Home Authentication Extension（MHAE）の Security Parameter Index（SPI; セキュリティ パラメータ インデックス）
- NAI 拡張機能
- マルチパス Normal Vendor Specific Extension（NVSE）
- 失効サポート拡張
- アドレス タイプ CVSE：MN の DHCP アドレス割り当てを示します。
- MR ダイナミック ネットワーク NVSE
- スタティック/ダイナミック プールの名前
- クラス アトリビュート：アカウンティング専用
- CUI：アカウンティングおよび WiMAX サブスクライバ用
- アカウンティング マルチセッション ID、アカウンティング暫定インターバル：WiMAX サブスクライバ用
- VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）名および対応する HA IP アドレス（存在する場合）
- In ACL および Out ACL の名前
- ホットラインの基本情報
- ホットラインのアカウンティング表示
- NVSE としてホットライン ルール/プロファイル ベースのリスト

ダイナミック同期中にスタンバイ HA の CP で受信された BindDeleteRequest

次のコール フローは、MN の登録解除 / 失効要求 /POD を受信後にアクティブ HA が送信する "BindDelete Request" をスタンバイ HA が処理する方法を示します。

1. スタンバイ CP はアクティブ CP から "BindDeleteRequest" を受信し、MN の認可を行います。
2. アクティブ HA/ スタンバイ HA 間で HHAE 認証が失敗した場合、スタンバイ CP は有限エラー コードを使用して "BindDelete ACK" を送信します。
3. 認可が正常に行われると、CP は IPC 高信頼性メカニズムを使用して対応する TP にバインディング情報を送信して、バインディングを削除します。削除要求の間は CP は TP からの応答を待機しません。
4. CP は MN アドレスとエラー コード **0** を使用して "BindDelete ACK" をアクティブ HA に送信します。

次の情報は、バインディング用に CP から TP に更新されます。

- メッセージ タイプとエラー コード
- MN ホーム アドレス
- HA アドレス
- 気付アドレス

ダイナミック同期中にスタンバイ HA の CP で受信された BindInterimUpdate

次のコール フローは、ダイナミック同期中にスタンバイ CP が "BindInterimUpdate" メッセージを処理する方法を示します。

1. スタンバイ CP はアクティブ CP から "InterimUpdateRequest" を受信し、MN の認可を行います。
2. アクティブ HA/ スタンバイ HA 間で HHAE 認証が失敗した場合、スタンバイ CP は有限エラー コードを使用して "InterimUpdateAck" を送信します。
3. 認証が正常に行われると、CP は CP 上で作成済みのバインディングに対してホットライニング ルールを使用して暫定更新情報を更新します。
4. CP は、応答を待たずに IPC 高信頼性メカニズムを使用して対応する TP に対してバインディング情報を更新します。CP は、エラー コード **0** の "interimupdate Ack" を使用してアクティブ HA に確認応答します。
5. CP が TP からエラー コードなしで確認応答を受信した場合は、CP は何の処理も行いません。
6. タイムアウトや TP から受信した応答が無効なために障害が発生した場合、CP はスタンバイ HA のバインディングを削除します。スタンバイ HA でバインディングを削除する場合、アクティブ HA のバインディング情報を損なわないようにする必要があります。

次の情報は、バインディング用に CP から TP に更新されます。

- MN アドレス
- HA IP アドレス
- ホットラインの基本情報
- ホットラインのアカウンティング表示
- NVSE としてホットライン ルール / プロファイルのリスト

バルク同期中にスタンバイ HA の CP で受信された BindUpdateRequest

バルク同期中に、アクティブ HA の CP はスタンバイ HA の CP に複数のバインディングのバインディング情報を送信します。スタンバイ HA の CP で各バインディングが正常に作成されると、バインディング情報は応答を待たずに IPC メカニズムを使用して更新されます。

いずれの段階でも、CP-TP 応答メッセージ ステータスがバルク同期メッセージ フローを妨げないようにする必要があります。応答が受信されると、"bindupdaterequest" メッセージ処理がそのバインディングに適用されます。

その他の場合

ホットライン タイマーの期限切れによる MIP セッション終了中は、アクティブ/スタンバイ HA の CP から TP に更新は送信されません。ホットライン タイマーの期限が切れると、バインディング情報はアクティブ/スタンバイ HA の CP/TP で自動的に削除されます。

登録ライフタイムに基づく MIP セッションの期限切れの間は、上記の機能はバインディングにも適用可能です。

フェールオーバーの単一インターフェイス

現在の SAMI 障害モードは可能な場合は常にプロセッサ単位の障害に使用します。単一 IP モデルの場合、ブレードで検出された障害はプロセッサ レベルのフェールオーバーで十分な場合でもブレード レベルのフェールオーバーになります。これには、SAMI プラットフォームにより検出可能な場合はインターフェイス障害も含まれます。これは、このような障害モードに対するプラットフォーム サポートを必要とします。

操作と管理

ここでは、操作と管理に関連する機能について説明します。

アプリケーション関連パラメータのシャーシ全体の MIB

この機能は、すべてのアプリケーション関連パラメータがシャーシ全体で報告される MIB を 1 つ提供します。HA の場合、この機能は HA ごとのインスタンス単位で提供されます。

1 つのサービス ブレード上のすべての HA インスタンスでは、この情報は SNMP Get を使用して単一 IP アドレスで使用できます。この情報は CISCO-MOBILE-IP-MIB および CISCO-IP-LOCAL-POOL-MIB で使用できます。SNMP マネージャは、SNMP GET 操作を必要な回数実行して HA インスタンスごとに MIB を取得する必要があります。このリリースの単一 IP HA 機能は、サービス ブレードごとに HA インスタンスを 1 つサポートします。それによって Get 操作の回数がサービス ブレードごとに 12 回から 2 回に減ります。

シャーシ全体のロードのアプリケーション インスタンス単位での報告

サービス プロバイダー ネットワークは通常、サブスクライバのネットワーク加入時に AAA 機能を使用してサブスクライバの HA を動的に割り当てます。HA 選択基準はサービス プロバイダーによって異なります。サービス プロバイダーは、シャーシ全体ではなく、シャーシ内に設定された各 HA インスタンスのロードの証明を必要とします。このロードは、その HA インスタンス内の IP アドレス プール使用率に基づいています。

この情報は CISCO-IP-LOCAL-POOL-MIB に含まれます。この情報を使用すると、IP アドレス プール使用率にだけ基づいて HA インスタンスを選択できます。MIB には、プールごとおよびプール グループごとの使用中のアドレスおよび空きアドレスの統計情報が含まれます。AAA サーバは、HA インスタンスで設定された IP プールごとおよびプール グループごとにこの情報を使用します。

また、プール使用率のしきい値を超えると生成される SNMP トラップが CISCO-IP-LOCAL-POOL-MIB を取得した同じ SNMP ホストに送信されます。

AAA 無応答に対するトラップ生成

この機能を使用すると、HA は MN の認証時に新しい SNMP トラップ / 通知を NMS サーバに送信して、AAA が無応答であることを通知できます。トラップはタイムアウトになったときに追加されます。ラウンドトリップ遅延にしきい値を設定して（最大応答時間のパーセンテージで設定）、そのしきい値を超えたときのトラップを生成できるようになりました。ラウンドトリップ遅延が 2 つ目のしきい値を下回ると、さらにトラップが生成されます。

各 Remote Authentication Dial-In User Service（RADIUS）サーバに対してしきい値のパーセンテージ値（*normal* または *high*）を設定できます。HA と AAA の間の RADIUS メッセージのラウンドトリップ時間が、設定されているしきい値を上回るか下回ると、AAA サーバの応答 / 無応答を示す通知が NMS サーバに送信されます。同様に、RADIUS 再送信メッセージ数が、設定されているしきい値を上回るか下回ると、AAA サーバの応答 / 無応答を示す SNMP トラップ / メッセージが NMS サーバに送信されます。

RADIUS-CLIENT-AUTHENTICATION-MIB には、AAA アクセスのタイムアウトに関するエントリが含まれます。CISCO-RADIUS-MIB には、トラップが追加されています。

この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# radius-server snmp-trap timeout-threshold normal high`	AAA の無応答を示す SNMP トラップを生成できます。 *normal* は、トラップ生成に使用する標準しきい値（パーセンテージ）です。 *high* は、トラップ生成に使用する上限しきい値（パーセンテージ）です。
ステップ 2	`Router(config)# radius-server snmp-trap retrans-threshold normal high`	このコマンドを設定すると、ラウンドトリップ時間または再送信時間が上限しきい値を超え、標準しきい値を下回ったときにトラップ（SNMP 通知）が生成されます。トラップは、ラウンドトリップ時間または再送信時間のいずれかに対して生成されます。 *normal* は、トラップ生成に使用する標準しきい値（パーセンテージ）です。 *high* は、トラップ生成に使用する上限しきい値（パーセンテージ）です。

（注）　この機能は 7600 の Cisco SAMI カードに限りサポートされます。

RADIUS-CLIENT-AUTHENTICATION-MIB には、AAA アクセスのタイムアウトに関するエントリが含まれます。このタイムアウトが発生したときにトラップが追加されます。また、ラウンドトリップ遅延にしきい値を設定して（最大応答時間のパーセンテージで設定）、そのしきい値を超えたときにトラップを生成することもできます。ラウンドトリップ遅延が 2 つ目のしきい値を下回ると、さらにトラップが生成されます。これにより、トラップを生成するためにある程度の遅延が発生します。

サブスクライバの表示

この機能を使用すると、シャーシ内の単一ポイントから、シャーシの HA インスタンスによってホスティングされるサブスクライバのリストを表示できます。Home Agent Release 5.0 はサービス ブレードごとに 1 つの HA インスタンスをサポートします。そのため、必要な手順は 1 つまたはすべてのサービス ブレードに対する IOS CLI コマンドを使用した必要な情報の要求に制限されます。

HA Named Service は、サービス ブレード上の HA インスタンスに対して IOS **hostname** コマンドを使用して設定された名前に対応しています。

表 3-1 に、この機能のリストを示します。

表 3-1　サブスクライバの表示機能のリスト

All	シャーシ上の全ユーザの一覧	シャーシ上のすべての登録ユーザの合計数を表示するには、コントロール プロセッサで **show ip mobile binding summary** コマンドをアクティブなサービス ブレードごとに 1 回使用します。各ブレードの合計数が合算され、この機能を開始したスーパーバイザに結果が表示されます。 1 つのコマンドで表示可能な最大サブスクライバ数を設定します。この値には 1000 を推奨します。登録サブスクライバ数がこの値を超えると、出力はファイルに保存され、ファイルの名前と場所が表示されます。
Card	1 つのカード/スロット上の全ユーザの一覧	1 つのサービス ブレード上のすべての登録ユーザの合計数を表示するには、**show ip mobile binding summary** コマンドを **total** 行の必要な結果で特定されたサービス ブレードのコントロール プロセッサで 使用します。
CPU	1 つの CPU 上の全ユーザの一覧	サービス ブレードの特定のトラフィック プロセッサ上のすべての登録ユーザの合計数を表示するには、**show ip mobile binding summary** コマンドをサービス ブレードおよびコマンド内で特定された TP で使用します。
Lifetime	ある値に対して MIP ライフタイムが >、<、= の全ユーザの一覧	このオプションは、付与登録ライフタイムによって出力をフィルタリングします。raw 出力は **show ip mobile binding** コマンドを使用して生成されます。これは All、Card、または CPU に対して実行できます。
LifetimeRem	ある値に対して MIP 残りライフタイムが >、<、= の全ユーザの一覧	このオプションは、残り登録ライフタイムによって出力をフィルタリングします。raw 出力は **show ip mobile binding** コマンドを使用して生成されます。これは All、Card、または CPU に対して実行できます。
Connect	ある時間値に対して接続時間が >、<、= の全ユーザの一覧	このオプションでは、サブスクライバが最後に再登録してからの時間ではなく、初めて登録してからの時間が表示されます。

表 3-1　サブスクライバの表示機能のリスト （続き）

FA	特定の FA の IP アドレスの全ユーザの一覧	このオプションは、外部エージェントの IP アドレスによって出力をフィルタリングします。raw 出力は **show ip mobile binding** コマンドを使用して生成できます。これは All、Card、または CPU に対して実行できます。
HA	特定の HA の IP アドレスの全ユーザの一覧	このオプションを使用して、HA IP アドレスに対応する HA インスタンスを判別し、その HA のコントロール プレーン プロセッサ上で **show ip mobile binding** コマンドを設定します。
HA-Name	特定の HA Named Service の全ユーザの一覧	このオプションを使用して、HA 名に対応する HA のコントロール プレーン プロセッサ上で **show ip mobile binding** コマンドを設定します。HA 名はサービス ブレード設定の **hostname** コマンドによって定義されます。
Pool	特定のプール名またはプール グループの全ユーザの一覧	このコマンドの raw 出力は、**show ip local pool** コマンドによって生成されます。このコマンドは、これらのプールの IP アドレス範囲を表示します。これに基づいて、該当する情報を show ip mobile binding コマンドおよび show ip mobile host コマンドを使用して取得できます。
CallType	このコール タイプ（MIP、WiMax、3G、PDIF など）の全ユーザの一覧	このオプションは、アクセスタイプによってフィルタリングします。raw 出力は **show ip mobile binding** コマンドを使用して生成できます。外部エージェントによってサポートされるアクセス タイプは **show ip mobile** コマンドによって決まります。これは All、Card、または CPU に対して実行できます。
NAI/User	この NAI の全ユーザの一覧（NAI でワイルドカードがサポートされている必要があります)。例：ボックス上で Push to Talk ユーザを検索する "show user summary nai *ptt*"	このオプションは、ワイルドカード付き NAI によってフィルタリングします。ネイティブ IOS CLI では、このようなワイルドカードの概念はサポートされていません。raw 出力は "show ip mobile binding" コマンドを使用して生成できます。これは All、Card、または CPU に対して実行できます。
ACL-IN	この入力 ACL が割り当てられた全ユーザの一覧	このオプションは、入力 ACL によってフィルタリングします。raw 出力は **show ip mobile binding** コマンドを使用して生成できます。これは All、Card、または CPU に対して実行できます。
ACL-OUT	この出力 ACL が割り当てられた全ユーザの一覧	このオプションは、出力 ACL によってフィルタリングします。raw 出力は **show ip mobile binding** コマンドを使用して生成できます。これは All、Card、または CPU に対して実行できます。

使用可能な出力表示形式は次のとおりです。

- Summary：合計だけが表示され、ユーザ単位の情報は表示されません。
- Summary Traffic：show ip mobile host コマンドによって出力される ACL ごとのトラフィックの合計、入出力バイト、入出力パケット、入力ドロップ、出力ドロップが追加されます。
- Brief：コマンド フィルタに一致するユーザごとに 1 行の出力。出力は、割り当てられた IP アドレス、NAI、HA IP アドレス、外部エージェント IP アドレス、残り登録ライフタイムで構成されます。
- Brief Traffic：上記 3 つに show ip mobile host コマンドによって出力される ACL ごとのトラフィックの合計、入出力バイト、入出力パケット、入力ドロップ、出力ドロップが追加されます。
- Verbose：show ip mobile binding コマンドと show ip mobile host コマンドの出力を結合したすべての表示。
- Verbose MIP：show ip mobile binding コマンドの出力によって提供されるすべての表示。

summary コマンドの出力には、クエリー オプションと一致するユーザの数が表示されます。また、ACL ごとの入出力バイト、入出力パケット、入出力ドロップなども照合します。

この機能は、HA の OSLER によってサポートされます。詳細については、この章の OSLER の項を参照してください。

この機能は SNMP ではサポートされません。

シャーシ間の設定同期

この機能によって、アクティブ ブレードで実行されたコンフィギュレーション コマンドはパートナー スタンバイ ブレード上で自動的に同期化されます。これは、アクティブ / スタンバイ パートナー モデルの設定に使用するコマンド（**ip mobile home-agent redundancy**）および冗長性の障害検出モードとして HSRP を設定するためのコマンド（**standby**）を除くすべてのコマンドに適用されます。

（注） スタンバイ HA ではコンフィギュレーション コマンドを実行できません。EXEC コマンドは実行できます。

アクティブ HA かスタンバイ HA を判別する方法は、SSO サポートおよびさまざまな mSEF ゲートウェイのセッション冗長性サポートに使用される Redundancy Framework（RF; 冗長フレームワーク）インフラストラクチャに基づいています。

初期化

SSO 設定同期はブートアップ時に自動的に行われ、事前に設定する必要はありません。これは、RF ネゴシエーションの前に冗長装置間の IP 接続が必要なため、HA には適用できません。そのため、アクティブ ブレードおよびスタンバイ ブレードには異なるが関連する設定が必要です。

また、SSO 設定同期機能は各冗長装置の固有の設定をサポートしません。HA では HSRP および RF Interdev プロトコルが必要です。この 2 つのプロトコルには冗長装置の固有の設定が必要です。

各装置の固有の設定が必要な既存コマンドは、同じコマンド内でピア装置の設定に対応するように変更されています。新しいコマンドはピア スロットを識別します。これらのコマンドは解析され、RF ネゴシエーション状態 RF_PROG_STANDBY_CONFIG を使用して自動的に設定同期を開始します。

RF クライアント

SSO 設定同期の場合のように、HA 設定同期も RF クライアントです。設定同期機能は、進行イベントおよびステータス イベントに対してコールバックを RF に登録します。RF は、イベントおよびステータス イベントの進行に伴い、各登録クライアントに順に通知します。これにより、HA はいつ設定ファイルを同期するかを認識します。

設定ファイルおよび同期

ここでは、設定同期機能を構成するスタートアップ コンフィギュレーションおよび実行コンフィギュレーションのプロセスについて簡単に説明します。

スタートアップ コンフィギュレーションは NVRAM にテキスト ファイルとして保存されます。このファイルは、"write memory"、"copy running startup" などの操作を実行すると同期されます。ファイルを書き込み操作用に開いた場合、ファイルを閉じると同期が開始されます。

実行コンフィギュレーションの同期は、ある特定の操作によって動的に行われます。したがって、同期が実行されるときは必ず実行コンフィギュレーションを生成する必要があります。

SSO 実装では、同期プロセスが開始される前にプライマリがロックされます。スタートアップ コンフィギュレーションおよび実行コンフィギュレーションのバルク同期が実行されます。バルク同期が完了すると、パーサー モード同期が実行されます。

両方のプロセッサが同期し、プライマリのロックが解除されると、ライン単位の同期が開始されます。

上記の同期プロセスでは、冗長装置間の通信に転送メカニズムが必要です。現在、各プラットフォームでは IPC またはその他の転送メカニズムが使用されています。

HA 設定同期機能では次の転送メカニズムを使用できます。

- 現在 CP-TP メッセージングに使用されている高信頼性 IPC メカニズム
- IPC メッセージングの RF/CF SCTP ベースのアプローチ
- IPC メッセージングの新しい SCTP ベースのアプローチ

1 つ目は実装の観点からは最速のソリューションですが、シャーシ間ソリューションとしては拡張性が不十分です。現在は 2 つ目のオプション RF/CF SCTP を使用しています。

スタートアップ コンフィギュレーションの同期

SSO 実装では、RF 状態がバルク同期を実行できるようになるとすぐに、スタートアップ コンフィギュレーションがブートアップ時に同期されます。スタートアップ コンフィギュレーションの同期を開始する前に、ルータをロックする必要があります。同じ設計が単一 IP HA 設定同期機能に採用されています。

write memory または **copy** ***file1*** **startup-config** を実行する場合、次の 2 つの方法があります。

- スタートアップ コンフィギュレーション ファイルのバルク同期
- EXEC コマンドのライン単位の同期

SSO 機能には 2 つ目のオプションを使用しますが、Single IP HA では 1 つ目のオプションを使用します。これは、アクティブ装置で設定変更を予備の場所に保存できるためです。

実行コンフィギュレーションの同期

実行コンフィギュレーションの同期では、冗長装置は同じステートの情報を保持します。

まず、セカンダリ装置が RF Interdev 通信を確立した後、実行コンフィギュレーション ファイルがバルク同期されます。バルク同期は、ブートアップ前にアクティブ装置で実行コンフィギュレーションに変更があった場合、スタンバイ装置にセルフ リロードを実行させます。リロード後、スタンバイ装置はアクティブ装置の実行コンフィギュレーションで起動します。

その後、2 台の装置間でライン単位の同期が行われます。各コマンドを設定すると、プライマリ側でコマンドが実行された後で同じコマンドがセカンダリ側に渡されます。

実行コンフィギュレーションのバルク同期は、SSO 実装の RCSF を使用して行われます。Single IP HA 機能でも同じです（RF Interdev SCTP を使用）。

バルク同期

バルク同期を開始する前に、2 台の装置間で RF Interdev 通信を確立する必要があります。各装置はスタートアップ コンフィギュレーションを解析します。これにより、装置はアクティブまたはスタンバイになります。ブートアップ後に実行/プライベート コンフィギュレーションに変更があった場合、アクティブ装置は実行コンフィギュレーション ファイルおよびプライベート コンフィギュレーション ファイルをスタンバイ装置と同期します。バルク同期が実行された後、スタンバイ装置は自身をリロードして変更後の設定で起動します。スタンバイ装置がリロードしている間は、アクティブ装置では設定を行うことはできません。

初期化中に同期する設定は次のとおりです。

- プライベート コンフィギュレーション
- 実行コンフィギュレーション

SUP 内のスタートアップ コンフィギュレーション ファイルは常に同期しているため、スタートアップ コンフィギュレーションは同期されません。

ブートアップ後にプライベート コンフィギュレーションが変更された場合は、アクティブ装置はプライベート コンフィギュレーション ファイルをバッファにコピーし、RF Interdev SCTP を使用してそのファイルをスタンバイ装置に転送します。

ブートアップ後に実行コンフィギュレーションが変更された場合は、アクティブ装置は実行コンフィギュレーション ファイルをバッファにコピーし、RF Interdev SCTP を使用してそのファイルをスタンバイ側に転送します。

これらの手順が完了すると、アクティブ装置は受信したバッファの解析を開始するようにメッセージをスタンバイ装置に送信します。

スタンバイ装置は、受信したバッファの内容をローカルで保存し、変更された設定を適用できるように自身をリロードします。

ライン単位の同期

アクティブ装置とスタンバイ装置の両方がアップ状態で稼動している場合、アクティブ装置から入力されたコマンドが最初に実行され、同じコマンドがスタンバイ装置に伝搬されて実行され、その結果がアクティブ装置に戻されます。

Parser Return Code（PRC）スキームを SSO 実装に使用すると、各コマンドのすべてのパーサー処理ルーチンで戻りコードが設定されます。この戻りコードは、エラー コードのクラス、コンポーネント ID、同期ビット、サブコードなどを含むすべての情報を結合した形式です。

パーサー モード同期は、同期を行うためにコマンドがスタンバイ装置に送信される前にアクティブ装置とスタンバイ装置の間で同じパーサー モードを維持します。

SSO 実装の同期プロセスは RPC を介して実行されます。これは、アクティブ RP がスタンバイ RP から戻りコード メッセージを受信するまで現行プロセスをブロックします。そのため、両方の装置でコマンドが順に実行されます。

スタンバイ装置でコマンドが失敗すると、その結果がアクティブ装置に送られます。アクティブ装置では、ポリシー メーカーのスタブ レジストリが起動して、返された結果をどう処理するかの決定を発信 / 上位レイヤに委ねます。

単一 IP H 設定同期機能では SSO ライン単位同期実装がそのまま使用されます。

設定の詳細

設定はそのまま同期する必要があるため、両装置の CLI は同じである必要があります。次のコマンドは現在各冗長装置に固有で、変更されています。

- **ipc zone default**
- **association** *no>*
- **protocol sctp**
- **unit1-port** *port1*
- **unit1-ip** *ip1*
- **unit2-port** ***port2***
- **unit2-ip** *ip2*

次の新しい CLI が導入されました。

```
interface GigabitEthernet0/0.23
redundancy ip address unit1 <ip1> <mask1> unit2 <ip2> <mask2>
```

redundancy ip address コマンド CLI はインターフェイス単位の CLI です。HSRP プロトコルは、通常の **ip address** コマンドを使用して設定された IP アドレスではなく、ネゴシエーション用に設定されたこの IP アドレスを使用します。**ip address** 設定は、ピアとの HSRP ネゴシエーション専用のサブインターフェイスには必要ありません。

```
redundancy unit1 slot <x> unit2 slot <y>
```

これはグローバル コンフィギュレーションで、ピア スロットの識別に使用されます。

シャーシ間の設定同期を設定するには、次のコマンドを使用します。

router(config)# **redundancy unit1 slot** <x> **unit2** slot *y*

router#(ipc-assoc-protocol-sctp)#**unit1-port** *portnum* , **unit2-port** *portnum*

router(config)#**unit1-ip** *address1* , **unit2**-ip *address2* : それぞれ ipc-unit1-port モードおよび ipc-unit2-port モードで設定します。

redundancy ip address unit1 *address1 mask1* unit2 *address2 mask2* : インターフェイス モードおよびサブインターフェイス モードで設定します。

次の設定手順は各カードで実行する必要があります。

	コマンド	目的
ステップ 1	Router#**show redundancy states**	冗長性コマンドを実行する前に、両方の SAMI で次のコマンドを実行します。**my state** は両方のカードでアクティブにする必要があります。
ステップ 1	Router(config)# **redundancy inter-device** **redundancy** unit1 slot 9 unit2 slot 6 interface GigabitEthernet0/0.2 encapsulation dot1Q 20 **redundancy ip address** unit1 4.0.0.1 255.255.255.0 unit2 4.0.0.2 255.255.255.0 standby 0 ip 4.0.0.4 standby 0 name hsrp	シャーシ間の設定同期をイネーブルにします。 グローバルな冗長装置/スロットのマッピングを設定します。 HSRP のインターフェイスを設定します。 HSRP ではアクティブ装置とスタンバイ装置に一意の IP が必要です。また、**redundancy ip address** コマンドを使用する必要があります。 **（注）** このインターフェイスでは **ip address** コマンドを設定しないでください。
ステップ 2	Router(donfig)# **redundancy unit1** *hostname name 1* **unit2** *hostname name2*	同じシャーシ内のピア スロットの特定および設定に使用します。
ステップ 3	Router(config)# **redundancy inter-device scheme standby hsrp** ipc zone default association 1 no shutdown protocol sctp unit2-port 5000 unit2-ip 4.0.0.2 unit1-port 5000 unit1-ip 4.0.0.1	HSRP スキーム名を RF Interdevice に関連付けます。 RF Interdevice の ipc 情報を設定します。

上記の設定を実行した後で、設定を保存していずれかのカード（スタンバイを推奨します）をリロードします。各カードは起動すると、HSRP ネゴシエーションに続いて RF Interdev ネゴシエーションを実行します。その後、設定同期機能が起動します。上記の手順は、新しいカードで初めて RF Interdev を稼動させるために必要な手順と同じです。

サブスクライバのモニタリング

この機能を使用すると、シャーシ内の単一ポイントから NAI または割り当てられた IP アドレスに基づいて条件付きデバッグを設定できます。これは、シャーシ内のどの HA インスタンスがサブスクライバ セッションをホスティングしているか、セッションがまだ確立されていない場合はどのインスタンスがサブスクライバ セッションをホスティングするために選択されているかを認識していなくても可能です。この機能では、IOS コマンドを一元的に実行でき、応答を受信してその応答をクリア形式および簡略形式で表示できる OSLER ツールを使用します。

出力形式には、デバッグ出力が簡単に表示される **brief** と、すべてのデバッグ出力が表示される **verbose** の 2 種類があります。

オペレータは、7600 のスーパーバイザにログインして、debug condition "qualifier" protocols コマンド、または同様のコマンドを実行する必要があります。

次の 2 段階のプロセスを実行します。

1. セッションをホスティングするシャーシ内の HA インスタンスを特定します。
2. セッションが存在する場合、その HA インスタンスで **debug** 条件付きコマンドを適用し、要求された特定の **debug** コマンド適用します。セッションが存在しない場合、シャーシ内に設定されたすべての HA インスタンスでデバッグのプリトリガー条件、次に要求された **debug** コマンドを設定します。

条件付きデバッグを適用するプロトコル サブシステムを指定できます。all、mobile-ip、または aaa（Radius を含む）から選択できます。

シャーシごとに同時にモニタリングされるサブスクライバの数は 10 に制限されています。ただし、シャーシ内の複数のブレード間のモニタリングされるサブスクライバの分散に関して制限はありません。

モニタリング セッションごとにモニタリングできるサブスクライバは 1 人だけです。サブスクライバ 10 人をモニタリングするには、10 のモニタリング セッションを確立する必要があります。

出力形式 **verbose** では、選択されたプロトコルに対して IOS によって生成されたすべてのデバッグが出力されます。これは大量の情報になり、活用するには専門家の分析が必要です。**brief** 形式では可能なデバッグの一部が出力されます。

Home Agent IOS コード ベースで使用可能な **debugs** に必要な変更はありません。

この機能は、HA の OSLER によってサポートされます。詳細については、OSLER の項を参照してください。

サブスクライバ セッションの表示

7600 のスーパーバイザに「ログイン」し、サブスクライバが NAI または IP アドレスで識別される **show subscriber session** コマンドを実行します。

これは次の 2 段階のプロセスになります。

- セッションをホスティングするシャーシ内の HA インスタンスを特定します。
- **show ip mobile host** *ip-address* | **nai**、**show ip mobile secure host** *ip-address* | **nai**、**show ip mobile violation address | nai** *string*、および **show ip mobile host-counters** コマンドを実行します。

バルク統計情報収集

この機能を使用すると、単一ポイントから次の機能を実行できます。

- シャーシ内のアクティブな各サービス ブレードから名前で識別可能な HA 統計情報の定期的な収集を開始する
- 選択した各サービス ブレードで IOS バルク統計情報の収集をイネーブルにして、特定の統計情報を収集する。このメカニズムでは MIB 変数の統計情報を収集できます。必要な測定値が MIB に含まれていない場合、バルク統計情報収集機能では収集できません。
- URL によって特定される外部 TFTP サーバにファイルを転送する

統計情報の収集期間は 15 分単位で設定できます。最小収集期間は 30 分です。最大収集期間は 24 時間です。

ファイルには、ブレードごとに収集された CPU 単位の CPU 使用率およびメモリ占有率に関する情報を除く、各ブレードの要約統計情報が含まれます。ブレード単位のファイルには、そのブレードの各アプリケーション CPU のエントリが含まれます。

ファイル形式は、カンマで区切られた一連の "variable_name value" のペアで構成されます。

HA Release 5.0 では、変数名は変数の OID です。これは IOS バルク統計情報収集 CLI から利用できるサポートのレベルであるためです。

HA アプリケーションでサポートされる MIB で使用可能な変数を含む、収集される統計情報が事前定義されたセットがあります。統計情報に割り当てられた OID は、関連する MIB の OID に直接対応します。

次の変数は MIB には含まれません。これらはバルク統計情報収集機能の一部としてサポートされません。

- HARegRevocationsSent
- HARegRevocationsReceived
- HARegRevocationsIgnored
- HARegRevocationAcksSent
- HARegRevocationAcksReceived
- HARegRevocationAcksIgnored

収集を行う期間は、yy:mm:dd:hh:mm:ss yy:mm:dd:hh:mm:ss という形式でファイル内に示されます。最初の日付は開始、2 番目の日付は終了を示します。

統計情報の収集をイネーブルにするサブシステムのセットを変更する場合は、まず進行中の統計情報収集をキャンセルして、新しい収集を開始する必要があります。キャンセルされたセッションで収集された情報は保存されます。

外部サーバが使用できない場合は、ファイルはローカルの不揮発性メモリに保存されます。最後に転送されたファイルは、次のファイルが正常に転送されるまでローカルに保存されます。新しいファイルが正常に転送されると、現在保存されているファイルは新しいファイルに置き換えられます。

単一 IP Home Agent Release 5.0 でバルク統計情報機能をサポートするために、新しい IOS コマンドは使用しません。

パフォーマンス要件

単一 IP HA は次のパフォーマンス機能をサポートします。

- サービス ブレードごとに 500,000 の登録サブスクライバ
- 5 Gbps スループット
- 500,000 のサブスクライバ登録をホスティングするアクティブ HA サービス ブレードをリロードされたスタンバイ HA サービス ブレードとバルク同期するために必要な時間は、「6 台の独立したプロセッサ」モデルで完全にロードされたアクティブ サービス ブレードをスタンバイ サービス ブレードとバルク同期するために要する時間より短くなります。バルク同期時間を x から x *（500,000 / 1,400,000）に比例的に短縮されることはありません。

単一 IP サポート - 再利用 CLI と新しい CLI

次の CLI は、IPC が IXP と通信できるようにし、GTP モジュール上で GTP と IPC が SAMI PPC 間で高信頼性、確認済み、および未確認の通信機能を提供できるようにします。

EXEC モード

- **debug sami ipc gtp ipc 3-8>**
- **debug sami ipc gtp ipc**

- **debug sami ipc gtp any**
- **debug sami ipc detail**
- **debug sami ipc**
- **debug sami ipc stats detail**
- **debug sami ipc stats**
- **debug sami configuration sync**
- **test sami tp-config [enable|disable]**（SingleIP イメージの TP で使用可能）

Show コマンド

- **show sami ipcp ipc gtp**
- **show sami ipcp ipc ixp**
- **show sami ipcp ipc processor**

設定モード

- **default sami ipc crashdump**
- **default sami ipc keepalive**
- **default sami ipc retransmit**
- **default sami ipc retries**
- **sami ipc crashdump**
- **sami ipc keepalive**
- **sami ipc retransmit**
- **sami ipc retries**

単一 IP HA の分散設定

分散 CLI エージェントは、IPC プロトコルを使用して CP から各 TP に設定情報を配信します。

デフォルトでは、CLI エージェントはすべてのコマンドを許可しますが、TP で不要な機能を開始する可能性があるコマンドだけをフィルタリングします。

単一 IP モデルの場合、TP にログインすると EXEC バナーが表示され、CP から「通常の」メンテナンス作業を行う必要があることをユーザに警告します。

表 3-2 に、HA の単一 IP でサポートされるコマンド、およびこれらのコマンドが CP でフィルタリングされるか、または TP にも送信されるかを示します。

コマンドが TP に送信されると、各 TP で実行されます。

表 3-2　　単一 IP の HA コマンド

コマンド（コンフィギュレーション コマンド）	目的	コントロール プロセッサで フィルタリング
aaa authentication ppp default group radius	RADIUS による PPP ユーザの認証をイネーブルにします。	なし

表 3-2　単一 IP の HA コマンド（続き）

aaa authentication login default group radius	ログイン時のデフォルト ユーザ認証方式として RADIUS を指定します。	なし
aaa authorization commands	**aaa authorization commands** コマンドが発行されたときに作成されたデフォルトを再設定します。	なし
aaa authorization ipmobile default group radius	モバイル IP を認可して、RADIUS を使用して AAA サーバからセキュリティ アソシエーションを取得します。	なし
aaa authorization network default group radius	ユーザのネットワーク アクセスを制限します。ネットワークに関連するあらゆるサービス要求に認可を実行します。デフォルトの認可方式として、group radius 認可方式を使用します。	なし
aaa accounting network default start-stop group radius	プロセスの開始時にアカウンティング「開始」通知、処理の終了時にアカウンティング「停止」通知を送信して、アカウンティングをイネーブルにします。	なし
aaa accounting system default start-stop group radius	HA によるシステム メッセージの送信をイネーブルにします。	なし
aaa accounting update newinfo	対象ユーザに関する新しいアカウンティング情報が発生するごとに、アカウンティング サーバに中間アカウンティング レコードを送信します。	なし
aaa session-id common	特定のコールに対して送信されたすべてのセッション ID 情報が同じになるようにします。	なし
aaa server radius dynamic author	受信した Change of Authorization メッセージに対するサポートをイネーブルにします。	なし
radius-server host *ip-addr* key *sharedsecret*	RADIUS サーバ ホストの IP アドレスを指定し、ルータと RADIUS サーバ間で使用する共有秘密文字列を指定します。	なし
radius-server retransmit *retries*	Cisco IOS ソフトウェアが RADIUS サーバ ホストのリストを検索する回数を指定します。	なし

表 3-2　単一 IP の HA コマンド（続き）

radius-server vsa send authentication 3gpp2	RADIUS IETF attribute 26 で定義されている Vendor-Specific Attribute（VSA; ベンダー固有のアトリビュート）を使用できるようにします。認識されるベンダー固有のアトリビュートのセットを認証アトリビュートだけに制限します。	なし
radius-server vsa send accounting 3gpp2	RADIUS IETF attribute 26 で定義されている Vendor-Specific Attribute（VSA; ベンダー固有のアトリビュート）を使用できるようにします。認識されるベンダー固有のアトリビュートのセットをアカウンティング アトリビュートだけに制限します。	なし
radius-server vsa send authentication wimax	WiMax 固有のアトリビュートを使用できるようにします。	なし
radius-server vsa send accounting wimax	WiMax 固有のアトリビュートを使用できるようにします。	なし
radius-server snmp-trap retrans-threshold *50 - 75*	再送信値が上限しきい値を超え、標準しきい値を下回ったときにトラップ（SNMP 通知）を生成します。	なし
radius-server snmp-trap timeout-threshold *50 - 75*	ラウンドトリップ値が上限しきい値を超え、標準しきい値を下回ったときにトラップ（SNMP 通知）を生成します。	なし
router mobile	ルータでモバイル IP をイネーブルにします。	なし
ip mobile host {***lower*** **[*upper*] | nai** ***string*** **[static-address {*addr1* [*addr2*] [*addr3*] [*addr4*] [*addr5*] | local-pool *name*}] [address {*addr* | pool {local *name* | dhcp-proxy- client [dhcp-server *addr*]}]} {interface *name* | virtual-network *network-address mask*} [aaa [load-sa [permanent]]] [authorized-pool *name*] [skip-aaa-reauthentication][care-of-access *access-list*] [lifetime *seconds*]**	HA でサポートされるモバイル ホストまたはモバイル ノード グループを設定します（範囲は下位アドレスから*上位*アドレス グループ）。	なし
ip mobile virtual-network ***netmask*** **[address** ***address*****]**	仮想ネットワークを定義します。	なし
router(config-if)#standby [*group-number*] ip ***ip-address***	HSRP をイネーブルにします。	あり

表 3-2　単一 IP の HA コマンド（続き）

router(config-if)#standby [*group-number*] [priority *priority*] preempt [delay [minimum | sync] *delay*]	アクティブ ルータの選択に使用するホットスタンバイ プライオリティを設定します。	あり
router(config-if)# standby name *hsrp-group-name*	スタンバイ グループの名前を設定します。	あり
ip mobile home-agent redundancy *hsrp-group-name*	HSRP グループ名を使用して、HA に冗長性を設定します。	あり
ip mobile home-agent dynamic-address *ip address*	登録応答パケットの Home Agent Address フィールドを設定します。Home Agent Address フィールドを ip address に設定します。	なし
ip mobile home-agent revocation	HA で MIPv4 登録失効のサポートをイネーブルにします。	あり
interface tunnel *10*	トンネル テンプレートを設定します。	なし
ip mobile home-agent template tunnel *10* address *10.0.0.1*	テンプレート トンネルを使用する HA を設定します。	なし
ip mobile home-agent accounting *list*	HA アカウンティングをイネーブルにし、HA の定義済みアカウンティング方式リストを適用します。list は、HA アカウンティング レコードの生成に使用する AAA アカウンティング方式です。	なし
ip mobile home-agent *method* redundancy [virtual-network address *address*] periodic-sync	アカウンティング アップデート イベントを使用して、各バインディングのバイトとパケットのカウントをスタンバイ装置に同期化します。同期が実行されるのは、最後の同期以降、バイト カウントが変更された場合だけです。	なし
ip mobile realm *realm* hotline redirect *redirect-server-ipaddress*	インバウンド ユーザ セッションをイネーブルにして、特定のアトリビュートが表示された場合にセッションを切断します。	なし
ip mobile home-agent dfp-max-weight *dfp-max-weight-value*	HA で許可できる最大 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。	なし
ip mobile home-agent max-cps *max-cps-value*	HA で許可できる最大 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。	なし

表 3-2　単一 IP の HA コマンド（続き）

ip mobile home-agent max-binding ***max-binding-value***	HA でオープンできるバインディングの数を制限します。max-binding-value のデフォルト値は 235,000 です。	なし
ip mobile home-agent host-config url ***url***	この機能の一部として、HA で URL を設定するための 新しい CLI が導入されました。この CLI が必要なのは、HA が MN から要求される設定を提供できない場合があるためです。こうした状況に対処するために、URL によって指定されるこの一般サイトが MN による設定パラメータのダウンロードに役立ちします。 設定例 **ip mobile home-agent host-config** url http://www.cisco.com	なし
ip mobile realm ***realm*** **hotline capability profile-based redirect ip**	ユーザに対し、ip リダイレクション ルールを使用したプロファイルベースのホットラインを設定します。realm には NAI またはレルムを指定します。プロファイルベースの ip リダイレクション ルールを削除するには、この CLI の no バージョンを使用します。	なし
ip mobile realm ***realm*** **hotline capability profile-based redirect http**	ユーザに対し、http リダイレクション ルールを使用したプロファイルベースのホットラインを設定します。realm には NAI またはレルムを指定します。プロファイルベースの http リダイレクション ルールを削除するには、この CLI の no バージョンを使用します。	なし
ip mobile home-agent aaa attribute framed-pool	認証時にダウンロードされた RADIUS Framed Pool 名のダウンロードをサポートします。	なし

表 3-2　単一 IP の HA コマンド（続き）

Router(config-cmap)#**match flow mip-bind** Router(config-pmap-c)#**police rate mip-binding [bc *bytes*] [peak-rate mip-binding [be *bytes*]]**	MN ユーザのクラスに属する各バインディングに対し、指定のレートでパケットを分類するために、Modular QoS CLI（MQC; モジュラ QoS CLI）class-map 設定モードで次の CLI を設定します。 指定のレートに基づいて、MQC に対して特定済みの個々の MN バインディングのポリシングを行うには、設定されたクラスに固有の policy-map 設定モードで次の CLI を指定します。 設定例 class-map class-mip match flow mip-binding policy-map policy-mip-flow class class-mip police rate mip-binding [bc <bytes>] [peak-rate mip-binding [be <byes>]] conform-action <action> exceed-action <action> violate-action <action>	なし
ip mobile home-agent service-policy [input *policy-name* [output *policy-name*]	service-policy コマンドを使用して HA を QoS ポリシング機能にアタッチします。service-policy を HA 仮想インターフェイス オブジェクトに関連付けることで、HA の特定に役立ちます。このコマンドは、トラフィックの両方向に対して設定します。	なし
ip local pool *poolname start_address end_address* group *customer-x* priority *0..255*	新しいオプション "priority 0..255" は ip local pool に対して任意です。このオプションを設定すると、新しく作成されたプールに優先順位が割り当てられ、同じ優先順位が IP アドレスの割り当てに使用されます。	なし
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] [ppp-regeneration [setup-time *number*]]	ドメイン @xyz.com の VRF を定義します。オプション "ppp-regeneration <setup-time <number>" は "ip mobile realm" コマンドに対して任意です。このオプションを設定すると、PPP 再生成機能がイネーブルになり、このレルムと一致するすべての MIP セッションが対応する L2TP セッションにマッピングされます。	なし

表 3-2　単一 IP の HA コマンド（続き）

router ospf *process-id*	OSPF ルーティングをイネーブルにします。これにより、ルータ設定モードが開始されます。	あり
network *ip-address wildcard-mask* **area** *area-id*	OSPF を実行するインターフェイスを定義し、そのインターフェイスのエリア ID を定義します。	あり
ip ospf cost ***cost***	OSPF インターフェイスでパケットを送信するコストを明示的に指定します。	あり
ip ospf retransmit-interval *seconds*	OSPF インターフェイスに属する隣接に対して Link-State Advertisement（LSA; リンクステート アドバタイズメント）が再送信される間隔の秒数を指定します。	あり
ip ospf transmit-delay *seconds*	OSPF インターフェイスでリンクステート更新パケットを送信するために必要な予測秒数を設定します。	あり
ip ospf priority ***number-value***	ネットワークの OSPF 指定ルータを確認するための優先順位を設定します。	あり
ip ospf hello-interval *seconds*	OSPF インターフェイスで Cisco IOS ソフトウェアが 送信する hello パケットの間隔の時間を指定します。	あり
ip ospf dead-interval *seconds*	デバイスが hello パケットを受信していないためネイバー OSPF ルータがダウンしていることを宣言するまでデバイスが待機する秒数を設定します。	あり
ip ospf authentication-key *key*	OSPF 簡易パスワード認証を使用しているネットワーク セグメント上で近接する OSPF ルータが使用するパスワードを割り当てます。	あり
ip ospf message-digest-key *key-id* ***md5*** *key*	OSPF MD5 認証をイネーブルにします。*key-id* および *key* 引数の値は、ネットワーク セグメント上の他のネイバーに対して指定された値と一致している必要があります。	あり
ip ospf authentication [**message-digest** | **null**]	インターフェイスの認証タイプを指定します。	あり
access-list ***access-list-number*** {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	標準 IP アクセス リストを定義します。	なし
ip access-list {**standard** | **extended**} *access-list-name*	名前を指定して IP アクセス リストを定義します。	なし

表 3-2　単一 IP の HA コマンド（続き）

snmp-server enable traps ipsec [**cryptomap** [**add** | **delete** | **attach** | **detach**] | **tunnel** [**start** | **stop**] | **too-many-sas**]	ルータが IP セキュリティ（IPSec）簡易ネットワーク管理プロトコル（SNMP）通知を送信できるようにします。	あり
snmp-server enable traps ipmobile	モバイル IP の簡易ネットワーク管理プロトコル（SNMP）セキュリティ通知をイネーブルにします。	あり
snmp mib [**bulkstat** | **community-map** | **notification-log** | **persist**]	バルク統計情報収集を定義します。	あり

（注）　コンフィギュレーション コマンドがフィルタリングされる場合、サブ コンフィギュレーション コマンドもフィルタリングされます。

Distributed Show および Distributed Debug

デフォルトでは、すべての **debug** コマンドは TP で実行し、トレースは CP から表示します。CP は、Distributed Debug の集約を実行しません。

debug AAA / RADIUS コマンドは TP および CP で実行されますが、TP では Radius トランザクションが発生しないためデバッグは表示されません。たとえば、受信した PoD または CoA に対する RADIUS トランザクションは CP でだけ処理されます。PoD/CoA が行われたが Radius トランザクションの形式ではないことを示す内部イベントが CP から該当する TP に渡されます。

サブスクライバ バインディングを作成する場合、CP と選択された TP の両方で行われるため、TP では **debug ip mobile** コマンドは実行されません。デバッグ出力のセットだけが必要です。

Distributed Show：デフォルトでは、すべての TP で show コマンドは実行されません。表 3-3 に示されているコマンドだけに対して、TP から収集されたデータの集約が CP で定期的に行われます（トラフィック カウンタは TP によって保持されます）。

（注）　**Execute On ... clear** コマンドは Service Internal コマンドになりました。

表 3-3 に、Single IP Home Agent Release 5.0 でサポートされる show および debug コマンドを示します。

表 3-3　単一 IP HA でサポートされる show/debug コマンド

コマンド（Show/Debug）	目的	集約の必要性（あり / なし）	EXEC コマンドの TP への送信
show ip mobile binding [**home-agent** *ip-address* | **nai** *string* [**session-id** *string*] | **police** [**nai** *string*] | **summary**]	Home Agent（HA）のモビリティ バインディング テーブルを表示します。	あり	なし

表 3-3　単一 IP HA でサポートされる show/debug コマンド （続き）

show ip mobile host [*address* | **interface** *interface* | **network** *address* | **nai** *string* | **group** | **summary**]	モバイル ノード情報を表示します。	あり	なし
show ip mobile traffic	HA のプロトコル カウンタを表示します。	あり	なし
show ip mobile tunnel [*interface*]	モバイル IP トンネルに関する情報を表示します。	あり	なし
show policy-map [apn *mn-apn-index* [realm *string*]]	EXEC モードの CLI は MN-Access Point Name（APN; アクセス ポイント ネーム）インターフェイスのフローの集約ポリシング統計情報を表示します。	なし	なし
show ip mobile hot-line capability [realm *word*] [all]	ユーザ名 /nai またはレルムのホットライン機能を表示します。ユーザ名またはレルムが指定されていない場合、現在 HA でホットライニングが適用されているすべてのユーザまたはレルムの情報を表示します。	なし	なし
show ip mobile globals	モバイル エージェントのグローバル情報を表示します。	なし	なし
show ip mobile secure	モバイル IP のモビリティ セキュリティ アソシエーションを表示します。	なし	なし
show ip route vrf	VRF に対応するルーティング テーブル情報を表示します。	なし	なし
show ip mobile redundancy	HA の冗長ステータスを表示します。	なし	なし
show ip mobile secure	モバイル IP のモビリティ セキュリティ アソシエーションを表示します。	なし	なし
show ip mobile ipc	CP-TP インターフェイスの ipc 情報を表示します。	なし	なし
debug ip mobile advertise	アドバタイズメント情報を表示します。	なし	なし
debug aaa authentication	AAA/TACACS+ 認可に関する情報を表示します。	なし	あり
debug aaa pod	AAA サブシステム レベルでの Radius Disconnect メッセージ処理のデバッグ情報を表示します。	なし	あり
debug ip mobile [advertise | dfp | host | local-area | redundancy | router | upd-tunneling | vpdn-tunneling [events | detail]| ipc | mib]	IP モビリティ アクティビティを表示します。	なし	なし
debug ip mobile host [***acl*** | **nai** | **mac** *H.H.H*]	モビリティ イベント情報を表示します。	なし	なし
debug ip mobile redundancy {**events** | **error** | **detail** | **periodic-sync**}	IP モビリティ イベントを表示します。	なし	なし

表 3-3　単一 IP HA でサポートされる show/debug コマンド （続き）

debug radius [accounting | authentication | brief | elog | failover | **periodic-sync** | retransmit | verbose]	RADIUS に関連した情報を表示します。	なし	あり
debug tacacs [accounting | authentication | authorization | events | packet]	Terminal Access Controller Access Control System（TACACS）に関連した情報を表示します。	なし	あり

show ip mobile binding [**nai** string | ip address] コマンドおよび **show ip mobile host** [**nai** *string* | *ip address*] コマンドの場合に限り、CP は Pull メカニズムを使用して TP から現在のカウンタを取得します。これらの **show** コマンドに表示されるカウンタの間隔が長すぎるため、カウンタを無関係にすることができません。

（注）　**clear mobile ip binding all load** コマンドは HA 製品には使用されなくなりました。このコマンドを使用するのではなく、リロードを実行する必要があります。

シャーシ管理の Show CLI の拡張

表 3-4 に、単一 IP HA のシャーシ全体の管理インターフェイスをサポートするために追加された **show** コマンドを示します。詳細については、該当する項を参照してください。

表 3-4　シャーシ管理に関連する show コマンド

CLI コマンド	目的	TP からの情報の収集（あり / なし）
show ip mobile binding fa [*coa-ip*]	対応する気付アドレスを使用して HA のモビリティ バインディング テーブルを表示します。	なし
show ip mobile binding fa [*coa-ip*] **summary**	対応する気付アドレスを使用して HA のモビリティ バインディング テーブルの要約を表示します。	なし
show ip mobile binding granted-lifetime greater [*time*]	granted-lifetime が *time* より大きい HA のモビリティ バインディング テーブルを表示します。	なし
show ip mobile binding granted-lifetime greater [*time*] **summary**	granted-lifetime が *time* より大きい HA のモビリティ バインディング テーブルの要約を表示します。	なし
show ip mobile binding granted-lifetime equals [*time*]	granted-lifetime が *time* に等しい HA のモビリティ バインディング テーブルを表示します。	なし
show ip mobile binding granted-lifetime equals [*time*] **summary**	grated-lifetime が *time* に等しい HA のモビリティ バインディング テーブルの要約を表示します。	なし
show ip mobile binding granted-lifetime less [*time*]	granted-lifetime が *time* より小さい HA のモビリティ バインディング テーブルを表示します。	なし

表 3-4　シャーシ管理に関連する show コマンド （続き）

show ip mobile binding granted-lifetime less [*time*] **summary**	granted-lifetime が *time* より小さい HA のモビリティ バインディング テーブルの要約を表示します。	なし
show ip mobile binding remaining-lifetime greater [*time*]	remaining-lifetime が *time* より大きい HA のモビリティ バインディング テーブルを表示します。	なし
show ip mobile binding remaining-lifetime greater [*time*] **summary**	remaining-lifetime が *time* より大きい HA のモビリティ バインディング テーブルの要約を表示します。	なし
show ip mobile binding remaining-lifetime equals [*time*]	remaining-lifetime が *time* に等しい HA のモビリティ バインディング テーブルを表示します。	なし
show ip mobile binding remaining-lifetime equals [*time*] **summary**	remaining-lifetime が *time* に等しい HA のモビリティ バインディング テーブルの要約を表示します。	なし
show ip mobile binding remaining-lifetime less [*time*]	remaining-lifetime が *time* より小さい HA のモビリティ バインディング テーブルを表示します。	なし
show ip mobile binding remaining-lifetime less [*time*] **summary**	remaining-lifetime が *time* より小さい HA のモビリティ バインディング テーブルの要約を表示します。	なし

ネットワーク管理と MIB

単一 IP 設計の目的の 1 つは、サービス ブレードごとに 1 つの MIB アクセスを提供することです。その結果、多くの MIB が、1 つのエントリではなく、6 つのエントリ（プロセッサごとに 1 つ）を持つようになりました。これは特に CISCO-PROCESS-MIB および CISCO-ENHANCED-MEMPOOL-MIB に該当します。

HA 管理で使用されるその他の MIB（RFC 2002 MIB、CISCO-MOBILE-IP-MIB、CISCO-IP-LOCAL-POOL-MIB、RADIUS 認証クライアント Client MIB）はこのシステム設計の影響を受けません。

Key Performance Indicator（KPI）のソースとして使用される MIB は次のとおりです。

- RFC 2002 MIB
- CISCO-MOBILE-IP-MIB
- RFC 2618 RADIUS 認証クライアント MIB
- IF-MIB
- CISCO-IP-LOCAL-POOL-MIB
- CISCO-PROCESS-MIB
- CISCO-MEMORY-POOL-MIB - Replaced by ENHANCED-MEMPOOL-MIB
- CISCO-ENHANCED-MEMPOOL-MIB

CISCO-PROCESS-MIB および CISCO-MEMORY-POOL-MIB は、サービス ブレードごとに 1 つの MIB を提供するために必要です。この 2 つの MIB にはプロセッサ単位の内容が含まれます。この設計には 1 つの SNMP GET で 6 台のアプリケーション プロセッサすべての情報が報告されることが必要なため、各 MIB には 6 つのエントリ（アプリケーション プロセッサごとに 1 つ）が含まれています。

IF-MIB には、コントロール プレーン プロセッサのインターフェイスに加えて、トラフィック プレーン プロセッサのインターフェイスの情報が含まれます。

CISCO-PROCESS-MIB には、すでに 1 つ以上の CPU の情報を提供するファシリティが含まれています。CISCO-MEMORY-POOL-MIB はこの機能をサポートしません。また、HA は現在 CISCO-ENHANCED-MEMPOOL-MIB をサポートしていません。

RADIUS 認証クライアント MIB は現在 HA イメージでサポートされていませんが、必要です。

表 3-5 に、サポートされる MIB を示します。

表 3-5　HA Release 5.0 の単一 IP MIB

MIB	説明	TP からの情報の必要性	必要がある場合のメカニズム
RFC2006-MIB	RFC 2006「*The Definitions of Managed Objects for IP Mobility Support Using SMIv2*」に規定されている定義を使用します。	なし。トラフィック カウンタがありません。	
CISCO-MOBILE-IP-MIB	NM を使用して HA モビリティ バインディングの合計数および FA ビジター バインディングの合計数をモニタリングできます。	なし。コントロール メッセージのカウンタだけがあります。	
RFC2618 RADIUS 認証クライアント MIB	RFC 2618 に規定されている定義を使用します。	なし。トラフィック カウンタがありません。	
IF-MIB	コントロール プレーン プロセッサのインターフェイスに加えて、トラフィック プレーン プロセッサのインターフェイスの情報が含まれます。	あり。	PUSH パラダイムに準拠した CP のデータ集約機能、TP のデータ提供機能。TP は毎分 CP にアップデートを送信します。
CISCO-IP-LOCAL-POOL-MIB	ローカル IP プールに関連する機能の設定およびモニタリングを定義します。	なし。トラフィック カウンタがありません。	
CISCO-ENHANCED-MEMPOOL-MIB	管理対象システムのすべての物理エンティティのメモリ プールをモニタリングするためのものです。	あり。	PUSH パラダイムに準拠した CP のデータ集約機能、TP のデータ提供機能。各 TP は毎秒 CP にアップデートを送信します。

表 3-5　HA Release 5.0 の単一 IP MIB （続き）

CISCO-PROCESS-MIB	IOS を実行するプロセッサ（2 つのドーター カード上の 6 台のプロセッサ）上のアクティブなシステム プロセスの統計を示します。	あり。	PUSH パラダイムに準拠した CP のデータ集約機能、TP のデータ提供機能。TP からの CPU 統計情報が毎秒 CP に送信され、その他の統計情報は毎分送信されます。
CISCO-ENTITY-MIB	1 つの SNMP エージェントによってサポートされる複数の論理エンティティを表すための MIB モジュール。	あり。	CP でのデータ集約機能、TP でのデータ提供機能。

サポートされない機能

次の機能は、Home Agent 5.0 単一 IP ソフトウェア リリースではサポートされません。

- MIP-LAC
- モバイル ルータ
- L2TP Network Server（LNS; L2TP ネットワーク サーバ）としての Home Agent

シャーシ管理

単一 IP 機能は、定義された機能セットに対して単一の OAM の視点を提供するためにシャーシ管理に依存します。これにより、シャーシ全体を 1 つのブラック ボックスとして見ることができます。複数のプロセッサを搭載した複数のサービス ブレードや別々のアクティブ / スタンバイ設定を気遣う必要はありません。

適切な HA インスタンスの適切な情報を取得あるいは設定するために、管理コマンドはシャーシ内のすべてのモジュールをチェックし、アクティブなモジュール上で適切なモジュール（アクティブな SAMI ブレード）および HA インスタンスを見つけます。Home Agent Release 5.0 ではサービス ブレードごとに HA インスタンスが 1 つだけ許可されます。

シャーシ管理情報を提供する次のコマンドは、アクティブな SUP カードから開始します。

- **サブスクライバの表示**
- **サブスクライバのモニタリング**
- **サブスクライバ セッションの表示**
- **収集した統計情報**

制約事項

単一 IP モデルでは、シャーシ内外でパケット ルーティング設定に制限事項があります。

（注）　すべての設定変更はメンテナンス ウィンドウで実行する必要があります。

（注）　リロード後に、カードをリブートして適切に動作していることを確認します。

（注）　シャーシ間の SR セットアップ用に **no auto-sync all** コマンドを設定する必要があります。シャーシ間の場合、コンフィギュレーション コマンドの "unit1/unit2" 形式は使用しません。

（注）
- モバイル サブネットのルートをアドバタイズするためのダイナミック ルーティング プロトコルはスーパーバイザで実行します。

（注）
- モバイル サブネットをスーパーバイザだけにアドバタイズするために、OSPF は各 SAMI ブレードの CP でだけ実行されます。

（注）
- ダイナミック ルート アップデートは CP から TP に伝搬されません。

（注）
- スタティック ルートは、SAMI ブレードからスーパーバイザに設定する必要があります。

（注）
- MN から送信されたトラフィックはすべて同じブレードからスーパーバイザにルーティングされます。これは、MN- ネットワーク トラフィックおよび MN-MN トラフィックの両方に適用されます。

（注）
- SAMI ブレード上の TP 内では MN-MN トラフィックのルーティングはできません。

（注）
- HSRP 仮想 IP アドレスは、HA のモバイル IP トンネル終端の IP アドレスとして使用されなくなりました。

（注）
- モバイル IP トンネル終端アドレスとして使用するために、HA でループバック アドレスを設定する必要があります。

（注）
- インターフェイスのループバック アドレスを DHCP、Radius サーバなどの外部サーバに設定する必要があります。HSRP 仮想 IP アドレスを使用しないでください。

（注）
- スタンバイ HA はスーパーバイザにルートをアドバタイズしません。

（注）
- スーパーバイザは、HSRP 仮想 IP アドレスおよび関連付けられた HSRP 仮想 Mac アドレスを使用して SAMI 上の HA ブレードにパケットをルーティングします。

（注）
- 設定同期機能を使用する場合にアクティブとスタンバイに正しいアドレスが割り当てられるように、パケットの外部ルーティングに使用される物理インターフェイスには、**redundancy ip address** コマンドを使用して割り当てられた IP アドレスが必要です。

CHAPTER 4

HA でのホーム アドレス割り当て

この章では、Cisco Mobile Wireless Home Agent がモバイル ノードにホーム アドレスを割り当てる方法、各種アドレス タイプについて説明し、設定の詳細および設定例を示します。

この章は、次の内容で構成されています。

ホーム アドレス割り当て

Home Agent（HA）は、モバイル IP 登録時に受信したユーザ NAI に基づいて、モバイル ノードにホーム アドレスを割り当てます。モバイル ステーションには、スタティックまたはダイナミックに IP アドレスを割り当てることができます。HA は、スタティック割り当てかダイナミック割り当てかを問わず、同じ IP アドレスで異なる NAI を同時に登録することを認めません。

アドレス割り当て機能

セッション上書き機能を備えたアドレス割り当て機能により、古いセッションを削除して、デバイスに新しいセッションを確立できます。デバイスの MAC アドレスは変更されませんが、NAI（外側の EAP ID から取得される可能性あり）と Home Address（HoA; ホーム アドレス）は変更されることがあります。

NAI レルム（つまり、Registration Request（RRQ; 登録要求）の [Home Address] フィールドではない）が、スタティック IP プールまたはダイナミック IP プールのアドレス管理が使用されているかどうかを判別します。

Home Agent Release 5.0 では、CMIPv4 および PMIPv4 がサポートされます。アドレス管理は、登録内の MAC アドレスに基づいて実行されます。

MAC アドレスを持つ RRQ と MAC アドレスを持たない RRQ に適用される条件を次に示します（PMIPv4 デバイス ID 拡張機能で提供される）。

- RRQ に MAC アドレス（CMIP）が含まれない場合、セッションは R4.0 マトリクスに基づいて管理されます。
- RRQ に MAC アドレス（PMIP）が含まれている場合、セッションは R5.0 マトリクスに基づいて管理されます。
- CMIP および PMIP 間にハンドオフはありません。
- CMIP ユーザと PMIP ユーザのドメインは同じではありません。
- CMIP ユーザと PMIP ユーザのホーム アドレスは同じではありません。VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）が使用されていて、CMIP ユーザと PMIP ユーザが異なる VRF 内にある場合、HoA アドレスが同じである場合があります。

クライアントベースのモバイル IPv4

CMIPv4 は HA Release 4.0 のアドレス割り当て方法に基づいています。次に設定例を示します。

スタティック IP プール：

```
ip mobile host nai @domain static-address local-pool pool_001
```

authentication, authorization, and accounting（AAA; 認証、認可、アカウンティング）は HoA を割り当て、HoA は初回登録時は MIP RRQ で設定されます。

スタティック アクセスを許可するダイナミック IP プール：

```
ip mobile host nai @domain static-address local-pool pool_002 address pool local pool_002
```

HoA は初回登録時は MIP RRQ で送信され、HA は HoA を使用してセッションを確立します。HoA が初回登録時に MIP RRQ で送信されない場合、HA は HoA を割り当てて、セッションを確立します。

ダイナミック IP プール：

```
ip mobile host nai @domain address pool local pool_003
```

HA は HoA を割り当てます。HoA は初回登録時は MIP RRQ で設定されません（0.0.0.0）。次に示すプール タイプを使用した既存のアドレス管理について以降で説明します。

プロキシ モバイル IPv4

PMIPv4 は HA Release 5.0 のアドレス割り当て方法に基づいています。HoA 上書き機能を備えたアドレス割り当て機能により、古いセッションを削除して、デバイスに新しいセッションを確立できます。デバイスの MAC アドレスは変更されませんが、NAI（外側の EAP ID から取得される可能性あり）と HoA は変更されることがあります。

NAI レルム（RRQ の [Home Address] フィールドではない）が、スタティック IP プールまたはダイナミック IP プールのアドレス管理が使用されているかどうかを判別します。次に設定例を示します。

スタティック IP プール：

```
ip mobile host nai @domain static-address local-pool pool_001
```

AAA は HoA を割り当てます。HoA は初回登録時は MIP RRQ で設定されません。

ダイナミック IP プール：

ip mobile host nai @*domain* **address pool local** *pool_003*

HA は HoA を割り当てます。HoA は初回登録時は MIP RRQ で設定されるか、または設定されません（0.0.0.0）。

古いバインディングの削除をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Router(config)# **ip mobile home-agent binding-overwrite**	HA、MAC アドレス、および登録要求の NAI 情報によって識別される古いバインディングの削除をイネーブルまたはディセーブルにします。
ステップ 2	router#**debug ip mobile host mac** *H.H.H*	MAC アドレスベースのデバッグをイネーブルにします。

（注）　VRF サポートに複数の HA IP アドレスが使用されていないため、失効メッセージに NAI 拡張機能を含める必要はありません。

アドレス割り当て機能の使用方法を示す 3 つの設定例を次に示します。

スタティック IP プールの HA 設定を使用した MAC ベースのセッション

HA Config

```
ip local pool cisco-static-pool 5.1.0.1 5.1.1.0

ip mobile host nai @cisco.com static-address local-pool
cisco-static-pool interface Null0 aaa load-sa
```

FA Config

```
simulator mip mn profile 1
    description ctc-mac-static
    registration lifetime 65535
    registration retries 0
    registration flags 42
    revocation flags 00
    home-agent 81.81.81.81
    home-address 5.1.0.1
    secure home-agent spi 100 key ascii cisco
    nai cisco-%f@cisco.com
    pmip skip subtype 2 idtype mac
    no extension fa-challenge
    no extension mn-fa
    no extension nat traversal
    extension revocation
```

ダイナミック IP プールを使用した MAC ベースのセッション

HA Config

```
ip local pool cisco-pool 5.1.0.1 5.1.1.0

ip mobile host nai @cisco.com address pool local cisco-pool
interface Null0 aaa load-sa
```

FA Config

```
simulator mip mn profile 1
  description ctc-mac-static
  registration lifetime 65535
  registration retries 0
  registration flags 42
  revocation flags 00
  home-agent 81.81.81.81
  home-address 5.1.0.1
  secure home-agent spi 100 key ascii cisco
  nai cisco-%f@cisco.com
  pmip skip subtype 2 idtype mac
  no extension fa-challenge
  no extension mn-fa
  no extension nat traversal
  extension revocation
```

既存のバインディングの上書き

HA Config

```
ip mobile home-agent binding-overwrite

ip local pool cisco-pool 5.1.0.1 5.1.1.0

ip mobile host nai @cisco.com address pool local cisco-pool
interface Null0 aaa load-sa
```

FA Config

```
simulator mip mn profile 3
  registration lifetime 65535
  registration retries 0
  registration flags 42
  revocation flags 00
  home-agent 81.81.81.81
  secure home-agent spi 100 key ascii cisco
  secure aaa spi 2 key ascii cisco
  nai cisco-%f@cisco.com
  pmip skip subtype 2 idtype mac
  no extension mn-aaa
  no extension mn-fa
  no extension nat traversal
  extension revocation

simulator mip mn profile 4
  registration lifetime 65535
  registration retries 0
  registration flags 42
  revocation flags 00
  home-agent 81.81.81.81
  home-address 5.0.0.2 0
  secure home-agent spi 100 key ascii cisco
  secure aaa spi 2 key ascii cisco
  nai pepsi-%f@cisco.com
  pmip skip subtype 2 idtype mac
  no extension mn-aaa
  no extension mn-fa
  no extension nat traversal
  extension revocation
```

```
simulator mip scenario 3
  mn profile 3
  fa 2.2.2.200
  mn id 20

  simulator mip scenario 4
  mn profile 4
  fa 2.2.2.200
  mn id 21
```

スタティック IP アドレス

スタティック IP アドレスは、モバイル ステーションに前もって割り当てられたアドレスであり、モバイル デバイスにすでに設定されていることもあります。HA はパブリック IP アドレスでも、プライベート ドメインのアドレスでも、スタティック アドレスをサポートします。

（注）　モバイル IP サービスにプライベート アドレスを使用するには、PDSN/FA と HA 間にリバース トンネリングが必要です。

モバイル ユーザは登録要求メッセージで、設定済みアドレスまたは使用可能アドレスを非ゼロのホーム アドレスとして提案します。HA は、このアドレスを受け付けることもあれば、登録応答メッセージで別のアドレスを返すこともあります。HA は、ホーム AAA サーバまたは Dynamic Host Configuration Protocol（DHCP）サーバにアクセスすることによって、IP アドレスを取得できます。ホーム AAA サーバは、ローカル プール名を返すこともあれば、単一の IP アドレスを返すこともあります。モバイル IP 登録が成功すると、ユーザはモバイル IP ベースのサービスを利用できるようになります。

NAI を使用しないスタティック ホーム アドレッシング

最初のモバイル IP 仕様でサポートしていたのは、モバイル ノードのスタティック アドレッシングだけでした。ホーム IP アドレスが認証の「ユーザ名」の部分として使用されていました。スタティック アドレッシングは、各デバイスがどこからネットワークに接続しようと、常に同じアドレスが維持されるので、便利な場合があります。この場合、ユーザは DNS をアップデートしたり、他の形式のアドレス形式を使用しなくても、モバイル終端サービスを実行できます。また、スタティック アドレッシングではホーム アドレスと HA が常に同じなので、Mobile Node（MN; モバイル ノード）の管理が容易です。しかし、スタティック アドレッシングの場合、アドレス割り当てを手動で処理し、HA と MN の両方をアップデートしなければならないので、プロビジョニングとメンテナンスははるかに困難になります。設定例を示します。

```
router (config)# ip mobile host 10.0.0.5 interface FastEthernet0/0
router (config)# ip mobile host 10.0.0.10 10.0.0.15 interface FastEthernet0/0
router (config)# ip mobile secure host 10.0.0.12 spi 100 key ascii secret
```

NAI を使用するスタティック ホーム アドレッシング

スタティック ホーム アドレッシングを NAI と組み合わせて使用することによって、NAI ベースの認証およびその他のサービスをサポートすることもできます。また、単一ユーザに同一デバイスまたは複数のデバイス上で複数のスタティック IP アドレスを使用させながら、なおかつ 1 つの AAA レコードとセキュリティ アソシエーションを維持することもできます。ユーザがアドレスを使用して認可を受けてからでなければ、登録は受け付けられません。アドレスはローカルで認可することも、AAA サーバを使用して認可することもできます。異なる NAI のバインディングとすでに関連付けられているアドレスを MN が要求した場合、HA はコマンドが設定されていない限り、プールに含まれている別のアドレスを返そうとします。

設定例を示します。

```
router (config)# ip mobile home-agent reject-static-addr
```

ローカル認可

スタティック アドレスの認可は、コンフィギュレーション コマンドを使用して MN ベースで、またはレルム ベースで行うことができます。MN ベースの設定には、*user* または *user@realm* の形式で具体的な NAI を定義する必要があります。レルム ベースの設定には、*@realm* の形式で総称 NAI を定義する必要があります。ローカル プールの指定だけが認められます。

設定例を示します。

```
router (config)# ip local pool static-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com static-address 10.0.0.1 10.0.0.2
   interface FastEthernet0/0
router (config)# ip mobile host nai user@staticuser.com static-address local-pool
   static-pool interface FastEthernet0/0
router (config)# ip mobile host nai @static.com static-address local-pool static-pool
    interface FastEthernet0/0
```

AAA の認可

認可されたアドレスまたはローカル プール名を AAA サーバに保管することもできます。各ユーザには、AAA サーバで設定された **static-ip-addresses** アトリビュートまたは **static-ip-pool** アトリビュートが必要です。コマンドラインでスタティック アドレスを設定する場合と異なり、**static-ip-addresses** アトリビュートは返すことのできるアドレスの数に制限がありません。

設定例を示します。

HA の設定

```
router (config)# ip local pool static-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com interface FastEthernet0/0 aaa
router (config)# ip mobile host nai @static.com interface FastEthernet0/0 aaa
```

Remote Authentication Dial-In User Service（RADIUS）のアトリビュート

Cisco-AVPair = "mobileip:static-ip-addresses=10.0.0.1 10.0.0.2 10.0.0.3"

Cisco-AVPair = "mobileip:static-ip-pool=static-pool"

ダイナミック HA 割り当て

次の条件が存在する場合、CDMA2000 ネットワークでは HA のダイナミック割り当てが可能です。

最初の条件は、HA が HA フィールドに 0.0.0.0 の値が指定されたモバイル IP 登録要求を受信することです。認証/認可時に、PDSN が HA の IP アドレスを取得します。PDSN はさらに、このアドレスを使用して HA に登録要求を転送します。ただし、登録要求の実際の HA アドレス フィールドはアップデートされません。

HA は登録応答を送信し、HA フィールドに専用の IP アドレスを格納します。この時点で受信する再登録要求は、HA フィールドに HA の IP アドレスが入ります。

第 2 の条件は、PDSN/FA の機能であり、それがここで含まれていないと完全ではありません。この場合、AAA サーバを使用してダイナミック HA 割り当て機能を実行します。ネットワーク トポロジに応じて、ローカル AAA サーバまたはホーム AAA サーバがこの機能を実行します。アクセス サービス プロバイダーが ISP でもある場合、HA はアクセス プロバイダーのネットワークに配置されます。このサービス環境では、ローカル AAA サーバが HA の割り当て機能を実行します。AAA サーバはアクセス要求メッセージで受け取ったユーザ NAI に基づいて、PDSN へのアクセス応答メッセージで選択した HA のアドレスを返します。

HA アドレス プールは通常、AAA サーバで設定されます。アクセス プロバイダーが ISP として機能する場合、ローカル AAA サーバで複数の HA プールを設定できますが、これはモバイル IP サービスまたはプロキシ モバイル IP サービスのサポート対象となるドメインのある SLA に依存します。ユーザ NAI 選択条件としてラウンドロビンまたはハッシュ アルゴリズムを使用すると、AAA サーバで HA 選択手順を設定できます。

PDSN/FA は HA に登録要求を送信しますが、MIP RRQ の HA フィールドに IP アドレスは含まれません（0.0.0.0）。PDSN は AAA から IP アドレスを受け取った時点で、MIP RRQ を更新せず、その RRQ を取得した HA アドレスに転送します。PDSN は MN-HA SPI およびキー値（[Home Agent] フィールドで指定された HA の IP アドレスが含まれる）が不明なので、MIP RRQ を変更できません。ネットワーク トポロジに応じて、ローカル AAA サーバまたはホーム AAA サーバがこの機能を実行します。HA がアクセス プロバイダーのネットワークに配置されている場合、ローカル AAA サーバが HA の割り当て機能を実行します。さらに、モバイル IP サービスまたはプロキシ モバイル IP サービスのサポート対象となるドメインのある SLA に応じて、ローカル AAA サーバで複数の HA プールを設定できます。

ダイナミック IP アドレス

パケット データ サービスにアクセスするモバイル ステーションで、ホーム IP アドレスを設定する必要はありません。モバイル ユーザは、登録要求メッセージですべてゼロのホーム アドレスを提出することによって、ダイナミック割り当てのアドレスを要求できます。HA がホーム アドレスを割り当て、登録応答メッセージで MN に返します。HA はホーム AAA サーバにアクセスすることによって IP アドレスを取得します。AAA サーバは、ローカル プール名または単一の IP アドレスを返します。登録が成功すると、ユーザはモバイル IP ベースのサービスを利用できるようになります。

固定アドレッシング

各 NAI に固定アドレスを指定して HA を設定できます。固定アドレスは、登録するたびに MN に割り当てられます。この場合、ユーザはスタティック アドレッシングのすべての利点を生かしながら、MN の設定を簡素化できます。固定アドレッシングは、大規模展開には推奨できません。全ユーザ メンテナンスを実行するために、HA 設定をアップデートしなければならないからです。

設定例を示します。

```
router# ip mobile host nai user@realm.com address 10.0.0.1 interface FastEthernet0/0
```

ローカル プール割り当て

ローカル プールを割り当てるには、HA 上で 1 つまたは複数のアドレス プールを設定する必要があります。HA は先着順方式で、プールからアドレスを割り当てます。MN は HA にアクティブ バインディングがある限り、アドレスを維持します。MN は割り当てられたアドレスまたは 0.0.0.0 をホーム アドレスとした RRQ を送信することによって、バインディングをアップデートできます。バインディングが期限切れになると、ただちにアドレスがプールに返されます。

（注） 現在、ピアツーピア HA 冗長モデルでローカル プール割り当てを使用することはできません。設定できるローカル プール数を制限するものは、ルータ上で使用できるメモリだけです。

設定例を示します。

```
router (config)# ip local pool mippool 10.0.0.5 10.0.0.250
router (config)# ip mobile host nai @localpool.com address pool local mippool
virtual-network 10.0.0.0 255.255.255.0
```

DHCP 割り当て

DHCP は、デスクトップ コンピュータの IP アドレス割り当てにすでに広く用いられている方式です。IOS モバイル IP は、IOS にすでにある DHCP プロキシ クライアントを活用して、DHCP サーバにホーム アドレスを割り当てさせます。NAI は Client-ID オプションで送信され、ダイナミック DNS サービスの提供に使用できます。

設定例を示します。

```
router(config)# ip mobile host nai @dhcppool.com address pool dhcp-proxy-client
dhcp-server 10.1.2.3 interface FastEthernet 0/0
```

（注） 現在、ピアツーピア HA 冗長モデルで DHCP を使用することはできません。

AAA からのダイナミック アドレッシング

AAA からのダイナミック アドレッシングを使用すると、MN または HA でアドレッシングを維持する手間をかけなくても、MN の固定アドレッシング、セッション単位のアドレッシング、またはその両方をサポートできます。AAA サーバは特定のアドレス、ローカル プール名、または DHCP サーバ アドレスを返すことができます。AAA サーバを使用して特定のアドレスを返す場合は、RADIUS データベースの NAI エントリでアトリビュートとしてホーム アドレスを設定することも、または使用する AAA サーバの機能によっては、プールからホーム アドレスを割り当てることもできます。AAA サーバは、HA で設定されているローカル プールの名前または DHCP サーバの IP アドレスを返すこともできます。

設定例を示します。

HA 上：

```
router (config)# ip local pool dynamic-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com interface FastEthernet0/0 aaa
router (config)# ip mobile host nai @static.com interface FastEthernet0/0 aaa
```

AAA アドレス割り当て：
Cisco-AVPair = "mobileip:ip-address=65.0.0.71"

AAA ローカル プール アトリビュート：
Cisco-AVPair = "mobileip:ip-pool=dynamic-pool"

AAA DHCP サーバ アトリビュート：
Cisco-AVPair = "mobileip:dhcp-server=10.1.5.10"

（注）　Framed-IP-Address アトリビュートもサポートされます。

同一 NAI に複数のスタティック アドレスを使用する場合のアドレス割り当て

Cisco HA は、同じ NAI に複数のスタティック アドレスを使用する、マルチ モバイル IP 登録をサポートします。これは、ホーム AAA サーバまたは DHCP サーバで static-ip-address pool（複数可）を設定することによって実現されます。モバイル ユーザから登録要求メッセージを受信すると、HA はホーム AAA にアクセスして認証を行い、さらに通常は、IP アドレスを割り当てます。モバイル ユーザが提供した NAI はホーム AAA に送信されます。ホーム AAA サーバは、その NAI に対応するスタティック IP アドレスまたはスタティック IP プール名のリストを返します。

同一 NAI に異なるモバイル端末を使用する場合のアドレス割り当て

2 つの異なるモバイルから同じ NAI を使用して登録を行う場合、動作は次のようになります。

- 両方のケースでスタティック アドレス割り当てを使用する場合、それぞれ独立したケースと見なされます。
- 両方のケースでダイナミック アドレス割り当てを使用する場合、2 番目の登録が最初の登録に取って代わります。
- 最初の登録にスタティックを使用し、2 番目の登録にダイナミックを使用する場合、ダイナミック アドレス割り当てがスタティック アドレス割り当てに取って代わります。
- 最初の登録にダイナミックを使用し、2 番目にスタティックを使用する場合は、それぞれ独立したケースと見なされます。

さらに、2 つの異なる HA ながら、同じ NAI を使用する同じモバイルから発生した 2 つのフローは、別々のケースと見なされます。

設定例

DHCP プロキシ クライアント設定

アクティブ HA の設定

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
```

```
aaa session-id common
!
ip subnet-zero
ip cef
!
interface Loopback0
ip address 10.0.0.1 255.255.255.255
interface Ethernet2/0
 description to PDSN/FA
 ip address 10.0.0.2 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 10.0.0.4
 standby priority 110
 standby preempt delay sync 100
 standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 172.16.1.8 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!
router mobile
!
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
ip mobile secure home-agent 10.0.0.3 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
!
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
radius-server host 172.16.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

スタンバイ HA の設定

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
interface Loopback0
ip address 10.0.0.2 255.255.255.255
interface Ethernet2/0
 description to PDSN/FA
 ip address 10.0.0.3 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 standby ip 10.0.0.4
 standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 172.16.1.7 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.255
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy
ip mobile secure home-agent 10.0.0.2 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
```

```
 shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

CHAPTER 5

ユーザ認証および認可

この章では、ユーザ認証および認可について、さらに Cisco Mobile Wireless Home Agent でこの機能を設定する方法について説明します。

この章は、次の内容で構成されています。

ユーザ認証および認可

Home Agent（HA）は、PAP または CHAP を使用してユーザを認証するように設定できます。Foreign Agent（FA: 外部エージェント）チャレンジ手順がサポートされ（RFC 3012）、次の機能拡張が組み込まれています。

- モバイル IP エージェント アドバタイズ チャレンジの機能拡張
- MN-FA チャレンジの機能拡張
- MN-AAA 認証拡張機能

（注） MN-AAA 拡張機能がない場合は PAP を使用します。MN-AAA が存在する場合は、必ず CHAP を使用します。PAP ユーザのパスワードは、**ip mobile home-agent aaa user-password** コマンドで設定できます。

ホーム AAA サーバでユーザを認証するように設定されているときに、HA が Registration Request（RRQ; 登録要求）で MN-AAA 認証機能拡張を受信した場合は、その内容が使用されます。機能拡張がない場合は、デフォルトの設定可能なパスワードが使用されます。このデフォルトのパスワードは "vendor" など、ローカルで定義された文字列です。

HA は最初の登録の MN-FA チャレンジ機能拡張および MN-AAA 認証機能拡張（存在する場合）を受け付けて維持し、その後の登録更新で使用します。

HA が設定されたタイムアウトまでに AAA サーバから応答を受信しなかった場合は、設定可能な回数だけ、メッセージを再送できます。AAA サーバ グループと通信するように HA を設定できます。この場合、サーバはラウンドロビン方式で、設定された使用可能サーバから選択されます。

HA 上で認証および認可を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile host {lower [upper] | nai string {static-address {addr1 [addr2] [addr3] [addr4] [addr5] | local-pool name} | address {addr | pool {local name | dhcp-proxy-client [dhcp-server addr]} {interface name | virtual-network network_address mask} [skip-chap | aaa [load-sa [permanent]] [authorized-pool pool name] [skip-aaa-reauthentication] [care-of-access acl] [lifetime seconds]`	HA 上でモバイル ホストまたはモバイル ノード グループを設定します。 **aaa load-sa** オプションを設定した場合、HA は最初の登録でローカルに SA をキャッシュします。この場合、HA は再登録のための Remote Authentication Dial-In User Service（RADIUS）認証手順を開始しません。 **aaa load-sa skip-aaa-reauthentication** を設定した場合、HA は最初の登録でローカルに SA をキャッシュしますが、再登録のための HA-CHAP 手順は開始しません。 **aaa load-sa permanent** オプションは Mobile Wireless Home Agent ではサポートされないので、設定しないでください。

HA は RADIUS access accept パケットの 3GPP2 およびシスコ独自のセキュリティ機能拡張アトリビュートをサポートします。HA 上で、RADIUS サーバへのアクセス要求で 3GPP2 MN-HA SPI を送信し、RADIUS サーバから受け取った MN-HA 秘密鍵を処理することを設定できます。

Cisco IOS には、それぞれのレルムに基づいてサブスクライバを認可するメカニズムがあります。これには「サブスクライバの認可」という機能を使用します。詳細については、http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080455cf0.html#wp1056463 を参照してください。

（注） HA はユーザ プロファイルを受け付けますが、グループ プロファイルで返された情報に基づいて、モバイル サブスクライバを認可することはありません。

認証設定拡張機能

HA を使用して、特定のモバイル IP イベントについて AAA を使用した外部認証がいつ行われるかを設定できます。複数の FA をまたがるハンドオフは登録および登録解除イベントとして処理され、ハンドオフに対する特定の設定はありません。

再登録要求が前回の登録またはこのセッションに対する再登録に使用されたものとは別の SPI を使用して受信された場合は、このユーザの再登録時の認証に使用する設定オプション **enable** | **disable** は無視されます。

設定の適用または修正は、特定のバインディングに関する次回のイベントで行われます。

次の設定は、レルム単位（VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング））で行われる可能性のある再登録および登録解除イベント向けのものです。

ip mobile host nai *string* aaa **load-sa skip-aaa-reauth** [*reregistration* | *deregistration*]

デフォルト設定では、認証は 3 つのイベントすべてに対して発生します（**ip mobile host nai** *string* **aaa load-sa**）。

デフォルト設定が適切であることを前提とした例を次に示します。

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** を実行すると、AAA 認証は登録に対してのみ発生します。

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** *deregistration* を実行すると、AAA 認証は登録および再登録に対して発生します。

ip mobile host nai *string* **aaa skip-chap** を実行すると、初回登録、再登録、および登録解除イベントに対して認証は発生しません。

ip mobile host nai *string* **aaa load-sa skip-aaa-reauth** ***reregistration*** を実行すると、AAA 認証は登録および登録解除に対してのみ発生します。

load-sa キーワードを使用すると、HA はセッション全体にわたって mobile-home 認証に関するセキュリティ アトリビュートをダウンロードしてローカルで保存します。このパラメータを使用しなかった場合、HA は mobile-home 認証に関するセキュリティ アトリビュートをローカルで保存しないため、以降の再登録または登録解除時には AAA からこれらの情報を取得します。

Mobile-Home Authentication Extension（MHAE）を持たない 3GPP2 登録要求（RRQ）

現在、HA は RRQ での MN-HA オーセンティケータの拡張機能を必須機能として扱います。HA が MHAE 拡張機能を持たない RRQ を受信した場合、その RRQ は無視されます。

ただし MHAE 拡張機能は、標準/RFC に従うと必須ではないため、3GPP2 PMIP RRQ はこの機能を持たない場合があります。Cisco HA Release 5.1 では、MHAE 拡張機能を持たない 3GPP2 PMIP RRQ が FA-HA 認証に成功すれば、それを許可するよう HA を設定できます。

この機能を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent options mhae optional`	設定すると、HA は、MHAE を持たず、有効な Foreign-Home Authentication Extension（FHAE）を持った 3GPP2 RRQ を受信した場合、RRQ を処理します。

（注）　MHAE を持たず、有効な FHAE を持った CMIP RRQ を受信し、コマンドが設定されている場合、HA は RRQ を処理します。HA がこの RRQ を拒否しない理由は、HA が PMIP RRQ と CMIP RRQ を区別できないことです。この状況を回避するには、必ず FA が CMIP RRQ をチェックするようにして、FA が MHAE を持たない CMIP RRQ を HA に転送しないようにします。

3GPP2 のローカル認証

既存の HA 5.0 では、AAA からダウンロードした SA、またはローカルで設定されている HA のいずれかを使用してユーザを認証できます。これは、**ip mobile host nai** コンフィギュレーション コマンドで **aaa** キーワードを使用することでプロビジョニングできます。

HA 5.0 の機能はユーザ/nai ごとに設定できますが、アクセス タイプごとには設定できません。

HA Release 5.1 では、この機能をローカルの MN-HA SPI と Key を備えた NAI 認証と併用することで、ダウンロードした SA またはアクセス タイプに基づくローカル SA のいずれかを使用した柔軟なユーザ認証が可能になります。

この機能は、3gpp2 アクセス タイプにローカル SA を使用したユーザの認証、および Wimax アクセス タイプに AAA SA を使用した同一ユーザの認証に関する要件に対応しています。3gpp2 アクセス タイプ使用時は、アクセス要求は AAA に送信されません。

イネーブルな場合、RRQ が MN-AAA 拡張機能を備えている場合でも、アクセス要求は AAA に送信されません。

HA が 3GPP2 に対してローカル認証を実行するよう設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent options`	サブモードをイネーブルにして、3GPP2 に対するローカル認証の設定を許可します。
ステップ 2	`Router(config)#access-type 3gpp2 suppress aaa access-request`	設定を許可して、AAA へのアクセス要求を抑制します。

この設定を **ip mobile host nai aaa** および **ip mobile secure host nai** と併用した場合、3gpp2 アクセスタイプにローカル SA を使用したユーザの認証、および Wimax アクセス タイプに AAA SA を使用した同一ユーザの認証に関する要件に対応します。

ローカル MN-HA SPI および Key を使用した NAI 認証

HA R5.0 は、MN-HA セキュリティ アソシエーション（SA）または AAA からダウンロードした MN-HA SA 向けのローカル設定をサポートしますが、これら両方を同時にはサポートしません。

HA Release 5.1 では、HA は MN-HA SA および AAA からダウンロードした SA のローカル設定の両方をサポートします。SA がローカルに設定されているかどうかにかかわらず、HA が AAA からのアクセス応答メッセージ内の SA を受信した場合は、AAA からダウンロードした SA だけが MN-HA 認証に使用されます。

制限事項および制約事項

- **ip mobile host** コマンドが完全な NAI 向けに設定されている場合、対応するレルムにローカルで設定されている SA（単数または複数）は適用されません。ローカル SA を適用する必要がある場合、SA を完全な NAI に対して個別に設定する必要があります。

  次の例を考えてみましょう。

  - **ip mobile host nai *@cisco.com* virtual-network *ip1 mask1* aaa**
  - **ip mobile host nai** *user1@cisco.com* virtual-network ip2 mask2 **aaa**
  - **ip mobile secure host nai** *@cisco.com* **spi** *100* **key ascii** *CISCO*

  ここで、*@cisco.com* に設定されている SA は *user1@cisco.com*. には適用されません。ローカル SA をこのユーザに適用する必要がある場合は、次に示すとおり SA を個別に設定する必要があります。

  ip mobile secure host nai *user1@cisco.com* **spi** *100* **key ascii** *YAHOO*

- この機能がサポートされるのは 3GPP2 ユーザだけで、Wimax ユーザではサポートされません。

再登録 / 登録解除に対する無認可

ローカル MN-HA SPI および Key 機能と NAI 認証を併用すると、ローカル設定された SA および AAA からダウンロードした SA が共にサポートされます。

ただし、次のコマンドを設定すると、再認証と再認可が回避されるのは、MN-HA 向けの SA が Access-Accept で受信された場合に限られます。

```
router (config)# ip mobile host nai realm virtual-network ip mask aaa load-sa
skip-aaa-reauth [rereg | dereg]
```

ローカル登録時に MN-HA 認証がローカル SA を使用している場合は、上記の設定を使用しても、再認証 / 再認可は省略されません。これは、**load-sa** がキャッシュするのは、AAA からダウンロードした SA だけであるためです。

load-sa が設定されていれば、ローカル設定されている SA を使用している場合でも、この機能は SA のキャッシングをサポートします。**load-sa** が設定されている場合、ローカル設定されている SA を使用しても、再認証は回避されます。さらに、**skip-aaa-reauth** が設定されている場合、ローカル設定されている SA を使用すると、AAA を使用した再認証は回避されます。

[**rereg** | **dereg**] オプションを指定した場合、再登録または登録解除のどちらか一方だけに対して、再認証と再認可の回避を選択できます。

MN-FA Challenge Extension（MFCE）による HA-CHAP の省略

この機能を使用すると、ホーム AAA サーバで HA-CHAP 手順を実行して、各登録要求のユーザに対応するセキュリティ アソシエーション（SA）をダウンロードするのではなく、HA に SA をダウンロードさせ、ディスクにローカルにキャッシュさせることができます。HA は、ユーザが初めて HA に登録したときに、HA-CHAP（MN-AAA 認証）を行い、SA をダウンロードして、ローカルにキャッシュします。その後、再登録要求があると、HA はローカル キャッシュの SA を使用してユーザを認証します。ユーザのバインディングが削除されると、SA キャッシュ エントリが削除されます。

この機能は、上記の **ip mobile host** コマンドを使用して、HA 上で設定します。

設定例

次に、仮想ネットワーク 10.99.1.0 に配置するモバイル ノード グループを設定し、AAA サーバからモバイル ノードの SA を取得してキャッシュする例を示します。その後の再登録には、キャッシュの SA が使用されます。

```
ip mobile host 10.99.1.1 10.99.1.100 virtual-network 10.99.1.0 aaa load-sa
```

次に、cisco.com ドメインのモバイル ノードに IP アドレスを割り当てるために使用する、ローカルなダイナミック アドレス プールの設定例を示します。AAA サーバから受け取った SA は、手動で削除されるまで、永久にキャッシュされます。

```
ip mobile host nai @cisco.com address pool local mobilenodes virtual network 10.2.0.0
255.255.0.0 aaa load-sa permanent lifetime 180
```

認証および認可の RADIUS アトリビュート

HA および RADIUS サーバは、認証および認可サービスに関して、表 1 の RADIUS アトリビュートをサポートします。

表 1　Cisco IOS がサポートする認証および認可 AVP

Cisco IOS 名でサポートされる認証および認可 AVP	タイプ	ベンダー	長さ	フォーマット	説明	アクセス要求	アクセス受諾での可否
User-Name	1	該当しない	64	ストリング	認証および認可のユーザ名	可	不可
User-Password	2	該当しない	>=18 && <=130	ストリング	PAP 使用時の認証パスワード HA で CLI を使用して設定されたパスワード	可	不可
CHAP-Password	3	該当しない	19	ストリング	CHAP パスワード	可	不可
NAS-IP-Address	4	該当しない	4	IP アドレス	RADIUS サーバとの通信に使用する HA インターフェイスの IP アドレス	可	不可
Service Type	6	該当しない	4	整数	ユーザが利用するサービスのタイプ サポートされる値： • PAP 用に送信されるアウトバウンド • CHAP 用に送信されるフレーム化 • 両方のケースで受信するフレーム化	可	可
Framed-Protocol	7	該当しない	4	整数	フレーミング プロトコル ユーザが使用。CHAP の場合の送信、PAP および CHAP の場合の受信 サポートされる値： • PPP	可	可
Framed Compression	13	該当しない	4	整数	圧縮方式 サポートされる値： • 0：なし	不可	可
Framed-Routing	10	該当しない	4	整数	ルーティング方式 サポートされる値： • 0：なし	不可	可
Vendor Specific	26	該当しない			ベンダー固有のアトリビュート	可	可
CHAP-Challenge（任意）	60	該当しない	>=7	ストリング	CHAP Challenge	可	不可

表 1　Cisco IOS がサポートする認証および認可 AVP （続き）

Cisco IOS 名でサポートされる認証および認可 AVP	タイプ	ベンダー	長さ	フォーマット	説明	アクセス要求 アクセス受諾での可否	
NAS-Port-Type	61	該当しない	4	整数	ポート タイプ サポート対象： • 0：非同期	可	不可
spi#*n*	26/1	Cisco	>=3	ストリング	*n* は、1 ユーザに複数の SA を許可する、**0** から始まる数値 ID MIP 登録時にモバイル ユーザを認証するための、Security Parameter Index（SPI; セキュリティ パラメータ インデックス）を提供します。 コンフィギュレーション コマンド **ip mobile secure host** *addr* と同じ構文の情報です。基本的に、そのストリングの後ろに残りのコンフィギュレーション コマンドを一字一句指定します。	不可	可
static-ip-addresses	26/1	Cisco	>=3	ストリング	同じ NAI でマルチ フローのスタティック アドレスに対応する IP アドレス リスト	不可	可
static-ip-pool	26/1	Cisco	>=3	ストリング	同じ NAI でマルチ フローのスタティック アドレスに対応する IP アドレス プール名	不可	可
ip-addresses	26/1	Cisco	>=3	ストリング	ダイナミック アドレス割り当てに使用する IP アドレス リスト	不可	可
ip-pool	26/1	Cisco	>=3	ストリング	ダイナミック アドレス割り当てに使用する IP アドレス プール名	不可	可
dhcp-server	26/1	Cisco	>=3	ストリング	指定された DHCP サーバからアドレスを取得	不可	可
MN-HA SPI Key	26/57	3GPP2	6	整数	MN HA 共有鍵に対応する SPI	可	不可
MN-HA Shared Key	26/58	3GPP2	20	ストリング	MHAE を認証するためのセキュア キー	不可	可

CHAPTER 6

HA の冗長性

この章では、Home Agent（HA）の冗長性、HA の冗長性の実現方法、および Cisco Mobile Wireless Home Agent に冗長性を設定する方法について説明します。

この章は、次の内容で構成されています。

HA 冗長性の概要

1:1 の冗長性を提供するようシスコ HA を設定できます。Cisco Hot Standby Routing Protocol（RFC 2281 の HSRP）に基づいて、2 つの HA はホットスタンバイ モードで設定されます。これにより、アクティブ HA をイネーブルにして、モバイル セッション関連の情報をスタンバイ HA に連続してコピーし、両方の HA で同期化されたステート情報を維持します。アクティブな HA に障害が発生した場合、スタンバイ HA はサービスを中断させることなく引き継ぎます。

（注） モバイル IP HA 冗長性機能の NAI サポートは、HA 冗長性に CDMA2000 固有の機能を提供します。CDMA2000 フレームワークは、NAI に基づいてアドレスを割り当て、ユーザ NAI ごとに複数のスタティック IP アドレスをサポートする必要があります。

HA 冗長性機能は、スタティック IP アドレスの割り当てと AAA による IP アドレスの割り当てでサポートされます。Release 2.0 以降、HA 冗長性機能は、ローカル IP アドレス プールを使用したダイナミック IP アドレスの割り当てと、プロキシ DHCP を使用したダイナミック IP アドレスの割り当てでサポートされます。

HA 冗長性にプロキシ DHCP を使用したダイナミック IP アドレスの割り当てが設定されている場合、バインディングがスタンバイ HA に同期化されても、バインディングの起動中は DHCP 情報はスタンバイとは同期化されません。ただし、スタンバイ HA がアクティブになると、この HA の DHCP 関連情報をアップデートするため、既存の各バインディングの DHCP 要求が DHCP サーバに送信されます。

モバイル IP 登録プロセス中、HA は、Mobile Node（MN; モバイル ノード）のホーム IP アドレスを現在の MN の Care-of Address（CoA; 気付アドレス）にマッピングするモビリティ バインディング テーブルを作成します。HA に障害が発生した場合、モビリティ バインディング テーブルが失われ、HA に登録されたすべての MN は接続を失います。HA の障害による影響を削減するため、Cisco IOS ソフトウェアは HA 冗長性機能をサポートします。

（注） Cisco 7600 シリーズ プラットフォームに基づいた設定では、バックアップ HA イメージはプライマリと異なる Service Application Module for IP（SAMI）カードに設定されます。

HA 冗長性の機能は、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）のトップで動作します。HSRP はシスコが開発したプロトコルであり、ユーザ トラフィックがただちに透過的に障害から回復できる方法でネットワークの冗長性を提供します。

（注） Cisco Home Agent Release 5.0 以上でサポートされている冗長機能は、MIP-LAC、モバイル ルータ、VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）、L2TP Network Server（LNS; L2TP ネットワーク サーバ）としての Home Agent、および HA アカウンティング機能以外、Release 4.0 でサポートされているものと同じです。Change of Authorization 機能と Packet of Disconnect 機能は、アカウンティング機能から独立しているため、引き続きサポートされます。アクティブとスタンバイの冗長性の相互動作は、アクティブとスタンバイのサービス ブレードのコントロール プロセッサ間で行われます。このリリースでは、HA アカウンティング機能がサポートされないため、トラフィック間のプロセッサの冗長性は必要ありません。

（注） HA Release 5.0 以上は、シャーシ内とシャーシ間の冗長性をどちらもサポートします。

HA セッション冗長性のインフラストラクチャ

HA セッション冗長性の制限

リリース 4.0 までの HA ステートフル セッション冗長性は HSRP で実装されていました。この実装で、アクティブ HA とスタンバイの HA 間の転送はホーム エージェント アプリケーションによって実装されていました。UDP/IP ベースの転送実装には次の制限があります。

- バルク同期シナリオの不整合。たとえば、バルク同期の実行中にアクティブでバインディングが削除されると、バルク同期完了時にアクティブおよびスタンバイでのバインディングの数が一貫しなくなります。
- 複数パケット同期データの同期不能。これは、ホットライニング ルールの同期時に見られます。ホットライニング ルールの数が多いと、同期に必要なデータの長さが 1 つのパケットに収まるよりも大きくなります。複数パケットに断片化されたこのようなデータを同期化する能力は、冗長転送で実装されているパケット シーケンシング、フラグメンテーション、およびデフラグメンテーションのサポートの欠如により一貫しません。

セッション冗長性インフラストラクチャ機能拡張では、以前に述べた制限が廃止されています。Home Agent 5.0 リリースで HA SR インフラストラクチャは Component Cluster Manager（CCM）で実装されています。CCM ソフトウェアは、Redundancy Framework（RF; 冗長フレームワーク）/RF-Interdev および Check-Pointing Facility（CF）/Stream Control Transport Protocol（SCTP）を含む IOS ハイ アベイラビリティ インフラストラクチャ上に構築されています。RF/RF-Interdev は冗長性コントロール シグナリングを処理し、CF/SCTP は転送メカニズムを提供します。この HA SR の改正は、堅牢な転送、シャーシ間とシャーシ内の冗長性のサポートなど、IOS ハイ アベイラビリティ機能の利点となります。

サポートされている冗長性イベント

次に、既存の HA 4.0 冗長性イベントについて説明します。5.0 機能に実装された新機能により発生する新しい冗長性イベントについては、その機能についての項で説明します。

ダイナミック同期イベント

バインディングの作成

この同期は、アクティブからスタンバイへの IPMOBILE_BINDUPDATE_REQ メッセージを使用して伝えられます。スタンバイは PMOBILE_BINDUPDATE_ACK を使用してバインディングの再作成に成功したことを確認応答します。

バインディングの削除

この同期は、アクティブからスタンバイへの IPMOBILE_BINDDELETE_REQ メッセージを使用して伝えられます。スタンバイはアクティブへの IPMOBILE_BINDDELETE_ACK メッセージを使用してバインディングの削除に成功したことを確認応答します。

バインディングのアップデート

ホットライン ステータスのアップデート結果としての CoA に起因します。バインディングのホットライン ステータスがアップデートされる CoA メッセージをアクティブ HA が受信すると、IPMOBILE_BINDINTERIM_REQ メッセージを使用して既存のバインディング日付のアップデートがスタンバイに伝えられます。スタンバイは上記のメッセージを受信し、既存のバインディングをアップデートして、IPMOBILE_BINDINTERIM_ACK を使用してアップデート ステータスを伝えます。

アカウンティング カウンタの同期化の結果としてのバインディングのアップデート

コールの継続時間中にアカウンティング カウンタがアップデートされると、すべてのアカウンティング アップデート メッセージが IPMOBILE_BINDSYNC_REQ メッセージをスタンバイに送ります。ここには、スタンバイへのアップデートされたカウンタが含まれます。スタンバイはバインディングのためにカウンタをアップデートし、IPMOBILE_BINDSYNC_ACK メッセージを使用してアップデートのステータスをアップデートします。

表 6-1 に、上記のダイナミック同期イベントのために実装された新しい同期イベントをまとめています。

表 6-1　ダイナミック同期イベント

現在のイベント名	新しいイベント名	コメント
IPMOBILE_BINDUPDATE_REQ、IPMOBILE_BINDUPDATE_ACK	IPMOBILE_BIND_CREATE	バインディング作成の同期化のために使用します。
IPMOBILE_BINDINTERIM_REQ、IPMOBILE_BINDINTERIM_ACK	IPMOBILE_BIND_HOTLINE_UPDATE	CoA 処理に起因するバインディング アップデートの同期化のために使用します。

表 6-1　ダイナミック同期イベント （続き）

IPMOBILE_BINDDELETE_REQ、IPMOBILE_BINDDELETE_ACK	IPMOBILE_BIND_DELETE	このイベントは、De-Registration、Packet of Disconnect（PoD; パケット オブ ディスコネクト）、または Revocation の存在下で同期します。バインディングの削除は、このメッセージを使用して伝えられます。
IPMOBILE_BINDSYNC_REQ、IPMOBILE_BINDSYNC_ACK	このリリースではサポートされていません	このイベントはアカウンティング カウンタの同期に使用されます。ただし、同期化された HA アカウンティング カウンタは 5.0 ではサポートされません。
IPMOBILE_BINDINTERIM_EXTND_REQ	サポートされていません	同期メッセージ サイズが大きく、複数のパケットで送信する必要がある場合に、同期にこの要求が使用されます。これは、新しい SR では必要ありません。

バルク同期イベント

ルータがスタンバイとしてアップすると、IPMOBILE_BINDINFO_REQ を既存のアクティブに送信し、既存のバインディングをすべて取得します。アクティブは IPMOBILE_BINDINFO_RSP メッセージで応答します。これにはバインディング情報が含まれています。スタンバイは IPMOBILE_BINDINFO_RSP メッセージを処理して、その上でバインディングを再作成し、IPMOBILE_BINDINFO_ACK メッセージで再作成のステータスをアクティブに応答します。アクティブがホストできるバインディングの数は、500K に上ります。このため、バルク同期プロセス中、複数の IPMOBILE_BINDINFO_RSP メッセージと IPMOBILE_BINDINFO_ACK メッセージがアクティブとスタンバイ間でやり取りされます。新しい実装中、アクティブは各バインディングの IPMOBILE_BIND_CREATE イベントをバインド同期情報を持つスタンバイと同期します。

CCM ソフトウェアは、アクティブからスタンバイへのバインディングの同期中に、バルク同期プロセスをバンドリング モードで実装します。このプロセスは、HA アプリケーションに対して完全に透過的です。バンドリング モードで、CCM は同期パケットごとに複数のバインディング情報をスタンバイ CCM に送ります。また、CCM は CLI を使用して、バルク同期プロセスをコントロールします。バルク同期プロセスが cpu を独占する場合、オペレータは CLI 冗長性レートを使用できます。

subscriber redundancy rate # *of Sessions Per Unit Time*

このコマンドはバルク同期プロセスをコントロールします。バルク同期プロセス中に同期するバインディングの数が多い場合、#Sessions Per Unit Time 以上は同期しません。このコマンドは、バルク同期プロセスによって CPU が過負荷にならないようにします。

同期イベントの動作

新しい SR インフラストラクチャで、スタンバイはアクティブからのイベントとメッセージのレシーバーとして動作します。スタンバイがステータスや確認応答メッセージをアクティブに送信して、アクティブからの同期イベントの処理ステータスを伝えることはありません。このため、スタンバイからの IPMOBILE_BINDUPDATE_ACK、IPMOBILE_BINDINTERIM_ACK、IPMOBILE_BINDDELETE_ACK メッセージを新しいフレームワークで使用し続けることができません。これは、HA 4.0 リリースからの大きな変更です。アクティブ HA は、スタンバイが同期メッセージを正常にデコードし、バインディングを再作成、アップデート、削除できることを前提としています。

単一 IP の考慮事項

HA 単一 IP アーキテクチャで、SAMI ブレードは Control Plane（CP; コントロール プレーン）と Traffic Plane（TP; トラフィック プレーン）という 2 つの論理エンティティに分割されます。物理的に、CP 機能は SAMI ブレードの 6 PPC の最初にあり、後の 5 PPC は TP 処理を行います。トラフィック プレーン（TP）プロセッサが 5 つの PPC に分散されたトラフィックを処理する間に、CP プロセッサはコントロール シグナリング（バインディングすべてに関連した登録、登録解除、CoA、PoD など）をすべて処理します。

SR の観点から、冗長性コンテキストはアクティブとスタンバイの両方の CP 上にあります。このため、冗長性コントロール シグナリングと SCTP チャネルはアクティブとスタンバイの 2 つの CP 間で発生します。スタンバイ上の CP でバインディングの作成、アップデート、削除を動的に同期させるのは、アクティブ上の CP の役割です。同期メッセージを受信した場合、アクティブ CP がバインディングを TP に伝達するのと同じような方法で、TP 上のバインディングを伝達するのはスタンバイ上の CP の役割です。

単一 IP 機能は HA ソフトウェアに組み込まれていますが、これはアーキテクチャに関連付けられた、プラットフォーム固有の機能です。モバイル IP 冗長性設計は、アーキテクチャ固有部分に左右されません。

RADIUS ダウンロード プール名を使用した冗長性

Cisco Mobile Wireless HA は、アドレス割り当ての AAA ダウンロード可能プール名をサポートします。アドレス割り当ての access accept で戻された radius pool-name アトリビュートは、ダイナミック アドレス割り当ての "ip-pool" と、スタティック アドレス許可の "static-ip-pool" です。access accept で HA に戻されたプール名は、通常のバルク同期動作中にスタンバイ HA に同期化されます。これは、スタンバイ HA の同じプールからのアドレス割り当てもイネーブルにします。

HSRP グループ

HA 冗長性を設定する前に、HSRP グループの概念を理解しておく必要があります。

HSRP グループは、IP アドレスと Media Access Control（MAC; メディア アクセス制御）（レイヤ 2）アドレスを共有し、単一の仮想ルータとして機能する、複数のルータで構成されます。たとえば、モバイル IP トポロジには、1 つのアクティブ HA と、トポロジの残りが単一の仮想 HA として表示する 1 つまたは複数のスタンバイ HA を含めることができます。

モバイル IP が冗長性を実装できるように、HA のインターフェイスの所定の HSRP グループのアトリビュートを定義する必要があります。グループを使用して、グループ（物理ネットワーク）ネットワークまたは仮想ネットワークのどちらかのインターフェイス上にホーム リンクのある MN に冗長性を提供します。仮想ネットワークは、プログラミングされ、一般的な物理インフラストラクチャを共有する論理回線です。

HA 冗長性の動作方法

HA 冗長性機能を使用すると、1 つのアクティブ HA と 1 つまたは複数のスタンバイ HA を設定できます。冗長グループの HA は、HA が物理ネットワークをサポートする場合はアクティブ HA/スタンバイ HA のロールに、仮想ネットワークをサポートする場合はピア HA/ ピア HA ロールに設定できます。

物理ネットワークをサポートする場合、アクティブ HA は 中心的な HA ロールを想定し、スタンバイ HA を同期化します。仮想ネットワークをサポートする場合、ピア HA は中心的な HA ロールを共有し、互いに「アップデート」します。どちらかの HA が Registration Request（RRQ; 登録要求）を受信するので、ピア HA 設定では着信 RRQ のロード バランシングが可能になります。いずれのシナリオでも、冗長グループに参加する HA は同様に設定する必要があります。現在のサポート構造は 1:1 で、フェールオーバー時に最大のロバストネスと透過性を提供します。

HA 機能は、ルータが提供するサービスでインターフェイス固有ではありません。したがって、HA および MN は、MN が登録要求を送信する HA インターフェイスと、反対に HA が登録要求を受信する HA インターフェイスに同意する必要があります。この同意は次の 2 つのシナリオを考慮する必要があります。

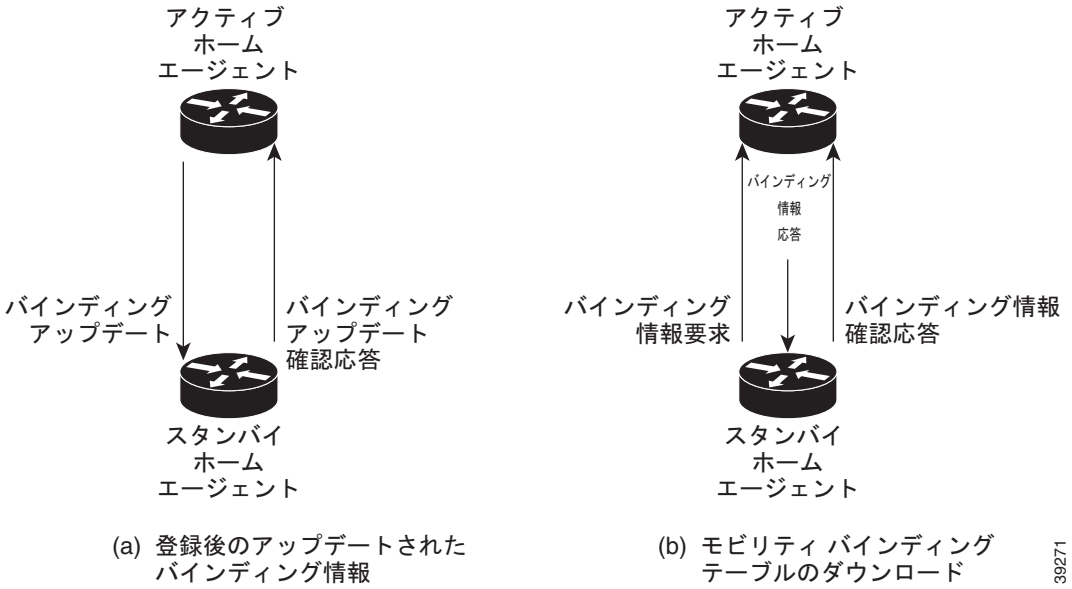
- MN には、MN と同じサブネット上にない HA インターフェイス（HA IP アドレス）があります。
- MN は、MN と同じサブネット上に HA インターフェイスを配置する必要があります。つまり、HA と MN は同じホーム ネットワーク上にいる必要があります。

物理ネットワークの MN の場合、アクティブ HA は MN からの登録要求を受け入れ、バインディング アップデートをスタンバイ HA に送信します。このプロセスでは、同期化されたアクティブおよびスタンバイ HA でモビリティ バインディング テーブルが維持されます。

仮想ネットワークの MN の場合、アクティブおよびスタンバイ HA はピアです。どちらかの HA が MN からの登録要求を処理し、モビリティ バインディング テーブルをピア HA でアップデートできます。

スタンバイ HA がアップすると、アクティブ HA からすべてのモビリティ バインディング情報を要求する必要があります。アクティブ HA は、モビリティ バインディング テーブルをスタンバイ HA にダウンロードすることで応答します。スタンバイ HA は、要求したバインディング情報を受信したことを確認応答します。図 1 に、モビリティ バインディングをスタンバイ HA にダウンロードするアクティブ HA を示します。この段階のプロセスの懸念事項は、スタンバイ HA が適切なモビリティ バインディング テーブルを取得するのに使用する HA IP インターフェイスと、バインディング要求が送信されるスタンバイ HA のインターフェイスです。

図 1　　HA 冗長性およびモビリティ バインディング プロセスの概要



（注）　アクティブ HA/スタンバイ HA はピア HA/ ピア HA 構成にすることもできます。

物理ネットワークのサポート

物理ネットワークの MN の場合、HA は図 2 および図 3 で示すアクティブ HA/スタンバイ HA 設定で設定されます。この物理ネットワークでサポートされる MN は、HA アドレスとして HSRP 仮想グループ アドレスで設定されます。したがって、HSRP 仮想グループ アドレスの所有者になるので、アクティブ HA だけが MN から RRQ を受信できます。認証された RRQ を受信すると、アクティブ HA はバインディング アップデートをスタンバイ HA に送信します。

アクティブ ステートである HA が 1 つだけで、スタンバイ ステートである HA が 1 つだけであっても、物理ネットワークの HA 冗長性は、冗長グループ内の複数の HA をサポートできます。たとえば、冗長グループに 4 つの HA があるシナリオを想定します（アクティブ HA が 1 つ、スタンバイ HA が 1 つ、リスニング ステートである HA が 2 つ）。アクティブ HA に障害が発生すると、スタンバイ HA がアクティブ HA になり、リスニング ステートで高いプライオリティのある HA がスタンバイ HA になります。

図 2　1 つの物理ネットワーク（ピア HA/ ピア HA）を使用した仮想ネットワークのサポート

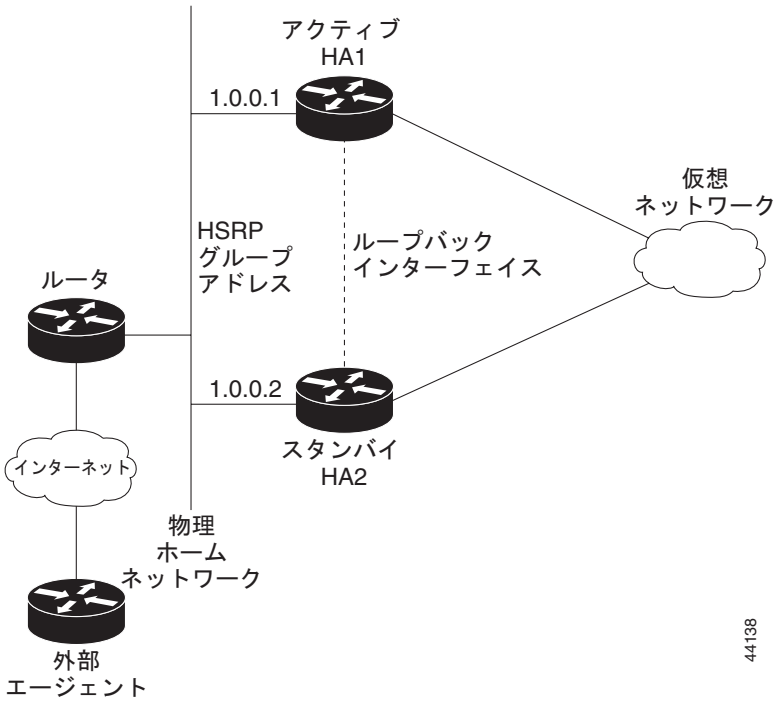
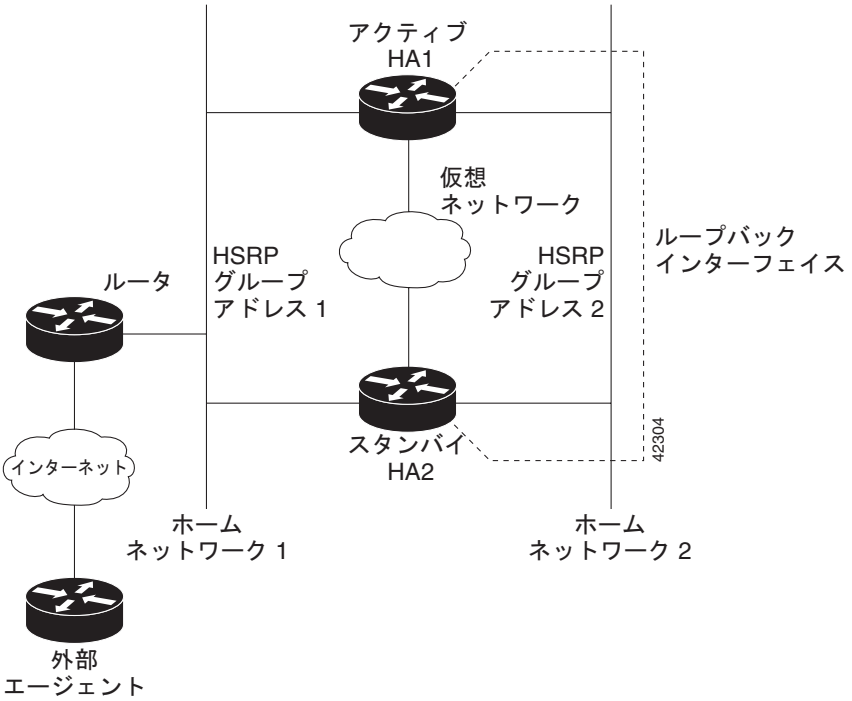


図 3　複数の物理ネットワーク（ピア HA/ ピア HA）を使用した仮想ネットワークのサポート



仮想ネットワーク

各 MN の モバイル IP コールは、MN のホーム IP アドレスの割り当て元であるホーム ネットワークに関連付けられています。これは物理ネットワークを想定していますが、ほとんどの展開の場合、各 MN を物理ネットワークに接続する意味はありません。IOS モバイル IP は、仮想ネットワークと呼ばれるソフトウェア インターフェイスの作成をサポートします。仮想ネットワークは、ループバック インターフェイスと非常に類似していますが、モバイル IP プロセスが所有します。仮想ネットワークを使用すると、Interface Descriptor Block（IDB; インターフェイス記述ブロック）を保存し、パケットのドロップ方法についてモバイル IP 固有の制御を実行できます。仮想ネットワークを使用すると、モバイル ノードは必ずローミングと見なされ、ホーム ネットワークに接続できません。実際の展開では、これにより一部の問題が発生します。たとえば、セルラー展開では、ユーザはホーム コーリング エリアにいますが、モバイル IP の観点ではローミングします。

仮想ネットワークは、ネットワーク数とマスク ペアによって設定され、参照されます。冗長目的で、仮想ネットワークと HA アドレスを関連付けることもできます。次に、例を示します。

```
ip mobile virtual-network 10.0.0.0 255.255.255.0 address 192.168.100.1
ip mobile host 10.0.0.1 10.0.0.254 virtual-network 10.0.0.0 255.255.255.0
```

仮想ネットワーク ルートはモバイル IP ルーティング プロセスによって所有されているので、伝播するため他のルーティング プロトコルに再配信する必要があります。次に、例を示します。

```
router rip
  redistribute mobile
```

同じレルムの不連続 IP アドレス プールのサポート

NAI を使用したモバイルが不連続 IP アドレス範囲のプールから割り当てられたホーム アドレスを持つことができるように、この機能では同じレルムの不連続 IP アドレス プールを指定できます。これにより、HA は同じホスト グループの複数の仮想ネットワークに属するモバイルを受け入れることができます。

これを実行するには、複数の仮想ネットワークの IP アドレス範囲をカバーした HA でローカル プールを設定し、所定のレルムのホーム ネットワークとして仮想ネットワークの 1 つを指定します。

次の設定を使用して、HA は同じホスト グループの複数の仮想ネットワークに属する MN を受け入れることができます。

```
ip local pool pool1 10.1.1.1 10.1.1.250
ip local pool pool1 10.1.2.1 10.1.2.250

ip mobile home-agent
ip mobile virtual-network 10.1.1.0 255.255.255.0
ip mobile virtual-network 10.1.2.0 255.255.255.0
ip mobile host nai @xyz.com address pool local pool1 virtual-network 10.1.1.0
255.255.255.0 aaa lifetime 65535
```

上記の設定では、2 つの仮想ネットワークが設定され、ローカル プール（pool1）は両方の仮想ネットワークの IP アドレスを含めるよう設定されます。**ip mobile host** コマンドで仮想ネットワークの 1 つとローカル プール名を指定することで、HA は同じレルムの両方のネットワークに属する MN を受け入れます。

ローカル プールのプライオリティ メトリック

アドレッシング スキームをダイナミックに変更する機能をサポートするには、ローカル アドレス プールのプライオリティ メトリックを設定します。これにより、新しいアドレス スキームのある高プライオリティ アドレス プールを作成します。新しいバインディングはこの新しいアドレス プールを使用します。既存のサブスクライバは切断されるまで、現在のアドレスを使用し続けます。再接続時、新しいプールからアドレスが割り当てられます。すべてのサブスクライバが古いアドレス プールをエージング アウトすると、プールは削除されます。

現在、異なるアドレッシング スキーム（アドレス範囲）が同じプール名の下に設定され、IP アドレスが設定順でプールから割り当てられます。まず、最初に設定されたアドレス範囲を使用して IP アドレスを割り当てます。すべてのアドレスを使用したら、以後の範囲を使用して IP アドレスを割り当てます。

上記のデフォルト動作を上書きし、異なるアドレス スキームを持つようサブスクライバを設定するには、プライオリティ値をプールに設定します。これにより、新しい登録要求が来たときに希望のプールから IP アドレスを割り当てることができるように、低いプライオリティ プールよりも高いプライオリティ プールを優先して使用できます。

デフォルトでは、プライオリティ値 255（高プライオリティ）が新しく作成されたローカル プールに割り当てられます。このプールのプライオリティ値は 1 ～ 255 です。0 は低いプライオリティで、255 は高いプライオリティです。

次に、例を示します。

```
ip local pool hapool 1.0.0.0 1.0.0.255
ip local pool hapool 2.0.0.0 2.0.0.255
```

この例では、プライオリティ 255 を持ったローカル プールを作成します。複数のアドレス スキームのプライオリティが同じである場合、IP アドレスは設定順に割り当てられます。まず、255 のホストすべてが最初のプールから割り当てられ、2 番目のプールは以後の要求に使用されます。

```
ip local pool hapool 1.0.0.0 1.0.0.255 priority 200
ip local pool hapool 2.0.0.0 2.0.0.255 priority 100
```

この例では、プライオリティ 255 を持ったローカル プールを作成します。この場合、IP アドレスはプライオリティ順に割り当てられます。まず、255 のホストすべてが 2 番目のプール（高プライオリティ 100）から割り当てられ、最初のプール（プライオリティ 200）は以後の要求に使用されます。

ローカル プールのプライオリティ値の設定

ローカル プールのプライオリティ値を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	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 point-to-point（p2p; ポイントツーポイント）インターフェイスに接続したときに使用され、プール使用率が上限または下限しきい値（パーセント単位）に達したときにトラップを生成するよう、IP アドレスのローカル プールを設定します。 新しいオプション **priority** *1-255* により、プライオリティを新しく作成されたプールに割り当てることができます。このプライオリティは IP アドレスの割り当てに使用されます。

HA 冗長性の設定

HA 冗長性の設定手順（モバイル IP に必須）

ルータにモバイル IP HA 冗長性を設定するには、次のセクションで説明する手順を実行します。

- 「モバイル IP のイネーブル化」（P.6-10）（必須）
- 「HSRP のイネーブル化」（P.6-10）（必須）
- 「HSRP グループのアトリビュートの設定」（P.6-11）
- 「物理ネットワークの HA 冗長性のイネーブル化」（P.6-11）（必須）
- 「HA ロード バランシングの設定」（P.6-11）

（注）　Cisco IOS Release 12.4(22)YD2 では、auto-sync all コマンドはデフォルトでディセーブルになっています。

モバイル IP のイネーブル化

ルータでモバイル IP をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)#router mobile`	ルータでモバイル IP をイネーブルにします。

HSRP のイネーブル化

インターフェイスで HSRP をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config-if)#standby [group-number] ip ip-address`	HSRP をイネーブルにします。

HSRP グループのアトリビュートの設定

ローカル ルータの HSRP への参加方法に影響を与える HSRP グループのアトリビュートを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドのいずれかを使用します。

	コマンド	目的
ステップ 1	Router(config-if)#**standby** [*group-number*] **priority** *priority* [**preempt** [**delay** [**minimum** | **sync**] *delay*]] or Router(config-if)#**standby** [*group-number*] [**priority** *priority*] **preempt** [**delay** [**minimum** | **sync**] *delay*]	アクティブ ルータの選択に使用するホットスタンバイ プライオリティを設定します。デフォルトでは、後でアップするルータはスタンバイになります。1 つのルータがアクティブ HA として指定されると、プライオリティは HSRP グループで最高位に設定され、プリエンプションが設定されます。ルータがアクティブになる前にすべてのバインディングがルータにダウンロードされるよう、**preempt delay min** コマンドを設定します。すべてのバインディングがダウンロードされる、またはいずれか早い方のタイマーが期限切れになると、ルータはアクティブになります。
ステップ 2	Router(config-if)# **standby** *group-number* **follow** *group-name*	follow グループの番号と、follow および共有ステータスに対するプライマリ グループの名前を指定します。 指定したグループ番号とプライマリ グループ番号が同じであることを推奨します。

物理ネットワークの HA 冗長性のイネーブル化

物理ネットワークの HA 冗長性をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router(config-if)#**standby** [*group-number*] **ip** *ip-address*	HSRP をイネーブルにします。
ステップ 2	Router(config-if)# **standby name** *hsrp-group-name*	スタンバイ グループの名前を設定します。
ステップ 3	Router(config)#**ip mobile home-agent redundancy**	HA の冗長性をイネーブルにします。
ステップ 4	Router(config)# **redundancy inter-device scheme standby** *hsrp-group-name* **ipc zone default** **association 1** **no shutdown** **protocol sctp** **local-port** *local-port-no* **local-ip** *local-ip-address* **remote-port** *remote-port-no* **remote-ip** *remote-ip-address*	HA 上で RF-Interdev を設定します。HA 冗長性は RF-Interdev 上に構築されます。

HA ロード バランシングの設定

HA ロード バランシング機能をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	Router(config)# **ip mobile home-agent dynamic-address** *ip address*	登録応答パケットの Home Agent Address フィールドを設定します。Home Agent Address フィールドを *ip address* に設定します。

HA 冗長性の設定例

アクティブ HA の設定

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
scheme standby cisco
!
!
!
redundancy
no keepalive-enable
logging message-counter syslog
!
!
ipc zone default
association 1
no shutdown
protocol sctp
local-port 5000
local-ip 10.0.0.2
remote-port 5000
remote-ip 10.0.0.3
!
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
no auto-sync all
!
ip subnet-zero
ip cef
!
interface GigabitEthernet0/0.10
description to PDSN/FA
encapsulation dot1Q 10
ip address 10.0.0.2 255.0.0.0
standby ip 10.0.0.4
standby priority 110
standby preempt delay min 100
standby name cisco
!
interface GigabitEthernet0/0.172
description to AAA
encapsulation dot1Q 172
ip address 172.16.1.8 255.255.0.0
!
```

```
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.254
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface
Ethernet2/0 aaa
!
radius-server host 172.16.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

スタンバイ HA の設定

```
~~~~~~~~~~~~~~~~~~~~
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
interface GigabitEthernet0/0.10
description to PDSN/FA
encapsulation dot1Q 10
ip address 10.0.0.2 255.0.0.0
standby ip 10.0.0.4
standby name cisco
!
interface Ethernet2/2
 description to AAA
 ip address 172.16.1.7 255.255.0.0
 no ip route-cache
 no ip mroute-cache
```

```
 duplex half
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.255
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface
Ethernet2/0 aaa
prefix-suffix
!
radius-server host 172.16.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
 shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

（注）　HA Release 5.0 以上では、冗長性のために **ip mobile secure home-agent** コマンドを設定する必要はありません。

ホットラインの冗長性サポート

（注）　Home Agent Release 5.1 は、3gpp2 バインディングと WiMax バインディングの両方のホットライニングに対する冗長性をサポートします。

QoS の冗長性サポート

Home Agent Release 4.0 以上では、アクティブ HA とスタンバイ HA の間のダイナミック実行時ポリシーマップ情報の連続したアップデートに関連する、フロー ベースの QoS（Quality of Service）ポリシングはサポートされません。HA は通常のバルク同期しかサポートしないので、ポリシング データまたはカウンタ統計情報の定期的なアップデートの正確度は低くなります。

コール アドミッション制御（CAC）の冗長性サポート

現在、Call admission control（CAC; コール アドミッション制御）の冗長性をサポートする必要はありません。ただし、バックアップ HA は自身のステートを維持します。

Framed-Pool 基準の冗長性サポート

冗長性はこの機能でサポートされます。追加コマンドをイネーブルにして、この機能をサポートする必要はありません。

ローカル プールのプライオリティ メトリックの冗長性サポート

冗長性はこの機能でサポートされます。追加コマンドをイネーブルにして、この機能をサポートする必要はありません。

モバイル IPv4 ホスト設定拡張の冗長性サポート

冗長性はこの機能でサポートされます。追加コマンドをイネーブルにして、この機能をサポートする必要はありません。

WiMAX AAA アトリビュートの冗長性サポート

冗長性はこの機能でサポートされます。追加コマンドをイネーブルにして、この機能をサポートする必要はありません。

HA 冗長性がイネーブルである場合、アクティブからのアクセス要求および Accounting メッセージに含まれるすべてのアトリビュートも、スイッチオーバー後のスタンバイからの対応するメッセージに含まれます。さらに、中間アカウンティング メッセージが、アクティブから送信されるのと同じインターバルでスタンバイから送信されます。これを実行するには、次のアトリビュートの値をスタンバイに同期化します。

- Chargeable User Identity（89）
- Acct-Multi-Session-Id（50）
- Acct-Interim-Interval（85）

SAMI 移行の冗長性サポート

シームレス移行に冗長性を設定し、サービスの中断を避ける必要があります。SAMI プラットフォームへの移行の詳細については、「Home Agent（HA）の設定プランニング」の「ユーザの移行」を参照してください。

CHAPTER 7

HA でのロード バランシングの設定

この章では、Cisco Mobile Wireless Home Agent でのサーバ ロード バランシングに関する概念と設定の詳細について説明します。

この章は、次の内容で構成されています。

HA サーバ ロード バランシング

HA Server Load Balancing（HA-SLB; HA サーバ ロード バランシング）機能は既存の IOS サーバ ロード バランシング（SLB）機能で構築されます。Server Load Balancing（SLB; サーバ ロード バランシング）によって、ネットワーク サーバのグループ（サーバ ファーム）を単一のサーバ インスタンスとして表示し、サーバへのトラフィックを分散させ、個別のサーバへのトラフィックを制限できます。サーバ ファームを示す単一のサーバ インスタンスは仮想サーバと呼ばれます。サーバ ファームを構成するサーバは実サーバと呼ばれます。

SLB は、実サーバに対するラウンド ロビンなどのメカニズムによってトラフィックを実サーバに配信できます。さらに、Dynamic Feedback Protocol（DFP）を使用して各実サーバのヘルスをモニタリングし、最小ロードを持ったサーバを選択し、アップ状態で稼動しているサーバを選択できます。SLB アーキテクチャの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps5940/products_white_paper0900aecd802921f0.shtml

HA-SLB 機能は Cisco 7600 シリーズ プラットフォームで使用できます。この機能により、Service Application Module for IP（SAMI）でそれぞれ稼動する一連の実 Home Agent（HA）を、Cisco 7600 スーパーバイザに存在する単一の仮想サーバの IP アドレスによって特定できます。

PDSN/FA はユーザの初期登録要求を仮想サーバの IP アドレスに送信します。SUP で稼動する HA-SLB はパケットを代行受信し、登録要求を実 HA の 1 つに転送します。

一般的なコール フローには次のイベント シーケンスがあります。

ステップ 1　PDSN/FA はモバイル IP Registration Request（RRQ; 登録要求）を仮想サーバ IP アドレス（HA-SLB）に転送します。Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）サーバが HA アドレスを PDSN/FA に戻す場合、仮想サーバ IP アドレスのアドレスを戻すよう AAA サーバを設定する必要があります。

ステップ 2　SLB は、サーバ ファームから実サーバ/HA の 1 つを選択し、モバイル IP RRQ をこのサーバに配信します。

ステップ 3　実 HA は Reply で MobileIP RRQ に応答し、メッセージは実 HA から PDSN/FA に送信されます。HA-SLB はこのパケットを代行受信しません。実 HA はバインディングとローカル トンネル エンドポイントを作成します。

ステップ 4　PDSN/FA は、ビジター テーブルとローカル トンネル エンドポイントを作成し、トンネル経由で実 HA から直接トラフィックを送受信します。

ステップ 5　PDSN/FA はライフタイム "0" を含んだモバイル IP RRQ を実 HA に送信してバインディングを終了します。

（注）　パケットは仮想 IP アドレス（HA-SLB）には送信されません。

ステップ 6　実 HA はモバイル IP RRP を PDSN/FA を送信します。HA-SLB はこのパケットを代行受信しません。実 HA は バインディングを終了します。

（注）　モバイル IP メッセージは RFC 2002 には準拠しませんが、draft-kulkarni-mobile-ip-dynamic-ha-assignment-frmwrk-00.txt に準拠します。

HA/SLB 仮想 IP アドレス宛てで、HA アドレス 0.0.0.0 または 255.255.255.255 のある RRQ は、重み付け「ラウンドロビン」、ロード バランシング アルゴリズムを使用して、実際の HA に転送されます。SLB メカニズムは、実サーバのヘルスをロード バランサに伝える機能を実サーバに与える DFP をサポートします。したがって、ロード バランシング アルゴリズムで実サーバの重みを調整します。

MN は、HA から RRP を受信する前に複数の RRQ を送信できるので（最初の RRQ を送信した後 MN の電源を再投入する、MN が最初の登録を複数送信するよう誤って設定されている、または RRP がネットワークによってドロップされる）、同じ MN から着信する登録を追跡することが重要です。これにより同じ MN が複数の HA で登録されるのを防ぐので、これらの HA では IP アドレスと他のリソースが浪費されます。この問題を解決するには、HA-SLB は RRQ を解析し、MN の Network Access Identifier（NAI; ネットワーク アクセス識別子）でインデックス化されたセッション オブジェクトを作成します。このセッション オブジェクトは、RRQ の転送先の実 HA IP アドレスを保存します。同じ MN からの以後の登録は、この同じ実 HA に転送されます。セッション オブジェクトは、設定可能な時間の間（デフォルトは 10 秒）保存されます。HA-SLB がこの時間内に MN からの RRQ を検出しない場合、セッション オブジェクトはクリアされます。HA-SLB が RRQ を検出すると、セッション オブジェクトに関連付けられたタイマーはリセットされます。

リトライ カウンタは各セッション オブジェクトに関連付けられ、ロード バランサによって検出され、再送信された RRQ ごとに増加します。検出された試行回数が設定された「再割り当て」しきい値よりも大きい場合、再送信するセッションは別の実 HA に再び割り当てられ、接続障害がオリジナルの実 HA に対して記録されます。接続障害が検出され、設定されたしきい値に到達すると、実サーバはダウン状態であると見なされ、RRQ を再転送しません。HA-SLB は、設定可能なタイム インターバルの経過後、または実サーバが DFP メッセージを HA-SLB に送信すると、その実サーバへのセッションの転送を再開します。

HA-SLB でのロード バランシング

HA-SLB は、ロード バランシング アルゴリズムの重み付けラウンドロビンを使用します。このアルゴリズムは、仮想サーバへの新しい接続に使用する実サーバを、サーキュラ方式でサーバ ファームから選択するよう指定します。実サーバごとに重み *n* が割り当てられます。仮想サーバに関連付けられた他の実サーバと比較した場合、これは接続を処理する容量を示します。たとえば、実サーバ ServerA（n = 3）、ServerB（n = 1）、ServerC（n = 2）を構成するサーバ ファームがあると想定します。仮想サーバへの最初の 3 つの RRQ は ServerA に、4 番目の RRQ は ServerB に、5 番目と 6 番目の RRQ は ServerC に割り当てられます。

スタティックまたはダイナミックなロード バランシングを実行するよう IOS SLB を設定できます。サーバ ファームの各 HA に重みをスタティックに割り当てることで、スタティック ロード バランシングを実行できます。SLB の DFP マネージャと実 HA の DFP クライアントそれぞれに、DFP を設定することで、ダイナミック ロード バランシングを実行できます。

HA-SLB の動作モード

HA-SLB は 2 つのモード（dispatched モードと Direct（NAT サーバ）モード）で動作します。

dispatched モードでは、仮想サーバ アドレスは HA に通知されます。HA-SLB は Media Access Control（MAC; メディア アクセス制御）レイヤでパケットを単に HA にリダイレクトします。これにより、HA は SLB に隣接するレイヤ 2 でなければいけません。

Direct モードでは、HA-SLB は NAT サーバ モードで動作し、RRQ の宛先 IP アドレスを実サーバの IP アドレスに変更することで、RRQ を HA へルーティングします。この場合、HA は SLB に隣接するレイヤ 2 である必要はありません。

ルータにモバイル IP HA 冗長性を設定するには、次のセクションで説明する手順を実行します。

- 「HA ロード バランシングの設定」（P.7-3）
- 「サーバ ロード バランシングの設定」（P.7-3）

HA ロード バランシングの設定

HA ロード バランシング機能をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent dynamic-address ip address`	登録応答パケットの Home Agent Address フィールドを設定します。Home Agent Address フィールドを *ip address* に設定します。このコマンドは HA で設定されます。

サーバ ロード バランシングの設定

HA でモバイル IP SLB 機能をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip slb vserver name` `Router(config-slb-vserver)# virtual ip address udp 434 service ipmobile`	モバイル IP SLB 機能をイネーブルにします。*ip address* は、PDSN/FA からの登録要求の送信先である仮想 HA のアドレスです。これは、SLB スーパーバイザで設定されます。

HA-SLB の設定例

次に、設定の詳細の検証方法を含めた、さまざまな HA-SLB 設定を示します。

スタティックな重みが設定された dispatched モード

SLB での設定：

次のコマンドは、サーバ ファーム "HAFARM" を設定し、2 つの実サーバ（HA）とサーバ ファームを関連付けます。実サーバにはスタティックな重みが設定されます。

```
ip slb serverfarm HAFARM
 real 10.1.1.51
  weight 1
  inservice
 !
 real 10.1.1.52
  weight 1
  inservice
```

次のコマンドは、SLB の "ipmobile" としてのサービスを仮想サーバに設定し、サーバ ファーム "HAFARM" と仮想サーバを関連付けます。任意で、**idle ipmobile request** *idle-time-val* コマンドは、セッション オブジェクトが存在する期間を設定します。

```
ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
```

HA での設定

次のコマンドは、HA にループバック アドレスとして仮想サーバ アドレスを設定します。この設定は、dispatched モードにだけ必要です。

```
interface Loopback1
ip address 10.1.1.10 255.255.255.0
```

次のコマンドは、実 HA のアドレスに対して、RRP の送信元アドレスおよび HA address フィールドを設定します。この設定は、dispatched モードにだけ必要です。

```
ip mobile home-agent dynamic-address 10.1.1.51
```

SLB での出力表示：

次のコマンドは、サーバ ファーム "HAFARM" のステータス、関連付けられた実サーバ、およびそのステータスを示します。各実サーバに割り当てられた接続の数も示します。

次の出力表示は、HA-SLB が 2 つの実 HA（HA ごとに 2 の接続）上で等しくロード バランシングした、4 つの MIP セッションを開始した後に取得されました。

```
SLB-7600#show ip slb reals

real                 farm name        weight  state          conns
---------------------------------------------------------------------
20.1.1.51            HAFARM           1       OPERATIONAL    2
20.1.1.52            HAFARM           1       OPERATIONAL    2
```

次のコマンドは、実行時またはセッション オブジェクトが存在する場合のセッションをすべて表示します。

```
SLB-7600#show ip slb sessions ipmobile

vserver         NAI hash           client             real                       state
-----------------------------------------------------------------------------------------
-
MIPSLB          A984DF0A00000000 15.1.1.51      20.1.1.52              IPMOBILE_ESTAB
MIPSLB          1DC0E31400000000 15.1.1.51       20.1.1.52              IPMOBILE_ESTAB
MIPSLB          2BDEE91100000000 15.1.1.51       20.1.1.51              IPMOBILE_ESTAB
MIPSLB          47E2FD1B00000000 15.1.1.51       20.1.1.51              IPMOBILE_ESTAB
SLB-7600#
```

HA での出力表示：

次のコマンドは、HA1 および HA2 で開始していた 2 つのバインディングを示します。

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7600#
```

DFP を使用した dispatched モード

SLB での設定：

次のコマンドは、サーバ ファーム "HAFAR" を設定し、2 つの実サーバ（HA）とサーバ ファームを関連付けます。

```
ip slb serverfarm HAFARM
 real 10.1.1.51
  inservice
 !
 real 10.1.1.52
  inservice
!
```

次のコマンドは、SLB の "ipmobile" としてのサービスを仮想サーバに設定し、サーバ ファーム HAFARM と仮想サーバを関連付けます。次の任意の idle ipmobile request *idle-time-val* コマンドは、セッション オブジェクトが存在する期間を設定します。

```
ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
```

次のコマンドは、HA-SLB に DFP マネージャを設定し、HA-SLB の接続先の 2 つの DFP エージェント（クライアント）を割り当てます。

```
ip slb dfp
 agent 10.1.1.51 500
 agent 10.1.1.52 500
!
```

HA での設定

次のコマンドは、HA にループバック アドレスとして仮想サーバ アドレスを設定します。この設定は、dispatched モードにだけ必要です。

```
interface Loopback1
ip address 10.1.1.10 255.255.255.0
!
```

次のコマンドは、実 HA に DFP エージェントを設定します。ここで設定されたポート番号は DFP マネージャで指定されたポート番号と一致する必要があります。

```
ip dfp agent ipmobile
 port 500
 inservice
!
```

次のコマンドは、実 HA のアドレスに対して、RRP の送信元アドレスおよび HA address フィールドを設定します。この設定は、dispatched モードにだけ必要です。

```
ip mobile home-agent dynamic-address 10.1.1.51
```

SLB での出力表示：

次のコマンドは、DFP の設定時に HA が最初の重み 25（デフォルトの重み）を報告することを検証します。

```
SLB-7600#show ip slb dfp weights
   Real IP Address: 10.1.1.51 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.51:500 at 14:59:23 UTC 04/21/03
   Real IP Address: 10.1.1.52 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.52:500 at 14:59:15 UTC 04/21/03
SLB-7600#
```

次のコマンドは、サーバ ファーム HAFARM のステータス、関連付けられた実サーバ、およびそのステータスを示します。各実サーバに割り当てられた接続の数も示します。

次の出力表示は、HA-SLB が 2 つの実 HA（HA ごとに 50 の接続）上で等しくロード バランシングした、100 の MIP セッションを開始した後に取得されました。

```
SLB-7600#show ip slb reals

real                  farm name        weight  state          conns
---------------------------------------------------------------------
10.1.1.51             HAFARM           24      OPERATIONAL    50
10.1.1.52             HAFARM           24      OPERATIONAL    50
SLB-7600#
```

HA での出力表示：

次のコマンドは、HA1 および HA2 で開始していた 50 のバインディングを検証します。

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA2-7600#
```

現在、バインディングの数とメモリ使用量は、HA-SLB のロード バランシングを計算するためのものと見なされます。各実サーバ（HA）の frequency of calls per second（CPS; 秒単位のコールの周波数）およびスループット パラメータを考慮することで、既存の DFP の重み計算式を修正できます。

毎分計算された HA での CPS は Usage CPS と呼ばれ、HA が処理できる最大値の一部（使用可能な CPS）に設定できます。Usage CPS が使用可能な CPS に到達したら、HA 実サーバは低い重みを SLB に戻します。

ルータでスループットを計算することは困難です。これはパケット処理のための割り込み CPU を使用することで解決できます。

上記の 2 つのパラメータから次の式が得られます。

dfp_weight = （Maxbindings – NumberofBindings）×（cpu+mem）×
（Available cps – Usage cps）× dftp_max_weight ÷（Maxbindings × 32 × Available cps）

（注） 現在、メトリックを含んだ MIB アイテムは使用できません。

スタティックな重みが設定された Direct モード

SLB での設定：

次のコマンドは、サーバ ファーム "HAFARM" を設定し、2 つの実サーバ（HA）とサーバ ファームを関連付けます。実サーバにはスタティックな重みが設定されます。**nat server** コマンドは、HA-SLB を動作の Direct（NAT サーバ）モードに設定します。

```
ip slb serverfarm HAFARM
nat server
real 10.1.1.51
  weight 1
  inservice
 !
 real 10.1.1.52
  weight 1
  inservice

ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
```

SLB での出力表示：

次に、サーバ ファーム HAFARM のステータス、関連付けられた実サーバ、およびそのステータスの例を示します。各実サーバに割り当てられた接続の数も示します。

次の出力表示は、HA-SLB が 2 つの実 HA（HA ごとに 2 つの接続）上で等しくロード バランシングした、4 つの MIP セッションを開始した後に取得されました。

```
SLB-7600#show ip slb reals

real                 farm name        weight  state          conns
-------------------------------------------------------------------
10.1.1.51            HAFARM           1       OPERATIONAL    2
10.1.1.52            HAFARM           1       OPERATIONAL    2
```

次のコマンドは、実行時またはセッション オブジェクトが存在する場合のセッションをすべて表示します。

```
SLB-7600#show ip slb sessions ipmobile

vserver         NAI hash         client          real                  state
-------------------------------------------------------------------------------
MIPSLB          A984DF0A00000000 15.1.1.51       10.1.1.52             IPMOBILE_ESTAB
MIPSLB          1DC0E31400000000 15.1.1.51       10.1.1.52             IPMOBILE_ESTAB
MIPSLB          2BDEE91100000000 15.1.1.51       10.1.1.51             IPMOBILE_ESTAB
MIPSLB          47E2FD1B00000000 15.1.1.51       10.1.1.51             IPMOBILE_ESTAB

SLB-7600#
```

HA での出力表示：

次に、HA1 および HA2 で開始していた 2 つのバインディングの例を示します。

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 2
HA2-7600#
```

イネーブルである次のデバッグは、NAT サーバ モードが動作中であることを示します。

```
SLB-7600#debug ip slb sessions ipmobile
SLB-7600#
*Apr 21 15:25:58: %SYS-5-CONFIG_I: Configured from console by console
*Apr 21 15:26:03: SLB_SESSION_IPMOBILE: client = 15.1.1.51, NAI:
mwts-mip-np-user1@ispxyz.com, length: 28
*Apr 21 15:26:03: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:26:03: SLB_SESSION: v_ip= 15.1.1.10:434 (  7), real= 10.1.1.51, NAT= S
*Apr 21 15:26:03: SLB_SESSION: client= 15.1.1.51:434 session_key= 47E2FD1B00000000
SLB-7600#
```

DFP を使用した Direct モード

SLB での設定：

次のコマンドは、サーバ ファーム "HAFARM" を設定し、2 つの実サーバ（HA）とサーバ ファームを関連付けます。**nat server** コマンドは、HA-SLB を動作の Direct（NAT サーバ）モードに設定します。

```
ip slb serverfarm HAFARM
nat server
real 10.1.1.51
  inservice
 !
 real 10.1.1.52
  weight 1
  inservice
!
```

次のコマンドは、SLB の "ipmobile" としてのサービスを仮想サーバに設定し、サーバ ファーム HAFARM と仮想サーバを関連付けます。任意の **idle ipmobile request** *idle-time-val* コマンドは、セッション オブジェクトが存在する期間を設定します。

```
ip slb vserver MIPSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm HAFARM
 idle ipmobile request 300
 inservice
!
```

次のコマンドは、HA-SLB に DFP マネージャを設定し、HA-SLB の接続先の 2 つの DFP エージェント（クライアント）を割り当てます。

```
ip slb dfp
 agent 10.1.1.51 500
 agent 10.1.1.52 500
```

HA での設定

次のコマンドは、実 HA に DFP エージェントを設定します。設定されたポート番号は DFP マネージャで指定されたポート番号と一致する必要があります。

```
ip dfp agent ipmobile
 port 500
 inservice
!
```

SLB での出力表示：

次のコマンドは、DFP の設定時に HA が最初の重み 25（デフォルトの重み）を報告することを検証します。

```
SLB-7600#show ip slb dfp weights
   Real IP Address: 10.1.1.51 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.51:500 at 14:59:23 UTC 04/21/03
   Real IP Address: 10.1.1.52 Protocol: UDP Port: 434 Bind_ID: 65535 Weight: 25
      Set by Agent 10.1.1.52:500 at 14:59:15 UTC 04/21/03
SLB-7600#
```

次のコマンドは、サーバ ファーム "HAFARM" のステータス、関連付けられた実サーバ、およびそのステータスを示します。各実サーバに割り当てられた接続の数も示します。

次の出力表示は、HA-SLB が 2 つの実 HA（HA ごとに 50 の接続）上で等しくロード バランシングした、100 の MIP セッションを開始した後に取得されました。

```
SLB-7600#show ip slb reals

real                 farm name        weight  state          conns
-------------------------------------------------------------------
10.1.1.51            HAFARM           24      OPERATIONAL    50
10.1.1.52            HAFARM           24      OPERATIONAL    50
SLB-7600#
```

HA での出力表示：

次のコマンドは、HA1 および HA2 で開始していた 50 のバインディングを示します。

```
HA1-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA1-7600#

HA2-7600#show ip mobile binding summary
Mobility Binding List:
Total 50
HA2-7600#
```

イネーブルである次のデバッグは、NAT サーバ モードが動作中であることを示します。

```
SLB-7600#debug ip slb sessions ipmobile
SLB-7600#
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: client = 10.1.1.51, NAI:
mwts-mip-np-user1@ispxyz.com, length: 28
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:47:16: SLB_SESSION: v_ip= 10.1.1.10:434 (  7), real= 20.1.1.51, NAT= S
*Apr 21 15:47:16: SLB_SESSION: client= 10.1.1.51:434 session_key= 47E2FD1B00000000
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: client = 15.1.1.51, NAI:
mwts-mip-np-user2@ispxyz.com, length: 28
*Apr 21 15:47:16: SLB_SESSION_IPMOBILE: event= IPMOBILE_REQ_REQUEST, state= IPMOBILE_INIT
-> IPMOBILE_ESTAB
*Apr 21 15:47:16: SLB_SESSION: v_ip= 10.1.1.10:434 (  7), real= 20.1.1.51, NAT= S
*Apr 21 15:47:16: SLB_SESSION: client= 10.1.1.51:434 session_key= 1DC0E31400000000
```

動作の Direct モードおよび暗号転送モードが Tunnel である場合

```
Configuration on SLB:
ip slb serverfarm FARM1
 nat server
 real 10.99.11.11
  inservice
 !
 real 10.99.11.12
  inservice
!
ip slb vserver IPSECSLB
 virtual 15.1.1.10 udp 434 service ipmobile
 serverfarm FARM1
 inservice
```

次のコマンドは、HA-SLB で IPSEC を設定します。

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.51
 set transform-set esp-des-sha-transport
 match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,15,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet6/2       (outside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
```

```
 switchport mode trunk
 cdp enable
!
interface FastEthernet3/15
 no ip address
 duplex full
 speed 100
 crypto connect vlan 15
!
!
interface Vlan15
 ip address 10.1.1.15 255.0.0.0
 no ip redirects
 no ip unreachables
 no mop enabled
 crypto map l2tpmap
!
!
access-list 101 permit ip host 10.1.1.10 host 10.1.1.51
```

PDSN での設定：

```
The following commands configure IPSEC on PDSN:
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 10.1.1.51 255.0.0.0
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 10.1.1.51 host 10.1.1.10
```

clear crypto isakmp および **clear crypto sa** を PDSN および SLB で実行します。複数の MIP フローを開きます。

PDSN での出力表示：

次のコマンドを使用して、PDSN から送信されたパケットが暗号化されているか確認します。

```
PDSN-7600#sh crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: l2tpmap, local addr. 10.1.1.51

   local  ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   current_peer: 10.1.1.15
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 4, #recv errors 0
```

```
     local crypto endpt.: 10.1.1.51, remote crypto endpt.: 10.1.1.15
     path mtu 1500, media mtu 1500
     current outbound spi: 1A274E9D

     inbound esp sas:
      spi: 0xD3D5F08B(3554013323)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3026)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0x7FEE86C3(2146338499)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3026)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0x1A274E9D(438783645)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3026)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
      spi: 0x5F9A83(6265475)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3026)
        replay detection support: Y

     outbound pcp sas:


PDSN-7600#
```

SLB での出力表示：

次のコマンドを使用して、HA-SLB が受信したパケットが復号化されているか確認します。

```
SLB1-7600#sh crypto ipsec sa

interface: Vlan15
    Crypto map tag: l2tpmap, local addr. 10.1.1.15

   local  ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   current_peer: 15.1.1.51
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

```
      local crypto endpt.: 15.1.1.15, remote crypto endpt.: 10.1.1.51
      path mtu 1500, media mtu 1500
      current outbound spi: D6C550E1

      inbound esp sas:
       spi: 0x267FCD46(645909830)
         transform: esp-des ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 11027, flow_id: 63, crypto map: l2tpmap
         sa timing: remaining key lifetime (k/sec): (4607999/3581)
         IV size: 8 bytes
         replay detection support: Y

      inbound ah sas:
       spi: 0xF779A01E(4151943198)
         transform: ah-sha-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 11025, flow_id: 63, crypto map: l2tpmap
         sa timing: remaining key lifetime (k/sec): (4607999/3581)
         replay detection support: Y

      inbound pcp sas:

      outbound esp sas:
       spi: 0xD6C550E1(3603255521)
         transform: esp-des ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 11028, flow_id: 64, crypto map: l2tpmap
         sa timing: remaining key lifetime (k/sec): (4608000/3581)
         IV size: 8 bytes
         replay detection support: Y

      outbound ah sas:
       spi: 0x325BEB84(844884868)
         transform: ah-sha-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 11026, flow_id: 64, crypto map: l2tpmap
         sa timing: remaining key lifetime (k/sec): (4608000/3581)
         replay detection support: Y

      outbound pcp sas:

SLB1-7600#sh ip slb sessions ipmobile

vserver         NAI hash         client          real                  state
-----------------------------------------------------------------------------
IPSECSLB        A984DF0A00000000 10.1.1.51       10.99.11.12           IPMOBILE_ESTAB
IPSECSLB        1DC0E31400000000 10.1.1.51       10.99.11.12           IPMOBILE_ESTAB
IPSECSLB        2BDEE91100000000 10.1.1.51       10.99.11.11           IPMOBILE_ESTAB
IPSECSLB        47E2FD1B00000000 10.1.1.51       10.99.11.11           IPMOBILE_ESTAB
SLB1-7600#
SLB1-7600#sh ip slb
SLB1-7600#sh ip slb rea
SLB1-7600#sh ip slb reals

real                  farm name        weight  state          conns
---------------------------------------------------------------------
10.99.11.11           FARM1            1       OPERATIONAL    2
10.99.11.12           FARM1            1       OPERATIONAL    2
SLB1-7600

Show output on SLB:
HA5-2#sh ip mob binding summary
```

```
Mobility Binding List:
Total 2
HA5-2#

HA5-3#sh ip mob binding summary
Mobility Binding List:
Total 2
HA5-3#
```

SLB でのデバッグの出力：

イネーブルである次のデバッグは、NAT サーバ モードが動作中であることを示します。

```
SLB1-7600#debug ip slb sessions ipmobile
*Jul  1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
*Jul  1 05:25:25.513: SLB_SESSION: v_ip= 15.1.1.10:434 (  7), real= 99.99.11.12, NAT= S
*Jul  1 05:25:25.513: SLB_SESSION: client= 15.1.1.51:434 session_key= A984DF0A00000000
*Jul  1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
*Jul  1 05:25:25.513: SLB_SESSION: v_ip= 15.1.1.10:434 (  7), real= 99.99.11.11, NAT= S
*Jul  1 05:25:25.513: SLB_SESSION: client= 15.1.1.51:434 session_key= 2BDEE91100000000
*Jul  1 05:25:25.513: SLB_SESSION_IPMOBILE: event= IPMOBILE_TIMEOUT, state= IPMOBILE_ESTAB
-> IPMOBILE_INIT
```

動作の Direct モードおよび暗号転送モードが Transport である場合

SLB での設定：

```
ip slb serverfarm FARM1
 nat server
 real 10.99.11.11
  inservice
 !
 real 10.99.11.12
  inservice
!
ip slb vserver IPSECSLB
 virtual 10.1.1.10 udp 434 service ipmobile
 serverfarm FARM1
 inservice
```

次のコマンドは、HA-SLB で IPSEC を設定します。

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.51
!
!
crypto ipsec transform-set esp-des-sha-transport ah-sha-hmac esp-des
 mode transport    (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.51
 set transform-set esp-des-sha-transport
 match address 101
!
interface GigabitEthernet6/1 (inside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,15,1002-1005
```

```
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet6/2       (outside port of the IPSEC module)
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,16,1002-1005
 switchport mode trunk
 cdp enable
!
interface FastEthernet3/15
 no ip address
 duplex full
 speed 100
 crypto connect vlan 15
!
!
interface Vlan15
 ip address 15.1.1.15 255.0.0.0
 no ip redirects
 no ip unreachables
 no mop enabled
 crypto map l2tpmap
!
!
access-list 101 permit ip host 15.1.1.10 host 15.1.1.51
```

PDSN での設定：

次のコマンドは、PDSN で IPSEC を設定します。

```
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.15
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport           (The crypto mode is configured as transport )
!
crypto map l2tpmap 10 ipsec-isakmp
 set peer 10.1.1.15
 set transform-set esp-des-sha-transport
 match address 101

interface FastEthernet1/0
 ip address 10.1.1.51 255.0.0.0
 duplex full
 crypto map l2tpmap

access-list 101 permit ip host 15.1.1.51 host 15.1.1.10
```

clear crypto isakmp および **clear crypto sa** を PDSN および SLB で実行します。複数の MIP フローを開きます。

PDSN での出力表示：

次のコマンドを使用して、PDSN から送信されたパケットが暗号化されているか確認します。

```
PDSN-7600#sh crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: l2tpmap, local addr. 10.1.1.51

   local  ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   current_peer: 10.1.1.15
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 4, #recv errors 0

     local crypto endpt.: 10.1.1.51, remote crypto endpt.: 10.1.1.15
     path mtu 1500, media mtu 1500
     current outbound spi: 6A0EBD82

     inbound esp sas:
      spi: 0x13E0E556(333505878)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2002, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3535)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0xEFEEE153(4025409875)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3535)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6A0EBD82(1779350914)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2003, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3535)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:
      spi: 0x49BE92A3(1237226147)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3535)
        replay detection support: Y

     outbound pcp sas:


PDSN-7600#
```

SLB での出力表示：

```
SLB1-7600#sh ip slb sessions ipmobile

vserver         NAI hash         client          real                    state
---------------------------------------------------------------------------
IPSECSLB        A984DF0A00000000 10.1.1.51       99.99.11.12             IPMOBILE_ESTAB
IPSECSLB        1DC0E31400000000 10.1.1.51       99.99.11.12             IPMOBILE_ESTAB
IPSECSLB        2BDEE91100000000 10.1.1.51       99.99.11.11             IPMOBILE_ESTAB
IPSECSLB        47E2FD1B00000000 10.1.1.51       99.99.11.11             IPMOBILE_ESTAB
SLB1-7600#
SLB1-7600#sh ip slb rea
SLB1-7600#sh ip slb reals

real                  farm name        weight  state          conns
-------------------------------------------------------------------
99.99.11.11           FARM1            1       OPERATIONAL    2
99.99.11.12           FARM1            1       OPERATIONAL    2
SLB1-7600#
SLB1-7600#
```

次のコマンドを使用して、HA-SLB が受信したパケットが復号化されているか確認します。

```
SLB1-7600#sh crypto ipsec sa

interface: Vlan15
    Crypto map tag: l2tpmap, local addr. 10.1.1.15

   local  ident (addr/mask/prot/port): (10.1.1.10/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.51/255.255.255.255/0/0)
   current_peer: 10.1.1.51
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 15.1.1.15, remote crypto endpt.: 15.1.1.51
     path mtu 1500, media mtu 1500
     current outbound spi: 13E0E556

     inbound esp sas:
      spi: 0x6A0EBD82(1779350914)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11031, flow_id: 65, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3527)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
      spi: 0x49BE92A3(1237226147)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11029, flow_id: 65, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4607999/3527)
        replay detection support: Y

     inbound pcp sas:

     outbound esp sas:
      spi: 0x13E0E556(333505878)
        transform: esp-des ,
```

```
        in use settings ={Tunnel, }
        slot: 0, conn id: 11032, flow_id: 66, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3527)
        IV size: 8 bytes
        replay detection support: Y

      outbound ah sas:
       spi: 0xEFEEE153(4025409875)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 11030, flow_id: 66, crypto map: l2tpmap
        sa timing: remaining key lifetime (k/sec): (4608000/3524)
        replay detection support: Y

      outbound pcp sas:


SLB1-7600#
```

HA での出力表示：

```
HA5-2#sh ip mob binding summary
Mobility Binding List:
Total 2
HA5-2#

HA5-3#sh ip mob binding summary
Mobility Binding List:
Total 2
HA5-3#
```

CHAPTER 8

IP 登録の終了

この章では、Cisco Mobile Wireless Home Agent が IP 登録を終了し、この機能を実行するよう Home Agent（HA）を設定する方法について説明します。

この章は、次の内容で構成されています。

モバイル IPv4 登録の失効

基本的なモバイル IP リソースの失効は、モビリティ エージェント（モバイル IP サービスをモバイル ノードに提供する）が他のモビリティ エージェントに、管理上の理由または Mobile IP（MIP; モバイル IP）ハンドオフによって登録の終了を通知できる方式を定義する IS-835-C イニシアチブです。

この機能は、Cisco MobileIP Bind Update 機能と類似しています。モバイルが接続ポイント（Foreign Agent（FA; 外部エージェント））を変更する、または管理上、セッションを終了する必要がある場合、HA は Registration Revocation メッセージを古い FA に送信します。古い FA はセッションを切断し、Registration Revocation acknowledgement（ACK）メッセージを HA に送信します。さらに、PDSN（Packet Data Serving Node）/FA が管理上、セッションを終了する必要がある場合、FA は Registration Revocation メッセージを HA に送信します。HA はモバイルのバインディングを削除し、Registration Revocation ACK を FA に送信します。

モバイル IPv4 の登録失効をサポートするよう設定された HA には、有効な登録失効拡張を含んだ PDSN から関連付けられた MIP Registration Request（RRQ; 登録要求）に対するすべての MIP RRP の失効サポート拡張が含まれます。HA が失効サポート拡張を受信し、以後の失効サポート拡張に応答した登録は、HA によって取り消し可能と見なされます。

次のコール フローでは、モバイル IP リソース失効（登録 フェーズ）を示します。

ステップ 1　MS はコールを発信し、Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）セッションがアップします。

ステップ 2　MIPv4 登録失効サポートをアドバタイズするよう PDSN/FA は設定されました。PDSN/FA は MIPv4 登録失効サポート ビット "X" セットのあるアドバタイズメントを送信します。

ステップ 3　PDSN/FA は Mobile Node（MN; モバイル ノード）から MIP RRQ を受信します。これには、FA-Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）時のアクセス要求で **2** に設定された Session Termination Capability（STC）アトリビュートが含まれます。RRQ を HA を転送すると、失効サポート拡張が Mobile-Home Authentication Extension（MHAE）の後に追加されます。失効サポート拡張の I-bit は **1** に設定され、必要な場合はいつでも MS がバインディングの失効に関する明示的な通知を受け取ったことを示します。

ステップ 4　失効拡張を含んだ MIP RRQ を受信すると、HA は失効サポート拡張を含み、I-bit を MIP RRQ で受信した値に設定する MIP RRP を戻します。HA-CHAP（MN-Authentication, Authorization and Accounting（AAA; 認証、許可、アカウンティング）認証）の場合、STC アトリビュート（値 **2**）は、AAA に送信されたアクセス要求に含まれます。

ステップ 5　PDSN は失効サポート拡張を含んだ MIP RRP を受信します。データ フローは取り消し可能と見なされます。

次のコール フローでは、モバイル IP リソース失効（HA が開始）を示します。

ステップ 1　モバイルは、PDSN/FA（1）のあるモバイル IP データ セッションを開始します。

ステップ 2　PDSN/FA（1）は、登録失効サポート拡張をモバイル登録要求に追加し、これを HA に転送します。

ステップ 3　応答として、HA は登録失効サポート拡張を登録応答に追加し、これを PDSN/FA（1）に送信します。

ステップ 4　PDSN/PDSN ハンドオフが発生し、モバイルは PDSN/FA（2）のあるモバイル IP データ セッションを再開します。

ステップ 5　PDSN/FA（2）は登録要求を HA に送信します。

ステップ 6　HA は登録応答を PDSN/FA（2）に送信します。

ステップ 7　HA はモバイル IP Resource Revocation メッセージを PDSN/FA（1）に送信します。

ステップ 8　PDSN/FA（1）はモバイル IP リソース失効 ACK を HA に送信し、モバイルのモバイル IP データ セッションを終了します。

次のコール フローでは、モバイル IP リソース失効（FA が失効を開始）を示します。

ステップ 1　モバイルは、PDSN/FA のあるモバイル IP データ セッションを開始します。

ステップ 2　PDSN/FA は、登録失効サポート拡張をモバイル登録要求に追加し、これを HA に転送します。

ステップ 3　応答として、HA は登録失効サポート拡張を登録応答に追加し、これを PDSN/FA に送信します。

ステップ 4　PDSN/FA では一部のイベントが発生し、PDSN/FA はセッションを終了するよう決定します。

ステップ 5　PDSN/FA はモバイル IP Resource Revocation メッセージを HA に送信します。

ステップ 6　HA はモバイル IP リソース失効 ACK を PDSN/FA に送信します。HA はバインディングをクリアし、PDSN/FA はセッションをクリアします。

I-bit のサポート

登録失効フェーズ中、Mobile Node（MN; モバイル ノード）に複数のモバイル IP フローがある場合に、I（Inform）ビットは、MN に対して失効したデータ サービスを通知します。登録フェーズ中、RRQ/RRP の失効サポート拡張のモビリティ エージェントによってこのビットが **1** に設定されている場合、エージェントが Revocation メッセージの "I" ビットの使用をサポートすることを示します。

現在の実装では、MobileIP RRQ が失効サポート拡張に設定された I ビットで受信された場合、HA も I-bit を **1** に設定します。I-bit は失効フェーズ中も使用できます。HA が失効を開始した（I ビットはネゴシエートされた）ときに、バインディングが管理上、解除された場合、HA は I ビットを Revocation メッセージで **1** に設定します。PDSN 間ハンドオフが HA によって検出された場合、I ビットを **0** に設定します。失効が PDSN によって開始され、Revocation メッセージで I-bit が **1** に設定されている場合、HA も Revocation ACK メッセージで I-bit を **1** に設定します。

MIPv4 登録失効の設定

HA で MIPv4 登録失効機能をイネーブルにするには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent revocation`	HA で MIPv4 登録失効のサポートをイネーブルにします。
ステップ 2	`Router(config)# ip mobile home-agent revocation timeout` *5* `retransmit` *6*	（任意）Revocation メッセージの再送信カウントおよびタイムアウト値を設定します。

次に、**ip mobile home-agent revocation** コマンドの例を示します。

```
Router(config)# ip mobile home-agent revoc timeout ?
  <1-100>  Wait time (default 3 secs)
Router(config)# ip mobile home-agent revoc retransmit ?
  <0-100>  Number of retries for a transaction (default 3)
```

モバイル IPv4 リソース失効の制約事項

次のリストでは、現在のリリースのモバイル IPv4 リソース失効機能の制約事項を特定します。

- HA-CHAP（MN-AAA 認証）時に access-accept で受信した STC アトリビュートは無視され、HA の機能設定が優先されます。
- Revocation メッセージ、Revocation ACK メッセージ、失効サポート拡張（Foreign-Home Authentication Extension（FHAE）または IPSec によって保護されない）は廃棄されませんが、処理されます。HA に FA-HA セキュリティ アソシエーションを設定する、または FA と HA の間に IPSec トンネルが存在することを推奨します。

- リリース失効とバインド アップデートを同時にイネーブルにはできません。いずれか 1 つを選択する必要があります。
- HA management information base（MIB; 管理情報ベース）は登録失効情報でアップデートされません。

同時バインディング

HA は次の理由で同時バインディングをサポートしません。

- 同じ Network Access Identifier（NAI; ネットワーク アクセス識別子）に複数のフローが確立されると、各フローに異なる IP アドレスが割り当てられます。したがって、この機能は同じ IP アドレスに対する複数のフローを維持するので、同時バインディングは必要ありません。

Remote Authentication Dial-In User Service（RADIUS）切断

RADIUS 切断（または Packet of Disconnect（POD; パケット オブ ディスコネクト））は、RADIUS サーバが Radius Disconnect メッセージを HA に送信してリソースを解放できるメカニズムです。リソースは管理上の目的で解放され、主に HA のモバイル IP バインディングです。

Cisco Home Agent での RADIUS 切断のサポートは RFC 3576 に準拠します。HA はリソース管理機能を Access Request メッセージでホーム AAA サーバに送信します。このメッセージは、3GPP2 ベンダー固有の Session Termination Capability（STC）Vendor-Specific Attribute（VSA; ベンダー固有のアトリビュート）を含めることで、認証/許可手順用に送信されます。STC VSA で送信された値は設定から取得されます。**radius-server attribute 32 include-in-access-req format** コマンドの設定時、HA には、Access Request の Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を含んだ Network Access Server（NAS; ネットワーク アクセス サーバ）-Identifier アトリビュートがあります。

Disconnect Request が HA で受信されると、次のイベントが発生します。

ステップ 1　ユーザ名に対応するユーザ セッションを検出します（NAI）。

ステップ 2　Framed-IP-Address アトリビュートが Disconnect Request で受信された場合、アドレスに対応するバインディングを終了します。

ステップ 3　Framed-IP-Address が Disconnect Request で受信されない場合、ユーザのすべてのバインディングを終了します（NAI）。

RADIUS 切断クライアントの設定

クライアントと関連したキーに RADIUS 切断を設定するため、次の手順を実行します。

コマンド	目的
`Router(config)# aaa server radius dynamic-author client` *a.b.c.d* `server-key hakey`	HA 上で POD と Care-Of Address（CoA; 気付アドレス）の処理をイネーブルにします。
`Router(config)#ip mobile radius disconnect`	HA で RADIUS Disconnect メッセージを処理する機能をイネーブルにします。

コマンド	目的
Router(config)#**radius-server attribute 32 include-in-access-req**	任意の NAS-Identifier アトリビュートをホーム AAA に対するアクセス要求に含めるのに、このコマンドが必要です。
Router# **debug aaa pod**	AAA サブシステム レベルでの Radius Disconnect メッセージ処理のデバッグ情報を表示します。

RADIUS 切断の制約事項

次のリストには、RADIUS 切断機能の制約事項が含まれます。

- RADIUS 切断情報では MIB はアップデートされません。
- モバイル IP 条件デバッグはサポートされません。

バインディングの同期化および削除のサポート

現在の HA 冗長性の実装では、アクティブ スタンバイ モードのアクティブ HA（またはピアツーピア モードのピア）で削除されるバインディングは、Revocation メッセージまたは RADIUS Disconnect メッセージの受信により、スタンバイ HA またはピア HA に同期化されます。また、Revocation および Radius Disconnect の追加の拡張およびアトリビュートはスタンバイにリレーされます。Registration Revocation および Radius Disconnect（**clear ip mobile binding** コマンドを使用）は、HA 冗長性でサポートされます。次のリストでは、このサポートの利点を示します。

HA 冗長性のアクティブ/スタンバイ モード

- トリガー（たとえば、Revocation メッセージまたは RADIUS Disconnect メッセージの受信）によって削除されるアクティブ HA 上のバインディングは、スタンバイ HA に同期化されます。
- 設定解除するコマンド（たとえば、**ip mobile host** など）によって削除されるバインディングは同期化されません。
- スタンバイ HA 上で削除されるバインディングは、アクティブ スタンバイ モードの場合にはアクティブに同期化されません。
- Revocation および Radius Disconnect の追加の拡張（失効サポート拡張）やアトリビュート（STC アトリビュート）はスタンバイ HA にリレーされます。

HA 冗長性のピアツーピア モード

- トリガー（たとえば、Revocation メッセージまたは RADIUS Disconnect メッセージの受信）によっていずれかのピアで削除されるバインディングは、他のピアに同期化されます。
- 設定解除するコマンド（たとえば、**ip mobile host** など）によって削除されるバインディングは同期化されません。
- Revocation および Radius Disconnect の追加の拡張（失効サポート拡張）やアトリビュート（STC アトリビュート）はピア HA にリレーされます。

バインディングの同期化

次のコール フローでは、モバイル IP フローを起動し、情報をスタンバイ HA に同期化するのに使用される、さまざまなネットワーク エンティティの間のシーケンスおよびメッセージ交換を示します。

1. MS はコールを発信し、PPP セッションがアップします。
2. PDSN は MN から MIP RRQ を受信し、FA-CHAP によって MN を認証します。適切な値（2 または 3）を持った STC VSA は、AAA に送信されたアクセス要求メッセージに含まれます。認証が成功すると、PDSN は RRQ を HA に転送し、失効サポート拡張を MHAE の後に含めます。
3. 失効拡張を含んだ MIP RRQ を受信すると、HA では PDSN に送信された MIP RRP に失効サポート拡張が含まれます。MS を認証する HA-CHAP 時、適切な値（2 または 3）を持った STC VSA は、AAA に送信されたアクセス要求メッセージに含まれます。HA でのバインディングは現在、取り消し可能であると見なされます。
4. PDSN は失効拡張を含んだ MIP RRP を受信します。MIP RRP に失効拡張が含まれているので、PDSN でのバインディングは取り消し可能です。
5. HA は冗長モードで設定されているので、Bind Update メッセージは追加情報（失効サポート拡張および STC Normal Vendor Specific Extension（NVSE））とともにスタンバイに送信されます。
6. スタンバイ HA は Bind Update メッセージで受信した情報を使用してバインディングを再生成し、スタンバイでバインディングを正常に作成したときのコード "accept" とともに Bind Update ACK メッセージを戻します。

バインディングの削除

このサポートの一部として 2 つの新しいメッセージ、"Bind Delete Request" と "Bind Delete ACK" が追加されました。これらのメッセージは、バインディングが削除されたときに冗長 HA の間で交換されます。次のコール フローでは、Revocation メッセージの受信によりバインディングがアクティブ HA で削除され、バインディングの削除がスタンバイ HA と同期するときを示します。

1. MS はコールを発信し、PPP セッションがアップします。モバイル IP フローは、登録失効機能がイネーブルとなりネゴシエートされたアクティブ HA でセットアップされます。同様にスタンバイ HA に同期化されます。
2. ユーザは administrative clear コマンドを発行し、PDSN は Revocation メッセージをアクティブ HA に送信し、ビジター エントリを削除し、関連付けられたリソースをクリアします。
3. MIP Revocation メッセージを受信すると、アクティブ HA は削除するバインディングを特定します。バインディングを特定すると、Bind Delete Request メッセージがスタンバイ HA に送信されます。
4. Bind Delete Request が送信されると、アクティブ HA は、着信した Revocation メッセージのバインディングに関連付けられたリソースを消去し、MIP Revocation ACK メッセージを PDSN に送信します。
5. Bind Delete Request メッセージを受信すると、スタンバイ HA は削除するバインディングを特定し、コード "accept" とともに Bind Delete ACK メッセージを戻します。
6. Bind Delete ACK メッセージが設定された時間内にアクティブ HA で受信されないと、Bind Delete Request メッセージは再送信されます。このプロセスは、最大再送信カウントの間繰り返されます。

バインディングの同期化中、拡張（失効サポート拡張）と、Revocation および RADIUS Disconnect のアトリビュート（STC アトリビュート）がアクティブ HA からスタンバイ HA へ同期化されます。アクティブ HA がダウンし、スタンバイがアクティブになるシナリオでは、現在のアクティブ HA は RADIUS Disconnect メッセージの受信時にバインディングを削除できます。失効の場合、現在のアクティブ HA のバインディングは取り消し可能です。HA は現在、Revocation メッセージを送受信できます。

Selective FA Revocation

3GPP2 環境では、サブスクライバが自分のサービス プロバイダーのネットワークと他のパートナーのサービス プロバイダーのネットワークの間でローミングすると、PDSN ゲートウェイは Resource Revocation メッセージを HA に送信してサブスクライバを削除します。これによりタイミング問題が発生します。したがって、Selective FA Revocation はこれらの "remove subscriber" 要求を選択して無視します。失効は FA に基づいて実行されます。所定の HA は、"remove subscriber" メッセージを無視する FA のリストをスタティックに設定します。

次に、Selective FA Revocation の詳細なコール フローを示します。

1. デュアル 1x/DO ハンドセットは Redundancy Framework（RF; 冗長フレームワーク）に登録し、DO でデータ コールを確立します。音声コールとは異なり、RF ネットワークは Evolved Data Optimized（EVDO）ネットワークを認識していないので（標準により）、このデータ コールを Visitor Location Register（VLR; ビジター ロケーション レジスタ）に登録しません。
2. ハンドセットは休止します（Samsung で 35 秒、RIM で 30 秒、Sierra で 40 秒）。
3. ハンドセットは DO カバレッジ エリアから 1x カバレッジ エリアに移行します。この移行の一部として、ハンドセットは、MTX 経由でアクティブ データ セッションがあることを 1x RF に通知しますが、休止している（DRS ビットは 0 に設定されている）ので送信するデータはありません。新しいセッションが MTX Packet Control Function（PCF; パケット制御機能）経由で PDSN に確立されます。
4. ステップ **3** のイベントに基づいて、1x PCF は、ハンドセットで述べたこのアクティブ データ セッションの VLR をクエリーします。ステップ **1** により、このようなセッションは検出できません。
5. ステップ **3** のイベントの一部として、PCF は現在、**0** に設定された Mobility Event Indicator（MEI）で PDSN メッセージを（OpenRP インターフェイス経由で）送信します。PDSN に対して、このイベントは、コール セットアップの一部としてまったく新しいセッション用であり、次のチェックを実行します。
   - **MEI=0**、および IMSI が既存のセッションに現在割り当てられていない新しい IMSI である場合、処理を進め、新しいセッションを確立します。
   - **MEI=0**、および IMSI が現在、セッションに割り当てられている場合、このセッションを古いものと見なし、セッションを切断します。
6. **MEI=0**、および IMSI が現在セッションに割り当てられているので（これは Hybrid PDSN であり、DO と 1X セッション両方を同時に処理するので）、PDSN は PPP TermReq をハンドセットし送信し、Resource Revocation を HA に送信します。
7. モバイル ノードは休止しており、TermReq を検出しません。MTX RF はしばらくメッセージをバッファリングします。
8. モバイル ノードはアクティブになりますが、送信するデータはありません。これは、まだ有効なモバイル IP セッションがあるかのように機能し、TermReq（バッファリングされた）メッセージおよび ACK メッセージを受信してからただちに RF セットアップ /RRQ を受信します。RRQ には、ハンドセットに割り当てられた IP アドレスや HA の IP アドレスなど、事前に割り当てられた値が含まれます。
9. PDSN はこれを新しいセッション（**MEI=0**、および IMSI は現在、セッションに割り当てられていません）と見なし、RRQ を HA に送信します。
10. 現在、HA は既存のバインディングがなく（ステップ 6 で失効）、RRQ にパラメータがある RRQ を検出し、これをスタティックに割り当てられた MN と見なします。
11. HA は Code-139（管理上の禁止）を MN に戻します。

Selectable FA Revocation ならば、Hybrid PDSN/FA は上記の条件を通り、Revocation を HA に送信します。ただし、HA が Revocation を無視すると、RR 応答を PDSN に送信します。

この結果、MN と HA にはまだバインディング ステートがありますが、PDSN/FA には PPP セッション/ビジター テーブル エントリはありません。実際にモバイルはアクティブになり、Data Ready to Send があります。これには 1x RF チャネル **DRS=1** が含まれます。このシナリオでは、VLR はクエリーされず、PDSN への OpenRP メッセージでは **MEI** が 1 に設定されています。MEI 値に関係なく、PDSN は PPP を開始し、事前に割り当てられたホーム アドレスのある RRQ を送信します。この場合、HA は Re-registration を受信します。

Selective FA Revocation の設定

Selective FA Revocation を設定するには、次の手順を実行します。

コマンド	目的
`Router(config)# ip mobile home-agent revocation ignore` *fa acl*	HA をイネーブルにして、Revocation ACK を PDSN/FA に送信しますが、バインディングは削除しません。*fa-acl* は ACK 番号 *1-99* または名前です。

次に、**ip mobile home-agent revocation ignore** コマンドの例を示します。

standard access-list 番号または **standard** access-list 名を指定することで、FA からの失効を無視できます。

COA 5.1.1.4 からの要求を無視するよう access-list 名を設定

```
Router(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
Router(config)#ip access-list standard fa_acl1
Router(config-std-nacl)#permit 5.1.1.4
```

COA 5.1.1.5 からの要求を無視するよう access-list 番号を設定

```
Router(config)#ip access-list standard ?
  <1-99>       Standard IP access-list number
  <1300-1999>  Standard IP access-list number (expanded range)
  WORD         Access-list name
Router(config)#ip access-list standard 1
Router(config-std-nacl)#permit 5.1.1.5
```

FA 5.1.1.4 からの要求を選択して、無視するよう access-list 名を設定。これは、上記で作成した ACK と **ip mobile home-agent revocation ignore** コマンドを関連付けます。

```
Router((config)#ip mobile home-agent revocation ignore ?
  <1-99>  fa Access-list number
  WORD    fa Access-list name
Router(config)#ip mobile home-agent revocation ignore fa_acl1
```

FA 5.1.1.5 からの要求を選択して、無視するよう access-list 番号を設定

```
Router(config)#ip mobile home-agent revocation ignore 1
```

（注）　**ip mobile home-agent revocation ignore** は現在、*1300 ～ 1999*（標準 IP access-list 番号（拡張範囲））の使用はサポートしていません。

Revocation メッセージでのオプションの NAI のサポート

3GPP2 標準仕様によると、Registration Revocation メッセージで NAI は必須アトリビュートであり、RFC3543 によると NAI はオプションのアトリビュートです。この機能は、NAI を Registration Revocation 要求メッセージに含めるようデフォルト動作を変更し、Revocation 要求メッセージから NAI を除外する CLI を提供します。Revocation Ack メッセージは Revocation 要求メッセージで受信したすべての拡張機能を保持します。

（注）　HA Release 5.1 まで、Registration Revocation メッセージで FHAE 拡張機能だけがサポートされます。

冗長性の考慮事項

- 冗長性がサポートされています。Calling Station ID（CLID; 発信ステーション ID）は、バックアップ HA に同期し、スタンバイでのバインディングの場合にも一意の代替 MN ID として機能します。

Revocation メッセージでのオプションの NAI の設定

この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent revocation exclude-nai`	（任意）IP Mobile Home Agent オプションの設定をイネーブルにして、IP Mobile Home Agent オプション コンフィギュレーション サブモードを開始します。

CHAPTER 9

ダイナミック ドメイン ネーム サーバ（DNS）アップデート

この章では、Domain Name Server（DNS; ドメイン ネーム サーバ）アップデートの方法、サーバのアドレス割り当て、およびこれらの機能の設定方法について説明します。

この章の内容は、次のとおりです。

IP 到達可能性

TIA/EIA/IS-835-D には、ホーム AAA サーバと Home Agent（HA）を使用したダイナミック DNS アップデートの方法が説明されています。AAA による DNS アップデートは簡易 IP およびモバイル IP の両方のサービスに適用できますが、HA による DNS アップデートを適用できるのはモバイル IP サービスだけです。次に、HA 上の IP 到達可能性の機能について説明します。

HA は、初回の登録要求を受信すると、ホーム Remote Authentication Dial-In User Service（RADIUS）サーバに RADIUS アクセス要求を送信します。RADIUS サーバが HA ベースの DNS アップデートを要求するように設定されていれば、ホーム RADIUS サーバは、HA に戻す RADIUS Access-Accept メッセージに DNS-Update-Required アトリビュートを付加します。初回のモバイル IP 登録に成功すると、HA は DNS サーバに DNS アップデート メッセージを送信し、MS のリソース レコードを追加します。HA は、DNS アップデート メッセージをプライマリおよびセカンダリ（存在する場合）の DNS サーバに送信します。

HA が、ライフタイム タイマーがゼロに設定された Mobile IP Registration Request（RRQ; 登録要求）を受信すると、モバイル IP のライフタイムが期限切れになった場合、または管理操作によって MS のモビリティ バインディングが無効にされた場合には、HA は DNS サーバに、関連リソース レコードを削除するための DNS アップデート メッセージを送信します。以降のコマンドは、特定のレルムについて、HA 上の IP 到達可能性をイネーブルにします。

（注） 再登録の場合は、その都度、DNS アップデートは送信されません。

（注）　この機能は、プロキシ モバイル IP フローでも同様にサポートされます。

次に、モバイル登録シナリオにおける、HA 上の IP 到達可能性のコール フローを示します。

1. HA が、Packet Data Serving Node（PDSN）/Foreign Agent（FA; 外部エージェント）から登録要求を受信します。
2. HA から RADIUS サーバにアクセス要求が送信されます。HA により、DNS Server Update Capability VSA が付加されます。
3. RADIUS サーバから、DNS Update Required VSA が付加されたアクセス受諾が送信されます。
4. HA から PDSN/FA に登録応答が送信されます。HA が冗長設定されている場合、アクティブ HA とスタンバイ HA のバインディング作成が同期化されます。
5. HA によりバインディングが作成され、DNS サーバに DNS アップデート要求メッセージが送信されます。
6. DNS サーバにより、NAI の DNS エントリが作成され、HA に DNS アップデート応答メッセージが戻されます。

次に、モバイル登録解除シナリオにおける、HA 上の IP 到達可能性のコール フローを示します。

1. HA が、PDSN/FA からライフタイムがゼロの登録要求を受信します。
2. SA がローカルに保管されていない場合、HA から RADIUS サーバにアクセス要求が送信されます（オプション）。
3. RADIUS サーバからアクセス受諾が戻されます（オプション）。
4. HA により、バインディングが削除されます。HA から PDSN/FA に、登録応答が戻されます。HA が冗長設定されている場合、アクティブ HA とスタンバイ HA のバインディング削除が同期化されます。
5. HA から DNS サーバに、DNS エントリを削除するための DNS アップデート要求メッセージが送信されます。
6. DNS サーバにより、NAI の DNS エントリが削除されます。DNS サーバから HA に、DNS アップデート応答メッセージが戻されます。

IP 到達可能性の設定

特定のレルムでこの機能をイネーブルにするには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# ip name-server x.x.x.x`	名前とアドレスの解決に使用する 1 つ以上のネームサーバのアドレスを指定します。
ステップ 2	`Router(config)# ip mobile realm @ispxyz1.com dns dynamic-update method word`	特定のレルムで DNS アップデートの手順をイネーブルにします。*word* に、ダイナミック DNS アップデート方式の名前を入力します。
ステップ 3	`Router(config)# ip mobile realm realm dns server primary dns server address secondary dns server address`	DNS サーバのアドレスをローカルで設定できます。

この機能によるバインディングがイネーブルかどうかを確認するには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# show ip mobile binding`	モビリティ バインディング テーブルを表示します。

次に、レルムに IP 到達可能性を設定する例を示します。

```
ip ddns update method sit-ha2-ddns2
 DDNS both
ip mobile realm @ispxyz2.com dns dynamic-update method sit-ha2-ddns2
```

DNS サーバのアドレスの割り当て

IS835D に、モバイル IP 登録応答で、ホーム DNS サーバのアドレスを Normal Vendor Specific Extension（NVSE）としてモバイルにプッシュする方法が定義されています。この手順により、モバイル ステーションで、ホーム ドメインのプライマリおよびセカンダリ DNS サーバのアドレスを学習できます。

RADIUS サーバは、モバイル認証中に、HA へのアクセス応答に DNS Server VSA を付加します。HA は、DNS Server VSA から DNS サーバの NVSE を作成し、モバイル IP 登録応答に付加します。認証時に DNS Server VSA を受信しない場合、HA 上で DNS サーバのアドレスがローカルに設定されていれば、ローカル設定から DNS サーバの NVSE が作成され、モバイル IP 登録応答に付加されます。

DNS Server VSA および DNS Server NVSE は、プライマリとセカンダリの DNS IP アドレスを保持します。

HA が冗長モードで配置されている場合、スタンバイ HA に DNS Server VSA が同期化されます。

特定のレルムでこの機能をイネーブルにするには、次のコマンドを使用します。

ip mobile realm *realm* **dns server assign**

ip name-server x.x.x.x

DNS サーバのアドレスをローカルで設定するには、次のコマンドを使用します。

ip mobile realm ***realm*** **dns server** ***primary dns server address secondary dns server address***

この機能によるバインディングがイネーブルかどうかを確認するには、**show ip mobile binding** コマンドを使用します。

（注）　DNS サーバのアドレスがローカルで設定されていて、かつ AAA からもダウンロードされた場合には、HA 上のローカル設定アドレスが優先されます。

HA 上での DNS リマッピングのサポート

Cisco Mobile Wireless Home Agent Release 5.0 で HA は HA でサポートされるサブスクライバの数に調整してステートフル Network Address Translation（NAT; ネットワーク アドレス変換）機能をサポートします。これによって特定のプロトコルとポートが一致するため、ユーザからの DNS 要求を認識できます。認識されると、宛先 IP アドレスが変更されるため、DNS 要求がオペレータによって定義された IP アドレスに送信されます。同様に、応答には要求に応答した DNS サーバのソース IP アドレスが含まれます。これは、その後、サブスクライバによって使用される元のアドレスにマッピングされます。

Mobile Node（MN; モバイル ノード）は、初めに、セッションの設定中にアクセスしたネットワークの DNS サーバ IP アドレスで設定されます。その後、MN はホーム ネットワーク経由で宛先に到達できないこの IP アドレス（つまり、HA へのリバース トンネル）に DNS メッセージを送信して、ホスト名を解決しようとします。この問題に対処するために、HA 5.0 では「DNS リマッピング」機能が追加されました。

モニタリングでの DNS リダイレクション

DNS リマッピングの問題の 1 つは、プライマリ DNS サーバに障害が発生すると、DNS クエリーが HA で設定されたセカンダリ DNS サーバでリダイレクトされないことです。さらに、HA は DNS クエリーの宛先アドレスを HA 上の設定された DNS アドレスにリマッピングするために NAT 設定を使用しません。

既存の DNS リマッピング機能上の DNS リダイレクション機能では、HA は HA でサポートされるサブスクライバの数に調整してステートフル NAT 機能をサポートできます。

この機能サポートの一環として、HA はアベイラビリティのために DNS サーバのモニタリングと同様に宛先アドレスのリマッピングに対処するようになりました。HA は、どちらが使用可能かに応じて、MN からプライマリまたはセカンダリ DNS サーバの設定された IP アドレスへの DNS メッセージの宛先 IP アドレスを書き直します。プライマリとセカンダリの両方の DNS が使用可能な場合、プライマリがアクティブ DNS の役割を果たします。プライマリ DNS サーバが使用できない場合、HA は HA 上で設定されたセカンダリ DNS サーバへの宛先 IP アドレスのリマッピングを開始します。

このソリューションによって、プライマリ DNS サーバに障害が発生した場合の潜在的な問題を解決できます。DNS クエリーは HA 上で設定されたセカンダリ DNS サーバにリダイレクトする必要があります。

HA は IP SLA の機能を使用して、HA からプライマリとセカンダリの DNS サーバのアベイラビリティを検出します。IP SLA はモニタリングされているノードの接続についての情報を Control Plane（CP; コントロール プレーン）にしか通知しないため、CP は（IPC 経由で）すべての Traffic Plane（TP; トラフィック プレーン）に CP が IP SLA から受信した接続についての情報を通知します。

HA がプライマリ DNS サーバが使用できることを検出した場合は、プライマリ DNS サーバがアクティブ DNS サーバとして使用され、トンネル上の FA から送信される DNS クエリーのリマッピングに使用されます。プライマリ DNS サーバがダウンしている場合、セカンダリ DNS サーバが DNS クエリーのリマッピングのためのアクティブ DNS サーバとして使用されます。プライマリとセカンダリの両方の DNS に HA がアクセスできる場合、プライマリ サーバが DNS リマッピングに使用されます。さらに、セカンダリ DNS サーバがアクティブ DNS サーバで、プライマリ DNS サーバがアップしたり、HA との接続が再開した場合、プライマリ DNS サーバがアクティブ DNS サーバの役割を再度引き継ぎます。

この機能についての重要な考慮事項は次のとおりです。

- スイッチオーバーが行われると、HA で DNS サーバからの応答を待っている保留中の DNS クエリーは新しいアクティブな HA ですべて失われます。このシナリオでは、モバイル ノードは DNS クエリーを再送する必要があります。
- DNS クエリーの宛先アドレスが HA 上で設定された DNS サーバのアドレスと一致すると、DNS リダイレクションが使用されず、HA はこのパケットを通常のデータ パケットとして処理します。
- DNS リダイレクションに NAT 設定を使用する必要はありません。

レルムベースの DNS リダイレクションをイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile realm` *word* `dns server` *primary DNS ip secondary DNS ip*	レルムのプライマリおよびセカンダリの DNS サーバを設定します。
ステップ 2	`Router(config)# ip mobile realm` *word* `dns server redirect` {all}	このレルムの DNS リダイレクション機能をイネーブルにします。

上記の 2 つのコマンドの動作

- **ip mobile realm** *word* **dns server redirect {all}** が **ip mobile realm** *word* **dns server** *primary DNS ip secondary DNS ip* の前に設定されている場合、HA は次のエラー メッセージを表示します。

エラー メッセージ　`Error: Primary and Secondary DNS not configured for realm`

- DNS リダイレクション機能はレルム ベースであるため、"@" または "@domain" だけが有効なレルムになります。たとえば、xyz@domain、xyz または xyz@ は有効なレルム オプションにはなりません。エラーの場合、HA は次のエラー メッセージを表示します。

エラー メッセージ　`DNS Redirection is allowed for realm only (e.g. @word)`

- プライマリ DNS サーバとセカンダリ DNS サーバを設定解除するコマンドが特定のレルムに対して実行されていない場合、そのレルムに対する DNS リダイレクションは自動的にディセーブルになります。
- **ip mobile realm** *word* **dns server redirect** コマンドの **no** バージョンを使用して DNS リダイレクション機能を設定解除する場合、そのレルムの既存のバインディングは HA から削除されません。DNS リダイレクション機能だけがディセーブルになります。

アベイラビリティをモニタリングしている DNS サーバをイネーブルにするには、次の IP SLA CLI を設定します。この IP SLA コンフィギュレーション コマンド セットは、HA によってモニタリングする必要のあるすべての DNS サーバ ノードに必要です。これらの IP SLA コマンドは 7600 シリーズ ルータすべてで使用できる既存のコマンドです。

	コマンド	目的
ステップ 1	`Router(config)# ip sla` *`ipsla-number`* `icmp-echo` *`ip-addr`* `frequency` *`freq`*	IPSLA 番号を割り当て、モニタリングする必要のある IP アドレスを設定します。
ステップ 2	`Router(config)# ip sla reaction-configuration` *`ipsla-number`* `react timeout threshold-type immediate action-type trapAndTrigger`	上記の設定済みの DNS サーバが使用できないことを通知するために IP SLA を設定します。
ステップ 3	`router(config)#ip sla reaction-configuration` *`ipsla-number`* `react connectionLoss threshold-type immediate action-type trapAndTrigger`	上記の設定済みの DNS サーバが使用できることを通知するために IP SLA を設定します。
ステップ 4	`router(config)#ip sla enable reaction-alerts`	上で設定した DNS サーバのアベイラビリティとアンアベイラビリティの通知を生成するよう IP SLA を設定します。
ステップ 5	`router(config)#ip sla sch` *`ipsla-number`* `start-time now life forever`	上で設定した設定済み DNS サーバのモニタリングを開始するよう IP SLA を設定します。

上記で

- ipsla-number は DNS サーバのチェックのために割り当てられている IP SLA 番号です。
- ip-addr は DNS サーバの IP アドレスです。
- freq は プローブの秒単位での周波数です（デフォルトは 60）。

Proximity Domain Name Server（PDNS; プロキシミティ ドメイン ネーム サーバ）または SDNS に一致する DNS クエリー

ここでは、DNS クエリーが設定済みの PDNS または SDNS に一致する場合のリダイレクション動作について説明します。

PDNS に一致する要求

DNS 要求が PDNS に一致し、PDNS がアクティブの場合、その要求はスキップされます。しかし、PDNS がダウンしている場合、要求は SDNS にリダイレクトされます（SDNS がアクティブの場合）。アクティブでない場合、要求は無視されます（通常のデータ パケットとして処理されます）。

SDNS に一致する要求

SDNS に一致する要求に関する動作は、設定 CLI によって制御されます。DNS のリダイレクトを設定するために使用される CLI は、次のとおりです。

ip mobile realm *@realm* dns server redirect {**all**}

redirect だけが設定されている場合、SDNS に送信される要求はリダイレクトされません（アップしている場合）。これらは SDNS サーバだけに送信されます。その他の DNS 要求は PDNS にリダイレクトされます。

redirect all が設定されている場合、（設定済みの SDNS IP に一致する要求を含む）すべての DNS 要求が PDN にリダイレクトされます。

IP SLA 経由の DNS サーバのモニタリング

IP SLA が設定済みのプライマリおよびセカンダリいずれかの DNS サーバとの接続切断または接続のアップ イベントを検出すると、CP 上でレジストリ API を起動します。CP が通知を受け取ると、このイベントについて IPC 経由ですべての TP に通知します。TP が CP からこの通知を受け取ると、プライマリ DNS とセカンダリ DNS 間にアクティブ DNS を設定します。

DNS リダイレクションは冗長性をサポートします。スイッチオーバー後、HA がアクティブになると、設定済みの DNS サーバのアベイラビリティのモニタリングを開始します。DNS クエリーが受信されると、HA 上の設定済みの DNS サーバにリマッピングされます。

唯一の制限は、スイッチオーバーが行われると、HA で DNS の応答を待っている保留中の DNS クエリーが新しいアクティブな HA ですべて失われることです。このシナリオでは、モバイル ノードは DNS クエリーを再送する必要があります。

例

次に、DNS 用のユーザ プロファイルを設定する例を示します。

```
[ //localhost/Radius/Profiles/mwts-mip-r20sit-haslb1-prof/Attributes ]
    CDMA-DNS-Server-IP-Address = 01:06:0A:4D:9B:0A:02:06:0A:4D:9B:09:03:03:01:04:03:01
    CDMA-DNS-Update-Required = "HA does need to send DNS Update"
    CDMA-HA-IP-Addr = 20.20.225.1
    CDMA-MN-HA-Shared-Key = ciscociscociscoc
    CDMA-MN-HA-SPI = 00:00:10:01
    CDMA-Reverse-Tunnel-Spec = "Reverse tunneling is required"
    class = "Entering the World of Mobile IP-3"
    Service-Type = Framed
```

次に、DNS サーバ アドレス割り当てレルムのコンフィギュレーション例を示します。

```
ip mobile realm @ispxyz2.com dns server 10.77.155.10 2.2.2.2
ip mobile realm @ispxyz2.com dns server assign
```

次に、AR ユーザ プロファイルでの同じ設定の例を示します。

```
set  CDMA-DNS-Server-IP-Address 01:06:0A:4D:9B:0A:02:06:0A:4D:9B:09:03:03:01:04:03:01
```

太字の部分が、プライマリおよびセカンダリの DNS サーバ アドレスです。

次に、IP 到達可能性および DNS サーバ アドレス割り当ての両方の設定例を示します。

```
ha2#show run
Building configuration...

Current configuration : 10649 bytes
!
! Last configuration change at 22:45:21 UTC Fri Nov 11 2005
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service udp-small-servers
!
hostname tb1-6513-ha2
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa group server radius MOT
 server 150.2.0.1 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local group MOT
aaa authorization config-commands
aaa authorization ipmobile default group MOT
aaa authorization network default group MOT
aaa authorization configuration default group MOT
aaa accounting session-duration ntp-adjusted
aaa accounting update newinfo periodic 3
aaa accounting network ha start-stop group MOT
aaa accounting system default start-stop group MOT
!
aaa server radius dynamic-author
 client 150.2.0.1
 server-key cisco
!
aaa session-id common
!
resource policy
!
ip subnet-zero
no ip gratuitous-arps
!
!
ip cef
ip dfp agent ipmobile
 port 400
 interval 15
 inservice
!
ip ftp source-interface GigabitEthernet0/0.10
ip ftp username root
ip ftp password pdsnmwg
no ip domain lookup
ip name-server 10.77.155.10
ip name-server 1.1.1.1
ip name-server 6.6.6.6
no ip dhcp use vrf connected
```

```
no ip dhcp conflict logging
ip dhcp ping packets 0
!
ip dhcp pool Subnet-Pool1
   utilization mark high 75
   utilization mark low 25
   origin dhcp subnet size initial /30 autogrow /30
!
!
ip vrf forwarding
!
ip vrf ispxyz
!
ip vrf ispxyz-vrf1
 rd 100:1
!
ip vrf ispxyz-vrf2
 rd 100:2
!
!
ip ddns update method sit-ha2-ddns1
 DDNS both
!
ip ddns update method sit-ha2-ddns2
 DDNS both
!
vpdn enable
vpdn ip udp ignore checksum
!
vpdn-group testsip1-l2tp
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
 l2tp tunnel hello 0
!
username user-ha2 password 0 cisco
!
!
!
interface Tunnel10
 no ip address
 ip access-group 150 in
!
interface Loopback0
 ip address 20.20.225.1 255.255.255.0
!
interface Loopback1
 description address of the LNS server
 ip address 20.20.206.20 255.255.255.0
!
interface Loopback2
 ip address 170.12.0.102 255.255.0.0
!
interface GigabitEthernet0/0
 no ip address
 no ip route-cache cef
 no ip route-cache
 no keepalive
 no cdp enable
!
interface GigabitEthernet0/0.10
 description TFTP vlan
```

```
 encapsulation dot1Q 10
 ip address 10.77.155.5 255.255.255.192
 no ip route-cache
 no snmp trap link-status
 no cdp enable
!
interface GigabitEthernet0/0.172
 description HAAA interface
 encapsulation dot1Q 172
 ip address 170.2.0.20 255.255.0.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 170.2.0.102
 standby 2 follow sit-ha2
!
interface GigabitEthernet0/0.202
 description PI interface
 encapsulation dot1Q 202
 ip address 20.20.202.20 255.255.255.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 20.20.202.102
 standby 2 ip 20.20.204.2 secondary
 standby 2 ip 20.20.204.3 secondary
 standby 2 ip 20.20.204.4 secondary
 standby 2 ip 20.20.204.5 secondary
 standby 2 ip 20.20.204.6 secondary
 standby 2 timers msec 750 msec 2250
 standby 2 priority 130
 standby 2 preempt delay minimum 180
 standby 2 name sit-ha2
!
interface GigabitEthernet0/0.205
 description REF interface
 encapsulation dot1Q 205
 ip address 20.20.205.20 255.255.255.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 20.20.205.102
 standby 2 follow sit-ha2
!
interface Virtual-Template1
 description To be used by VPDN for PPP tunnel
 ip unnumbered Loopback1
 peer default ip address pool LNS-pool
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
router mobile
!
ip local pool LNS-pool 7.0.0.1 7.0.0.255
ip local pool ispxyz-vrf1-pool 50.0.0.1 50.0.0.255
ip local pool mobilenodes 40.0.0.1 40.0.100.255
```

```
ip default-gateway 10.77.155.1
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0.202
ip route 10.77.139.29 255.255.255.255 10.77.155.1
ip route 150.2.0.0 255.255.0.0 170.2.0.1
no ip http server
!
!
ip mobile debug include username
ip mobile home-agent template Tunnel10 address 20.20.202.102
ip mobile home-agent revocation timeout 5 retransmit 4
ip mobile home-agent dynamic-address 20.20.202.102
ip mobile home-agent accounting ha broadcast lifetime 3600 replay 8 suppress-unreachable
unknown-ha deny
ip mobile home-agent redundancy sit-ha2 virtual-network address 20.20.202.102
periodic-sync
ip mobile radius disconnect
ip mobile virtual-network 50.0.0.0 255.0.0.0
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai mwts-pmp-r20sit-base-user1@ispxyz1.com virtual-network 40.0.0.0
255.0.0.0 aaa load-sa lifetime 600
ip mobile host nai @ispxyz2.com address pool local mobilenodes virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 180
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns server 10.77.155.10 1.1.1.1
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns server assign
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns dynamic-update method
sit-ha2-ddns1
ip mobile realm @ispxyz2.com vrf ispxyz-vrf2 ha-addr 20.20.204.6
ip mobile realm @ispxyz2.com dns server 10.77.155.10 2.2.2.2
ip mobile realm @ispxyz2.com dns server assign
ip mobile realm @ispxyz2.com dns dynamic-update method sit-ha2-ddns2
ip mobile secure foreign-agent 20.20.201.10 20.20.201.100 spi 100 key ascii cisco replay
timestamp within 7 algorithm md5 mode prefix-suffix
ip mobile secure foreign-agent 20.20.210.10 20.20.210.100 spi 100 key ascii cisco replay
timestamp within 5 algorithm md5 mode prefix-suffix
ip mobile secure home-agent 20.20.202.10 20.20.202.95 spi 100 key ascii cisco replay
timestamp within 7 algorithm md5 mode prefix-suffix
!
ip radius source-interface Loopback2
no logging trap
logging source-interface GigabitEthernet0/0.201
access-list 150 permit ip host 40.0.0.1 host 20.20.205.220 log
access-list 150 permit ip host 20.20.205.220 host 40.0.0.1 log
access-list 150 deny   ip any any log
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source Loopback0
snmp-server host 150.2.0.100 version 2c private
snmp-server host 150.2.0.100 public
no cdp run
!
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req
radius-server attribute 55 access-request include
radius-server host 150.2.0.1 auth-port 1645 acct-port 1646 key 7 121A0C041104
radius-server host 150.2.0.100 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 4
radius-server timeout 2
radius-server deadtime 5
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

```
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
alias exec shc sh cdma pdsn
alias exec ua undebug all
alias exec ui undebug ip packet
!
line con 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
line vty 5 15
 exec-timeout 0 0
!
!
end

ha2#
```

CHAPTER 10

ユーザ単位パケット フィルタリング

この章では、ユーザ単位パケット フィルタリング、および Cisco IOS Mobile Wireless Home Agent ソフトウェアでのこの機能の実装について説明します。

この章は、次の内容で構成されています。

パケット フィルタリングでのモバイル ユーザ アクセス コントロール リスト（ACL）

Home Agent（HA）は、ユーザ単位パケット フィルタリングをサポートしています。この機能を使用すると、登録要求が正常に認証された場合、Remote Authentication Dial-In User Service（RADIUS）サーバから HA に戻されるアクセス応答に、"inACL" および "outACL" アトリビュートが含まれます。"inACL" および "outACL" アトリビュートは、モビリティ バインディングに適用される HA 上の設定済み Access Control List（ACL; アクセス コントロール リスト）を識別します。入力 ACL は、ユーザからトンネル経由で発信されたトラフィックに適用されます。出力 ACL は、トンネル経由でユーザ宛てに送信されたトラフィックに適用されます。これらのアトリビュートは、標準同期およびバルク同期処理により、スタンバイ HA に同期化されます。

モビリティ バインディングに適用された ACL は、**show ip mobile binding** コマンドによって表示できます。初回認証時にダウンロードされた ACL だけが適用されます。ライフタイム更新用のモバイル再認証時にダウンロードされた ACL は適用されません。

HA は、各ユーザについて、1 つの入力 ACL 名と 1 つの出力 ACL 名を受け入れます。

この機能でサポートされるのは、名前付き拡張アクセス リストだけです。

（注） 多数のモビリティ バインディングにモバイル ユーザ ACL を適用すると、パフォーマンスが著しく劣化します。

HA では、外部データ ネットワークからの出力パケット、および Foreign Agent または Mobile Node（MN; モバイル ノード）の IP アドレスに基づく入力データ パケットの両方をフィルタリングできます。

トンネル インターフェイス上での ACL の設定

テンプレート トンネル機能を使用して特定のトラフィックをブロックする ACL を設定するには、次の作業を実行します。

コマンド	目的
Router(config)# **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	トンネル テンプレートを設定します。 ACL を設定します。 テンプレート トンネルを使用する HA を設定します。

トンネルへの ACL 適用の確認

次に、**show ip mobile binding** コマンドの出力例を示します。

モビリティ バインディングに適用された ACL、アカウンティング セッション ID、およびアカウンティング カウンタ

```
router# show ip mobile binding
Mobility Binding List:
Total 1
Total VPDN Tunnel'ed 0
user1-flow8@abc.com (Bindings 1):
    Home Addr 30.0.0.5
    Care-of Addr 7.0.0.2, Src Addr 7.0.0.1
    Lifetime granted 00:03:20 (200), remaining 00:03:03
    Flags sBdmg-T-, Identification CB32792C.A7E22A29
    Tunnel0 src 7.0.0.242 dest 7.0.0.2 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Acct-Session-Id: 0x0000009D
    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

router# show ip mobile tunnel

Mobile Tunnels:
    Total mobile ip tunnels 1
    Tunnel0:
    src 46.0.0.3, dest 55.0.0.11
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 1, Output ACL users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Ethernet1/0
    HA created, fast switching enabled, ICMP unreachable enabled
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes
```

ネットワーク アクセス識別子（NAI）/ レルム単位の入力/出力 アクセス リスト

HA R5.0 は、HA が Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）からの access-response メッセージで ACL 名を受け取った場合に、モバイル ユーザに対してアップストリーム/ダウンストリーム（入力/出力）ACL をサポートします。ただし、AAA が access-response で ACL 名を送信しない場合は、モバイル ユーザに対して入力/出力 ACL を適用できません。HA R5.1 は、トンネル テンプレートを使用するトンネル単位の入力/出力 ACL をサポートしますが、これはそのトンネル上のすべてのユーザに適用されます。特定のユーザまたは一連のユーザだけに ACL を適用することはできません。

- この機能では、レルム/Network Access Identifier（NAI; ネットワーク アクセス識別子）単位の入力/出力 ACL 名の設定がサポートされます。ACL 名に対応する ACL は、**ip access-list extended** *acl-name* コマンドを使用して設定します。
- ACL 名をレルム/NAI に関連付けた後で ACL を修正、更新、作成、または削除すると、その特定の ACL を使用しているモバイル ユーザに修正がただちに適用されます。
- レルム/NAI に関連付けられている入力/出力 ACL 名を変更または追加すると、そのレルム/NAI に属する現在のすべてのバインディングに新しい ACL が適用されます。
- レルム/NAI に関連付けられている入力/出力 ACL 名を削除した場合、削除された ACL は、そのレルム/NAI に属する現在のバインディングに適用されません。
- 入力/出力 ACL 名がレルム/NAI に設定されているかどうかに関係なく、HA が access-response メッセージで入力/出力 ACL 名を受け取ると、AAA から受け取った ACL 名がモバイル ユーザに適用されます。

NAI/ レルム機能単位の入力/出力アクセス リストの設定

Cisco HA Release 5.1 で NAI/ レルム機能単位の入力/出力アクセス リストをイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile realm` *nai* `|` *realm* `in-acl` *in-acl-name* `Router(config)# [no] ip mobile realm` *nai* `|` *realm* `out-acl` *out-acl-name*	

制限事項および制約事項

- レルム/NAI 単位の入力/出力 ACL を設定する場合、名前付き拡張アクセス リストだけがサポートされます。
- セッションに対する最初の正常な access-response で受け取られた ACL 名だけが適用されます。後続の access-response の ACL 名は考慮されません。

CHAPTER 11

HA のセキュリティ

セキュリティ

この章では、Cisco IOS Mobile Wireless Home Agent ソフトウェアのセキュリティ機能における各種コンセプトについて説明します。

この章は、次の内容で構成されています。

3 DES 暗号化

Cisco Home Agent（HA）には、HA 上で IP Security（IPSec）をサポートする 3DES 暗号化が統合されています。Cisco 7600 プラットフォーム上では、Service Application Module for IP（SAMI）は Cisco VPN-SPA IPSec アクセラレーション カードを使用します。

HA では、Packet Data Serving Node（PDSN; パケット データ サービス ノード）と HA 間にモバイル IP データ トラフィック トンネルを確立する前に、各 PDSN のパラメータを設定する必要があります。

（注） この機能の使用は、ハードウェアのサポートに限定されます。

モバイル IP の IPSec

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）は、加入ピア間にデータ機密保持、データ整合性、およびデータ認証を実現する IP Security（IPSec）と呼ばれるオープン標準フレームワークを開発しました。IPSec は、IP レイヤでこれらのセキュリティ サービスを提供し、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）を使用して、ローカル ポリシーに基づいてプロトコルとアルゴリズムのネゴシエーションを処理し、IPSec で使用する暗号化および認証キーを生成します。IPSec を使用することにより、ホスト ペア間、セキュリティ ゲートウェイ ペア間、またはセキュリティ ゲートウェイとホスト間の 1 つ以上のデータ フローを保護できます。

HA は、スタティックに設定された任意の共有秘密を使用して、モバイル IP 登録メッセージ内の認証拡張を処理します。

HA は、IS-835-B の要件に基づいて、IPSec、IKE、Authentication Header（AH; 認証ヘッダー）、および IP Encapsulating Security Payload（ESP）をサポートしています。

IS835-B は、IPSec セキュリティの提供において、3 つのメカニズムを指定しています。

- 証明書
- ダイナミックに分散された事前共有秘密
- スタティックに設定された事前共有秘密

（注）　Cisco IOS IPSec 機能は、Cisco 7600 スイッチ プラットフォーム上で使用できます。HA 2.0（以上）のリリースは、IPSec IKE について、スタティックに設定された事前共有秘密だけをサポートしています。

IS-835-B に規定されているように、HA および Authentication, Authorization and Accounting（AAA; 認証、許可、アカウンティング）には、PDSN の同じセキュリティ レベルを設定する必要があります。PDSN は、AAA サーバからセキュリティ レベルを受信して IKE を開始します。HA は、IKE 要求に応答して、セキュリティ ポリシーを確立します。

PDSN が AAA サーバからセキュリティ レベルを受信して IKE を開始すると、HA は IKE 要求に応答して、セキュリティ ポリシーを確立します。クリプト コンフィギュレーションのアクセスリストに指定されているすべてのトラフィックが、IPSec トンネルによって保護されます。アクセスリストは、PDSN と HA 間のすべてのトラフィックが保護されるように設定します。指定した PDSN/HA ペアに属すすべてのバインディングが保護されます。

IPSec は、コロケーション Care-Of Address（CoA; 気付アドレス）を使用するモバイルには適用されません。

（注）　Cisco 7600 プラットフォーム上の Cisco Home Agent Release 2.0（以上）には、Catalyst 7600 ルータ上で実行するブレードとして、Cisco IPSec Services Module（VPN-SPA）のサポートが必要です。VPN-SPA には、物理的な WAN または LAN インターフェイスはありません。VPN ポリシー用の VLAN セレクタが使用されます。Cisco 7600 インターネット ルータの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps368/prod_installation_guides_list.html

IPSec ベースのセキュリティは、ホーム AAA サーバから受信するパラメータに応じて、PDSN と HA 間のトンネルに適用できます。各 PDSN/HA ペア間に、1 つのトンネルを確立できます。PDSN/HA ペア間の単一トンネルでは、3 種類のトラフィック ストリームを使用できます。コントロール メッセージ、IP-in-IP カプセル化データ、および GRE-in-IP カプセル化データです。トンネルを通過するすべてのトラフィックに、IPSec による同レベルの保護が適用されます。

IS835 には、RFC 2002 に基づくモバイル IP サービスが定義されています。Cisco HA は、モバイル IP サービスおよびプロキシ モバイル IP サービスを提供します。

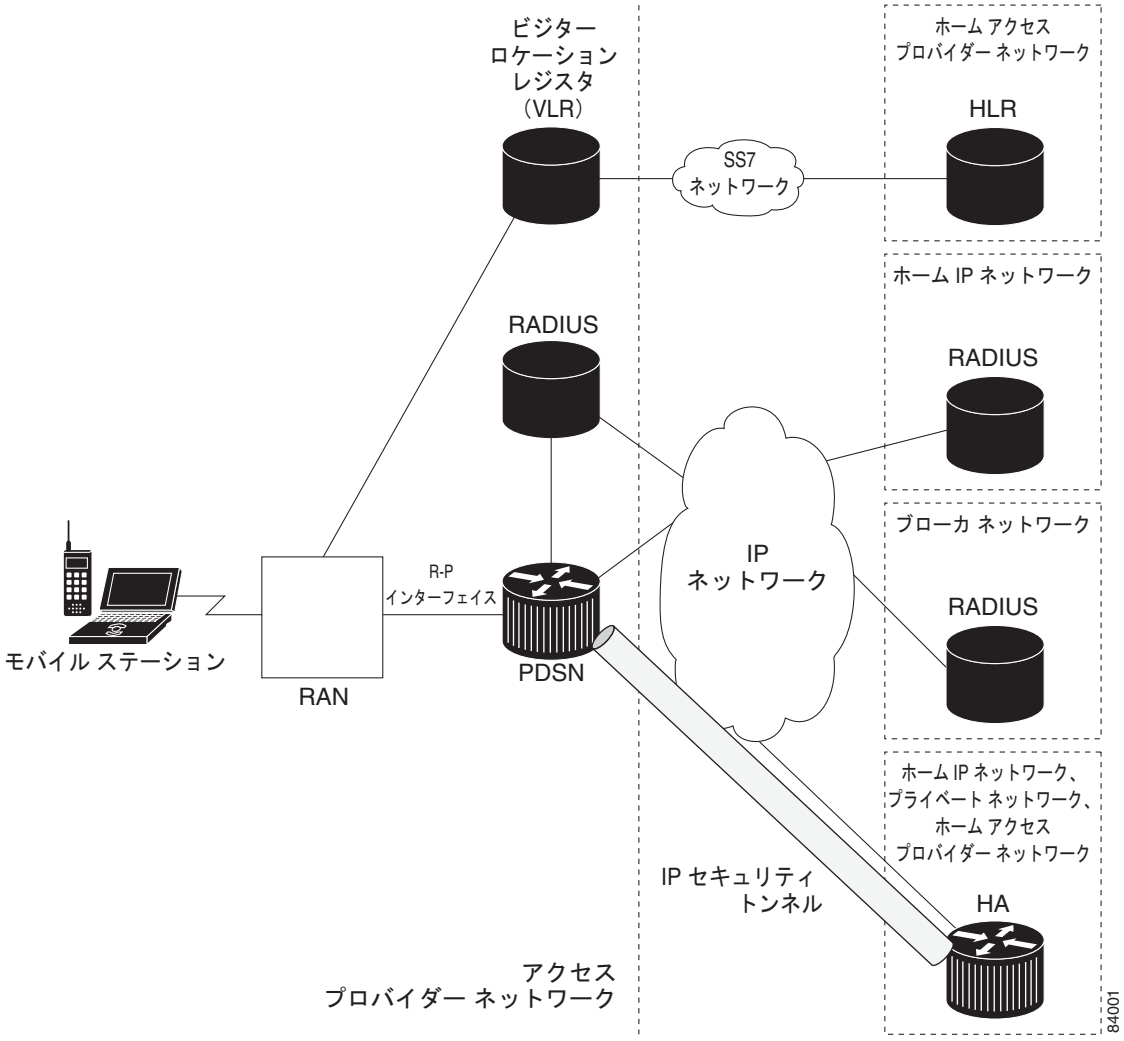
プロキシ モバイル サービスでは、Mobile-Node（MN; モバイル ノード）は簡易 IP によって PDSN/FA に接続し、PDSN/FA が HA への MN のモバイル IP プロキシとして動作します。

Security Association（SA; セキュリティ アソシエーションまたはトンネル）は、一度確立されると、トンネルにトラフィックが存在しなくなるか、SA のライフタイムが期限切れになるまで、アクティブとして存続します。

（注）　IPSec SA は、フェールオーバー時にスタンバイに複製されないので、IPSec は HA 冗長設定とは併用できません。

図 11-1 に、IS835 の IPSec ネットワーク トポロジを示します。

図 11-1　　IS835 IPSec ネットワーク



PDSN と HA 間の IPSec 相互運用性（IS-835-C）

IS-835C に基づく IPSec ルールでは、接続は常に PDSN から HA の IP アドレスに対して開始される必要があります。一部の PDSN は、IPSec コンフィギュレーションに柔軟に対応していません。これらの PDSN では、リモート IPSec の終端地点が常に HA の IP アドレスである場合を除き、リモート IPSec 終端地点のコンフィギュレーションを適用できません。

次のセクションでは、Home Agent Release 2.0 以上を使用する場合の、これらの PDSN と HA 間の IPSec 相互運用性の対処方法について説明します。

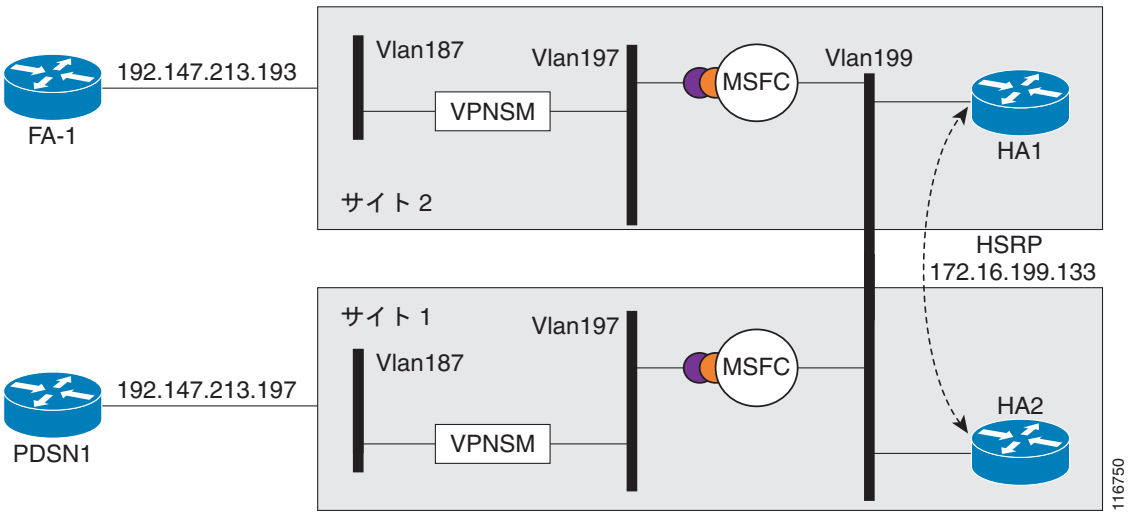
コンフィギュレーションの変更により、HA の IP アドレスへの IPSec 接続と、Virtual Private Network Services Module（VPNSM; VPN サービス モジュール）による終端が可能になります。

単一 HA インスタンスの処理

このソリューションでは、SUP IOS に同じ HA IP アドレスを割り当てます。HA へのトラフィックは、ポリシーにより、正しい HA にルーティングされます。

図 11-2 に、実現可能なコンフィギュレーションを示します。

図 11-2　　単一 HA の相互運用性



次に、スーパーバイザのコンフィギュレーション例を示します。PDSN の IP アドレスは 14.0.0.1、HA3 のアドレスは 13.0.0.50、HA4 のアドレスは 13.0.0.51 です。

単一 HA インスタンスの相互運用性

```
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 60000
crypto isakmp key cisco address 10.0.0.0 0.0.0.0
!
crypto ipsec transform-set mobile-set1 esp-3des

# Comment: testmap is used for HA3

crypto map testmap local-address Loopback21
crypto map testmap 20 ipsec-isakmp
 set peer 10.0.0.1
```

```
 set transform-set mobile-set1
 match address 131
!

interface Loopback21
 description corresponds to ha-on-proc3
 ip address 10.0.0.50 255.255.255.255
!

interface GigabitEthernet4/1
description encrypt traffic from vlan 151 to vlan 201& 136 to 139
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,136,146,151,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet4/2
 description decrypts traffic from vlan 201 to 151, 139 to 136
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,139,149,201,1002-1005
 switchport mode trunk
 cdp enable

interface Vlan136
 description secure vlan
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap
!
interface Vlan137
 description internal vlan to HA3
 ip address 10.0.0.1 255.255.0.0
!
interface Vlan139
 no ip address
 crypto connect vlan 136
!

access-list 131 permit ip host 10.0.0.1 host 10.0.0.50
access-list 131 permit ip host 10.0.0.50 host 10.0.0.1
access-list 131 permit ip 10.0.0.0 0.0.0.255 10.0.0.0 0.0.0.255

access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any

route-map RRQ-HA3 permit 10
 match ip address 2000
 set ip next-hop 10.0.0.2
!
```

6 CPU SAMI 搭載 Cisco 7600 での IPSec サポート

PDSN と HA 間のモバイル IP トンネル上に、IPSec トンネルの確立が必要になることがあります。PDSN は外部ネットワークに、HA はホーム ネットワークに常駐します。IS-835B 仕様に基づいて、IPSec 接続は常に PDSN から HA に対して開始します。したがって、IPSec トンネルのエンドポイントは、PDSN IP アドレスおよび HA IP アドレスです。

Cisco 7600 HA ソリューションでは、IPSec は SUP で終端しますが、実際の HA アプリケーションは 1 枚以上の SAMI カード上に常駐します。各 SAMI カードには 6 つの CPU があり、それぞれ 1 つの HA インスタンスを実行します。各 HA に、独自の IP アドレスがあります。IPSec エンドポイントである SUP と HA エンドポイントである SAMI の IP アドレスが異なる場合には､HA IP アドレスの PDSN によって生成された IKE メッセージは、SUP でドロップされます。

この問題を回避するには、SAMI 上に設定されている HA IP アドレスと同じ IP アドレスを SUP に使用させる必要があります。そのためには、各 PDSN/HA ペアが正しく処理されるように、異なる HA IP アドレス宛ての IPSec トラフィックを、異なる IPSec VLAN に割り当てます。このコンフィギュレーションにより、HA アプリケーションを実行する SAMI 上の 6 つのすべての CPU をサポートし、それぞれに IPSec エンドポイントとなる独自の IP アドレスを設定できます。

この場合、SUP720 上で VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）IPSec 機能を使用します。PDSN から発信されたトラフィックはすべて、HA IP アドレスに基づいて異なる VLAN に割り当てられます。各 VLAN は 1 つの VRF に対応し、SUP 上の各 HA インスタンスに 1 つの VRF が存在します。つまり、IPSec の VRF モードにより、トラフィックは SAMI 上の 6 つの異なる HA インスタンスにそれぞれ分類されます。パケットは、クリプト VLAN によって復号化されると、特定の HA に対応する内部 VLAN のポリシーに基づいて、SAMI 上の正しい HA CPU にルーティングされます。

この場合、複数のシャーシ間および単一シャーシ内での IPSec 冗長設定がサポートされます。

この動作のコール フローは、次のとおりです。

1. SUP 上で、PDSN と HA IP アドレスの各ペア間の IPSec SA が開始されます。PDSN から、PDSN IP アドレスと、特定の HA IP アドレスであるピア IP アドレスを持つ IKE メッセージが送信されます。IKE メッセージ内の PDSN IP アドレスと HA IP アドレスに基づいて、PDSN/HA ペア用の正しい ISAKMP プロファイルが選択され、各ペアに対応する VRF が指示されます。これにより、PDSN/HA ペアに対応する個別の security parameter index（SPI; セキュリティ パラメータ インデックス）が確立されます。
2. HA IP アドレス単位で 1 つの VLAN が定義され、SUP 上のそのアドレス用に定義された VRF に割り当てられます。したがって、SUP は、PDSN の IPSec 終端地点となる HA IP アドレスを所有します。
3. 各 PDSN/HA IP アドレス ペア間に IPSec SA が確立されると、入力パケットの SPI に基づいて、暗号化パケットが正しい VRF に割り当てられます。
4. 暗号化パケットは、HA アドレスに対応する IPSec VLAN で復号化されると、SUP と MWAM 上の HA インスタンス間の内部 VLAN を使用して、HA IP アドレスをホスティングしている MWAM カード上の対応する CPU にポリシー ルーティングされます。
5. リターン パスでは、SAMI 上の HA インスタンスからのパケットが内部 VLAN に渡され、その HA に対応する IPSec VLAN に割り当てられます。これにより、パケットが暗号化され、出力インターフェイスを通じて PDSN に送出されます。

制約事項

同時バインディング

Cisco HA は、同時バインディングをサポートしていません。同じ Network Access Identifier（NAI; ネットワーク アクセス識別子）に複数のフローが確立されると、各フローに異なる IP アドレスが割り当てられます。つまり、同時バインディングは不要です。同時バインディングは、同じ IP アドレスへの複数のフローを維持する場合に使用されるからです。

セキュリティ

HA は、IS-835-B の要件に基づいて、IPSec、IKE、IPSec 認証ヘッダー（AH）、および IP Encapsulating Security Payload（ESP）をサポートしています。HA は、制御トラフィック用またはユーザ トラフィック用の個別のセキュリティはサポートしていません。両方のセキュリティを有効にするか無効にするかのどちらかです。

HA は、IS-835-B に定義されているダイナミックな鍵の割り当て、または共有秘密はサポートしていません。

モバイル IP SA の設定

モバイル ホスト、Foreign Agent（FA; 外部エージェント）、および HA の SA を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile secure {host | visitor | home-agent | foreign-agent | proxy-host} {lower-address [upper-address] | nai string} {inbound-spi spi-in outbound-spi spi-out | spi spi} key {hex | ascii} string [replay timestamp [number]] algorithm md5 mode prefix-suffix`	IP モバイル ユーザの SA を指定します。

HA の IPSec の設定

HA の IPSec を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)# **crypto map** *map-name seq-num* **ipsec-isakmp** **set peer** *ip address of ha* **set transform-set** transform-set-name **match address** *acl name* **crypto map** *map name* **local-address** *interface*	1 つのクリプトマップ セットに 1 つの HA のクリプト マップ エントリを作成します。 クリプト マップの定義を完了するには： 1. 関連する ACL を定義します。 2. クリプト マップをインターフェイスに割り当てます。1 つのクリプト マップ セットで、各 HA に個別のシーケンス番号を使用することにより、複数の HA のクリプト マップを設定できます。 IPSec トラフィックのクリプト マップに使用するインターフェイスを識別し、名前を指定します。
ステップ 2	Router# **access-list** *acl-name* **deny udp host** *HA IP addr* **eq mobile-ip host** *PDSN IP addr* **eq mobile-ip** **access-list** *acl-name* **permit ip host** *PDSN IP addr* **host** *HA IP addr* **access-list** *acl-name* **deny ip any any**	アクセス リストを定義します。 "acl-name" に、クリプト マップの設定と同じ ACL 名を指定します。
ステップ 3	Router# **Interface** *Physical-Interface of PI interface* **crypto map** *Crypto-Map set*	Pi インターフェイスにクリプト マップを割り当てます。HA は、このインターフェイス上で、PDSN 間とのモバイル IP トラフィックを送受信します。

アクティブ/スタンバイ HA SA の作成

アクティブ/スタンバイ HA SA を表示するには、次の IOS コマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)#**show ip mobile secure ?** **foreign-agent** **home-agent** **host** **summary**	アクティブおよびスタンバイの HA SA を表示します。 FA の SA を表示します。HA の SA を表示します。モバイル ホストの SA を表示します。SA の要約を表示します。

次に、このコマンドの例を示します。

```
Router# show ip mobile secure home-agent
Security Associations (algorithm,mode,replay protection,key):
30.0.0.30:
   SPI 100,  MD5, Prefix-suffix, Timestamp +/- 7,
   Key 'red'
HA#
```

設定例

HA の IPSec 設定

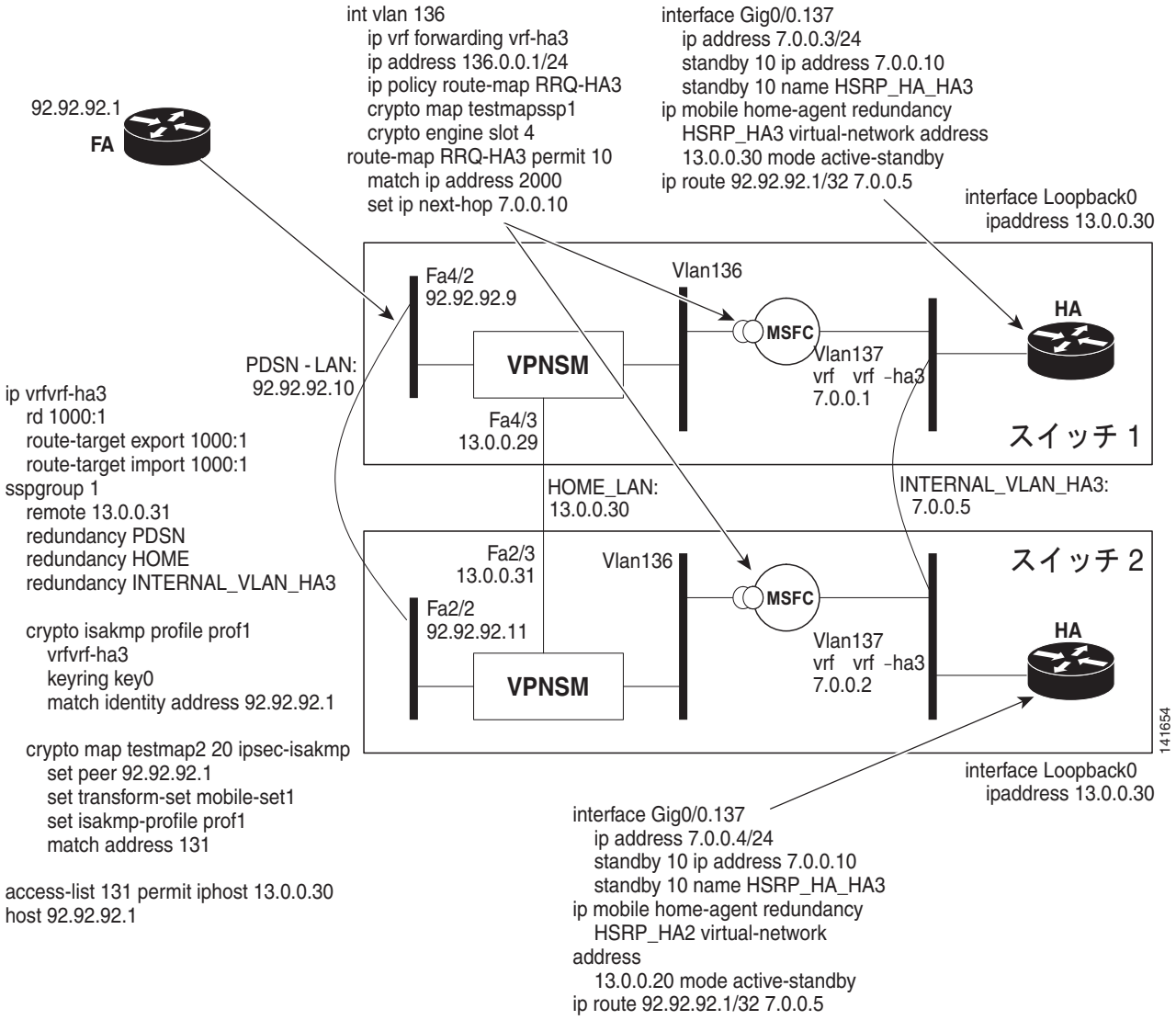
（注）　暗号化するホストおよびサブネットを許可する場合には、必ず、明示的な拒否ステートメントを指定してください。拒否ステートメントにより、他のすべてのパケットが暗号化されないように設定します。

（注）　Cisco Catalyst 6500 および 7600 の IPSec は、HA ではなく、スーパーバイザ上で設定します。

6 HA インスタンス用の SUP 720 および VRF-IPSec の設定

次に、SUP 720 および VRF-IPSec の詳細な設定例を示します。図 11-3 を参照してください。

図 11-3　SUP 720 / VRF-IPSec の設定



SUP の設定：スイッチ 1：

```
ip vrf vrf-ha2
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ip vrf vrf-ha3
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
ip vrf vrf-ha4
 rd 4000:1
 route-target export 4000:1
 route-target import 4000:1
!
```

```
ip vrf vrf-ha5
 rd 5000:1
 route-target export 5000:1
 route-target import 5000:1
!
ip vrf vrf-ha6
 rd 6000:1
 route-target export 6000:1
 route-target import 6000:1
!
ssp group 1
 remote 13.0.0.31
 redundancy PDSN-LAN
 redundancy HOME-LAN
 redundancy INTERNAL_VLAN_HA3
 redundancy HOME-LAN-2
 redundancy INTERNAL_VLAN_HA2
 redundancy HOME-LAN-4
 redundancy HOME-LAN-5
 redundancy HOME-LAN-6
 redundancy INTERNAL_VLAN_HA4
 redundancy INTERNAL_VLAN_HA5
 redundancy INTERNAL_VLAN_HA6
 port 4098
!
crypto keyring key0
  pre-shared-key address 92.92.92.1 key cisco
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 60000
crypto isakmp ssp 1
!
crypto isakmp profile prof1
   vrf vrf-ha2
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 12.0.0.30
crypto isakmp profile prof2
   vrf vrf-ha3
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 13.0.0.30
crypto isakmp profile prof4
   vrf vrf-ha4
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 14.0.0.30
crypto isakmp profile prof5
   vrf vrf-ha5
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 15.0.0.30
crypto isakmp profile prof6
   vrf vrf-ha6
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 16.0.0.30
!
crypto ipsec transform-set mobile-set1 esp-des esp-sha-hmac
!
crypto map testmap local-address FastEthernet4/3
crypto map testmap 20 ipsec-isakmp
 set peer 92.92.92.1
```

```
 set transform-set mobile-set1
 set isakmp-profile prof2
 match address 131
!
crypto map testmap1 local-address FastEthernet4/4
crypto map testmap1 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof1
 match address 121
!
crypto map testmap4 local-address FastEthernet4/7
crypto map testmap4 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof4
 match address 141
!
crypto map testmap5 local-address FastEthernet4/9
crypto map testmap5 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof5
 match address 151
!
crypto map testmap6 local-address FastEthernet4/11
crypto map testmap6 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof6
 match address 161
!
crypto engine mode vrf
!
interface FastEthernet4/2
 ip address 92.92.92.9 255.255.0.0
 ip policy route-map RRQ-HA10
 speed 100
 duplex half
 standby delay minimum 30 reload 60
 standby 1 ip 92.92.92.10
 standby 1 preempt
 standby 1 name PDSN-LAN
 standby 1 track FastEthernet4/2
 standby 1 track FastEthernet4/3
 standby 1 track FastEthernet4/4
 standby 1 track FastEthernet4/7
 standby 1 track FastEthernet4/9
 standby 1 track FastEthernet4/11
 standby 1 track GigabitEthernet6/1
 standby 1 track Vlan136
 standby 1 track Vlan137
 standby 1 track Vlan127
 standby 1 track Vlan126
 standby 1 track Vlan146
 standby 1 track Vlan147
 standby 1 track Vlan156
 standby 1 track Vlan157
 standby 1 track Vlan166
 standby 1 track Vlan167
 standby 1 track Vlan200
 crypto engine slot 6
!
interface FastEthernet4/3
```

```
 ip address 13.0.0.29 255.255.0.0
 standby delay minimum 30 reload 60
 standby 3 ip 13.0.0.30
 standby 3 preempt
 standby 3 name HOME-LAN
 standby 3 track FastEthernet4/2
 standby 3 track FastEthernet4/3
 standby 3 track FastEthernet4/4
 standby 3 track FastEthernet4/7
 standby 3 track FastEthernet4/9
 standby 3 track FastEthernet4/11
 standby 3 track GigabitEthernet6/1
 standby 3 track Vlan136
 standby 3 track Vlan137
 standby 3 track Vlan127
 standby 3 track Vlan126
 standby 3 track Vlan146
 standby 3 track Vlan147
 standby 3 track Vlan156
 standby 3 track Vlan157
 standby 3 track Vlan166
 standby 3 track Vlan167
 standby 3 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/4
 ip address 12.0.0.29 255.255.255.0
 duplex half
 standby delay minimum 30 reload 60
 standby 2 ip 12.0.0.30
 standby 2 preempt
 standby 2 name HOME-LAN-2
 standby 2 track FastEthernet4/2
 standby 2 track FastEthernet4/3
 standby 2 track FastEthernet4/4
 standby 2 track FastEthernet4/7
 standby 2 track FastEthernet4/9
 standby 2 track FastEthernet4/11
 standby 2 track GigabitEthernet6/1
 standby 2 track Vlan136
 standby 2 track Vlan137
 standby 2 track Vlan127
 standby 2 track Vlan126
 standby 2 track Vlan146
 standby 2 track Vlan147
 standby 2 track Vlan156
 standby 2 track Vlan157
 standby 2 track Vlan166
 standby 2 track Vlan167
 standby 2 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/5
 switchport
 switchport access vlan 137
 switchport mode access
 no ip address
!
interface FastEthernet4/6
 switchport
 switchport access vlan 127
 switchport mode access
 no ip address
 speed 100
```

```
 duplex half
!
interface FastEthernet4/7
 ip address 14.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 4 ip 14.0.0.30
 standby 4 preempt
 standby 4 name HOME-LAN-4
 standby 4 track FastEthernet4/2
 standby 4 track FastEthernet4/3
 standby 4 track FastEthernet4/4
 standby 4 track FastEthernet4/7
 standby 4 track FastEthernet4/9
 standby 4 track FastEthernet4/11
 standby 4 track Vlan136
 standby 4 track Vlan137
 standby 4 track Vlan127
 standby 4 track Vlan126
 standby 4 track GigabitEthernet6/1
 standby 4 track Vlan146
 standby 4 track Vlan147
 standby 4 track Vlan156
 standby 4 track Vlan157
 standby 4 track Vlan166
 standby 4 track Vlan167
 standby 4 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/8
 switchport
 switchport access vlan 147
 switchport mode access
 no ip address
!
interface FastEthernet4/9
 ip address 15.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 5 ip 15.0.0.30
 standby 5 preempt
 standby 5 name HOME-LAN-5
 standby 5 track FastEthernet4/2
 standby 5 track FastEthernet4/3
 standby 5 track FastEthernet4/4
 standby 5 track FastEthernet4/7
 standby 5 track FastEthernet4/9
 standby 5 track FastEthernet4/11
 standby 5 track Vlan136
 standby 5 track Vlan137
 standby 5 track Vlan127
 standby 5 track Vlan126
 standby 5 track GigabitEthernet6/1
 standby 5 track Vlan146
 standby 5 track Vlan147
 standby 5 track Vlan156
 standby 5 track Vlan157
 standby 5 track Vlan166
 standby 5 track Vlan167
 standby 5 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/10
 switchport
 switchport access vlan 157
 switchport mode access
```

```
 no ip address
!
interface FastEthernet4/11
 ip address 16.0.0.29 255.255.255.0
 standby delay minimum 30 reload 60
 standby 6 ip 16.0.0.30
 standby 6 preempt
 standby 6 name HOME-LAN-6
 standby 6 track FastEthernet4/2
 standby 6 track FastEthernet4/3
 standby 6 track FastEthernet4/4
 standby 6 track FastEthernet4/7
 standby 6 track FastEthernet4/9
 standby 6 track FastEthernet4/11
 standby 6 track Vlan136
 standby 6 track Vlan137
 standby 6 track Vlan127
 standby 6 track Vlan126
 standby 6 track GigabitEthernet6/1
 standby 6 track Vlan146
 standby 6 track Vlan147
 standby 6 track Vlan156
 standby 6 track Vlan157
 standby 6 track Vlan166
 standby 6 track Vlan167
 standby 6 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/12
 switchport
 switchport access vlan 167
 switchport mode access
 no ip address
!
interface GigabitEthernet6/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 126,136,146,156,166
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet6/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan126
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha2
 ip address 126.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA2
 no mop enabled
 crypto map testmap1 ssp 1
```

```
 crypto engine slot 6
!
interface Vlan127
 description internal vlan to HA2
 ip vrf forwarding vrf-ha2
 ip address 6.0.0.1 255.255.0.0
 standby 12 ip 6.0.0.5
 standby 12 preempt
 standby 12 name INTERNAL_VLAN_HA2
 standby 12 track FastEthernet4/2
 standby 12 track FastEthernet4/3
 standby 12 track FastEthernet4/4
 standby 12 track FastEthernet4/7
 standby 12 track FastEthernet4/9
 standby 12 track FastEthernet4/11
 standby 12 track Vlan136
 standby 12 track Vlan137
 standby 12 track Vlan127
 standby 12 track Vlan126
 standby 12 track GigabitEthernet6/1
 standby 12 track Vlan146
 standby 12 track Vlan147
 standby 12 track Vlan156
 standby 12 track Vlan157
 standby 12 track Vlan166
 standby 12 track Vlan167
 standby 12 track Vlan200
!
interface Vlan136
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha3
 ip address 136.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap ssp 1
 crypto engine slot 6
!
interface Vlan137
 description internal vlan to HA3
 ip vrf forwarding vrf-ha3
 ip address 7.0.0.1 255.255.0.0
 standby 13 ip 7.0.0.5
 standby 13 preempt
 standby 13 name INTERNAL_VLAN_HA3
 standby 13 track FastEthernet4/2
 standby 13 track FastEthernet4/3
 standby 13 track FastEthernet4/4
 standby 13 track FastEthernet4/7
 standby 13 track FastEthernet4/9
 standby 13 track FastEthernet4/11
 standby 13 track Vlan136
 standby 13 track Vlan137
 standby 13 track Vlan127
 standby 13 track Vlan126
 standby 13 track GigabitEthernet6/1
 standby 13 track Vlan146
 standby 13 track Vlan147
 standby 13 track Vlan156
 standby 13 track Vlan157
 standby 13 track Vlan166
 standby 13 track Vlan167
```

```
 standby 13 track Vlan200
!
interface Vlan146
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha4
 ip address 146.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA4
 no mop enabled
 crypto map testmap4 ssp 1
 crypto engine slot 6
!
interface Vlan147
 description internal vlan to HA4
 ip vrf forwarding vrf-ha4
 ip address 8.0.0.1 255.255.0.0
 standby 14 ip 8.0.0.5
 standby 14 preempt
 standby 14 name INTERNAL_VLAN_HA4
 standby 14 track FastEthernet4/2
 standby 14 track FastEthernet4/3
 standby 14 track FastEthernet4/4
 standby 14 track FastEthernet4/7
 standby 14 track FastEthernet4/9
 standby 14 track FastEthernet4/11
 standby 14 track Vlan136
 standby 14 track Vlan137
 standby 14 track Vlan127
 standby 14 track Vlan126
 standby 14 track GigabitEthernet6/1
 standby 14 track Vlan146
 standby 14 track Vlan147
 standby 14 track Vlan156
 standby 14 track Vlan157
 standby 14 track Vlan166
 standby 14 track Vlan167
 standby 14 track Vlan200
!
interface Vlan156
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha5
 ip address 156.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA5
 no mop enabled
 crypto map testmap5 ssp 1
 crypto engine slot 6
!
interface Vlan157
 description internal vlan to HA5
 ip vrf forwarding vrf-ha5
 ip address 9.0.0.1 255.255.0.0
 standby 15 ip 9.0.0.5
 standby 15 preempt
 standby 15 name INTERNAL_VLAN_HA5
 standby 15 track FastEthernet4/2
 standby 15 track FastEthernet4/3
 standby 15 track FastEthernet4/4
 standby 15 track FastEthernet4/7
 standby 15 track FastEthernet4/9
```

```
 standby 15 track FastEthernet4/11
 standby 15 track Vlan136
 standby 15 track Vlan137
 standby 15 track Vlan127
 standby 15 track Vlan126
 standby 15 track GigabitEthernet6/1
 standby 15 track Vlan146
 standby 15 track Vlan147
 standby 15 track Vlan156
 standby 15 track Vlan157
 standby 15 track Vlan166
 standby 15 track Vlan167
 standby 15 track Vlan200
!
interface Vlan166
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha6
 ip address 166.0.0.1 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA6
 no mop enabled
 crypto map testmap6 ssp 1
 crypto engine slot 6
!
interface Vlan167
 description internal vlan to HA6
 ip vrf forwarding vrf-ha6
 ip address 10.0.0.1 255.255.0.0
 standby 16 ip 10.0.0.5
 standby 16 preempt
 standby 16 name INTERNAL_VLAN_HA6
 standby 16 track FastEthernet4/2
 standby 16 track FastEthernet4/3
 standby 16 track FastEthernet4/4
 standby 16 track FastEthernet4/7
 standby 16 track FastEthernet4/9
 standby 16 track FastEthernet4/11
 standby 16 track Vlan136
 standby 16 track Vlan137
 standby 16 track Vlan127
 standby 16 track Vlan126
 standby 16 track GigabitEthernet6/1
 standby 16 track Vlan146
 standby 16 track Vlan147
 standby 16 track Vlan156
 standby 16 track Vlan157
 standby 16 track Vlan166
 standby 16 track Vlan167
 standby 16 track Vlan200
!
interface vlan 200
 ip address 200.0.0.2 255.0.0.0
 standby 250 ip 200.0.0.3
 standby 250 preempt
 standby 250 name NON_IPSEC_VLAN
 standby 250 track FastEthernet4/2
 standby 250 track FastEthernet4/3
 standby 250 track FastEthernet4/4
 standby 250 track FastEthernet4/7
 standby 250 track FastEthernet4/9
 standby 250 track FastEthernet4/11
 standby 250 track Vlan136
```

```
 standby 250 track Vlan137
 standby 250 track Vlan127
 standby 250 track Vlan126
 standby 250 track GigabitEthernet6/1
 standby 250 track Vlan146
 standby 250 track Vlan147
 standby 250 track Vlan156
 standby 250 track Vlan157
 standby 250 track Vlan166
 standby 250 track Vlan167
!
ip route vrf vrf-ha2 92.92.92.0 255.255.255.0 Vlan126 92.92.92.1 global
ip route vrf vrf-ha3 92.92.92.0 255.255.255.0 Vlan136 92.92.92.1 global
ip route vrf vrf-ha4 92.92.92.0 255.255.255.0 Vlan146 92.92.92.1 global
ip route vrf vrf-ha5 92.92.92.0 255.255.255.0 Vlan156 92.92.92.1 global
ip route vrf vrf-ha6 92.92.92.0 255.255.255.0 Vlan166 92.92.92.1 global
!
access-list 121 permit ip host 12.0.0.30 host 92.92.92.1
access-list 121 remark Access List for HA2
access-list 131 permit ip host 13.0.0.30 host 92.92.92.1
access-list 131 remark Access List for HA3
access-list 141 permit ip host 14.0.0.30 host 92.92.92.1
access-list 141 remark Access List for HA4
access-list 151 permit ip host 15.0.0.30 host 92.92.92.1
access-list 151 remark Access List for HA5
access-list 161 permit ip host 16.0.0.30 host 92.92.92.1
access-list 161 remark Access List for HA6
access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any
access-list 2001 permit ip 95.95.95.0 0.0.0.255 host 120.0.0.30
access-list 2002 permit ip 96.96.96.0 0.0.0.255 host 130.0.0.30
access-list 2003 permit ip 97.97.97.0 0.0.0.255 host 140.0.0.30
access-list 2004 permit ip 98.98.98.0 0.0.0.255 host 150.0.0.30
access-list 2005 permit ip 99.99.99.0 0.0.0.255 host 160.0.0.30
!
arp vrf vrf-ha6 10.0.0.10 0000.0c07.ac32 ARPA
arp vrf vrf-ha4 8.0.0.10 0000.0c07.ac1e ARPA
arp vrf vrf-ha5 9.0.0.10 0000.0c07.ac28 ARPA
arp vrf vrf-ha2 6.0.0.10 0000.0c07.ac0a ARPA
arp vrf vrf-ha3 7.0.0.10 0000.0c07.ac14 ARPA
!
route-map RRQ-HA5 permit 10
 match ip address 2000
 set ip next-hop 9.0.0.10
!
route-map RRQ-HA4 permit 10
 match ip address 2000
 set ip next-hop 8.0.0.10
!
route-map RRQ-HA6 permit 10
 match ip address 2000
 set ip next-hop 10.0.0.10
!
route-map RRQ-HA3 permit 10
 match ip address 2000
 set ip next-hop 7.0.0.10
!
route-map RRQ-HA2 permit 10
 match ip address 2000
 set ip next-hop 6.0.0.10
!
route-map RRQ-HA10 permit 10
 match ip address 2001
 continue 11
```

```
 set ip next-hop 200.0.0.5
!
route-map RRQ-HA10 permit 11
 match ip address 2002
 continue 12
 set ip next-hop 200.0.0.15
!
route-map RRQ-HA10 permit 12
 match ip address 2003
 continue 13
 set ip next-hop 200.0.0.25
!
route-map RRQ-HA10 permit 13
 match ip address 2004
 continue 14
 set ip next-hop 200.0.0.35
!
route-map RRQ-HA10 permit 14
 match ip address 2005
 set ip next-hop 200.0.0.45
```

SUP の設定：スイッチ 2：

```
ip vrf vrf-ha2
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ip vrf vrf-ha3
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
ip vrf vrf-ha4
 rd 4000:1
 route-target export 4000:1
 route-target import 4000:1
!
ip vrf vrf-ha5
 rd 5000:1
 route-target export 5000:1
 route-target import 5000:1
!
ip vrf vrf-ha6
 rd 6000:1
 route-target export 6000:1
 route-target import 6000:1
!
ssp group 1
 remote 13.0.0.29
 redundancy PDSN-LAN
 redundancy HOME-LAN
 redundancy INTERNAL_VLAN_HA3
 redundancy HOME-LAN-2
 redundancy INTERNAL_VLAN_HA2
 redundancy HOME-LAN-4
 redundancy HOME-LAN-5
 redundancy HOME-LAN-6
 redundancy INTERNAL_VLAN_HA4
 redundancy INTERNAL_VLAN_HA5
 redundancy INTERNAL_VLAN_HA6
 port 4098
```

```
!
crypto keyring key0
  pre-shared-key address 92.92.92.1 key cisco
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 60000
crypto isakmp ssp 1
!
crypto isakmp profile prof1
   vrf vrf-ha2
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 12.0.0.30
crypto isakmp profile prof2
   vrf vrf-ha3
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 13.0.0.30
crypto isakmp profile prof4
   vrf vrf-ha4
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 14.0.0.30
crypto isakmp profile prof5
   vrf vrf-ha5
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 15.0.0.30
crypto isakmp profile prof6
   vrf vrf-ha6
   keyring key0
   match identity address 92.92.92.1 255.255.255.255
   local-address 16.0.0.30
!
crypto ipsec transform-set mobile-set1 esp-des esp-sha-hmac
!
crypto map testmap local-address FastEthernet2/3
crypto map testmap 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof2
 match address 131
!
crypto map testmap1 local-address FastEthernet2/5
crypto map testmap1 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof1
 match address 121
!
crypto map testmap4 local-address FastEthernet2/7
crypto map testmap4 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof4
 match address 141
!
crypto map testmap5 local-address FastEthernet2/9
crypto map testmap5 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof5
 match address 151
```

```
!
crypto map testmap6 local-address FastEthernet2/11
crypto map testmap6 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof6
 match address 161
!
crypto engine mode vrf
!
interface FastEthernet2/2
 ip address 92.92.92.11 255.255.0.0
 ip policy route-map RRQ-HA10
 speed 100
 duplex full
 standby delay minimum 30 reload 60
 standby 1 ip 92.92.92.10
 standby 1 preempt
 standby 1 name PDSN-LAN
 standby 1 track FastEthernet2/2
 standby 1 track FastEthernet2/3
 standby 1 track FastEthernet2/5
 standby 1 track FastEthernet2/7
 standby 1 track FastEthernet2/9
 standby 1 track FastEthernet2/11
 standby 1 track GigabitEthernet4/1
 standby 1 track Vlan136
 standby 1 track Vlan137
 standby 1 track Vlan127
 standby 1 track Vlan126
 standby 1 track Vlan146
 standby 1 track Vlan156
 standby 1 track Vlan157
 standby 1 track Vlan166
 standby 1 track Vlan167
 standby 1 track Vlan147
 standby 1 track Vlan200
 crypto engine slot 4
!
interface FastEthernet2/3
 ip address 13.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 3 ip 13.0.0.30
 standby 3 preempt
 standby 3 name HOME-LAN
 standby 3 track FastEthernet2/2
 standby 3 track FastEthernet2/3
 standby 3 track FastEthernet2/5
 standby 3 track FastEthernet2/7
 standby 3 track FastEthernet2/9
 standby 3 track FastEthernet2/11
 standby 3 track GigabitEthernet4/1
 standby 3 track Vlan136
 standby 3 track Vlan137
 standby 3 track Vlan127
 standby 3 track Vlan126
 standby 3 track Vlan146
 standby 3 track Vlan156
 standby 3 track Vlan157
 standby 3 track Vlan166
 standby 3 track Vlan167
 standby 3 track Vlan147
 standby 3 track Vlan200
crypto engine slot 4
```

```
!
interface FastEthernet2/4
 switchport
 switchport access vlan 137
 switchport mode access
 no ip address
!
interface FastEthernet2/5
 ip address 12.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 2 ip 12.0.0.30
 standby 2 preempt
 standby 2 name HOME-LAN-2
 standby 2 track FastEthernet2/2
 standby 2 track FastEthernet2/3
 standby 2 track FastEthernet2/5
 standby 2 track FastEthernet2/7
 standby 2 track FastEthernet2/9
 standby 2 track FastEthernet2/11
 standby 2 track GigabitEthernet4/1
 standby 2 track Vlan136
 standby 2 track Vlan137
 standby 2 track Vlan127
 standby 2 track Vlan126
 standby 2 track Vlan146
 standby 2 track Vlan156
 standby 2 track Vlan157
 standby 2 track Vlan166
 standby 2 track Vlan167
 standby 2 track Vlan147
 standby 2 track Vlan200
 crypto engine slot 4
!
interface FastEthernet2/6
 switchport
 switchport access vlan 127
 switchport mode access
 no ip address
!
interface FastEthernet2/7
 ip address 14.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 4 ip 14.0.0.30
 standby 4 preempt
 standby 4 name HOME-LAN-4
 standby 4 track FastEthernet2/2
 standby 4 track FastEthernet2/3
 standby 4 track FastEthernet2/5
 standby 4 track FastEthernet2/7
 standby 4 track FastEthernet2/9
 standby 4 track FastEthernet2/11
 standby 4 track Vlan136
 standby 4 track Vlan137
 standby 4 track Vlan127
 standby 4 track Vlan126
 standby 4 track GigabitEthernet4/1
 standby 4 track Vlan146
 standby 4 track Vlan156
 standby 4 track Vlan157
 standby 4 track Vlan166
 standby 4 track Vlan167
 standby 4 track Vlan147
 standby 4 track Vlan200
crypto engine slot 4
```

```
!
interface FastEthernet2/8
 switchport
 switchport access vlan 147
 switchport mode access
 no ip address
!
interface FastEthernet2/9
 ip address 15.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 5 ip 15.0.0.30
 standby 5 preempt
 standby 5 name HOME-LAN-5
 standby 5 track FastEthernet2/2
 standby 5 track FastEthernet2/3
 standby 5 track FastEthernet2/5
 standby 5 track FastEthernet2/7
 standby 5 track FastEthernet2/9
 standby 5 track FastEthernet2/11
 standby 5 track Vlan136
 standby 5 track Vlan137
 standby 5 track Vlan127
 standby 5 track Vlan126
 standby 5 track GigabitEthernet4/1
 standby 5 track Vlan146
 standby 5 track Vlan156
 standby 5 track Vlan157
 standby 5 track Vlan166
 standby 5 track Vlan167
 standby 5 track Vlan147
 standby 5 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/10
 switchport
 switchport access vlan 157
 switchport mode access
 no ip address
!
interface FastEthernet2/11
 ip address 16.0.0.31 255.255.0.0
 standby delay minimum 30 reload 60
 standby 6 ip 16.0.0.30
 standby 6 preempt
 standby 6 name HOME-LAN-6
 standby 6 track FastEthernet2/2
 standby 6 track FastEthernet2/3
 standby 6 track FastEthernet2/5
 standby 6 track FastEthernet2/7
 standby 6 track FastEthernet2/9
 standby 6 track FastEthernet2/11
 standby 6 track Vlan136
 standby 6 track Vlan137
 standby 6 track Vlan127
 standby 6 track Vlan126
 standby 6 track GigabitEthernet4/1
 standby 6 track Vlan146
 standby 6 track Vlan156
 standby 6 track Vlan157
 standby 6 track Vlan166
 standby 6 track Vlan167
 standby 6 track Vlan147
 standby 6 track Vlan200
 crypto engine slot 4
```

```
!
interface FastEthernet2/12
 switchport
 switchport access vlan 167
 switchport mode access
 no ip address
!
interface GigabitEthernet4/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 126,136,146,156,166
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan none
 switchport mode trunk
 no ip address
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface Vlan126
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha2
 ip address 126.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA2
 no mop enabled
 crypto map testmap1 ssp 1
 crypto engine slot 4
!
interface Vlan127
 description internal vlan to HA2
 ip vrf forwarding vrf-ha2
 ip address 6.0.0.2 255.255.0.0
 standby 12 ip 6.0.0.5
 standby 12 preempt
 standby 12 name INTERNAL_VLAN_HA2
 standby 12 track FastEthernet2/2
 standby 12 track FastEthernet2/3
 standby 12 track FastEthernet2/5
 standby 12 track FastEthernet2/7
 standby 12 track FastEthernet2/9
 standby 12 track FastEthernet2/11
 standby 12 track Vlan136
 standby 12 track Vlan137
 standby 12 track Vlan127
 standby 12 track Vlan126
 standby 12 track GigabitEthernet4/1
 standby 12 track Vlan146
 standby 12 track Vlan156
 standby 12 track Vlan157
 standby 12 track Vlan166
 standby 12 track Vlan167
 standby 12 track Vlan147
 standby 12 track Vlan200
```

```
!
interface Vlan136
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha3
 ip address 136.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA3
 no mop enabled
 crypto map testmap ssp 1
 crypto engine slot 4
!
interface Vlan137
 description internal vlan to HA3
 ip vrf forwarding vrf-ha3
 ip address 7.0.0.2 255.255.0.0
 standby 13 ip 7.0.0.5
 standby 13 preempt
 standby 13 name INTERNAL_VLAN_HA3
 standby 13 track FastEthernet2/2
 standby 13 track FastEthernet2/3
 standby 13 track FastEthernet2/5
 standby 13 track FastEthernet2/7
 standby 13 track FastEthernet2/9
 standby 13 track FastEthernet2/11
 standby 13 track Vlan136
 standby 13 track Vlan137
 standby 13 track Vlan127
 standby 13 track Vlan126
 standby 13 track GigabitEthernet4/1
 standby 13 track Vlan146
 standby 13 track Vlan156
 standby 13 track Vlan157
 standby 13 track Vlan166
 standby 13 track Vlan167
 standby 13 track Vlan147
 standby 13 track Vlan200
!
interface Vlan146
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha4
 ip address 146.0.0.2 255.0.0.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA4
 no mop enabled
 crypto map testmap4 ssp 1
 crypto engine slot 4
!
interface Vlan147
 description internal vlan to HA4
 ip vrf forwarding vrf-ha4
 ip address 8.0.0.2 255.255.0.0
 standby 14 ip 8.0.0.5
 standby 14 preempt
 standby 14 name INTERNAL_VLAN_HA4
 standby 14 track FastEthernet2/2
 standby 14 track FastEthernet2/3
 standby 14 track FastEthernet2/5
 standby 14 track FastEthernet2/7
 standby 14 track FastEthernet2/9
 standby 14 track FastEthernet2/11
```

```
 standby 14 track Vlan136
 standby 14 track Vlan137
 standby 14 track Vlan127
 standby 14 track Vlan126
 standby 14 track GigabitEthernet4/1
 standby 14 track Vlan146
 standby 14 track Vlan156
 standby 14 track Vlan157
 standby 14 track Vlan166
 standby 14 track Vlan167
 standby 14 track Vlan147
 standby 14 track Vlan200
!
interface Vlan156
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha5
 ip address 156.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA5
 no mop enabled
 crypto map testmap5 ssp 1
 crypto engine slot 4
!
interface Vlan157
 description internal vlan to HA5
 ip vrf forwarding vrf-ha5
 ip address 9.0.0.2 255.255.0.0
 standby 15 ip 9.0.0.5
 standby 15 preempt
 standby 15 name INTERNAL_VLAN_HA5
 standby 15 track FastEthernet2/2
 standby 15 track FastEthernet2/3
 standby 15 track FastEthernet2/5
 standby 15 track FastEthernet2/7
 standby 15 track FastEthernet2/9
 standby 15 track FastEthernet2/11
 standby 15 track Vlan136
 standby 15 track Vlan137
 standby 15 track Vlan127
 standby 15 track Vlan126
 standby 15 track GigabitEthernet4/1
 standby 15 track Vlan146
 standby 15 track Vlan156
 standby 15 track Vlan157
 standby 15 track Vlan166
 standby 15 track Vlan167
 standby 15 track Vlan147
 standby 15 track Vlan200
!
interface Vlan166
 description secure vlan
 ethernet point-to-point
 ip vrf forwarding vrf-ha6
 ip address 166.0.0.2 255.255.255.0
 no ip redirects
 no ip unreachables
 ip policy route-map RRQ-HA6
 no mop enabled
 crypto map testmap6 ssp 1
 crypto engine slot 4
!
interface Vlan167
```

```
 description internal vlan to HA2
 ip vrf forwarding vrf-ha6
 ip address 10.0.0.2 255.255.0.0
 standby 16 ip 10.0.0.5
 standby 16 preempt
 standby 16 name INTERNAL_VLAN_HA6
 standby 16 track FastEthernet2/2
 standby 16 track FastEthernet2/3
 standby 16 track FastEthernet2/5
 standby 16 track FastEthernet2/7
 standby 16 track FastEthernet2/9
 standby 16 track FastEthernet2/11
 standby 16 track Vlan136
 standby 16 track Vlan137
 standby 16 track Vlan127
 standby 16 track Vlan126
 standby 16 track GigabitEthernet4/1
 standby 16 track Vlan146
 standby 16 track Vlan156
 standby 16 track Vlan157
 standby 16 track Vlan166
 standby 16 track Vlan167
 standby 16 track Vlan147
 standby 16 track Vlan200
!
interface vlan 200
 ip address 200.0.0.1 255.0.0.0
 standby 250 ip 200.0.0.3
 standby 250 preempt
 standby 250 name NON_IPSEC_VLAN
 standby 250 track FastEthernet2/2
 standby 250 track FastEthernet2/3
 standby 250 track FastEthernet2/5
 standby 250 track FastEthernet2/7
 standby 250 track FastEthernet2/9
 standby 250 track FastEthernet2/11
 standby 250 track Vlan136
 standby 250 track Vlan137
 standby 250 track Vlan127
 standby 250 track Vlan126
 standby 250 track GigabitEthernet4/1
 standby 250 track Vlan146
 standby 250 track Vlan156
 standby 250 track Vlan157
 standby 250 track Vlan166
 standby 250 track Vlan167
 standby 250 track Vlan147

ip route vrf vrf-ha2 92.92.92.0 255.255.255.0 Vlan126 92.92.92.1 global
ip route vrf vrf-ha3 92.92.92.0 255.255.255.0 Vlan136 92.92.92.1 global
ip route vrf vrf-ha4 92.92.92.0 255.255.255.0 Vlan146 92.92.92.1 global
ip route vrf vrf-ha5 92.92.92.0 255.255.255.0 Vlan156 92.92.92.1 global
ip route vrf vrf-ha6 92.92.92.0 255.255.255.0 Vlan166 92.92.92.1 global
!
access-list 121 permit ip host 12.0.0.30 host 92.92.92.1
access-list 121 remark Access List for HA2
access-list 131 permit ip host 13.0.0.30 host 92.92.92.1
access-list 131 remark Access List for HA3
access-list 141 permit ip host 14.0.0.30 host 92.92.92.1
access-list 141 remark Access List for HA4
access-list 151 permit ip host 15.0.0.30 host 92.92.92.1
access-list 151 remark Access List for HA5
access-list 161 permit ip host 16.0.0.30 host 92.92.92.1
access-list 161 remark Access List for HA6
```

```
access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any
access-list 2001 permit ip 95.95.95.0 0.0.0.255 host 120.0.0.30
access-list 2002 permit ip 96.96.96.0 0.0.0.255 host 130.0.0.30
access-list 2003 permit ip 97.97.97.0 0.0.0.255 host 140.0.0.30
access-list 2004 permit ip 98.98.98.0 0.0.0.255 host 150.0.0.30
access-list 2005 permit ip 99.99.99.0 0.0.0.255 host 160.0.0.30
!
arp vrf vrf-ha6 10.0.0.10 0000.0c07.ac32 ARPA
arp vrf vrf-ha4 8.0.0.10 0000.0c07.ac1e ARPA
arp vrf vrf-ha5 9.0.0.10 0000.0c07.ac28 ARPA
arp vrf vrf-ha2 6.0.0.10 0000.0c07.ac0a ARPA
arp vrf vrf-ha3 7.0.0.10 0000.0c07.ac14 ARPA
!
route-map RRQ-HA5 permit 10
 match ip address 2000
 set ip next-hop 9.0.0.10
!
route-map RRQ-HA4 permit 10
 match ip address 2000
 set ip next-hop 8.0.0.10
!
route-map RRQ-HA6 permit 10
 match ip address 2000
 set ip next-hop 10.0.0.10
!
route-map RRQ-HA3 permit 10
 match ip address 2000
 set ip next-hop 7.0.0.10
!
route-map RRQ-HA2 permit 10
 match ip address 2000
 set ip next-hop 6.0.0.10
!
route-map RRQ-HA10 permit 10
 match ip address 2001
 continue 11
 set ip next-hop 200.0.0.5
!
route-map RRQ-HA10 permit 11
 match ip address 2002
 continue 12
 set ip next-hop 200.0.0.15
!
route-map RRQ-HA10 permit 12
 match ip address 2003
 continue 13
 set ip next-hop 200.0.0.25
!
route-map RRQ-HA10 permit 13
 match ip address 2004
 continue 14
 set ip next-hop 200.0.0.35
!
route-map RRQ-HA10 permit 14
 match ip address 2005
 set ip next-hop 200.0.0.45
```

HA の設定：スイッチ 1：

HA1:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 12.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.126
 encapsulation dot1Q 126
 ip address 126.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.127
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 127
 ip address 6.0.0.3 255.255.255.0
 standby 10 ip 6.0.0.10
 standby 10 preempt
 standby 10 name HSRP_HA_HA2
 standby 10 track GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.4 255.0.0.0
 no snmp trap link-status
 standby 200 ip 200.0.0.5
 standby 200 preempt
 standby 200 track GigabitEthernet0/0.127
!
router mobile
!
ip local pool ha-pool2 10.1.2.1 10.1.2.255
ip route 92.92.92.1 255.255.255.255 6.0.0.5
ip route 95.95.95.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA2 virtual-network address 12.0.0.30 mode
active-standby
ip mobile virtual-network 12.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool2 virtual-network 12.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 6.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA2:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 13.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.136
 encapsulation dot1Q 136
 ip address 136.0.0.83 255.255.255.0
!
interface GigabitEthernet0/0.137
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 137
 ip address 7.0.0.3 255.255.255.0
 standby 20 ip 7.0.0.10
```

```
 standby 20 preempt
 standby 20 name HSRP_HA_HA3
 standby 20 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.14 255.0.0.0
 no snmp trap link-status
 standby 201 ip 200.0.0.15
 standby 201 preempt
 standby 201 track GigabitEthernet0/0.137
!
router mobile
!
ip local pool ha-pool3 10.1.3.1 10.1.3.255
ip route 92.92.92.1 255.255.255.255 7.0.0.5
ip route 96.96.96.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA3 virtual-network address 13.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool3 virtual-network 13.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA3:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 14.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.146
 encapsulation dot1Q 146
 ip address 146.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.147
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 147
 ip address 8.0.0.3 255.255.255.0
 standby 30 ip 8.0.0.10
 standby 30 preempt
 standby 30 name HSRP_HA_HA4
 standby 30 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.24 255.0.0.0
 no snmp trap link-status
 standby 202 ip 200.0.0.25
 standby 202 preempt
 standby 202 track GigabitEthernet0/0.147
!
router mobile
!
ip local pool ha-pool4 10.1.4.1 10.1.4.255
ip route 92.92.92.1 255.255.255.255 8.0.0.5
ip route 97.97.97.0 255.255.255.0 200.0.0.3
```

```
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA4 virtual-network address 14.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile virtual-network 14.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool4 virtual-network 14.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 8.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA4:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 15.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.156
 encapsulation dot1Q 156
 ip address 156.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.157
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 157
 ip address 9.0.0.3 255.255.255.0
 standby 40 ip 9.0.0.10
 standby 40 preempt
 standby 40 name HSRP_HA_HA5
 standby 40 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.34 255.0.0.0
 no snmp trap link-status
 standby 203 ip 200.0.0.35
 standby 203 preempt
 standby 203 track GigabitEthernet0/0.157
!
router mobile
!
ip local pool ha-pool5 10.1.5.1 10.1.5.255
ip route 92.92.92.1 255.255.255.255 9.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA5 virtual-network address 15.0.0.30 mode
active-standby
ip mobile virtual-network 15.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool5 virtual-network 15.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 9.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA5:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 16.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.166
 encapsulation dot1Q 166
 ip address 166.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.167
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 167
 ip address 10.0.0.3 255.255.255.0
 standby 50 ip 10.0.0.10
 standby 50 preempt
 standby 50 name HSRP_HA_HA6
 standby 50 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.44 255.0.0.0
 no snmp trap link-status
 standby 204 ip 200.0.0.45
 standby 204 preempt
 standby 204 track GigabitEthernet0/0.167
!
router mobile
!
ip local pool ha-pool6 10.1.6.1 10.1.6.255
ip route 92.92.92.1 255.255.255.255 10.0.0.5
ip route 99.99.99.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA6 virtual-network address 16.0.0.30 mode
active-standby
ip mobile virtual-network 16.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool6 virtual-network 16.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 10.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA の設定：スイッチ 2：

HA1:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 12.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.126
 encapsulation dot1Q 126
 ip address 126.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.127
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 127
 ip address 6.0.0.4 255.255.255.0
 standby 10 ip 6.0.0.10
 standby 10 preempt
```

```
 standby 10 name HSRP_HA_HA2
 standby 10 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.6 255.0.0.0
 no snmp trap link-status
 standby 200 ip 200.0.0.5
 standby 200 preempt
 standby 200 track GigabitEthernet0/0.127
!
router mobile
!
ip local pool ha-pool2 10.1.2.1 10.1.2.255
ip route 92.92.92.1 255.255.255.255 6.0.0.5
ip route 95.95.95.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA2 virtual-network address 12.0.0.30 mode
active-standby
ip mobile virtual-network 12.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool2 virtual-network 12.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 6.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA2:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 13.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.136
 encapsulation dot1Q 136
 ip address 136.0.0.33 255.255.255.0
!
interface GigabitEthernet0/0.137
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 137
 ip address 7.0.0.4 255.255.255.0
 standby 20 ip 7.0.0.10
 standby 20 preempt
 standby 20 name HSRP_HA_HA3
 standby 20 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.16 255.0.0.0
 no snmp trap link-status
 standby 201 ip 200.0.0.15
 standby 201 preempt
 standby 201 track GigabitEthernet0/0.137
!
router mobile
!
ip local pool ha-pool3 10.1.3.1 10.1.3.255
ip route 92.92.92.1 255.255.255.255 7.0.0.5
ip route 96.96.96.0 255.255.255.0 200.0.0.3
!
```

```
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA3 virtual-network address 13.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool3 virtual-network 13.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA3:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 14.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.146
 encapsulation dot1Q 146
 ip address 146.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.147
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 147
 ip address 8.0.0.4 255.255.255.0
 standby 30 ip 8.0.0.10
 standby 30 preempt
 standby 30 name HSRP_HA_HA4
 standby 30 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.26 255.0.0.0
 no snmp trap link-status
 standby 202 ip 200.0.0.25
 standby 202 preempt
 standby 202 track GigabitEthernet0/0.147
!
router mobile
!
ip local pool ha-pool4 10.1.4.1 10.1.4.255
ip route 92.92.92.1 255.255.255.255 8.0.0.5
ip route 97.97.97.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA4 virtual-network address 14.0.0.30 mode
active-standby
ip mobile virtual-network 14.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool4 virtual-network 14.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 8.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA4:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 15.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.156
 encapsulation dot1Q 156
 ip address 156.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.157
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 157
 ip address 9.0.0.4 255.255.255.0
 standby 40 ip 9.0.0.10
 standby 40 preempt
 standby 40 name HSRP_HA_HA5
 standby 40 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.36 255.0.0.0
 no snmp trap link-status
 standby 203 ip 200.0.0.35
 standby 203 preempt
 standby 203 track GigabitEthernet0/0.157
!
router mobile
!
ip local pool ha-pool5 10.1.5.1 10.1.5.255
ip route 92.92.92.1 255.255.255.255 9.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA5 virtual-network address 15.0.0.30 mode
active-standby
ip mobile virtual-network 15.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool5 virtual-network 15.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 9.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

HA5:

```
interface Loopback0
 description Advertised Home Agent Virtual IP Address
 ip address 16.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.166
 encapsulation dot1Q 166
 ip address 166.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.167
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 167
 ip address 10.0.0.4 255.255.255.0
 standby 50 ip 10.0.0.10
 standby 50 preempt
 standby 50 name HSRP_HA_HA6
```

```
 standby 50 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.46 255.0.0.0
 no snmp trap link-status
 standby 204 ip 200.0.0.45
 standby 204 preempt
 standby 204 track GigabitEthernet0/0.167
!
router mobile
!
ip local pool ha-pool6 10.1.6.1 10.1.6.255
ip route 92.92.92.1 255.255.255.255 10.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA6 virtual-network address 16.0.0.30 mode
active-standby
ip mobile virtual-network 16.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool6 virtual-network 16.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 10.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

CHAPTER 12

HA のアカウンティング

この章では、Cisco Mobile Wireless Home Agent のアカウントに関するコンセプト、およびこの機能の設定方法について説明します。

この章は、次の内容で構成されています。

HA アカウンティングの概要

この機能は主として、CMX ソリューションにおいて、Home Agent（HA）と Service Selection Gateway（SSG）を相互運用する目的で開発されました。しかし、SSG と相互運用しない場合でも、この機能を使用できます。

このリリースは、次のアカウンティング機能をサポートしています。

- 冗長設定での HA アカウンティング
- アカウンティング レコードのパケット カウントおよびバイト カウント
- アカウンティング レコードで追加されたアトリビュート
- 追加されたアカウンティング方式：中間アカウンティングのサポート

バイトおよびパケットのカウントは HA 上で実行されるので、このアカウンティング機能では、完全なアカウンティング情報を生成するためにネットワーク上の SSG を使用する必要はありません。

HA のアカウンティング機能には、次のアクティビティが含まれます。

- HA は、モバイルの初回バインディングの作成時に、アカウンティング開始レコードを送信します。
- HA は、モバイルの最終バインディングの削除時に、アカウンティング停止レコードを送信します。

- HA は、ハンドオフの発生時にアカウンティング アップデートを送信します。
- スタートストップおよび中間アカウンティング方式がサポートされます。
- 認証済み Network Access Identifier（NAI: ネットワーク アクセス識別子）について、エラー コードを含むモバイル IP 登録応答が送信されると（その NAI のバインディングが存在しない場合など）、アカウンティング停止レコードが送信されます。
- 既存バインディングの再登録に失敗すると、認証済み NAI について、対応する拒否コードを含むウォッチドッグ メッセージが送信されます。

次のアトリビュートが、アカウンティング レコードにより送信されます。

- Username アトリビュートの NAI（1）
- Framed IP Address アトリビュートの MN IP アドレス（8）
- HA IP アドレス（26/7、3gpp2 アトリビュート）
- トンネル エンド ポイントの Care-of-Address（CoA; 気付アドレス）（66）
- Network Access Server（NAS）IP アドレス アトリビュート（4）
- Accounting Status Type アトリビュート（40）
- アカウンティング セッション ID（44）
- アカウンティング終了理由（49）：アカウンティング停止時のみ
- アカウンティング遅延時間（41）
- Acct-Input-Octets（42）
- Acct-Output-Octets（43）
- Acct-Input-Packets（47）
- Acct-Output-Packets（48）
- Acct-Input-Gigawords（52）
- Acct-Output-Gigawords（53）
- "mobileip-mn-flags" cisco-avpair アトリビュートの登録フラグ
- "mobileip:ip-vrf" cisco-avpair アトリビュートの Vrf 名

単一 IP HA アカウンティングのサポート

単一 IP HA 設計により、単一 IP モデルのトラフィック プロセッサで AAA サービスを実行するための基盤となる機能がサポートされます。アカウンティング サービスの場合、Radius アカウンティングはトラフィック プロセッサで実行されます。各トラフィック プロセッサは、Radius トラフィックを発信する際に固有の UDP ソース ポートを使用します。Radius 応答はこのポートを UDP 宛先ポートとして使用し、Radius メッセージを発信したトラフィック プロセッサを識別する際に使用します。

これらのメッセージには、**Start**、**Update**、および **Stop** が含まれます。

この機能がサポートされるのは、Service Application Module for IP（SAMI）ブレードを備えた Cisco 7600 スイッチだけです。

単一 IP HA アカウンティング サポートを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	Router(config)# **sami balance ports** *start-port end-port*	この設定は、リロード後に限り有効です。特定のプロセッサ向けにポートを設定して、AAA へアカウンティング メッセージを送信するようポートを設定します。このコマンドが設定されていない場合、45000 ～ 46535 のデフォルト ポートはカード用に設定されます。このコマンドで指定する範囲は、6 の倍数であることが必要です。 **（注）** デフォルト設定を使用することをお勧めします。
ステップ 2	router#**show sami port-range**	show コマンドは、現在設定されているポート範囲を表示します。またリロード後に有効になるポート範囲も表示します。
ステップ 3	router#**debug radius**	このデバッグにより、Remote Authentication Dial-In User Service（RADIUS）デバッグがイネーブルになり、アカウンティング パケットが目的のポート上の AAA に送信されているかどうかをチェックできます。
ステップ 4	router#**debug aaa accounting**	アカウンティング デバッグ メッセージをイネーブルにします。

次に設定例を示します。

```
Slot4#show sami port-range
Current Start Port range 30000 End port range 35999 Range Per PPC 1000
 Port ranges for
    Processor 3: 30000 to 30999
    Processor 4: 31000 to 31999
    Processor 5: 32000 to 32999
    Processor 6: 33000 to 33999
    Processor 7: 34000 to 34999
    Processor 8: 35000 to 35999

After Reload Start Port range 30000 End port range 35999 Range Per PPC 1000


aaa authentication login default local
aaa authentication ppp default group radius
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa accounting update periodic 1
aaa accounting network default start-stop group radius

ip local pool fasim-pool-82 16.82.0.1 16.82.100.254
ip forward-protocol nd
ip mobile home-agent revocation
ip mobile home-agent dynamic-address 48.48.48.48
ip mobile home-agent accounting default
ip mobile host nai @fasim48.com address pool local fasim-pool-82 virtual-network
16.82.0.0 255.255.0.0 aaa load-sa lifetime 7400

radius-server host 12.1.3.2 auth-port 1645 acct-port 1646 key lab
radius-server vsa send accounting
```

ドメイン単位のアカウンティング

HA の VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）機能を使用して、アカウンティング グループや認証グループを設定したり、アカウンティングが VRF 定義の一部としてイネーブルかどうかを設定できます。Cisco Mobile Wireless Home Agent Release 5.0 では、VRF 内でアカウンティングの中間アップデート間隔タイマーをレルム単位の設定として定義できるようになりました。

この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)#ip mobile realm @xyz.com ha-addr ip-address [aaa-group [accounting aaa-acct-group | authentication aaa-auth-group]] periodic minutes`	VRF に依存せず、レルム単位の設定をイネーブルにします。
ステップ 2	`Router(config)#ip mobile realm @xyz.com vrf vrf-name ha-addr ip-address [aaa-group [accounting aaa-acct-group | authentication aaa-auth-group]] periodic minutes`	VRF コンフィギュレーション コマンドが、アカウンティング サポートを行うよう強化されます。 **periodic** キーワードは、中間アカウンティング レコードを *minutes* 値で設定された間隔で送信する方法を定義します。

（注）　VRF 単位の設定はレルム単位の設定よりも優先され、レルム単位の設定は **aaa accounting update periodic** 設定より優先されます。

show コマンドには、従来表示されていたパラメータに加えて、期間（分）に関するパラメータも含まれるようになりました。

次に、ドメイン単位のアカウンティングのルータ設定例を示します。

```
ip mobile host nai @yahoo.com address pool local mypool virtual-network 60.0.0.0
255.255.0.0 aaa load-sa
ip mobile host nai @cisco.com address pool local hapool virtual-network 65.0.0.0
255.255.0.0 aaa load-sa
ip mobile host nai @xyz.com address pool local nextpool virtual-network 61.0.0.0
255.255.0.0 aaa load-sa
ip mobile host nai @abc.com address pool local vrf-pool1 virtual-network 55.1.1.0
255.255.255.0 aaa load-sa
ip mobile realm @yahoo.com aaa-group accounting mylist authentication mylist periodic 2
accounting
```

中間アカウンティングの同期化

Home Agent Release 5.0 では、次のセッション単位のフィールドがスタンバイ HA と定期的に同期化されます。

- Input octets
- Output octets
- Input bytes
- Output bytes
- Input octets gigawords
- Output octets gigawords
- Input packet gigawords

- Output packet gigawords
- Data Path Idle Timer

アップデート間隔は分単位で設定可能で、中間アカウンティング アップデートの Radius メッセージを送信する設定からは独立しています。

入力/出力カウントの値に変更があった場合に限り、情報がスタンバイ HA へ送信されます。

この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# redundancy periodic-sync interval` *minutes* `limit cpu` *Percentage cpu Threshold* `rate` *rate*#	アカウンティング カウンタについてアクティブおよびスタンバイ HA 間の定期アップデートをイネーブルにします。これを使用して同期メッセージを伝播し、設定された期間にわたって負荷を均等に分散させます。デフォルト値は **5** 分です。**0** 分を入力すると、冗長性の同期がディセーブルになります。 CPU のしきい値が CPU の制限値を超えた場合、HA は 5 秒ごとに 500 バインディングを送信することで調整を開始します。デフォルトのしきい値は 70 % です。 CPU の負荷またはメモリのしきい値が超過していることが原因で、指定したレートでは適合しない可能性があります。 デフォルトの同期レートを達成するには、最大バインディングに適合する間隔を選択することをお勧めします。したがって、500,000 バインディングに対して **1** 分の間隔を選択しても、レートが CLI でも指定されていない限り、計算されたレートとして受け付けられません（必要なレートは 8500/秒、最大 5000/秒）。
ステップ 2	`Router# show redundancy inter-device`	次に示す冗長性に関する統計値を表示します。 • Input octets • Output octets • Input bytes • Output bytes • Input octets gigawords • Output octets gigawords • Input packet gigawords • Output packet gigawords • Data Path Idle Timer
ステップ 3	`Router#debug redundancy periodic-sync`	モバイル IP のステートフル セッションの冗長性に関する定期的な同期デバッグ情報を表示します。

基本的なアカウンティング メッセージ

Home Agent Release 2.1 以上は、Cisco Service Selection Gateway（SSG）をサポートしています。このリリースで HA が送信するのは、統計情報を含まない 3 つのアカウンティング メッセージだけです。SSG は、すべてのネットワーク トラフィックが SSG を通過するように設計され、配置されます。

すべてのトラフィックが通過するので、SSG はすべての統計情報を保持しますが、モバイル IP セッション情報は保持しません。HA は、モバイル IP セッション情報を保持しているので、この情報を SSG に送信します。

HA は、SSG/AAA サーバに次のメッセージを送信します。

- アカウンティング開始：HA は、次の場合に、このメッセージを SSG/AAA サーバに送信します。
  - Mobile Node（MN; モバイル ノード）が初回登録に成功した場合。これは、MN の新規モバイル IP セッションの開始を示しています。
  - 冗長設定の HA の場合、スタンバイ HA は、アクティブになった時点で以前のバインディングが存在しない場合にのみ、アカウンティング開始メッセージを送信します。これにより、SSG で、障害 HA 上の MN のホスト オブジェクトが保持されます。ただし、Phase-1 では、冗長性はサポートされません。
- アカウンティング アップデート：HA は、定期的なアカウンティング アップデート メッセージが設定され、モバイル ノードの Point of Attachment（POA）が変更されると、アカウンティング アップデート メッセージを生成します。モバイル IP セッションの場合、これは、モバイルノードが CoA 変更後の再登録に成功したことを意味します。CoA は、外部ネットワーク上のモバイル ノードの現在位置です。また、既存バインディングの再登録に失敗した場合、HA は適正な拒否コードを含むアカウンティング アップデート メッセージを送信します。
- アカウンティング停止：HA は、認証済み NAI について、その NAI にバインディングが存在しないという理由で、エラー コードを含む RRP が送信された場合（MobileIP エラー コード 136 を除く）、アカウンティング停止メッセージを送信します。

すべてのメッセージに、次の情報が含まれます。

- **Network Access Identifier（NAI）**：MN の名前です。abc@service_provider1.com のような名前になります。
- **Network Access Server（NAS）IP**：アカウンティング ノードの IP アドレスです。HA はアカウンティング ノードなので、このフィールドには HA のアドレスが含まれます。
- **Framed IP Address**：MN の IP アドレスです。通常、登録に成功すると、HA により MN に IP アドレスが割り当てられます。
- **Point Of Attachment（POA）**：ネットワーク上の MN の接続ポイントです。モバイル IP セッションの場合、MN の気付アドレス（CoA）になります。

HA のシステム アカウンティング

HA のサービス開始時点（つまり、ボックスのリロード後の初期化時点）で、アクティブな HA が存在しない場合、Accounting On が送信されます。

accounting-off は、アクティブ HA のサービスが停止（グレースフルその他）し、HA サービスを提供するスタンバイ HA が存在しない場合には、送信されるはずです。accounting-off は、常に送信されるとは限りません。

スタンバイ HA のサービス停止（グレースフルその他）の場合、accounting-off は送信されません。

モバイル IP HA から送信されないメッセージ

次のメッセージは、モバイル IP HA から送信されません。

- HA ボックスがオンラインになった時点、またはブートアップ時の Accounting On メッセージ（Acct-Status-Type=Accounting-On）：このメッセージは、モバイル IP コンフィギュレーションに関係のない、プラットフォームのグローバル エンティティです。このメッセージは通常、モバイル IP などのサービスではなく、プラットフォームのコードによって初期化中に実装されます。
- HA ボックスのシャットダウン時の Accounting Off メッセージ（Acct-Status-Type=Accounting-Off）：このメッセージは、モバイル IP コンフィギュレーションに関係のない、プラットフォームのグローバル エンティティです。このメッセージは通常、モバイル IP などのサービスではなく、プラットフォームのコードによってリブート中に実装されます。

HA アカウンティングの設定

モバイル IP では現在、AAA コマンドを使用して認証パラメータを設定しています。次のすべてのコマンドが必要です。デフォルトでは、HA アカウンティング機能はディセーブルです。設定しない場合、HA は AAA サーバにアカウンティング メッセージを送信しません。HA アカウンティング機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent accounting list`	HA アカウンティングをイネーブルにし、Home Agent の定義済みアカウンティング方式リストを適用します。*list* は、HA アカウンティング レコードの生成に使用する AAA アカウンティング方式です。
ステップ 2	`Router(config)# redundancy periodic-sync interval`	（アクティブおよびスタンバイ HA 間の）冗長性設定でバインディング統計値の定期的同期と、バインディングの残りのアイドル時間を制御します。
ステップ 3	`Router(config)# aaa accounting network method list name start-stop group group name`	処理の開始時にアカウンティング「開始」通知、処理の終了時にアカウンティング「停止」通知を送信します。アカウンティング「開始」レコードは、バックグラウンドで送信されます。要求したユーザ プロセスは、アカウンティング サーバがアカウンティング「開始」通知を受信したかどうかに関係なく、開始されます。
ステップ 4	`Router(config)# aaa accounting update newinfo`	対象ユーザに関する新しいアカウンティング情報が発生するごとに、アカウンティング サーバに中間アカウンティング レコードを送信します。
ステップ 5	`Router(config)# aaa accounting system default start-stop group radius`	HA によるシステム メッセージの送信をイネーブルにします。
ステップ 6	`Router(config)# ip mobile homeagent switchover aaa swact-notification`	各 MIP セッションに対するアカウンティングのウォッチドッグ/停止メッセージの後、Switchover-Action（swact）Notification を送信します。
ステップ 7	`Router# debug aaa accounting`	HA アカウンティング メッセージのデバッグをイネーブルにします。

	コマンド	目的
ステップ 8	Router# **debug radius** Router# **debug tacacs**	セキュリティ プロトコル特定メッセージのデバッグをイネーブルにします。
ステップ 9	Router# **debug ip mobile**	モバイル IP 関連デバッグ メッセージをイネーブルにします。アカウンティングでは、デバッグ メッセージが出力されるのはエラー発生時だけです。

HA アカウンティングの設定例

最初のコマンド ブロックは、AAA の設定です。ネットワーク アカウンティング用に、アカウンティング方式リスト（mylist）が作成されています。Start-Stop キーワードは、HA から 開始および終了レコードを送信することを意味します。詳細については、『*IOS Security Configuration Guide*』を参照してください。

2 行目は、気付アドレス（CoA）が変更された場合、アカウンティング アップデート レコードを送信するように HA に指示しています。

```
ip mobile home-agent accounting mylist address 10.3.3.1
ip mobile host 10.3.3.2 3.3.3.5 interface Ethernet2/2
ip mobile secure host 10.3.3.2 spi 1000 key ascii test algorithm md5 mode prefix-suffix
```

これらは、モバイル IP コマンドです。1 行目で、アカウンティング方式リスト mylist を HA に適用し、HA のアカウンティングをイネーブルに設定しています。

```
!
!
radius-server host 172.16.162.173 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
!
```

これらは、RADIUS コマンドです。1 行目で、RADIUS サーバのアドレスを指定します。HA が AAA サーバにアクセスでき、適切なアクセス権限があることを確認してください。

次に、HA アカウンティングの設定例を示します。

アクティブ HA：

```
router#
router#show run
Building configuration...

Current configuration : 4927 bytes
!
! Last configuration change at 05:12:03 UTC Thu Oct 13 2005
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname cisco7600
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
```

```
!
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default local group radius
aaa authorization configuration default group radius
aaa accounting update newinfo periodic 2
aaa accounting network mylist start-stop group radius
aaa accounting system default start-stop group radius
!
!
aaa session-id common
!
resource manager
!
no ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
ip dhcp ping packets 0
!
!
ip dhcp-server 99.107.0.13
vpdn-group 1
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
!
!
no virtual-template snmp
!
!
username cisco7600 password 0 cisco
!
interface Loopback1
 ip address 11.0.0.1 255.0.0.0
!
interface FastEthernet0/0
 description "LINK TO HAAA.................!"
 ip address 150.2.13.40 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 4 ip 150.2.0.252
 standby 4 priority 110
 standby 4 preempt delay reload 300
 standby 4 name cisco1
!
interface FastEthernet1/0
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface FastEthernet2/0
```

```
 description "LINK TO PDSN.................!"
 ip address 7.0.0.10 255.0.0.0
 no ip route-cache cef
 no ip route-cache
 duplex half
 standby 2 ip 7.0.0.2
 standby 2 priority 110
 standby 2 preempt delay reload 300
 standby 2 name cisco
!
interface FastEthernet3/0
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
 bridge-group 4
 bridge-group 4 spanning-disabled
!
interface Ethernet6/0
 description ""LINK TO REFLECTOR...."
 ip address 99.107.0.19 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 3 ip 99.107.89.67
 standby 3 priority 110
 standby 3 preempt delay reload 300
 standby 3 name reflector
!
interface Ethernet6/1
 description "LINK TO TFTP....."
 ip address 1.7.130.10 255.255.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet6/2
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/3
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/4
 no ip address
 no ip route-cache cef
```

```
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/5
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/6
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/7
 no ip address
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 shutdown
 duplex half
 no cdp enable
!
interface Virtual-Template1
 no ip address
!
router mobile
!
ip local pool LNS-Pool 8.3.0.1 8.3.0.100
ip local pool ispabc-pool 40.0.0.101 40.0.0.255
ip default-gateway 10.1.2.13
ip classless
ip route 8.0.0.1 255.255.255.255 7.0.0.1
ip route 9.0.0.1 255.255.255.255 7.0.0.1
ip mobile home-agent accounting mylist broadcast
ip mobile home-agent ip mobile home-agent redundancy
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai @ispxyz.com address pool local ispabc-pool virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 250
ip mobile secure home-agent 7.0.0.2 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.67 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
!
no ip http server
!
!
ip radius source-interface Loopback1
access-list 120 deny   ip 40.0.0.0 0.255.255.255 40.0.0.0 0.255.255.255
access-list 120 permit ip any any
dialer-list 1 protocol ip permit
!
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
```

```
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
dial-peer cor custom
!
!
gatekeeper
 shutdown
!
alias exec shb sh ip mob bin
alias exec shr sh ip route
alias exec sht sh ip mob tun
alias exec shh sh ip mob host
alias exec clr clear ip mob bin all
!
line con 0
 exec-timeout 0 0
 length 0
 stopbits 1
line aux 0
 exec-timeout 0 0
 password 7 0507070D
 length 0
 stopbits 1
line vty 0 4
 password 7 0507070D
!
no scheduler max-task-time
ntp master 1
ntp update-calendar
ntp server 30.1.0.1
!
end

router#
```

スタンバイ HA：

```
router#
router#show run
Building configuration...

Current configuration : 3995 bytes
!
! No configuration change since last restart
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname cisco7600
!
boot-start-marker
boot system tftp /auto/tftpboot-users/tennis/c7600-h1is-mz.123-3.8.PI2 171.69.1.129
boot-end-marker
```

```
!
enable password 7 00445566
!
no spd enable
aaa new-model
!
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default local group radius
aaa authorization configuration default group radius
aaa accounting update newinfo periodic 2
aaa accounting network mylist start-stop group radius
aaa accounting system default start-stop group radius
!
!
aaa session-id common
!
resource manager
!
ip subnet-zero
!
!
no ip cef
ip ftp username pdsn-team
ip ftp password 7 pdsneng
ip host PAGENT-SECURITY-V3 32.68.10.4 38.90.0.0
ip name-server 11.69.2.133
no ip dhcp use vrf connected
!
!
vpdn enable
vpdn ip udp ignore checksum
!
vpdn-group 1
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
!
!
no virtual-template snmp
!
username mwt13-7600b password 0 cisco
!
interface Loopback1
 ip address 11.0.0.1 255.0.0.0
 no ip route-cache
!
interface FastEthernet0/0
 ip address 4.0.10.2 255.0.0.0
 no ip route-cache
 duplex half
 no cdp enable
!
interface FastEthernet1/0
 no ip address
 no ip route-cache
 duplex half
 no cdp enable
!
interface FastEthernet2/0
```

```
 description "LINK TO HAAA.................!"
 ip address 15.2.13.20 255.255.0.0
 no ip route-cache
 duplex full
 no cdp enable
 standby 4 ip 15.2.0.252
 standby 4 name cisco1
!
interface FastEthernet5/0
 description "LINK TO PDSN.................!"
 ip address 7.0.0.67 255.0.0.0
 no ip route-cache
 duplex full
 standby 2 ip 7.0.0.2
 standby 2 name cisco
!
interface Ethernet6/0
 description "LINK TO REFLECTOR....!"
 ip address 22.107.0.12 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 duplex half
 no cdp enable
 standby 3 ip 22.107.89.67
 standby 3 name reflector
!
interface Ethernet6/1
 description "LINK TO TFTP....."
 ip address 1.7.130.2 255.255.0.0
 no ip route-cache
 duplex half
 no cdp enable
!
interface Ethernet6/2
 no ip address
 no ip route-cache
 shutdown
 duplex half
 no cdp enable
!
interface Ethernet6/3
 no ip address
 no ip route-cache
 shutdown
 duplex half
 no cdp enable
!
router mobile
!
ip local pool LNS-Pool 8.3.0.1 8.3.0.100
ip local pool ispabc-pool 40.0.0.101 40.0.0.255
ip default-gateway 10.1.2.13
ip classless
ip route 8.0.0.1 255.255.255.255 7.0.0.1
ip route 9.0.0.1 255.255.255.255 7.0.0.1
ip mobile home-agent accounting mylist broadcast
ip mobile home-agent ip mobile home-agent redundancy
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai @ispxyz.com address pool local ispabc-pool virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 250
ip mobile secure home-agent 7.0.0.2 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.10 spi 1001 key ascii cisco algorithm md5 mode
prefix-suffix
```

```
!
no ip http server
!
!
ip radius source-interface Loopback1
dialer-list 1 protocol ip permit
!
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane

!
gatekeeper
 shutdown
!
alias exec shb sh ip mob bin
alias exec shr sh ip route
alias exec sht sh ip mob tun
alias exec shh sh ip mob host
alias exec clr clear ip mob bin all
!
line con 0
 exec-timeout 0 0
 length 0
 stopbits 1
line aux 0
 exec-timeout 0 0
 length 0
 stopbits 1
line vty 0 4
 password 7 0507070D
!
no scheduler max-task-time
ntp master 1
ntp update-calendar
ntp server 30.1.0.1
!
end
```

HA アカウンティングの設定の確認

HA アカウンティングのステータスを確認するには、**show ip moEnables periodic updates betweenbile global** コマンドを使用します。現在のアカウンティング ステータスが、次のように表示されます。

```
router# sh ip mobile global
IP Mobility global information:

Home Agent

    Registration lifetime: 10:00:00 (36000 secs)
    Broadcast enabled
    Replay protection time: 7 secs
    Reverse tunnel enabled
    ICMP Unreachable enabled
    Strip realm disabled
```

```
    NAT Traversal disabled
    HA Accounting enabled using method list: mylist
    NAT UDP Tunneling support enabled
    UDP Tunnel Keepalive 110
    Forced UDP Tunneling disabled
    Standby groups
        cisco (virtual network - address 7.0.0.2)
    Virtual networks
        40.0.0.0 /8

Foreign Agent is not enabled, no care-of address

0 interfaces providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled, cef switching enabled
Tunnel path MTU discovery aged out after 10 min
Radius Disconnect Capability disabled

router#
```

CHAPTER 13

Home Agent（HA）でのマルチ VPN ルーティングおよびフォワーディング（VRF）

この章では、マルチ VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）Customer Edge（CE; カスタマー エッジ）ネットワーク アーキテクチャの機能要素、および Cisco IOS Mobile Wireless Home Agent ソフトウェアでの実装について説明します。

この章は、次の内容で構成されています。

HA での VRF サポート

Home Agent（HA）は、異なるレルムで開かれたモバイル IP フローのモバイル ノードについて、オーバーラップ IP アドレスをサポートします。この機能は、マルチ VPN VRF CE ネットワーク アーキテクチャを基盤とし、単一の CE デバイスで複数の VPN（つまり複数のカスタマー）をサポートできるように、BGP/MPLS VPN アーキテクチャに拡張したものです。これにより、必要な機器数を削減し、管理を簡素化しながら、CE ネットワーク内でオーバーラップ IP アドレス スペースを使用できます。

マルチ VRF CE は、これらの問題に対応している Cisco IOS Release 12.2(4)T で導入された新機能です。マルチ VRF CE は、VRF-Lite とも呼ばれ、MPLS-VPN モデル内の CE に、限定された Provider Edge（PE; プロバイダー エッジ）機能を提供します。CE ルータで個別の VRF テーブルを保持できるので、MPLS-VPN のプライバシーおよびセキュリティを、PE ルータ ノードだけでなく、ブランチ オフィスにも拡張して適用できます。CE は、カスタマー ネットワーク間、または単一カスタマー ネットワーク内のエンティティ間のトラフィック分離をサポートしています。CE ルータ上の各 VRF は、PE ルータ上の対応する VRF にマッピングされます。

マルチ VRF CE ネットワーク アーキテクチャの詳細については、次の URL にある Cisco Product Bulletin 1575 を参照してください。
http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/1575_pp.pdf.

図 13-1　Cisco パケット データ サービス ノード（PDSN）/HA アーキテクチャの VRF-Lite

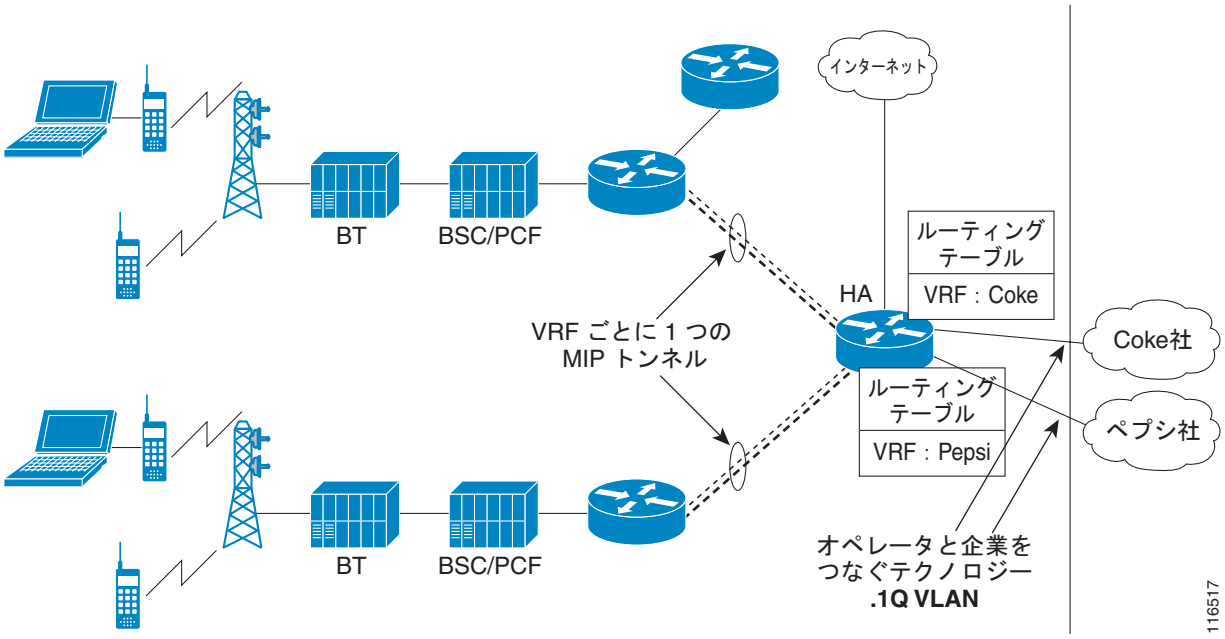


図 13-1 は、Packet Data Serving Node（PDSN; パケット データ サービス ノード）アーキテクチャ、および複数の異なるレルムおよび企業の HA への VRF-Lite ソリューションの適用方法、つまり、企業間のデータの分離方法を示しています。

VRF ソリューションの要点は、次のとおりです。

- ユーザのドメインまたはレルムに基づいて、ユーザの VRF を識別できます。
- 異なる企業に属している異なるモバイルが同じオーバーラップ IP アドレスを共有している場合、PDSN 経由で、モバイルにパケットを確実に配信できます。
- VRF 単位で IP アドレスおよびルーティング テーブルを管理できます。
- 企業またはドメイン単位で VRF を管理できます。
- VRF 単位で Authentication, Authorization and Accounting（AAA; 認証、許可、アカウンティング）認証およびアカウンティング グループをサポートできます。

レルムは、企業ネットワークを識別するために使用します。各レルムに 1 つの仮想 HA が設定されます。Network Access Identifier（NAI; ネットワーク アクセス識別子）は、モバイル IP Registration Request（RRQ; 登録要求）の一部で、PDSN および HA におけるモバイル IP ユーザの主要識別名です。仮想 HA の識別には、NAI のレルム部分が使用されます。モバイル ノードは、*username@company* の NAI 表記を使用し、*company* にサブスクライバのコミュニティを示すレルム名を識別します。

HA では、PDSN への異なる企業接続または VRF を示すために、複数の IP アドレスが使用されます。したがって、各レルムまたは VRF に、PDSN と HA 間の 1 つのモバイル IP トンネルが設定されます。

HA が 2 つの企業、"abc.com" および "xyz.com" に接続している場合、HA に 2 つの固有 IP アドレスが設定されます（通常、ループバック インターフェイスに設定されます）。PDSN には、"abc.com" に到達するアドレス LA1 への MoIP トンネル、および "xyz.com" に到達するアドレス LA2 へのもう 1 つの MoIP トンネルが設定されます。LA1 および LA2 は、ループバック インターフェイスに設定された IP アドレスです。

ホーム AAA Remote Authentication Dial-In User Service（RADIUS）サーバでは、NAI/ ドメイン コンフィギュレーションにより、PDSN は、FA-CHAP または HA-CHAP（MN-AAA 認証）のアクセス応答の一部として、LA1 を "xyz.com" 企業の HA の IP アドレスとして受信し、LA2 を "mnp.com" 企業の HA の IP アドレスとして受信します。

この機能は、HA ロード バランシングを提供する HA Server Load Balancing（HA-SLB; HA サーバ ロード バランシング）ソリューションと併用できます。

モバイル IP トンネルの確立

HA-SLB および VRF をイネーブルにした場合、モバイル IP フローが確立されるまでの手順は、次のとおりです。このコール フローには、2 つのモバイル ノード（MN-1 および MN-2）が存在し、それぞれ ENT-1 および ENT-2 の企業に属しています。

ステップ 1　モバイル IP RRQ が HA に到達すると、HA は入力 RRQ の NAI フィールドを読み取り、設定済み IP アドレスを選択し、この IP アドレスをトンネルの送信元アドレスとして使用して、PDSN に戻すモバイル IP トンネルを形成します。

ステップ 2　PDSN に送信される RRP の "Home-Agent address" フィールドが、上記の IP アドレスに変更されます。

ステップ 3　HA は、レルムに定義された VRF に対応するルーティング テーブルに、モバイルに割り当てられた IP アドレスに対応するホスト ルートを追加します。

ステップ 4　HA のトンネル エンドポイントも、VRF ルーティング テーブルに挿入されます。これにより、モバイルは、同じ HA 上の異なるレルム間で共通 IP アドレスを共有できます。

ステップ 5　MN-1 が、R-P セッションにより、HA アドレスを 0.0.0.0（ダイナミック HA）に設定したモバイル IP RRQ を、PDSN に送信します。

ステップ 6　PDSN は FA-CHAP を開始し、AAA にアクセス要求を送信します。

ステップ 7　AAA は、アクセス応答を戻します。戻される HA アドレスは、HA-SLB の IP アドレスです。

ステップ 8　PDSN は、MIP RRQ を HA-SLB に転送します。

ステップ 9　HA-SLB は、ロードに基づいて実 HA を判別し、HA1 に RRQ を転送します。

ステップ 10　HA-1 が MIP RRQ を受信します。HA-1 は、メッセージ内の NAI を解析し、ユーザのレルム（Ent-1 企業）に基づいてユーザの VRF を判別します。さらに、HA-CHAP（MN-AAA 認証）を実行して、モバイルに Ent-1 の IP アドレスを割り当てます。モバイルのバインディングを作成して、VRF、FIB などのルート テーブル内のルート エントリなど、VRF 特定のデータ構造を読み込みます。

ステップ 11　HA1 は PDSN に MIP RRP を送信し、PDSN と HA 間にモバイル IP トンネルを確立します。HA 上のトンネルのエンド ポイントは、LI-IP-1 になります（MIP RRQ の入力インターフェイスの IP アドレスではありません）。

RADIUS サーバ上の VRF マッピング

Release 3.0 では、VRF 機能が拡張され、RADIUS サーバ上で NAI から VRF へのマッピングを設定できます。この拡張により、モバイルから VRF へのマッピングは、次のように学習されます。HA は、モバイル IP 登録要求を受信すると、RADIUS アクセス要求を送信します。AAA サーバは、アクセス受諾により、RADIUS アトリビュート "cisco-avpair = mobileip:ip-vrf" 内の VRF 名、および RADIUS アトリビュート "cisco-avpair = mobileip-vrf-ha-addr" 内の対応する HA アドレスを、HA に送信します。HA は、この情報を使用し、バインディングを開いて、正しい VRF に関連付けます。これらのアトリビュートが AAA サーバからダウンロードされない場合は、ローカル設定の VRF（存在する場合）が使用されます。

また、HA が PDSN/FA により要求されたアドレスとは異なるアドレスを割り当てる必要がある場合には、コード 136 および新しい HA アドレスで登録応答を送信できるオプションがあります。コード 136 の登録応答を受信すると、モバイルは新しいアドレスを使用して、もう 1 つの登録要求を送信します。HA は、この要求を処理し、バインディングを開き、登録応答（success）を送信することにより、登録プロセスを完了します。

VRF 機能の制約事項

VRF 機能には、次の制約事項があります。

- HA 単位でサポートされる VRF 数は、最大 130 です。
- HA MIB は、VRF 情報ではアップデートされません。

レルム単位の認証およびアカウンティング サーバ グループ

各レルムに、個別の認証およびアカウンティング グループを指定できます。HA は、ユーザのレルムに基づいて、HA 上のそのレルムに指定された認証グループに基づく AAA 認証サーバを選択します。同様に、レルムにアカウンティング グループが指定されている場合、ユーザのレルムに基づいて、AAA アカウンティング サーバが選択されます。

（注） この機能は、VRF 機能と併用できます。

HA の VRF の設定

HA 上に VRF 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(config)#ip mobile realm` *@xyz.com* `vrf` *vrf-name* `ha-addr` *ip-address* [`aaa-group` [`accounting` *aaa-acct-group* | `authentication` *aaa-auth-group*]]	ドメイン *@xyz.com* の VRF を定義します。 また、VRF に対応する HA の IP アドレスを、MOIP トンネルの終端ポイントに定義します。 HA の IP アドレスは、ボックス上のルーティング可能な IP アドレスにする必要があります。 オプションで、VRF 単位の AAA アカウンティングおよび認証サーバ グループを定義できます。 AAA アカウンティング サーバ グループを定義すると、レルムのユーザのすべてのアカウンティング レコードが、指定したグループに送信されます。 AAA 認証サーバ グループを定義すると、HA-CHAP（MN-AAA 認証）が、そのグループに定義されているサーバに送信されます。

	コマンド	目的
ステップ 2	Router(config)# **ip vrf** *vrf-name* description VRF for domain1 rd 10:1	ボックス上に VRF を定義します。 VRF の説明。 VRF のルータ記述子。ルート識別子を指定して、VRF テーブル作成します。 **（注）** 各 HA CPU 上で、各ドメインに 1 つの VRF を設定する必要があります。
ステップ 3	router# **interface Loopback1** ip address 192.168.11.1 255.255.255.0 secondary ip address 192.168.10.1 255.255.255.0	各 VRF の IP アドレスを設定するループバック インターフェイスを定義します。これらのアドレスは、レルムのモバイル IP トンネルの送信元 IP アドレスとして使用されます。 IP アドレスに設定するマスクは、VRF ルーティング テーブルで使用されます。ホスト マスク（255.255.255.255）またはブロードキャスト マスク（0.0.0.0）は、設定しないでください。

次に、VRF のユーザ プロファイルを設定する例を示します。

```
[ //localhost/Radius/Profiles/mwts-mip-r20sit-haslb1-prof/Attributes ]
    CDMA-HA-IP-Addr = 20.20.225.1
    CDMA-MN-HA-Shared-Key = ciscociscociscoc
    CDMA-MN-HA-SPI = 00:00:10:01
    CDMA-Reverse-Tunnel-Spec = "Reverse tunneling is required"
    cisco-avpair = mobileip-vrf-ha-addr=20.20.204.2
    cisco-avpair = ip:ip-vrf#0=ispxyz-vrf1
    class = "Entering the World of Mobile IP-3"
    Service-Type = Framed
```

VRF の設定例

次に、MWAM HA 上での VRF サポートの設定例を示します。

```
CiscoHA#show running-config
Building configuration...

Current configuration : 3366 bytes
!
...
!
aaa new-model
!
!
aaa group server radius vrf-auth-grp1
 server 9.15.100.1 auth-port 1645 acct-port 1646
!
aaa group server radius vrf-auth-grp2
 server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa authorization configuration default group radius
```

```
aaa accounting network default start-stop group radius
aaa accounting network vrf-auth-grp1 start-stop group vrf-auth-grp1
aaa accounting network vrf-auth-grp2 start-stop group vrf-auth-grp2
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip cef
no ip domain lookup
!
!
ip vrf moip-vrf-grp1
 rd 100:1
!
ip vrf moip-vrf-grp2
 rd 100:2
!
no virtual-template snmp
!
!
!
interface Loopback1
 ip address 172.16.11.1 255.255.255.0 secondary
 ip address 172.16.10.1 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.11
 encapsulation dot1Q 11
 ip address 9.15.42.111 255.255.0.0
 no cdp enable
!
interface GigabitEthernet0/0.82
 description Interface towards PDSN
 encapsulation dot1Q 82
 ip address 10.82.82.2 255.255.0.0
!
router mobile
!
ip local pool vrf-pool1 10.5.5.1 5.5.5.254 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.1 5.5.5.254 group vrf-pool-grp2
ip classless
ip route 10.15.47.80 255.255.255.255 GigabitEthernet0/1
ip route 10.76.86.8 255.255.255.255 9.15.0.1
ip route 10.1.0.0 255.255.0.0 GigabitEthernet0/0.82
no ip http server
!
ip mobile home-agent
ip mobile host nai @xyz.com address pool local vrf-pool2 interface GigabitEthernet0/0.82
aaa
ip mobile host nai @cisco.com address pool local vrf-pool1 interface GigabitEthernet0/0.82
aaa
ip mobile realm @xyz.com vrf moip-vrf-grp2 ha 172.16.11.1 aaa-group accounting
vrf-auth-grp1 authentication vrf-auth-grp2
ip mobile realm @cisco.com vrf moip-vrf-grp1 ha 172.16.10.1 aaa-group accounting
vrf-auth-grp2 authentication vrf-auth-grp1
!
!
!
radius-server host 10.15.100.1 auth-port 1645 acct-port 1646 key cisco
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
!
```

```
control-plane
!
...
!
end
```

HA 冗長性を使用した VRF の設定例

次に、HA 冗長性と VRF を使用した Cisco HA の設定例を示します。次の手順が必要です。

ステップ 1　パブリッシュした HA IP アドレスについて、標準 Hot Standby Routing Protocol（HSRP; ホット スタンバイ ルーティング プロトコル）および HA 冗長性を設定します。

ステップ 2　ループバック上の IP アドレス（またはトンネル エンド ポイントの任意の他のインターフェイス IP アドレス）を設定するのではなく、HSRP インターフェイス上に、セカンダリのスタンバイ IP アドレスとして設定します。

ステップ 3　IP モバイルを冗長設定するために、VRF トンネル ポイント サブネットに仮想ネットワークを追加します。

ステップ 4　VRF 関連コマンドを設定します。

ステップ 5　アクティブ HA からスタンバイ HA へのバインディング アップデート メッセージには NAI が含まれているので、スタンバイ HA は、メッセージ内の NAI のドメインに基づいて、適切な VRF を使用したバインディングを作成できます。

アクティブ HA：

```
HA1#sh run
...
aaa new-model
!
!
aaa group server radius vrf-auth-grp1
 server 9.15.100.1 auth-port 1645 acct-port 1646
!
aaa group server radius vrf-auth-grp2
 server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local group radius
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa authorization configuration default group radius
aaa session-id common
ip subnet-zero
ip gratuitous-arps
!
!
ip cef
no ip domain lookup
!
!
ip vrf moip-vrf
 rd 100:1
```

```
!
ip vrf moip-vrf1
 rd 100:2
!
...
!
interface FastEthernet1/0
 ip address 10.92.92.2 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
 standby 10 ip 10.92.92.12
 standby 10 ip 172.16.11.1 secondary
 standby 10 ip 172.16.12.1 secondary
 standby 10 priority 130
 standby 10 preempt delay sync 10
 standby 10 name cisco
!
!
router mobile
!
ip local pool vrf-pool1 10.5.5.5 5.5.5.55 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.5 5.5.5.55 group vrf-pool-grp2
ip classless
ip mobile home-agent address 10.92.92.12
ip mobile home-agent ip mobile home-agent redundancy
ip mobile host nai @cisco.com address pool local vrf-pool1 interface FastEthernet1/0 aaa
ip mobile host nai @xyz.com address pool local vrf-pool2 interface FastEthernet1/0 aaa
ip mobile realm @cisco.com vrf moip-vrf home-agent-address 192.168.11.1 aaa-group
authentication vrf-auth-grp1
ip mobile realm @xyz.com vrf moip-vrf1 home-agent-address 192.168.12.1 aaa-group
authentication vrf-auth-grp2
ip mobile secure home-agent 10.92.92.3 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 172.16.11.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
...
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
radius-server host 10.15.100.1 auth-port 1645 acct-port 1646 key cisco
!
...
end
```

スタンバイ HA：

```
HA2#sh run
...
!
aaa new-model
!
aaa group server radius vrf-auth-grp1
 server 10.15.100.1 auth-port 1645 acct-port 1646
!
aaa group server radius vrf-auth-grp2
 server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp default group radius
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
```

```
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa session-id common
ip subnet-zero
!
!
ip cef
!
!
ip vrf moip-vrf
 rd 100:1
!
ip vrf moip-vrf1
 rd 100:2
!
...
!
interface FastEthernet1/0
 ip address 10.92.92.3 255.255.255.0
 duplex auto
 speed auto
 standby 10 ip 10.92.92.12
 standby 10 ip 172.16.11.1 secondary
 standby 10 ip 172.16.12.1 secondary
 standby 10 preempt delay sync 10
 standby 10 name cisco
!
...
!
router mobile
!
ip local pool vrf-pool1 10.5.5.5 5.5.5.55 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.5 5.5.5.55 group vrf-pool-grp2
ip mobile home-agent address 10.92.92.12
ip mobile home-agent ip mobile home-agent redundancy
ip mobile host nai @cisco.com address pool local vrf-pool1 interface FastEthernet1/0 aaa
ip mobile host nai @xyz.com address pool local vrf-pool2 interface FastEthernet1/0 aaa
ip mobile realm @cisco.com vrf moip-vrf home-agent-address 192.168.11.1 aaa-group
authentication vrf-auth-grp1
ip mobile realm @xyz.com vrf moip-vrf1 home-agent-address 192.168.12.1 aaa-group
authentication vrf-auth-grp2
ip mobile secure home-agent 10.92.92.2 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 172.16.11.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix ignore-spi
ip mobile secure home-agent 172.16.12.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
no ip http server
!
...
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
radius-server host 10.15.100.1 auth-port 1645 acct-port 1646 key cisco
...
end
```

CHAPTER 14

Home Agent（HA）の サービス品質（QoS）

ここでは、Cisco Mobile Wireless Home Agent での Quality of Service（QoS; サービス品質）の概念について説明します。また、この機能の設定方法についても詳しく説明します。

この章は、次の内容で構成されています。

HA QoS の概要

Home Agent（HA）は現時点では、Voice over IP（VoIP）、Push-to-Talk（PTT）などのさまざまなユーザ加入サービスに対し、ユーザ単位で指定したレートに基づくトラフィック制限機能をサポートしていません。バインディング単位のフロー ポリシング機能により、NAI ベースのユーザによって有効にされ、HA に登録された各バインディングに適したレートでパケットを転送できます。

（注） バインディング単位のフローとは、1 つの NAI に対し 1 つのバインディングという意味です。

この機能の主な利点は次のとおりです。

- QoS アクションの実行に、安定した Modular QoS Command Line Interface（MQC; モジュラ QoS コマンドライン インターフェイス）が使用されます。
- インターネットから Mobile Node（MN; モバイル ノード）に送信されるダウンストリーム パケットにおいて、元の DSCP オプションが確実に維持されます。これには、内側の DSCP が外側のトンネル ヘッダーにコピーされます。
- HA に登録したレルム内の個々のユーザまたは全ユーザに対し、トラフィックの識別、分類、およびポリシングを行えます。これは、アップストリームおよびダウンストリーム両方のトラフィックに対して実行されます。オペレータは MQC を使用することで、クラスマップとポリシーマップに従いユーザ トラフィックをグループ化できます。また、バインディング フローを識別する際、帯域幅要件を動的に指定できます。

QoS ポリシング

Cisco HA では、QoS ポリシングが次のようにイネーブルにされます。

ステップ 1　ユーザが、QoS インフラストラクチャで認識される APN 仮想インターフェイスにサービス ポリシーをアタッチします。これには拡張 **ip mobile realm** コマンドを使用すると、グループ化した NAI ベース ユーザに対し、ポリシングを一括して実行できるので便利です（レルム単位の実行）。この場合、ユーザ設定したポリシーマップを APN インターフェイスに適用でき、HA を通過するモバイル IP データ パケットの分類が容易になります。また、MQC では、入力方向（ダウンストリーム）と出力方向（アップストリーム）のどちらに対してもピーク レートを指定できます。

ステップ 2　MQC classmap/policymap コマンドを使用する際に "match flow pdp" フィルタを設定して、フロー（バインディング）ごとにパケットが分類されるようにし、フローの識別時にポリシング パラメータを送信するように HA に通知します。マッチ タイプがフロー **pdp** であるクラスマップに対しては、Police rate pdp peak-rate pdp コマンド、バースト値、および必要となるさまざまなアクションがポリシーマップに指定されます。アップストリームおよびダウンストリームのピーク レート値は、**ip mobile realm** コマンドを使用して設定します。

最初の Registration Request（RRQ; 登録要求）が処理され、バインディングが HA に登録されると、バインディングに対応する最初のパケットが CEF パスで代行受信され、このパケットにポリシング ルールが適用されます。この動作を基に、設定したピーク レート、適合バースト値、および超過バースト値に従い、以降のパケットにもポリシング アクションが実行されます。MQC QoS はユーザのポリシング要求が設定値を超過したかどうかをモニタリングし、これに応じてパケットを許可またはドロップします。すべてのアクティブ バインディングに対してそれぞれ QoS フローが存在し、それぞれの実行時の状態が HA に保存されます。

制約事項

次の制約事項に注意してください。

- 有効となるのはシングルレート ポリシングだけです。帯域予約はできないため、ポリシングはユーザの設定した最大帯域幅レートに基づいて実行されます。
- サービス ポリシーのアタッチメントおよびポリシング アクションは、いったん設定した後は変更できません。ポリシーまたは関連パラメータを変更する場合は、既存のサービス ポリシーを削除してから、代わりに新たなサービス ポリシーを設定する必要があります。
- ポリシングは、NAI ユーザ名を使用して登録したユーザだけに適用できます。
- MQC コマンド セットにおいて、クラスに対して **match flow pdp** を設定した場合は、police コマンドだけを設定できます。他のアクションは使用できません。
- トラフィック シェーピング機能は実装されていません。

HA QoS の設定

HA QoS 機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Router(config)**ip mobile realm** [*nai* | *realm*] [**service-policy** {**input** *policy-name* [**peak-rate** *rate*] |**output** *policy-name* [**peak-rate** *rate*]}]	NAI またはレルム単位で、ポリシーに関連付けられた 1 つ以上のユーザ バインディングに対し、ポリシーおよび対応レートを設定します。これは、アップストリームおよびダウンストリーム両方のトラフィックに対して設定できます。
ステップ 2	Router(conf t)# **class-map** *class-name*	クラスマップ名を指定し、グローバル クラスマップ モードを有効にします。
ステップ 3	Router(config-cmap)#**match flow pdp**	MN ユーザのクラスに属する各バインディングに対し、指定のレートで HA パケットを分類します。
ステップ 4	Router(config-pmap-c)# **police rate pdp** [**burst** *bytes*] [**peak-rate pdp** [**peak-burst** *bytes*]] **conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]	バインディング フローに対し、指定のポリシング アクションを起動します。**peak-rate pdp** キーワードを指定すると、各バインディング フローに指定したレートに基づいてポリシングが行われるようになります。

上記の設定内容には、次の制限があります。

- 入力および出力の両方のポリシーを設定している場合は、どちらか 1 つを削除できません。
- レルムに対して既存のサービス ポリシーを変更するには、設定をいったん解除してから、新たに設定し直す必要があります。
- 出力ポリシーを設定してから入力ポリシーを設定できません。

QoS の設定例

次に、Cisco Mobile Wireless HA に対する QoS 機能の設定例を示します。

```
class-map match-all class-mip
 match flow pdp

policy-map policy-mip-flow
 class class-mip
   police rate pdp burst 1400  peak-rate pdp peak-burst 1700
     conform-action transmit
     exceed-action drop
     violate-action drop

ip mobile realm @cisco.com service-policy input policy-mip-flow peak-rate 9000 output
policy-mip-flow peak-rate 8000
```

設定の確認

HA QoS 機能に関するさまざまな統計情報を表示するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Router#**show ip mobile binding police nai** *@example.com*	QoS ポリシングがイネーブルになっている場合、個々のバインディングに対する統計情報を表示します。これは、既存の **show ip mobile binding** コマンドの拡張機能として提供されています。表示されるのは、ポリシング レート（bps 単位）、レートに適合、超過、または違反したパケットの数などの詳細情報です。
ステップ 2	Router# **show policy-map apn realm** *string*	レルム単位の合計統計値を表示します。

show コマンドの例

次に、QoS バインディング統計値および合計統計値の出力例を示します。

```
Router#sh ip mob bind police nai mip-qos-user1@cisco.com:
Mobility Binding List:
Total number of QoS bindings is 1
mip-qos-user1@cisco.com:
Downlink Policing

      police:
          rate 8000 , bc 1400 bytes
         peak-rate 9000, be 1700 bytes
        conformed 3000 packets, 312000 bytes; actions:
          drop
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
Uplink Policing

      police:
          rate 8000 , bc 1400 bytes
         peak-rate 8000, be 1700 bytes
        conformed 6000 packets, 516000 bytes; actions:
          drop
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
Router#

Router#sh policy-map apn realm cisco.com
 APN 566497294

  Service-policy input: toMN

    Class-map: HA4.0 (match-all)
      1 packets, 118 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: flow pdp
      police:
          rate pdp, bc 1400 bytes
         peak-rate pdp, be 1700 bytes
```

```
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any

  Service-policy output: fromMN

    Class-map: HA4.0 (match-all)
      1 packets, 100 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: flow pdp
      police:
          rate pdp, bc 1400 bytes
         peak-rate pdp, be 1700 bytes
        conformed 1 packets, 100 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
Router#
```

CHAPTER 15

ユーザ トラフィックのモニタリング

ここでは、ホットライン機能を使用してアップストリームおよびダウンストリームのユーザ トラフィックをモニタリングする方法、および Cisco Mobile Wireless Home Agent でこの機能を設定する方法について詳しく説明します。

この章は、次の内容で構成されています。

ホットライニング

ワイヤレス オペレータはホットライニングを使用することで、パケット データ サービスに不正アクセスしようとするユーザに関する問題に、効果的に対処できます。ユーザのパケット データ サービスの使用許可が失効してしまったといった問題が生じた場合、この機能を使用するワイヤレス オペレータは、ユーザにホットラインを適用します。問題が無事に解決すると、ホットライン条件が解除された時点で、ユーザのパケット データ サービスは通常モードに戻ります。ユーザにホットラインを適用すると、このユーザに対するパケット データ サービスはホットライン アプリケーションにリダイレクトされます。このアプリケーションにより、ホットラインが適用された理由がユーザに通知され（可能な場合）、ホットラインの理由となった問題を解決するための手段が提示されます。この間、通常のパケット データ サービスへのアクセスはブロックされます。

Home Agent（HA）では、3gpp2/wimax 環境サブスクライバ用の新規セッションおよびアクティブ セッション ホットラインを使用することにより、Filter、IPRedirection、または HTTPRedirection によるプロファイル ベースのホットライニングがサポートされます。

その他のホットライニング機能

Home Agent では、HA Challenge Handshake Authentication Protocol（CHAP）中にホットライニング ポリシーがダウンロードされた場合に限り、ホットライニング ポリシーが適用されます。ユーザからリバース トンネルが要求されていない場合に、このユーザに対してホットライニング ポリシーがダウンロードされると、Home Agent は Registration Request（RRQ; 登録要求）をドロップします。

（注）　この機能に対しては、Management Information Base（MIB; 管理情報ベース）サポートは予定されていません。

ホットライニング機能を使用すると、アクティブ セッション、新規セッションの 2 つのシナリオにおいて、アップストリームのユーザ トラフィックをモニタできます。特定のユーザに対してホットライニングがアクティブになると、このモバイル端末からのアップストリーム IP パケットは、この特定のレルムに設定されたリダイレクト サーバにリダイレクトされます。リダイレクションは、IP パケットの宛先アドレスをリダイレクト サーバのアドレスに変更することで行われます。Home AAA（HAAA; ホーム AAA）からの Change of Authorization（CoA）メッセージで唯一サポートされている必須アトリビュートは、Home Agent 上の特定のユーザを識別するための User-Name アトリビュートです。オプションとして、CoA メッセージに IP アドレスも含めて送信することで、特定ユーザに対する特定のバインディングを指定できます。

3gpp2 用の新規セッションのホットライニング

ここでは、新規セッションに対してホットラインを適用する場合のプロセスを説明します。

ステップ 1　HAAA はホットライン アプリケーションから、ユーザのパケット データ サービスに対するホットラインの適用を示すシグナルを受信します。

ステップ 2　HAAA はこの情報を、自身のユーザ プロファイル ストアに記録します。ユーザがアクティブでない場合は、HAAA はユーザがパケット データ サービスを開始するまで待機し、サービスが開始されるとただちにホットラインを適用します。また、ホットライン アプリケーションがユーザのホットライン ステータスを通常に戻すこともあります。この場合、HAAA はユーザのプロファイルを更新し、その内容を保存します。

ステップ 3　ホットライン適用対象となるユーザがパケット データ セッションを開始すると、HAAA は HA のホットライン機能を示す Remote Authentication Dial-In User Service（RADIUS）アクセス要求を受信します。

ステップ 4　HAAA はローカル ポリシー、および受信した hotline capability パラメータを使用して、ホットライニング Vendor-Specific Attribute（VSA; ベンダー固有のアトリビュート）を受信した HA を判断します。HAAA は RADIUS Access-Accept メッセージ内にホットライニング VSA を含めて送信することで、ホットライニング デバイスに対してユーザのホットライン ステータスを通知します。HAAA は、hot-line accounting indication VSA を RADIUS Access-Accept メッセージ内に含める場合もあります。

ステップ 5　HA でアカウンティングがイネーブルにされている場合は、HA は RADIUS Accounting-Request (start) パケットを生成し、RADIUS Access-Accept メッセージ内で hot-line accounting indication VSA を受信している場合は、これをパケットに含めます。HA が RADIUS Access-Accept パケットで受信したホットライニング VSA を処理できない場合は、HA は RADIUS Access-Accept を RADIUS Access-Reject パケットと見なし、セッションの確立を終了します。

ステップ 6　ホットライン セッションが開始されると、トラフィックはブロックされるか、またはホットライン アプリケーションに転送されます。

3gpp2 用のアクティブ セッションのホットライニング

アクティブ セッションのホットライニングで発生するイベントは、次のとおりです。

ステップ 1　現在ユーザは、ホットラインが適用されていないパケット データ セッションに携わっています。

ステップ 2　HAAA は、パケット データ セッションをすでに開始しているユーザに対してホットライン アプリケーションからホットライン シグナルを受信すると、アクティブ セッション ホットライニング手順を開始します。

ステップ 3　HAAA はユーザのホットライン状態を、ユーザのプロファイル内に保存します。

ステップ 4　HAAA はローカル ポリシー、および受信した hotline capability パラメータを使用して、ホットライニング VSA を受信した HA を判断します。HAAA は RADIUS Change of Authorization（COA）メッセージ内にホットライニング VSA または RADIUS filter-id (11) アトリビュートを含めて送信することで、HA に対してユーザのホットライン ステータスを通知します。HAAA は、hot-line accounting indication VSA を 3gpp2 環境ユーザ用の RADIUS CoA メッセージ内に含める場合もあります。

ステップ 5　HA が要求を処理できる場合は、COA Acknowledgment（ACK; 確認応答）パケットで応答します。HA がホットライニング要求を処理できない場合は、COA Negative Acknowledgment（NAK; 否定応答）メッセージで応答します。受信した COA NAK メッセージに、管理者による禁止（Administratively Prohibited (501)）を示す error-cause (101) が含まれる場合は、HAAA はローカル ポリシーに基づき、ホットライニング シグナルの HA への送信を再試行するか、HA に RADIUS disconnect-request メッセージを送信するか、または別のデバイスに対してセッションのドロップを指示します。

ステップ 6　また、アカウンティング パケットを生成可能な HA は（アカウンティングがイネーブルにされている場合）、RADIUS accounting-request (stop) メッセージを生成して、現在のアカウンティング セッションを終了します。3gpp2 環境のユーザに対してのみ、リリース インジケータ（F13）は 14（ホットライン ステータスの変更）に設定されます。

ステップ 7　また、アカウンティング パケットを生成可能な HA は、COA パケットで受信した hot-line accounting indication VSA を含む RADIUS accounting-request (start) メッセージを生成します。

ステップ 8　これに対し、ホットライニング デバイスは、COA パケットに指定されたホットライニング プロファイルをただちに実行します。

ステップ 9　ユーザにホットラインが適用されると、ホットライン アプリケーションは必要に応じてユーザにホットライン状態を通知し、ホットラインが適用された理由となる問題を修正するための処理を支援します。それでもなお、処理結果がホットライン アプリケーションの規定に適合しない場合は、ユーザのホットライン状態が維持されるか、またはユーザ セッションが終了されます。問題が正しく修正された場合は、ユーザのセッションは通常モードに戻されます。

ステップ 10　ホットライン アプリケーションは、通常状態への復帰を HAAA に通知します。ホットライン アプリケーションとユーザとの相互動作については、このマニュアルの範囲外です。

ステップ 11　HAAA はユーザのプロファイルを更新します。

ステップ 12　セッションがアクティブの場合は、HAAA は現在ホットライン ルールを適用している HA に対し、COA パケットを送信します。これは、セッションのホットライン状態を最初に設定したデバイスと同じであるとは限りません（ハンドオフが行われている可能性があります）。ステップ 9 で説明した受信通知が、ホットライン アプリケーションからのセッションの終了を示すものであれば、HAAA はユーザの終了ステータスをユーザのポリシー ストアに記録します。この時点でセッションがまだアクティブである場合は、HAAA は適切なデバイスに対して RADIUS disconnect-request メッセージを送信します。これは、ホットライン ルールを適用していないデバイスとなる可能性もあります。RADIUS disconnect-request メッセージを受信したデバイスは、セッションを終了します。アカウンティング メッセージを生成できるデバイスの場合は、リリース インジケータ（F13）を 6（リソース管理による終了）に設定した RADIUS accounting-request (stop) メッセージを生成します。

ステップ 13　ユーザを通常モードに戻すシグナルを受信した場合、この要求を処理できない HA は、COA NAK パケットで応答します。HAAA は COA NAK を受信すると、状況に応じて、RADIUS disconnect-request メッセージを送信してユーザのセッションを終了します。または、ホットライニング デバイス、またはセッションの終了を処理できる別のデバイスに対し、RADIUS disconnect-request メッセージを送信します。一方、ユーザを通常の状態に戻すことができるホットライニング デバイスの場合は、COA ACK パケットを送信します。

ステップ 14　アカウンティング メッセージを生成可能なホットライニング デバイスは、ホットライニング セッションの終了を示す RADIUS accounting-request (stop) メッセージを生成し、COA メッセージ内で受信した hot-line-accounting indication VSA を含めます。リリース インジケータ（F13）は 14（ホットライン ステータスの変更）に設定されます。

ステップ 15　RADIUS accounting-request (stop) メッセージの後には、通常のパケット データ セッションの開始を示す RADIUS accounting-request (start) メッセージが生成されます。

ステップ 16　この時点で、ユーザのセッションは通常モードに戻されます。

ホットラインの冗長性サポート

HA Release 5.0 では、冗長フレームワーク / インフラストラクチャが Component Cluster Manager（CCM）および Redundancy Framework Inter-device (RF-Interdev) の下に配置されるように修正されています。

HA Release 5.2 では、RADIUS アトリビュート 11 を使用する Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）サーバからホットライン プロファイルをダウンロードすることによってホットラインをサポートします。HA 5.2 は、新規セッションおよびアクティブ セッションの両方のホットラインをサポートします。HA 5.1 もまた、Change of Authorization (COA) メッセージを使用するホットラインをサポートします。

さらに、HA Release 5.2 は、上記のすべてに対して冗長性をサポートします。

次のバインディングのホットライン情報は、スタンバイに同期化されます。

- Hotlining Status：バインディングの現在のステータス（アクティブまたは通常）を指定。
- ホットライン プロファイル：いずれかの RADIUS アトリビュート 11 を使用する AAA からダウンロードしたホットライン プロファイルを指定。
- Session-Timeout：ホットラインのユーザに対して提供される最大秒数を指定。

さらに、次の情報も同期化されます。

- User-Name：ユーザの Network Access Identifier（NAI; ネットワーク アクセス識別子）。
- Bind address：バインディングの Home Address（HoA; ホーム アドレス）。
- Accounting-Session-Id：HA が生成するアカウンティング セッション ID。ユーザがアクティブから通常（または通常からアクティブ）に状態を変更するたびに、新規のアカウンティング セッション ID が作成されます。

フェールオーバーが発生し、スタンバイがアクティブになると、ユーザに対してホットライン プロファイルが適用されます。スタンバイでは、フェールオーバー前に同期化されたものと同じ Accounting-Session-Id を使用します。

制約事項および制限事項

この機能には、次の制約事項および制限事項が適用されます。

- ホットラインのカウンタと一致する Access Control List（ACL; アクセス コントロール リスト）ルールは、スタンバイに同期化されません。
- **show ip mobile traffic** コマンドの "Change of Authorization" カウンタはスタンバイと同期化されません。

ホットライン対応 HA の要件

ここでは、登録、再登録、および COA 中に、サブスクライバの Mobile IP（MIP; モバイル IP）フローに対するホットライン情報を処理するために適用可能な HA の各要件について説明します。

1. HA は、新規セッションおよびアクティブ セッションの両方のホットラインをサポートする必要があります。
2. ホットラインの実行により、パケット データ セッションの確立が干渉を受けないようにしてください。HA がパケット データ セッションの完了、および MIP シグナリングの再登録を中断させないようにしてください。
3. HA は MIP サブスクライバに対するホットラインをサポートする機能を示すため、RADIUS アクセス要求メッセージに Hot-line Capability VSA を含める必要があります。
4. HA は次を含む RADIUS Access-Accept メッセージまたは COA メッセージを受信した場合、RADIUS Access-Accept メッセージを Access-Reject メッセージとして扱うか、または Error-Cause (101) によって "Administratively Prohibited" (501) を示す COA NAK メッセージを使用して応答する必要があります。
   a. デコードできない RADIUS Filter-Id(11) アトリビュート。
5. RADIUS Filter-Id(11) アトリビュートを含む RADIUS Access-Accept メッセージを受信した HA は、RADIUS Filter-Id(11) アトリビュートによって指定されたルールと一致する、ローカルにプロビジョニングされたホットライン ルールをただちに適用する必要があります。
6. RADIUS Filter-Id(11) アトリビュートを含む COA メッセージを受信した HA は、RADIUS Filter-Id(11) アトリビュートによって指定されたプロファイルと一致するホットライン ルールを特定します。この処理に成功した場合、HA は HAAA に COA ACK メッセージで応答します。HA は以前に指定された RADIUS Filter-Id(11) アトリビュートをすべて削除し、新たに受信した RADIUS Filter-Id(11) アトリビュートに関連付けられたルールの適用を開始します。HA は、アカウンティング メッセージ accounting stop および accounting start を送信します。新たに受信した RADIUS Filter-Id(11) アトリビュートが該当のルールに一致しない場合は、HA は Error-Cause (101) が "Administratively Prohibited" (501) を示す COA NAK を送信します。この場合は、ホットライン状態、および既存のすべてのルールは変更されません。
7. Session-Timeout (27) アトリビュートを受信した場合は、HA はセッションに規定されたタイムアウト時間（秒）が経過した後、セッションを終了します。RADIUS アカウンティングに対応している HA の場合は、RADIUS Accounting-Request (Stop) メッセージを送信します。受信した RADIUS Access-Accept または COA メッセージに Hot-Lining Accounting Indication VSA が含まれていた場合は、この VSA もメッセージに含めます。
8. HA は、プロファイルの下に設定されているルールに対して、HTTP Pass、HTTP Redirection、IPRedirection、IPFilter Rules の順に優先順位を与えます。

ホットライニング時間の制限

ホットラインを適用したセッションであっても、高価なネットワーク リソースが消費される可能性があります。このため、AAA ではセッションにホットラインを適用する時間を制限することができます。これには、COA または Access-Accept に Session-Timeout アトリビュートを含めて送信します。オペレータは、次の 2 つの方法を使用できます。

1 つには、Disconnect Message を送信することで、セッション（ホットラインを適用 / 非適用）をただちに終了する方法です。Disconnect Message は、HA を対象とする必要はありません。

もう 1 つの方法は、Home RADIUS サーバがホットライン インジケータを HA に送信する際、Session-Timeout (27) アトリビュートを含めるように Home RADIUS サーバを設定する方法です。Session-Timeout には、ユーザにセッションの続行を許可する時間を 1 ～（232 - 1）秒の範囲で指定します。Session-Timeout に指定した時間が経過すると、パケット データ セッションは終了します。この機能は、プロファイル ベースおよびルール ベースの両方のホットラインでサポートされます。

ホットラインを適用していないユーザのための IP リダイレクト

この機能を使用すると、IP リダイレクト ルールをレルム単位で設定し、指定した IP アドレスにアップストリーム パケットをリダイレクトできます。これにより、非ホットライン プロファイルが作成され、レルムに関連付けられます。非ホットライン プロファイルの下には、IP リダイレクト ルールが設定されます。

この設定により、HA は、パケットの内容と設定された ACL 値をレイヤ 4 まで照合し、destination-ip と destination-port を修正することによって、設定された IP アドレスとポートへのパケットのリダイレクトを試みます。profile の下に値が設定されている場合、destination-port は修正されます。

非ホットライン ユーザに対してホットラインをイネーブルにするには、次の作業を実行します。

コマンド	目的
router(config)# **ip mobile home-agent non-hotline profile** *profile-id* router(non-hotline-rules)# **redirect ip access-group** {*100-199* | *2000-2699* | *WORD*} **in redirect-ip** *redirect-ip-address* [**redirect-port** *redirect-port*]	非ホットライン ユーザに対してホットライン機能をイネーブルにします。

（注） この機能は、アップストリーム（Mobile Node（MN; モバイル ノード）からネットワーク）トラフィックに対してのみ適用できます。

（注） リダイレクトされたトラフィックの場合、この機能の一部として Network Address Translation（NAT; ネットワーク アドレス変換）機能がサポートされている必要があります。この特別な機能は、ホットラインを適用したユーザとホットラインを適用していないユーザのトラフィックの両方に共通です。

（注） Home Agent MIB は、ホットライン情報によって更新されません。

ホットライニングの設定

ホットラインを設定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

コマンド	目的

Router(config)# [no] **ip mobile home-agent hotline** ?
  profile defines hotline profiles
Router(config)# [no] **ip mobile home-agent hotline profile** *word*
Router(hotline-rules)#
 	
Router(hotline-rules)#?
  exit Exit from hotline profile configuration mode
  firewall Defines Firewall filter Rules
  no Negate the hotline rules
  redirect Redirection Rules
	各ユーザ（MN）に対し、プロファイル ベースまたはルール ベースのホットラインを設定および指定します。
	profile キーワードは、一式のルールを設定するためのサブコンフィギュレーション モードを指定します。

Router(hotline-rules)# [no] **Redirect ip access-group** {*acl-no* | *word*} {**in**|**out**} {**redirect** *ip-addr* [**port**]}	IP が、リダイレクトされるプロファイルベースの設定であることを指定します。設定する ACL は、拡張 ACL である必要があります。ACL 番号の範囲は 100 ～ 199 および 2000 ～ 2699 です。
Router(hotline-rules)# [no] **Redirect http access-group** {*acl-no* | *word*} {**redir-url** *url*}	HTTP が、リダイレクトされるプロファイル ベースの設定であることを指定します。設定する ACL は、拡張 ACL である必要があります。ACL 番号の範囲は 100 ～ 199 および 2000 ～ 2699 です。
Router(hotline-rules)#[no] **firewall ip access-group** {*acl-no* | *word*} {**in**|**out**}	IP ファイアウォールがプロファイルベースの設定であることを指定します。設定する ACL は、拡張 ACL である必要があります。ACL 番号の範囲は 100 ～ 199 および 2000 ～ 2699 です。
router(config)# **ip mobile home-agent non-hotline profile** *profile-id* router(non-hotline-rules)# **redirect ip access-group** {*100-199* | *2000-2699* | *WORD*} **in redirect-ip** *redirect-ip-address* [**redirect-port** *redirect-port*]	非ホットライン ユーザに対してホットライン機能をイネーブルにします。

コマンド	目的

Router(config)#[no] **ip mobile realm** {*realm* | *nai*} **hotline** ?
  capability Hotlining Capability of the mobile hosts
  redirect Redirect ip address for upstream traffic
	モバイル ホストのホットライン機能を設定します。

Router(config)#[no] **ip mobile realm** { *realm* | *nai*} **hotline capability** ?
  all Support all Hotline Capabilities
  httpredir HTTPRedir Rule-based Hot-Lining
  ipfilter IPFilter Rule-based Hot-Lining
  ipredir IPRedir Rule-based Hot-Lining
  profile Profile-based Hot-Lining
	プロファイル ベースまたはルールベースのホットライン、またはすべての形式のホットラインを設定します。*word* は **nai** | **realm** として指定し、*@cisco.com*|*username@cisco.com* というフォーマットを使用する必要があります。それ以外の形式でこのコマンドを実行すると、エラー メッセージが表示されます。
	最低限 1 つの形式のホットラインを選択する必要があります。ユーザに対してルールベースのホットラインを有効にするデフォルト ルールはありません。このコマンドに何も設定しないと、ユーザに対するルールベースのホットラインが消去されます。この設定の値はフラグとして指定します。
	1 各フラグ値の意味は次のとおりです。

Router(config)# **ip mobile realm** *realm* **hotline capability ipredir**	ユーザに対し、IP リダイレクション ルールを使用したプロファイルベースのホットラインを設定します。realm には NAI またはレルムを指定します。
Router(config)#**ip mobile realm** *realm* **hotline capability httpredir**	ユーザに対し、HTTP リダイレクション ルールを使用したプロファイルベースのホットラインを設定します。realm には NAI またはレルムを指定します。
Router(config)# **ip mobile realm** *realm* **hotline capability rule-based** *flag*	ユーザに対し、ルールベースのホットラインを設定します。realm には NAI またはレルムを指定します。
router# **clear ip mobile traffic**	トラフィックに対し、IP モバイル関連のカウンタをすべて消去し、ホットライン関連のカウンタも消去します。

1 各フラグ値の意味は次のとおりです。

0x00000001 プロファイルベースのホットラインがサポートされます（RADIUS Filter-Id アトリビュートを使用）。

0x00000002 フィルタ ルールを使用したルールベースのホットラインがサポートされます。

0x00000004 HTTP リダイレクション ルールを使用したルールベースのホットラインがサポートされます。

0x00000008 IP リダイレクション ルールを使用したルールベースのホットラインがサポートされます。

ダイナミック ACL の設定に関する詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080430e5b.html

設定の確認

HA のホットライニングに関するさまざまな情報を表示するには、次の作業を実行します。

コマンド	目的
Router# **show ip mobile hotline**[**profile** *profile-id*] | **summary** | **users** [**nai** *id*]	ホットラインを適用した特定のユーザ、またはホットラインの対象となる全ユーザに対する情報を表示します。
Router# **show ip mobile hotline users** ? nai MN identified by NAI	ホットラインを適用した特定のユーザ、またはホットラインの対象となる全ユーザに対する情報を表示します。

Router# **show ip mobile hotline profile** ?
  WORD Profile-Id
  Output modifiers
	全ホットライン プロファイルのリスト、または特定のホットライン プロファイルを表示します。

router# **show ip mob hot summary**	ホットラインを適用したサブスクライバの現在の統計情報を一覧表示します。このコマンドを実行すると、ホットラインの対象となる MIP セッションが 1 つ以上存在する場合に各カウンタが表示されます。
router# **show ip mobile traffic** [**since**]	ホットライン セッション関連の各カウンタを組み合わせて表示します（ホットラインの対象となるセッション数、ホットラインの対象となるアクティブ セッション数、ホットラインの対象となる新規セッション数の累積カウンタ）。

次に、ホットライン ユーザ情報の出力例を示します。

```
HA#show ip mobile hotline users nai mip1@cisco.com
blrmip1@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com

HA#show ip mobile hot-lined users
Hotline Binding List:
blrmip1@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com

blrmip2@cisco.com (Bindings 1):
  Rule Based HotLining (Rules 1)
    RuleType HTTPPRedir, Dynamic ACL Number 10
    Direction - in
    Redirect url - www.cisco.com
```

次に、ホットライン プロファイル情報の出力例を示します。

```
HA#Show ip mobile hotline profile cisco
Hotline Profile List:
 Profile: cisco (Rules 1)
    RuleType HTTPRedir, Extended ACL Number 100
    Direction - in
    Redirected Url - cisco.com

HA#show ip mobile hotline profile
```

```
Hotline Profile List:
Total 2
 Profile: cisco (Rules 1)
    RuleType HTTPRedir, Extended ACL Number 100
    Direction - in
    Redirected Url - cisco.com

 Profile: ht-prof1 (Rules 3)
    RuleType IPRedir, Extended ACL Name ht-acl1
    Direction - in
    Redirected IPAddr 16.1.1.102

    RuleType IPRedir, Extended ACL Number 100
    Direction - in
    Redirected IPAddr 1.1.1.1

    RuleType IPFilter, Extended ACL Name cisco
    Direction - out
    HA#
```

次に、ホットラインに関する統計情報の出力例を示します。

```
HA#sh ip mob hot summary
HomeAgent Hotlining Summary:
    Number of Sessions Hotlined 2
    Number of Profile-Based Hotlined 0
    Number of Rule-Based Hotlined 2
HA#
```

次に、ホットライン セッション カウンタの出力例を示します。

```
HA# show ip mobile traffic
IP Mobility traffic:
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register requests rcvd 1351, denied 0, ignored 0, dropped 0, replied 1
    Register requests accepted 1351, No simultaneous bindings 0
    Register requests rcvd initial 149, re-register 1132, de-register 70
    Register requests accepted initial 149, re-register 113, de-register 7
    Register requests replied 1281, de-register 70
    Register requests denied initial 0, 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 0, 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 14, sent 0 total 0 fail 1351
    Binding Update acks received 0 sent 14
    Binding info requests received 0, sent 1 total 2 fail 1
    Binding info reply received 1 drop 0, sent 0 total 0 fail 0
    Binding info reply acks received 0 drop 0, sent 1
    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 0, 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 SW IDBs: 1 no resource: 0 deleted: 0


Change of Authorization:
  Request rcvd 0, accepted 0
  Request Errors:
    Unsupported Attribute 0, Missing Attribute 0
    Invalid Request 0, NAS 0
    Session Cxt Not Found 0, Session Cxt Not Removable 0
    Unsupported Service 0
Dynamic DNS Update (IP Reachability):
Number of DDNS Update Add request sent 0
  Number of DDNS Update Delete request sent 0
Home Agent Hotlining:
    Number of Hotline Sessions 6
    Number of Active-Session Hotlined 0
    Number of New-Session Hotlined 6
    Number of Active-Sessions Reconciled 0
    Number of New-Sessions Reconciled 0
```

Worldwide Interoperability for Microwave Access（WiMAX）ホットラインの CoA

HA Release 5.2 は、Worldwide Interoperability for Microwave Access（WiMAX）サブスクライバのホットラインをサポートします。ここでは、次のシナリオにおける詳細なコール フローについて説明します。

- この機能は、Access-Accept または COA の一部として AAA から 1 つ以上の filter-id（11）アトリビュートをダウンロードすることにより、Wimax の新規セッションおよびアクティブ セッションのホットラインをサポートします。
- ダウンロードされた filter-id アトリビュートは、HA 上でローカルに設定された profile-id のいずれかにマッピングされます。この profile-id は、1 つ以上の IP リダイレクション ルールおよびファイアウォール（フィルタ）ルールで構成されます。
- HA は、Wimax-capability 内のホットライン機能を sub-TLV として AAA サーバに送信します。
- HA は、ホットライン セッションを維持するために標準の RADIUS アトリビュートである Session-Timeout (27) をサポートします。このアプローチは、HA 4.0 機能と下位互換性があります。ユーザ セッションは、hotline-session-timer で指定された期間中、ホットラインの対象となり続けるように制限されています。
- HA は、サブスクライバのホットライン ステータスが修正されるたびに、セッションの Accounting Stop および Accounting Start を送信します。HA は、ホットライン ステータスが修正されるまでは、以前に生成され、利用された Accounting-Session-Id を使用して Accounting Stop を送信します。HA は、ホットライン ステータスが修正されると、新しい Accounting-Session-Id を生成して Accounting Start を送信します。
- ホットラインの対象となるセッションのリコンシリエーションは、再登録中の Access-Accept または CoA において filter- id（11）を "Hot-Line Normal" としてダウンロードすることによって行います。

WiMAX ホットラインのコール フロー

次に、WiMAX バインディングの新規セッション ホットラインおよびアクティブ セッション ホットラインのコール フローを示します。

WiMAX バインディングの新規セッション ホットライン

1. HA は、アクセス要求メッセージ内の設定値に含まれる Wimax capability type を AAA サーバに送信する必要があります。このために必要な設定は、**ip mobile realm** *realm* ***hotline capability*** { *ipredir ipfilter httpredir profile all* } です。
2. 新規セッション ホットライン中に、HA は、HA 上でローカルに設定された profile-id 値とともに 1 つまたは複数の filter-id（11）を受け取ることができます。プロファイルは、Command-Line Interface（CLI; コマンドライン インターフェイス）で **ip mobile home-agent hotline profile** *profile-id* を使用して、HA 上でローカルに設定できます。
3. HA が Access-Accept メッセージの一部として "session-timeout" （27）を受け取ると、ユーザは、このアトリビュートで指定された hotline-session-timer 期間中、ホットライン状態にとどまることができます。その後、ユーザは切断されます。
4. HA は、ホットライン ステータスが修正されるたびに、Accounting Stop および Accounting Start を送信します。

WiMAX バインディングのアクティブ セッション ホットライン

1. アクティブ セッション ホットライン中に、HA は、**ip mobile home-agent hotline profile** *profile-id* コマンドを使用して、HA 上でローカルに設定された CoA メッセージに含まれる profile-id 値とともに 1 つまたは複数の filter-id（11）を受け取ります。
2. HA が Access-Accept メッセージの一部として "session-timeout" （27）をダウンロードすると、ユーザは、hotline-session-timer 期間中のみ、ホットライン セッションにとどまることができます。
3. HA は、ホットライン ステータスが修正されるたびに、Accounting Stop および Accounting Start を送信します。

WiMAX ホットライン セッションのリコンシリエーション

「リコンシリエーション」という用語は、ホットラインを適用したユーザがいつ通常の状態に戻るのかを表します。これは、ダウンロードされたプロファイルをユーザに適用できなくなることを意味します。

ホットラインの対象となるセッションのリコンシリエーションは、再登録中の Access-Accept 値または CoA において filter- id（11）を "Hot-Line Normal" としてダウンロードすることによって行います。

ホットライン セッションのリコンシリエーションが完了したら、HA は、以前に生成された Accounting-Session-Id に対する Accounting Stop を送信し､新しい Accounting-Session-Id を生成して Accounting-Start を開始します。

（注） HA 4.0 では、ホットライン セッションのリコンシリエーションを行うため、HA は "3GPP2 Hot-Line Normal" ストリングを待ちます。Release 5.1 では、ストリング値は "Hot-Line Normal" に修正されています。

制約事項

次のソフトウェア制限があります。

- Wimax Hotline-Accounting-Indicator は、この機能の一部としてサポートされません。
- WiMAX ホットラインについては、NWG R1.1 Stage 3 に定義されているように、ルールベースのホットライン ルールおよびプロファイル ID はサポートされません。

ホットライン リダイレクションと非ホットライン リダイレクションのネットワーク アドレス変換（NAT）

HA は、ホットラインを適用した（またはホットラインを適用していない）IP でリダイレクトされたユーザのデータ パケットの実際の宛先 IP アドレスとリダイレクト先の IP アドレスの間のマッピングを維持する必要があります。HA は、リダイレクト先のサーバから応答を受け取るたびに、応答パケットの送信元 IP アドレスを要求パケットの実際の宛先 IP アドレスに修正します。

HA は、実際の宛先 IP アドレス/ポートとリダイレクト IP アドレス/ポート間でマッピングを行うため、NAT 機能を使用してアップストリーム パス中の NAT 変換を維持します。

アップストリーム パケットのパケット処理

アップストリーム パケットの場合、HA は、トンネル ヘッダーの非カプセル化後にパケットを代行受信し、ホットライン/非ホットライン プロファイル情報に定義されているように、パケットの宛先 IP アドレスをリダイレクト先の IP アドレスに修正します。Transmission Control Protocol（TCP; 伝送制御プロトコル/）パケットまたは User Datagram Protocol（UDP; ユーザ データグラム プロトコル）パケットの場合、HA は宛先 IP アドレスを修正する以外に、ホットライン/非ホットライン プロファイル情報に含まれるリダイレクト ポート情報のアベイラビリティに基づいて、宛先ポート アドレスをリダイレクト ポート アドレスに修正します。修正した宛先 IP アドレスの隣接関係を調べる前に、HA は、パケットのリダイレクト先の IP アドレスと実際の宛先 IP アドレス間の NAT 変換を維持します。また、この変換には、**IP** アドレスのほかに、リダイレクト ポートと実際の宛先ポートの情報が含まれます。

ダウンストリーム パケットのパケット処理

ダウンストリーム パス内でリダイレクトされたパケットをリダイレクト サーバから応答を受け取ると、HA は、まず隣接関係を調べ、idb に基づいて Home Agent アプリケーションにパケットを渡します。HA は、パケット情報（たとえば、送信元 IP アドレス（TCP パケットまたは UDP パケットの場合）や Internet Control Message Protocol（ICMP）ID（ICMP パケットの場合））に基づいて、NAT 変換を調べます。HA は、対応する NAT 変換を取得し、パケットの送信元 IP アドレスを実際の宛先 IP アドレスに修正します。着信/発信 ACL、トンネル テンプレートと QOS、ホットライン/非ホットラインの各ルールを適用する前に、パケットに対して NAT 変換を実行する必要があります。その後、HA は、Home Agent アプリケーションを使用してパケットを検査し、そのパケットをカプセル化して、Foreign Agent（FA）の方へルーティングします。

この機能は、NAT サポートを使用して実行できます。ここで、HA は、リダイレクト IP アドレス、宛先 IP アドレスへのリダイレクト ポート、および宛先ポート間の NAT 変換を維持します。ポート情報は、UDP パケットおよび TCP パケットだけに適用できます。

NAT 変換の作成および維持

- リダイレクトされたパケットの NAT 変換を維持するために、インターフェイスを "nat inside" および "nat outside" とマークできません。
- NAT 変換は、ホットラインを適用した（またはホットラインを適用していない）IP でリダイレクトされたアップストリーム パケットに対してのみ作成できます。

NAT 変換のタイムアウト

さまざまな形式のパケットのタイムアウトは次のとおりです。

  - TCP パケットの FIN/RST タイムアウトは 30 秒です。
  - TCP パケットの SYN タイムアウトは 30 秒です。
  - TCP パケットのタイムアウトは 60 秒です。
  - UDP パケットのタイムアウトは 30 秒です。
  - ICMP パケットのタイムアウトは 5 秒です。

- ICMP パケットの NAT 変換は、変換済みパケットのリダイレクト先のサーバによって送信される応答に関係なく、NAT 変換の作成が 5 秒間実行されるとタイムアウトします。NAT 変換の有効期限内（5 秒）にリダイレクト サーバから応答パケットを受け取った場合、HA は、パケットの送信元 IP アドレスと実際の宛先 IP アドレスを使用してパケットを再変換します。
- TCP パケットで、HA 上の NAT 変換済みパケットに対して syn および ack が指定されていない場合、NAT 変換は 20 秒後にタイムアウトします。
- TCP パケットの場合、受信した FIN パケットまたは RST パケットに対する NAT 変換は 30 秒後にクリアされます。
- TCP パケットで、TCP 接続に対して TCP フラグ FIN または RST を含むパケットがない場合、NAT 変換のエントリは 60 秒後にクリアされます。
- UDP パケットで、対応する NAT エントリに対するパケットがない場合、NAT 変換のエントリは 30 秒後にクリアされます。

冗長性サポート

HA の冗長ピア間の NAT 変換を更新するための冗長性サポートは提供されません。冗長ピア間のスイッチオーバー後の遷移時間中に、現在アクティブな HA がリダイレクト先のサーバからの応答パケットの変換に失敗する場合があります。これは、宛先 IP アドレスとリダイレクト IP アドレスを含む実際に要求されたパケットに対する NAT エントリがないために発生します。

制約事項および制限事項

- Home Agent 上にアクティブ セッションが存在する場合は、この機能の CLI コマンドの設定を解除できません。
- 各 NAT 変換でタイマーが期限切れになった場合や、**clear ip nat translations** コマンドを使用して変換を削除した場合は、HA 上で NAT 変換がクリアされます。MIP セッションをクリアし、**ip mobile home-agent ipredirect nat-enable** コマンドの設定を解除しても、NAT 変換はクリアされません。
- CP では、**show running-config** を実行しても **ip nat translations** タイムアウト 値は示されません。しかし、TP 上ではデータ パスがサポートされるため、これらの値が示されます。これらのタイマー値には、"write memory" は必要ありません。これらの値は、**ip mobile home-agent ipredirect nat-enable** 機能を使用して設定されている場合に開始されます。
- HA は、各 NAT 変換を維持するために 360 バイトのメモリを必要とします。これは、次の理論計算に基づきます。
  - 1GB カードでは、各 TP は最大 50K の変換を作成できます。
  - 2GB カードでは、各 TP は最大 100K の変換を作成できます。
- HA は、NAT 変換を作成し、維持するためのディープ パケット インスペクションによる影響を受けます。つまり、ホットラインを適用してリダイレクトされたパケットを処理する際に、CPU 使用率が 15 ～ 20% 高くなります。

CHAPTER 16

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（HA）ソフトウェアの次の機能について、その概念と設定作業を詳しく説明します。

HA：レルム ケース インセンシティブ オプション

Network Access Identifiers（NAI; ネットワーク アクセス識別子）には、ユーザ名とレルムの 2 つのパラメータが含まれています。ユーザ名 @ レルムの形式で記述されます。HA 5.0 では、ユーザ名とレルムの両方ともがケース センシティブです。Foreign Agent（FA; 外部エージェント）から、NAI とともに Registration Request（RRQ; 登録要求）を受信した場合、HA は設定されたコマンドと照合する必要があります。HA 5.0 は、ユーザ名とレルムの両方にケース センシティブで一致するものを検索します。

レルム ケース インセンシティブ機能によって、ケース インセンシティブのレルム パラメータを使用して、RRQ NAI と設定されたコマンドを照合できます。ただし、その場合もユーザ名はケース センシティブと見なされます。

例 1：

ローカル設定

```
router(config)#ip mobile host nai @sprintpcs.com interface Null0
```

次の NAI （同一のレルムの異なるケース）は、上述の設定に一致します。

- mobile1@sprintpcs.com
- mobile2@sprintPCS.com
- mobile3@sprintPCS.COM
- mobile4@SPRINTPCS.COM
- mobile5@sPrInTpCs.cOm

例 2：

ローカル設定

```
router(config)#ip mobile host nai mobile6@sprintpcs.com interface Null0
```

次の NAI（同一のユーザ名の異なるケース）は、上述の設定 Command-Line Interface（CLI; コマンドライン インターフェイス）に一致しません。

- Mobile6@sprintpcs.com
- MoBiLe6@SPRINTPCS.COM
- MOBILE6@sprintpcs.com

レルム ケース インセンシティブ機能の設定

レルム ケース インセンシティブ機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile options`	モバイル IP オプションを入力するためのサブ コンフィギュレーション モードを開始します。
	`Router(config)# realm case-insensitive`	レルム ケース インセンシティブ機能をイネーブルにします。

次に、例を示します。

```
HA(config)#ip mobile options
HA(config-ipmobile-options)#realm case-insensitive
```

次は、コマンドを確認する方法の例です。

```
router#show ip mobile options
IP Mobility Options information:

Realm (Domain) match is case insenstive
```

制限事項および制約事項

この機能の制限事項および制約事項は次のとおりです。

- レルムがケース インセンシティブである同一の NAI を持つ RRQ は、同一の Mobile Node（MN; モバイル ノード）から送信されたと見なされます。たとえば、"user1@cisco.com" と "user1@CISCO.COM" は、同一の MN から送信されたと見なされます。
- アクティブなセッションが存在するときは、レルム ケース インセンシティブのイネーブルまたはディセーブルを変更できません。
- レルム ケース インセンシティブは、ユーザ名、**debug condition username** *nai* を使用する条件付きデバッグでは機能しません。あるユーザで条件付きデバッグをイネーブルにするには、ケース センシティブ NAI を使用する必要があります。

FA-HA 認証エクステンションの義務化

HA は、HA が Mobile IP（MIP; モバイル IP）RRQ 内で FA-HA エクステンションを要求するか、または、RRQ を拒否することを強制できる必要があります。この機能は、該当する **ip mobile secure foreign-agent** コマンドが設定されていない RRQ を拒否します。現時点で、RRQ を HA に送信し、FA-HA エクステンションを省略し、さらに、その FA IP アドレスに **ip mobile secure foreign-agent** コマンドが設定されていない場合、RRQ は受け入れられます。これはセキュリティ リスクであると考えられます。

現時点で、HA は、**FA Access-Type** コマンドのローカル設定に基づいた、RRQ または失効メッセージで Wimax FA から受信した Foreign-Home Authentication Extension（FHAE）エクステンションを許可します。HA は、Wimax FA の受信 MIP RRQ の FHAE を許可する次のコマンドをサポートします。

ip mobile home-agent foreign-agent *fa-address mask* **access-type wimax {enable-fhae | disable-fhae}**

上のコマンドは、3gpp2 アクセス タイプのために変更され、3gpp2 FA に対するキーワード **enable-fhae** および **disable-fhae** が追加されました。この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent foreign-agent {default	{fa-address mask}} access-type {wimax	3gpp2} [enable-fhae	disable-fhae]`	Wimax または 3gpp2 FA から RRQ または失効メッセージ内で受信される FHEA エクステンションを設定します。

次は、設定の詳細です。

- 同一のアドレスおよび option-less/enable-fhae から disable-fhae までの FA のマスク値に対するコマンド オプションが変更されるときは必ず、HA はすでに保存されたこれらの FA の FA-HA キーをクリアします。
- 設定されたアドレスおよびマスク値に対する Access-type オプションが変更される場合、HA はすでに保存された FA-HA キーを削除します。

HA 上の RRQ 処理

次のシナリオは、HA がこれらのシナリオの RRQ を処理する方法を示します。

シナリオ -1

次のコマンドでは、FA のアクセス タイプは、**enable-fhae** または **disable-fhae** を使用して設定されません。

```
ip mobile home-agent foreign-agent default access-type 3gpp2
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax.
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2.
```

次のコマンドを使用して、3gpp2 FA の FA-HA キー値を HA 上でローカルに設定します。

ip mobile secure foreign-agent *start-ip end-ip* spi …..

ケース 1：

3GPP2 FA、RRQ に FHAE がある。

a. FA-HA キーはローカルに設定されます。
RRP は、FHAE とともに正常に送信されます。

b. FA-HA キーはローカルに設定されません。
RRP はエラーコード 132 とともに（FHAE なしで）送信されます。

3GPP2 FA、RRQ に FHAE がない。

a. FA-HA キーはローカルに設定されます。
RRP はエラー コード 132 および FHAE とともに送信されます。

b. FA-HA キーはローカルに設定されません。
RRP は、FHAE なしで正常に送信されます。

ケース 2：

Wimax FA、RRQ に FHAE がある。

a. FA-HA キーは、HA-RK から作成済みであるか、または、HA-RK がすでに存在します。
アクセス要求は HA-RK のためには送信されないが、別の目的で送信される可能性があります。
RRP は FHAE とともに正常に送信されます。

b. FA-HA キーは存在せず、かつ、HA-RK は存在しません。アクセス要求が送信されます。
- HA-RK はダウンロードされます。
- RRP は FHAE とともに正常に送信されます。

c. HA-RK はダウンロードされません。

- RRQ はドロップされ、RRP は送信されません。

Wimax FA、RRQ に FHAE がない。

a. FA-HA キーは、HA-RK から作成済みです。または、この FA からの以前の RRQ に FHAE があります。
RRP は、エラー コード 132 および FHAE とともに送信されます。

b. FA-HA キーが存在しません。この FA からの RRQ に FHAE が 1 つもありません。
RRP は正常に送信されます。

シナリオ -2

FA のアクセス タイプは、次のコマンドで **enable-fhae** を使用して設定されます。

```
ip mobile home-agent foreign-agent default access-type 3gpp2 enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 enable-fhae
```

3gpp2 FA の FA-HA キーを HA 上でローカルに設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	3gpp2 の FA-HA キーを HA 上でローカルに設定します。

ケース 1：

3GPP2 FA、RRQ に FHAE がある。

a. FA-HA キーはローカルに設定されます。
RRP は、FHAE とともに正常に送信されます。

b. FA-HA キーはローカルに設定されません。
RRP はエラーコード 132 とともに（FHAE なしで）送信されます。

3GPP2 FA、RRQ に FHAE がない。

a. FA-HA キーはローカルに設定されます。
RRP には FHAE が追加され、エラー コード 132 とともに送信されます。

b. FA-HA キーはローカルに設定されません。
RRP はエラーコード 132 とともに、FHAE なしで送信されます。

ケース 2：

Wimax FA、RRQ に FHAE がある。

a. FA-HA キーは、HA-RK から作成済みであるか、または、HA-RK がすでに存在します。
アクセス要求は HA-RK のためには送信されないが、別の目的で送信される可能性があります。
RRP は FHAE とともに送信されます。

b. FA-HA キーは存在せず、かつ、HA-RK は存在しません。
アクセス要求が送信されます。

a.HA-RK はダウンロードされます。
RRP は FHAE とともに送信されます。

b.HA-RK はダウンロードされません。
RRQ はドロップされ、RRP は送信されません。

Wimax FA、RRQ に FHAE がない。

a. FA-HA キーは、HA-RK から作成済みです。この FA からの以前の RRQ に FHAE があります（この結果は、HA-RK ライフタイムの期限が切れたために FA-HA キーが削除される場合でも同様です。この FA に FHAE を 1 回使用するだけで、この条件を満たします）。
RRP は、FHAE なしで送信されます - （FA 認証失敗エラーコード）。

b. FA-HA キーが存在しません。
HA-RK がダウンロードされるかどうかに関係ありません。RRP は、エラー コード 132 とともに、FHAE なしで送信されます。

シナリオ -3

FA のアクセス タイプは、次のコマンドで **disable-fhae** を使用して設定されます。

```
ip mobile home-agent foreign-agent default access-type 3gpp2 disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 disable-fhae
```

FA-HA キー値を HA 上でローカルに設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile secure foreign-agent` *start-ip end-ip* spi	FA-HA キーを HA 上でローカルに設定します。

ケース 1：

3GPP2 FA、RRQ に FHAE がある。

a. FA-HA キーは、ローカルに設定されません。
アクセス要求は（FA-HA 入手のために）送信されません。
RRP は、エラー コード 132 とともに（FHAE なしで）送信されます。

3GPP2 FA、RRQ に FHAE がない。

a. FA-HA キーはローカルに設定されません。
RRP は、（FHAE なしで）正常に送信されます。

ケース 2 :

Wimax FA、RRQ に FHAE がある。

a. FA-HA キーは存在せず、かつ、HA-RK は存在しません。
アクセス要求が送信されます。
a.HA-RK はダウンロードされます。
b.RRP は FHAE なしで送信されます。

b. HA-RK はダウンロードされません。
RRP は FHAE なしで送信されます。

Wimax FA、RRQ に FHAE がない。

a. FA-HA キーが存在しません。
RRP は FHAE なしで送信されます。

失効メッセージの処理および開始

シナリオ -1

次のコマンドでは、FA のアクセス タイプは、**enable-fhae** または **disable-fhae** を使用して設定されません。

```
ip mobile home-agent foreign-agent default access-type 3gpp2
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax.
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2.
```

3gpp2 FA の FA-HA キー値を HA 上でローカルに設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	3gpp2 の FA-HA キーを HA 上でローカルに設定します。

- 3ggp2 FA の場合、HA は FHAE ベースの FA-HA キー設定を使用して（または使用せずに）Registration Revocation メッセージを認証することによって、Registration Revocation メッセージを FA に送信します。
- Wimax FA の場合、HA-RK キー タイマーが期限切れになるか、または HA-RK キーか FA-HA キーが利用できないときは、HA は Registration Revocation メッセージを FA に送信しません。
- Registration Revocation メッセージに FHAE があり、対応する FA の FA-HA キーを HA がローカルに持たない場合、HA は FA から受信した Registration Revocation メッセージをドロップします。これは、3gpp2 FA および Wimax FA の両方に当てはまります。
- 受信メッセージに FHAE がなく、一方で 3gpp2 の FA-HA キーによって HA 上でローカルに設定されているか、または、Wimax の FA-HA キーがすでに生成されている場合、HA は FA から受信した Registration Revocation メッセージをドロップします。
- その他の場合は、HA は Registration Revocation メッセージを処理または開始します。

シナリオ -2

FA のアクセス タイプには、次のコマンドの **enable-fhae** にオプションがあります。

```
ip mobile home-agent foreign-agent default access-type 3gpp2 enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 enable-fhae
```

3gpp2 FA の FA-HA キーを HA 上でローカルに設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	3gpp2 の FA-HA キーを HA 上でローカルに設定します。

- 3ggp2 FA の場合、HA は FA-HA キーがローカルに利用できない場合、Registration Revocation メッセージを FA に送信しません。
- Wimax FA の場合、HA-RK キー タイマーが期限切れになるか、または HA-RK キーか FA-HA キーが利用できないときは、HA は Registration Revocation メッセージを FA に送信しません。
- 受信メッセージに FHAE がなく、一方で 3gpp2 の FA-HA キーによって HA 上でローカルに設定されているか、または、Wimax のキーがすでに生成されている場合、HA は FA からの受信した Registration Revocation をドロップします。
- その他の場合は、HA は Registration Revocation メッセージを開始します。

シナリオ -3

```
ip mobile home-agent foreign-agent default access-type 3gpp2 disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 disable-fhae
```

FA-HA キー値を HA 上でローカルに設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	FA-HA キー値を HA 上でローカルに設定します。

- HA は Registration Revocation メッセージに FHAE がある場合、FA から受信した Registration Revocation メッセージをドロップします。これは、3gpp2 FA および Wimax FA の両方に当てはまります。
- その他の場合は、HA は Registration Revocation メッセージを開始します。

NAI ごとの絶対タイムアウト

データパス アイドル タイマーの場合、設定されたインターバルの間中アイドル（トラフィックがない）のままであるときは常にユーザが削除されます。しかし、絶対タイマーは開始されたときに、ユーザがアクティブであってもユーザを削除します。

この機能は、ユーザがトラフィックを送信しているかいないかにかかわらず、タイマーが期限切れになったときにユーザのセッションを切断するために、セッションに絶対タイムアウトをローカルにまたは Radius Access Accept を使用して設定します。現時点で、HA はホットラインユーザの場合に Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）アトリビュート、session-timeout（27）をサポートします。絶対タイマーに同じアトリビュートが拡張されます。

絶対タイマーの開始は、登録中だけに限る必要があります。また、絶対タイマーは、バインディングが削除されるまで変更しないでください。絶対タイマーが登録中に受信されず、再登録中に受信された場合、絶対タイマーは開始されません。絶対タイマーは、初期登録に対してだけ意味を持ちます。

絶対タイマーは、ホットライン タイマーからは独立して動作します。絶対タイマーが設定されると、クロックが進み、期限切れになったときにバインディングを削除します。

冗長構成の場合でも使用でき、絶対タイムアウト値は、スタンバイと同期する必要があります。

絶対タイムアウト機能の設定

HA がセッションに対する絶対タイムアウトをセットすることをイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile realm realm absolute-time interval-in seconds`	**absolute-time** を HA 上でローカルに設定します。Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）から Session- Timeout（27）がダウンロードされる場合、より高い優先順位が与えられ、ローカルに設定された **absolute-time** 値が上書きされます。

設定の確認

次に、設定の確認とトラブルシューティングに役立つ複数の例を示します。

3GPP2 バインディングの場合、出力は次のとおりです。

```
# show ip mobile binding

Mobility Binding List:
Total 1
derath5@cisco.com (Bindings 1):
    Home Addr 65.0.0.2
    Care-of Addr 50.1.1.92, Src Addr 50.1.1.92
    Lifetime granted 02:00:00 (7200), remaining 01:59:52
    Flags sBdmg-T-, Identification CD735149.00000005
    Tunnel0 src 14.0.0.2 dest 50.1.1.92 reverse-allowed
    Tunnel0 Output ACL: p1_test - ACL is empty or not configured
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Acct-Session-Id: 0x00000002
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Absolute session time granted 00:01:00 (60), remaining 00:00:52
    Traffic Plane Id:6
```

WiMAX バインディングの場合、出力は次のとおりです。

```
HA-Slot3#show ip mobile binding
Mobility Binding List:
Total 1
sony6@cisco.com (Bindings 1):
    Home Addr 65.0.0.3
    Care-of Addr 50.1.1.90, Src Addr 50.1.1.90
    Lifetime granted 02:00:00 (7200), remaining 01:59:07
    Flags sBdmg-T-, Identification CD7352EA.00000006
    Tunnel0 src 14.0.0.2 dest 50.1.1.90 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: WiMAX(802.16e)
    Acct-Session-Id: 0x00000004
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Absolute session time granted 00:02:00 (120), remaining 00:01:07
    Traffic Plane Id:5
```

ホットライン タイマーおよび絶対タイマーの両方がバインディングに存在する場合、出力は次のとおりです。

```
HA-Slot3#show ip mobile binding
Mobility Binding List:
Total 1
derath5@cisco.com (Bindings 1):
    Home Addr 65.0.0.2
    Care-of Addr 50.1.1.92, Src Addr 50.1.1.92
    Lifetime granted 02:00:00 (7200), remaining 01:59:49
    Flags sBdmg-T-, Identification CD7358E6.00000005
    Tunnel1 src 14.0.0.2 dest 50.1.1.92 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Acct-Session-Id: 0x00000009
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Hotline status Active
    Hotline session granted 00:01:00 (60), remaining 00:00:49
    Radius Disconnect Enabled
    Absolute session time granted 00:01:00 (60), remaining 00:00:49
    Traffic Plane Id:6
```

この機能が設定されている場合、次の新しいデバッグ ステートメントが表示されます。

```
MobileIP: Absolute timer expired for MN derath5@cisco.com
MobileIP: MN id for addr freeing is derath5@cisco.com careof 50.1.1.92
MobileIP: De-allocating AAA ID: 0x00000009
MobileIP: MN derath5@cisco.com Tunnel route deleted for 65.0.0.2/255.255.255.255 via
gateway50.1.1.92
MobileIP: Deleted Tunnel1 src 14.0.0.2 dest 50.1.1.92
MobileIP: Delete database info. for MN 65.0.0.2
MobileIP: MN id for addr freeing is derath5@cisco.com careof 50.1.1.92
MobileIP: MN derath5@cisco.com Tunnel route deleted for 65.0.0.2/255.255.255.255 via
gateway50.1.1.92
MobileIP: Deleted Tunnel0 src 14.0.0.2 dest 50.1.1.92
MobileIP: De-allocating AAA ID: 0x00000007
MobileIP: Delete database info. for MN 65.0.0.2
```

制約事項および制限事項

- HA は、スタンバイ Control Plane（CP; コントロール プレーン）のバインディングを削除しないでください。そうでない場合、アクティブからのバインディングの削除が失敗し、エラー統計情報に表示されます。

  次の特殊なケース/レース コンディションは、個別に処理されます（例、1 レース コンディション）。

  - アクティブ/スタンバイ上にバインディングが作成されます。
  - アクティブおよびスタンバイ上でタイマーが期限切れになります。
  - タイマーが期限切れになったため、バインディングがアクティブから削除されますが、スタンバイからは削除されません。
  - アクティブからスタンバイにバインディング削除イベントが送信される前に切り替えが発生します。
  - スタンバイがアクティブになり、絶対タイマーが期限切れになったバインディングを所持します。

  上のケースを処理するには、スタンバイ上で絶対タイマーを停止し、最初に開始したときのインターバルで再スタートします。このインターバルが終了した後、バインディングは削除されます。

トンネル インターフェイスでのアクセス制御リスト（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 Access Control List（ACL; アクセス制御リスト）設定を Home Agent 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、Home Agent と PDSN/Foreign Agent の間のトンネルに定義され、適用されます。

モバイル IP トンネル テンプレート機能の設定

モバイル 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`	Home Agent 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）　モバイル 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。

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

Cisco Home Agent 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 Mobile-Home Authentication Extension（MHAE）Security Parameter Index（SPI; セキュリティ パラメータ インデックス）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。

（注）　MN-HA キーおよび SPI が 3gpp2 アトリビュート（57/58）を使用する AAA からダウンロードされている場合、HA は MD5 アルゴリズムだけを使用して MHAE を認証します。

ユーザ プロファイル

Home Agent 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、モバイル 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 Home Agent 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。

Home Agent は最大 200,000 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。Service Application Module for IP（SAMI）では、HA は 6 × 200,000 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

Home Agent 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。

- Care-of-Address（CoA; 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
- Signaling identification フィールド

アップストリーム パスでのモバイル ステーション（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、Home Agent 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 IP 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。

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付けられているモバイル 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 Home Agent 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モバイル 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 Home Agent はこのようなアイドル状態の PPP セッションにバインディング アップデートとバインディング確認のメッセージをできる限り早く送信します。PDSN 間ハンドオフとモバイル IP 登録が発生すると、Home Agent 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 の気付アドレス（CoA）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、Home Agent はバインディング アップデート 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 はバインディング確認メッセージで確認応答し、必要に応じて、そのモバイル 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 Mobile Station（MS; 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） Home Agent がバインディング アップデート 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 Home Agent 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、Home Agent 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 以外の値に設定できません。

移動体識別番号（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、Home Agent 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 Normal Vendor Specific Extension（NVSE）は、PDSN ノードによってモバイル 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。

Offset=0 による第 1 パケットのフラグメント サイズの設定

この機能を使用すると、ネットワークでの第 2 フラグメントのさらなるフラグメンテーションを避けるために、第 1 フラグメント サイズを設定できます。また、IP フラグメンテーションの発生時には、第 1 フラグメントに内部パケットの L4 ヘッダー情報は含まれません。これが原因となって、L4 までのディープ インスペクションを実施するネットワークのファイアウォールで、第 1 フラグメントがドロップされる可能性があります。

この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Router#**ip fragment first minimum size** *size*	さらなるフラグメンテーションを避けるために第 1 セグメント サイズを設定します。範囲は *8* ～ *560* バイトです。サイズは、ペイロードだけを含み、ヘッダーは含まれません。

（注）　「ペイロード サイズ」は 8 バイトの倍数である必要があります。そうでない場合は、"%% First fragment payload size is not in multiples of 8 bytes" というエラーメッセージとともにコマンドが拒否されます。

これは、IP レベルのコマンドであり、サイズ設定は IP パケットのペイロードだけを考慮に入れます。

たとえば、第 1 フラグメント サイズを 48 バイトと設定すると、20 バイトの IP ヘッダーを含めて、68 バイトのサイズで第 1 フラグメントが作成されます。

IP-IP トンネル パケットの場合、設定されたペイロード サイズは内部 IP ヘッダーを含みます。フラグメンテーション コードの場合、内部 IP は、外部 IP ヘッダーへのペイロードと見なされます。

- コマンド設定は、第 1 フラグメントのペイロードの最小値を示すだけです。Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）の既存のフラグメンテーション メカニズムが、設定値より大きい第 1 フラグメントを選択する場合は、設定は実施されません。そうでない場合は、Broadband Wireless Gateway（BWG）は想定よりも多くのフラグメントを生成します。
- また、設定された第 1 フラグメント サイズが出力インターフェイスの Maximum Transmission Unit（MTU; 最大伝送ユニット）を上回る場合は、設定値は実現されません。

次の例は、IP パケット、および IP-IP トンネルパケットの場合のパケットの状態を示しています。

```
router(config)# ip fragment first minimum size 80
IP Packet:

10:27:59.660 IST Mon Apr 13 2009                Relative Time: 2.990258
Packet 8 of 26                                  In: FastEthernet0/1

Ethernet Packet:  114 bytes
      Dest Addr: 0003.FEAB.D871,   Source Addr: 001F.6C89.0D74
      Protocol: 0x0800

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 100,   ID: 0x0092,   Flags-Offset: 0x2000 (more fragments)
      TTL: 255,   Protocol: 1 (ICMP),   Checksum: 0x582D (OK)
      Source: 50.1.1.200,     Dest: 13.2.2.15

ICMP  Type: 8,   Code: 0  (Echo Request)
      Checksum: 0x1A45 ERROR: C661
      Identifier: 006A,  Sequence: 0000
Echo Data:
    0 : 0000 0000 E794 B5A4 ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   20 : ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   40 : ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   60 : ABCD ABCD ABCD ABCD ABCD ABCD ............


IP-IP tunnel packet:
20:39:40.394 IST Sun Apr 12 2009                Relative Time: 2.967188
Packet 7 of 22                                  In: FastEthernet0/1

Ethernet Packet:  114 bytes
      Dest Addr: 0003.FEAB.D871,   Source Addr: 001F.6C89.0D74
      Protocol: 0x0800

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 100,   ID: 0x8008,   Flags-Offset: 0x2000 (more fragments)
      TTL: 255,   Protocol: 4 (IP-IP),   Checksum: 0xD9F5 (OK)
      Source: 14.0.0.1,     Dest: 50.1.1.150

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 1500,   ID: 0x0086,   Flags-Offset: 0x0000
      TTL: 255,   Protocol: 1 (ICMP),   Checksum: 0x40D0 (OK)
      Source: 50.1.1.200,     Dest: 65.0.0.2

ICMP  Type: 8,   Code: 0  (Echo Request)
      Checksum: 0x72CB ERROR: 7C6A
```

```
      Identifier: 005E,  Sequence: 0000
Echo Data:
    0 : 0000 0000 E49E 6020 ABCD ABCD ABCD ABCD ABCD ABCD
```

FA-HA IP-in-IP トンネルに対する一意の IP ID の保護

この機能は、単一 IP アーキテクチャにおける数十万のセッションをサポートします。これは、パケットがフラグメントする可能性があるときにだけ、IP ヘッダーに一意の ID を設定することで実現されます。そうでない場合は、IP ヘッダーの ID フィールドは **0** に設定されます。

この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Router#**ip mobile tunnel ip-ip conserve-ip-id threshold** *value*	パケットがフラグメントする可能性があるとき、IP ヘッダーに一意の ID を設定します。しきい値の範囲は *576-1500* であり、外部 IP パケット サイズを示します。 この機能は、IP-IP トンネルの場合にだけサポートされます。

ip mobile tunnel ip-ip conserve ip-id threshold コマンドを設定する場合、パケット サイズが**しきい値**を上回るときは、パケットは、外部 IP ヘッダーに一意の IP ID を設定されて送信されます。そうでない場合は、ID フィールドは **0** に設定されます。しきい値を 1400 バイトに設定すると、サイズが 1401 以上のパケットは、一意の IP ID を設定されて送信されます。

この機能は、デフォルトの動作ではありません。このコマンドを使用してイネーブルにする必要があります。さらに、デフォルトのしきい値はありません。

China Telecom アトリビュートの Vendor-Specific Extensions（VSE）サポート

HA リリース 5.1（単一 IP アーキテクチャである）では、この機能のサポートの一部として、次の点が変更されました。

- アクティブとスタンバイの間のこれらの NVSE / アトリビュートの同期が、HA 5.0 に導入された SR インフラストラクチャを使用して正しく作動することを保証する。
- CP と Traffic Plane（TP; トラフィック プレーン）の間のこれらの NVSE の同期が正しいことを保証する。
- インターフェイスとアカウンティングが正しく動作することを保証する。
- **show ip mobile binding** の出力がこの情報を示すアトリビュートを表示することを保証する。

  次は、出力の例です。

```
Active-HA#sh ip mobile binding
    Mobility Binding List:
Total 1
ct-cisco@cisco.com (Bindings 1):
        Home Addr 60.0.2.1
    Care-of Addr 4.0.2.3, Src Addr 4.0.2.3
    Lifetime granted 00:33:20 (2000), remaining 00:33:15
    Flags sbdmg-t-, Identification C1F3C1D5.0000000F
    Tunnel1 src 40.0.11.20 dest 4.0.2.3 reverse-allowed
```

```
Routing Options -
Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
Acct-Session-Id: 0x00000005
Sent on tunnel to MN: 0 packets, 0 bytes
Received on reverse tunnel from MN: 0 packets, 0 bytes
Radius Disconnect Enabled
Correlation Id cisco-ha(vendor id 20942)
Calling Station Id cisco
Served MDN CT-MDN
Charging Type 0x00000001
Traffic Plane Id:7
```

次のアトリビュートは、この機能の一部としてサポートされます。

- Correlation-Id
- Calling-Station-Id
- Served-MDN
- Charging-Type
- HA-Service-Address

また、この機能のサポートの一部として、FA および AAA サーバとの相互動作が若干変更されました。次のサブセクションに詳細情報を示します。

FA との相互動作

この機能のサポートによって、HA は RRQ で受信される次のアトリビュートを処理します

- **Calling-Station-Id**

  HA は、RRQ で受信される CT NVSE Calling Station ID（CLID; 発信ステーション ID）アトリビュートの処理をサポートします。これによって、PDSN/FA はユーザの IMSI を CT NVSE アトリビュートとして HA に送信できます。

- **Correlation-Id**

  HA は、MobileIP のベンダー固有アトリビュートのために RFC 3115 に定義される形式で、FA から受信した Correlation-Id を処理します。

  HA が再登録中に RRQ で correlation-id アトリビュートまたは calling-station-id アトリビュートの新しい値を受信したとき、HA は MIP セッションの Accounting Stop および Accounting Start を送信します。

AAA との相互動作

HA は、AAA との認証とアカウンティングのための相互動作中に、次のアトリビュートを処理します。

- **Correlation-Id**

  RRQ で受信した Correlation-Id は、Accounting Start/Stop/Interim メッセージで、AAA サーバへ送信されます。このアトリビュートは、AAA との認証中には含められません。

- **Calling-Station-Id**

  RRQ で受信した Calling-Station-Id は、AAA との MN サブスクライバの認証中にアクセス要求で送信されます。このアトリビュートも、Accounting Start/Stop/Interim メッセージで AAA サーバへ送信されます。HA は、Calling-Station-Id を RFC 2865 で定義された標準 RADIUS Attribute（31）の形式で AAA へ送信します。

- **Served-MDN**

  HA は、AAA サーバとの認証の成功後に、Served MDN 値を Access-Accept で受信します。受信したアトリビュートは、Accounting Start/Stop メッセージで、アカウンティングの目的のために AAA にだけ送信されます。

- **Charging-Type**

  HA は、AAA サーバとの認証の成功後に、Charging-Type 値を Access-Accept で受信します。受信したアトリビュートは、Accounting Start/Stop メッセージで、アカウンティングの目的のために AAA にだけ送信されます。

  Charging-Type 値は次を含みます。

  - 0x00000001：ポストペイド アカウンティング
  - 0x00000002：プリペイド アカウンティング
  - 0x00000003：ポストペイド アカウンティングおよびプリペイド アカウンティングの両方

- **HA-Service-Address**

  HA は、ユーザの HA サービス アドレスをアカウンティング開始メッセージの中で AAA に送信します。

表 16-1 は、HA が AAA との相互動作の中でどのように各種の Radius メッセージ（RFC 2865 および 2866）に組み込むかを示しています。

表 16-1　AAA 中の HA アトリビュート Radius メッセージ

アトリビュート	アトリビュート値	Access-Request	Access-Accept	Accounting-Start	Accounting-Stop	Accounting-Interim-Update
Calling-Station-Id	31	0-1	0	0-1	0-1	0-1
Correlation-Id	26/5535/44	0	0	0-1	0-1	0-1
Served-MDN	26/ 20942/ 100	0	0-1	0-1	0-1	0
Charging-Type	26/ 20942/ 101	0	0-1	0-1	0-1	0
HA-Service-Addres	26/5535/7	0	0	0-1	0-1	0

代替 MN ID のサポート

現時点で、Home Agent はサブスクライバの一意な識別に NAI を使用しています。China Telecom オペレータ ネットワークでは、すべてのモバイル ノードが同一の NAI を持ち、発信ステーション ID（CLID）で識別されます。このため、Home Agent は、サブスクライバを一意に識別するために別のアトリビュートを使用するように拡張されます。China Telecom の場合、代替 MN ID は CLID です。

CLID の形式仕様は、NAI 形式のサブセットです。CLID モードでは、HA はシステム内のバインディング識別に CLID を使用します。したがって、NAI には同じ値を持ち、CLID には異なる値を持つ 2 つの RRQ が 2 つの異なるバインディングとして識別されます。

認証、認可、アカウンティングのために、RRQ で受信された NAI のレルム部分がシステム内の設定の識別のために使用されます。

このモードでは、HA が CT CLID NVSE のない RRQ を受信した場合、HA は RRQ を拒否し、該当するカウンタ（Bad Request）が増分されます。

HA は、（グローバル コンフィギュレーションに基づいて）NAI または CLID ベースのバインディング ID のいずれかをサポートします。システムにアクティブ バインディングがある場合、代替 MN ID オプションの動的変更はできません。

この機能を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent options`	（任意）IP Mobile Home Agent オプションの設定をイネーブルにして、IP Mobile Home Agent オプション コンフィギュレーション サブモードを開始します。
ステップ 2	`Router(config-ipmobile-ha-options)#mn-identifier calling-station-id`	（任意）CLID を代替モバイル ノード ID としてイネーブルにします。システムにアクティブなバインディングがある場合は、この CLI をイネーブルまたはディセーブルにできません。

設定を確認するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router# show ip mobile binding`	モビリティ バインディング テーブルを表示します。

次に、例を示します。

```
router#sh ip mob bind
Mobility Binding List:
Total 1
Total VPDN Tunnel'ed 0
111111111111450 (Bindings 1):
    Home Addr 1.1.1.14
    Care-of Addr 10.5.1.2, Src Addr 10.5.1.2
    Lifetime granted 00:08:20 (500), remaining 00:05:17
    Flags sbdmg-t-, Identification CDE8617E.00000008
    Tunnel0 src 86.6.6.6 dest 10.5.1.2 reverse-allowed
    Routing Options -
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Revocation negotiated - I-bit set
    Acct-Session-Id: 0x00000015
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Correlation Id 8(vendor id 20942)
    Calling Station Id 111111111111450
    NAI  ctc_user8@ispxyz.com <--- RRQ nai for this binding.
    Traffic Plane Id:4
```

コール アドミッション制御（CAC）のサポート

現在、HA Server Load Balancing（HA-SLB; HA サーバ ロード バランシング）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使用量です。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 calls per second（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 Server Load Balancing（SLB; サーバ ロード バランシング）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)
```

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 でオープンできるバインディングの数を制限します。max-binding-value のデフォルト値は 235,000 です。

輻輳制御機能

Cisco Mobile Wireless Home Agent Release 5.0 では、輻輳制御機能のために、Home Agent が実施するコール アドミッション制御アルゴリズムを、輻輳状態に到達したと判定したときにアクションを実行するように変更することが必要です。

輻輳が発生したかどうかを判定するために、DFP 重みを設定できます。一般に、DFP 値は輻輳状態の 70% に対応します。デフォルトで、DFP 重みは **0 ～ 24** の範囲内です。値の必須範囲を設定するために、最大重みを設定できます。**0** は、使用される最大リソースに対応し、最大スケール値はリソースが 100 % 使用できることを示します。

使用される DFP 値は、単に、単一 IP モデルのコントロール プロセッサ向けにだけ計算されます。トラフィック プレーン プロセッサ リソース利用が輻輳の一因となることは予想されません。

輻輳状態に到達した場合、次の 4 つのアクションが実行可能です。

- Reject : 新しい発呼をすべて拒否します。エラーコード 130 （不十分なリソース）を含む MIP Registration Reply が送信されることで、拒否が示されます。
- Abort : 新しい発呼をすべて拒否し、「進行中」のコールを打ち切ります。進行中とは、Registration Request が受信され、Registration Reply が送信されていない MIP Registration を意味します。エラーコード 130 （不十分なリソース）を含む MIP Registration Reply が送信されることで、拒否が示されます。
- Redirect : 新しい発呼をすべて拒否し、「進行中」のコールを打ち切ります。進行中とは、Registration Request が受信され、Registration Reply が送信されていない MIP Registration を意味します。エラーコード 136（未知の Home Agent アドレス）を含む MIP Registration Reply が送信されることで、拒否が示されます。Home Agent アドレス フィールドには、発呼のリダイレクト先の Home Agent のアドレスが含まれます。to-be-redirected-to-address は、Home Agent でグローバルに設定されます。
- Drop : 既存のコールがデータ パス アイドル タイマー評価に基づいてドロップされます。設定された値を超えるデータ パス アイドル タイムのあるバインディングは解放されます。このとき、Resource Revocation メッセージが（設定されていれば）送信されます。Resource Revocation が設定されていない場合は、ローカル バインディングのクリアが要求されたときのように、バインディングがメッセージなしに削除されます。

（注）　一度に 1 つのアクションしか設定できません。第 2 のアクションを設定しようとすると、第 1 のアクションが上書きされます。

輻輳制御機能の設定

輻輳トリガーが発生したときのコール アドミッション制御アクションを定義するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent congestion` *dfp_weight* **action | reject | abort | redirect** *HA-address* **| drop data-path-idle** *minutes*	輻輳トリガーが発生したときのコール アドミッション制御アクションを定義します。
ステップ 2	`Router# show ip mobile home-agent congestion`	次の情報を表示します。 • 輻輳状態：混雑しているか、いないか。 • 設定された congestion-threshold 値 = 設定された CLI での dfp_weight。 • 現在の DFP 値。現在の DFP 値とは、最近 5 分間の DFP 値の平均値です。

さらに、CISCO-SLB-CLIENT-MIB には、次の情報が含まれています。

- DFP 輻輳開始しきい値。この値を超えると Congestion On Trap が生成されます。
- DFP 輻輳減少しきい値。輻輳がこの値を下回ると Congestion Off Trap が生成されます。
- 現在の DFP 値。

次は、輻輳制御機能の出力例です。

```
router#show ip mobile home-agent congestion
Home Agent congestion information :
Current congestion level:  Congested
Configured Action : Reject
Configured threshold : 10
Current DFP value = 7
```

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。

Home AAA（HAAA; ホーム AAA）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、次の作業を実行します。

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。Remote Authentication Dial-In User Service（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。

次に、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、または 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付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。すべてのサブスクライバ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、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）Management Information Base（MIB; 管理情報ベース）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 オブジェクトが追加され、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、次の作業を実行します。

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 point-to-point（p2p; ポイントツーポイント）インターフェイスに接続したときに使用され、プール使用率が上限または下限しきい値（パーセント単位）に達したときにトラップを生成するよう、IP アドレスのローカル プールを設定します。 新しいオプション **priority** *1-255* により、プライオリティを新しく作成されたプールに割り当てることができます。このプライオリティは IP アドレスの割り当てに使用されます。
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。

次に、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

設定の確認作業は次のとおりです。

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。

次に、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
```

モバイル 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、モバイル 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 Domain Name Server（DNS; ドメイン ネーム サーバ）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 Dynamic Host Configuration Protocol（DHCP）または Point-to-Point Protocol/IP Control Protocol（PPP/IPCP IP; ポイントツーポイント プロトコル/IP コントロール プロトコル）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。モバイル IPv4 では、アクセス ネットワーク（外部ネットワークともいいます）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ている必要があります。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 Home Agent に指示します。Home Agent 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、Home Agent 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、モバイル 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 Cisco Vendor-Specific Extensions 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。

その他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 Home Agent 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

（注）　DHCP サーバからダウンロードされる場合は、DNS サフィクスは RRP に付加されません。

WiMAX AAA アトリビュート

Cisco Home Agent Release 4.0 以降には、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 : **ip mobile home-agent send-mn-address** コマンドが設定されている場合、モバイル IP RRQ で受信されたホーム アドレスはアクセス要求メッセージの Framed-IP-Address アトリビュートの値として送信されます。

（注） Home Agent Release 4.0 ソフトウェアでは、MIP フロー（Wimax）を開くとき、アクセス要求に Framed-IP-Address アトリビュートはありません。

- WiMAX Capability：このアトリビュートは、HA の WiMax 機能を特定し、すべてのアクセス要求メッセージで送信されます。HAAA による Access-Accept メッセージでも送信されます。このアトリビュートが 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アクセス要求で 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-Accept で受信した WiMAX Capability VSA を処理せず、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：このアトリビュートは、要求を作成している HA の IP アドレスを特定します。このアトリビュートは HA からのすべてのアクセス要求メッセージに含まれます。既存のバインディングでは（再登録および削除に対応するアクセス要求）、値はそのバインディングの Home Agent アドレスに設定されます。新しいバインディングでは、このアトリビュートの値は、HA 設定でバインディングに割り当てられた HA IP アドレス（ホームアドレスではない）に設定されます。この値は RRP で Home Agent IP アドレスとして送信されます。「バインディングの Home Agent IP アドレスの設定」セクションを参照してください。
- RRQ-HA-IP：モバイル IP RRQ の Home Agent 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、HA がこのアトリビュートをアクセス要求メッセージに含めます。その場合、値はモバイル IP RRQ 内の Home Agent 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 サブスクライバ用の 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 を識別します。このアトリビュートはアクセス要求メッセージに含まれ、MN-HA-SPI と類似しています。

表 16-2 に、Home Agent の WiMAX AAA Authorization アトリビュートを示します。

表 16-2　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 以降でのサポート
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
Chargeable User Identity（CUI）	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です。	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

表 16-2　WiMAX AAA Authorization アトリビュート （続き）

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 アドレス。	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
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

"ip mobile host/realm" の AAA アトリビュート

次のアトリビュートは、この機能の一部としてサポートされます。

- アトリビュート "data-path-idle" : これは、AAA アトリビュートとして、モバイル単位でデータ パス アイドル タイマーを設定します。これは Cisco の Attribute Value pairs （AV pair; AV のペア）としてダウンロード可能です。値が AAA からダウンロードされ、ローカルにも設定される場合は AAA からダウンロードされた値が優先されます。RSIM サブスクライバ プロファイルでは、config は次のようになります。

  vsa cisco generic 1 string "mobileip:data-path-idle=300"

  変更点：

  - AAA アトリビュート "data-path-idle" を使用してバインディングが作成済みの場合で、後で **ip mobile realm** *realm* **data-path-idle** が設定されるかまたは変更されると、AAA アトリビュートなしで作成されたバインディングだけが更新されます。これによって、AAA 優先順位が維持されることが保証されます。
  - 再登録がデータ パス アイドル タイマーをアップデートする可能性があります。

- アトリビュート "Nexthop" : これは、AAA アトリビュートとして、モバイルごとにネクストホップ IP を設定します。これは Cisco の AV のペアとしてダウンロード可能です。この値が AAA からダウンロードされ、ローカルにも設定される場合は AAA からダウンロードされた値が優先されます。RSIM サブスクライバ プロファイルでは、config は次のようになります。

  vsa cisco generic 1 string "mobileip:nexthop=1.1.1.1"

  変更点：

  - AAA からダウンロードしたネクストホップを使用してバインディングが作成済みの場合で **ip mobile realm** *realm* ***any-traffic nexthop*** *ip* コマンドが設定されると、CLI は受け入れられません。

- バインディングが作成済みで、**nexthop ip** が CLI で設定されるときは、バインディングの削除の確認だけで、値が更新されます。
- 再登録はダウンロードされた nexthop アトリビュートをアップデートしません。

MN および外部エージェント認証

HA は MHAE で受信した SPI を MN-HA-MIP4-SPI アトリビュートとして HA-IP-MIP4 とともにアクセス要求に含めます。モバイル IP RRQ 内の MHAE の検証およびモバイル IP RRP の MHAE の生成には、MN-HA-MIP4-SPI アトリビュート内の HA-IP-MIP4 および 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。

次の情報が Registration Request から抽出されます。

- MN-HA Authentication エクステンションの MN-HA SPI
- Home Agent フィールドの HA IP アドレス
- 宛先 IP アドレス フィールドの受信者 IP アドレス
- FA-HA Authentication エクステンションの FA-HA SPI（このエクステンションがメッセージにある場合）

HA は、AAA サーバに送信されるアクセス要求に MN-HA-MIP4-SPI および HA-IP-MIP4 アトリビュート（それぞれに、MN-HA SPI および HA IP アドレスが含まれる）を含めます。AAA サーバからの Access-Accept には、アクセス要求のこの 2 つのアトリビュートに対応する MN-HA-MIP4-KEY アトリビュートが含まれます。HA は、ダウンロードされたキーを使用して MN-HA セキュリティ アソシエーションを設定します。セキュリティ アソシエーションは、Registration Request 内の MN-HA Authentication エクステンションの認証、および Registration Reply でのこのエクステンションの生成に使用されます。

Registration Request の Home Agent フィールドに、ダイナミック HA 割り当てを示す、すべてが 1 または 0 に設定された IP アドレスが含まれることがあります。この場合、HA は、アクセス要求内に Home Agent フィールド値に設定された追加の RRQ-HA-IP アトリビュートを含めます。MN-HA-MIP4-SPI アトリビュートは、前述のとおりです。その代わりに、HA-IP-MIP4 アトリビュートは、受信者 IP アドレスに設定されます。AAA サーバは、追加の RRQ-MN-HA-KEY アトリビュート（RRQ-HA-IP に対応）を Access-Accept に含めます。HA はこのキーを使用して、Registration Request の MN-HA Authentication を認証します。認証に成功したら、HA は Registration Reply を送信するために MN-HA-MIP4-KEY を使用して MN-HA セキュリティ アソシエーションを設定します。後続の登録認証は、このセキュリティ アソシエーションを使用します。

CMIP の場合、RRQ に ALL-ZERO-ONE-ADDR である HA IP 、および、MN-HA-MIP4-SPI と HA-IP-MIP4 が含まれる場合、RRQ-HA-IP も RRQ の HA IP と同じ値に設定され、アクセス要求で送信されます。HA は RRQ-HA-IP の RRQ-MN-HA-KEY 、および、MN-HA-MIP4-SPI に対応する HA-IP-MIP4 の MN-HA-MIP4-KEY をダウンロードします。HA は RRQ-MN-HA-KEY を使用してモバイル IP の MHAE を検証し、MN-HA-MIP4-KEY を使用してモバイル IP の MHAE を生成します。

FA から受信した RRQ に FHAE が含まれている場合は、該当する FA の外部エージェント認証が発生します。また、その FA から受信したすべてのサブ シーケンス RRQ には FHAE が含まれます。HA で FA を認証する場合、HA-RK が HA に存在する必要があります。HA に HA-RK が存在しない場合は、HA は AAA から HA-RK をダウンロードします。

HAAA は、各 HA-IP 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 Extensible Authentication Protocol（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 は AAA から HA-RK をダウンロードする必要がある場合、HA は、アクセス要求で HA-RK-Key-Request VSA の値を 1 に設定して、Access-Accept で HA-RK-KEY アトリビュートを受信することを期待していることを示します。アクセス要求には 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。HAAA は、アクセス要求で送信された HA-IP-MIP4 アトリビュートに関連する Access-Accept で、HA-RK-KEY、HA-RK-SPI、および HA-RK-Lifetime 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存在している場合は、すべてが存在している必要があります。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。

HA-RK キー（26/15）、HA-RK SPI（26/16）、HA-RK ライフタイム（26/17）がスタンバイまたは冗長 HA と同期されます。

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 です。RFC 2104 で規定されます。HMAC：Keyed-Hashing for Message Authentication

HA-IPv4 はアクセス要求で送信される HA-IP-MIP4 アトリビュートです（バインディング Home Agent IP など）。

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上述のアルゴリズムを使用して生成された FA-HA キーと SPI が使用されます。

次の **show ip mobile secure home-agent ha-rk** *ha-ip* コマンドを使用して、ダウンロードした HA-RK キー、SPI、およびライフタイムを表示できます。

次に、例を示します。

```
router#show ip mobile secure home-agent
HomeAgent HA-RK List:
15.1.1.80:
    SPI 102, Lifetime 00:10:30 (630), Remaining 00:10:24
    Key 31323334353637383930313233343536373839 30
```

show ip mobile secure foreign-agent *fa-ip* コマンドを使用して生成された FA-HA キーを表示できます。

次に、例を示します。

```
router#show ip mobile secure foreign-agent
Security Associations (algorithm,mode,replay protection,key):
14.1.1.28:
    SPI 102,  HMAC-MD5, Timestamp +/- 7, HA-IP 15.1.1.80
    Key b932c46406dcfe411f8bd147103ac53ca0c7fe65
```

HA-RK ライフタイムが期限切れになると、上述のダウンロードされた HA-RK と、生成された FA-HA キーは削除されます。ライフタイムが期限切れになる前に新しい HA-RK キーがダウンロードされると、両方のキーが共存を続け、認証はいずれかのキーを使用して成功します。**clear ip mobile secure all** コマンドを使用して、同一のキーを削除できます。このコマンドはすべてのキー、MN、FA、および（生成された、または AAA からダウンロードされた）HA-RK を削除します。

WiMAX の場合、MHAE または FHAE 検証のために、ローカルに SPI およびキーを設定できません。

バインディングの Home Agent IP アドレスの設定

Home Agent IP アドレスをバインディングに割り当てるために Home Agent を設定する方法が複数あります。次の作業を実行して、この機能をイネーブルにします。

ステップ 1	**ip mobile realm @cisco.com vrf** *vrf-name* **ha-addr** ***vrf-ha-address***	インバウンド ユーザ セッションをイネーブルにして、特定のレルムに対する特定のアトリビュートが存在した場合にセッションを切断します。
ステップ 2	**ip mobile home-agent dynamic-address** *dynamic-ha-address*	Registration Response パケットの Home Agent Address フィールドを設定します。
ステップ 3	**ip mobile virtual-network** *virtual-net-start mask* **address** *virtual-net-ha-address*	仮想ネットワークを定義します。
ステップ 4	**ip mobile home-agent address** *global-ha-address*	仮想ネットワークの IP アドレスをイネーブルにします。
ステップ 5	**HA HSRP redundancy virtual IP address** *hsrp-ha-ip-address*	Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）IP アドレスを指定します。

前述の設定詳細情報を使用して、バインディングの Home Agent IP アドレスが選択されます。同一の Home Agent IP アドレスがアクセス要求で HA-IP-MIP4 として、または、RRP で Home Agent IP が送信されます。次のロジックは、以前に存在したバインディングの RRQ には適用されません。既存のバインディングの場合、現在のバインディングの Home Agent IP アドレスが使用されます。

- RRQ HA IP と RRQ 宛先 IP は同一です。

  HA-IP-MIP4 = RRP HA IP アドレス =

  - *vrf-ha-address*（設定されている場合）
  - RRQ 宛先 IP アドレス

- RRQ HA IP は、RRQ 宛先 IP と等しくありません（ダイナミック HA の場合 true を保持し、RRQ HA IP は 0.0.0.0 または 255.255.255.255 です）。

  HA-IP-MIP4 = RRP HA IP アドレス =

  - *vrf-ha-address*（設定されている場合）
  - **ip mobile home-agent address** *global-ha-address* **unknown-ha accept reply** が設定されている場合、RRQ HA IP（ダイナミック HA ではない場合）
  - *dynamic-ha-address*（設定されている場合）
  - RRQ 宛先 IP アドレス

- RRQ HA IP または RRQ 宛先 IP は、サブネット ダイレクト ブロードキャスト アドレスです（RRQ HA IP は 255.255.255.255 と等しくありません）。HA 検出!

  HA-IP-MIP4 = RRP HA IP アドレス =

  - MN は物理インターフェイス上にあります（物理インターフェイスに対応する前述の IP）

    hsrp-ha-ip-address（設定されている場合）

    物理インターフェイス IP アドレス

  - MN は仮想ネットワーク上にあります（仮想ネットワークに対応する前述の IP）。これによって、*virtual-net-ha-address* または *global-ha-address* のいずれかが設定されていると推測されます。

    virtual-net-ha-address（設定されている場合）

global-ha-address.

WiMAX 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 16-3 に、Cisco HA の WiMAX AAA Accounting アトリビュートを示します。

表 16-3　WiMAX AAA Accounting アトリビュート

名前	タイプ	説明	Start	Int	Stop
Acct-Multi-Session-Id	50	この ID は、認証の成功後に AAA によって生成され、Access- Accept メッセージで Network Access Server（NAS; ネットワーク アクセス サーバ）に配信された AAA-Session-Id の値に設定されます。これは CSN ごとに一意であり、セッション内ですべてのアカウンティング レコードと照合するために使用されます。	1	1	1
Framed-IP-Address	8	MS に割り当てられた IPv4 アドレス。これは、IP セッションを特定します。	0-1	0-1	0-1
Chargeable User Identity（CUI）	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です。	0-1	0-1	0-1
HA-IP-MIP4	26/6	Home Agent の IP アドレス。	1	1	1
Event-Timestamp	55	イベント発生時刻。	1	1	1
GMT-Time-Zone-Offset	26/3	NAS または HA での Greenwich Mean Time（GMT; グリニッジ標準時）からのオフセット秒数。	0-1	0-1	0-1

WiMAX サポートの設定

HA はデフォルトで、すべてのバインディングは 3gpp2 アクセス タイプであると推定します。WiMAX の場合、**per foreign-agent access type** コマンドが設定される必要があります（「外部エージェント別アクセス タイプ サポート」セクションを参照）。さらに、WiMAX AAA サポートのイネーブルにするには、次の作業を実行します。

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 が生成するアクセス要求メッセージに次の 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（26/6） • RRQ-HA-IP（26/18） • MN-HA-MIP4-SPI（26/11）
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（26/6） • 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、モバイル IP RRQ で受信されたホーム アドレスがアクセス要求メッセージの 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`	アクセス要求に 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、次の作業を実行します。

ステップ 6	`Router# show ip mob bind`	サブスクライバの認証中に 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。

次に、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
```

使用済みの場合のフレーム化された IP の拒否

AAA から受信したフレーム化された IP アドレスが、すでに既存のバインディングに割り当てられていた場合、HA は現在、設定された IP のプールから別の IP アドレスを割り当てます。リリース 5.2 のこの新しい機能によって、HA は AAA がすでにセッションのバインディングに割り当てられているフレーム化された IP アドレスを返したときに、新しいセッションを拒否できます。

この機能がイネーブルである場合、AAA 応答がバインディングに割り当てられている "Framed IP-Addr" を返したときは、エラーコードに "Insufficient Resources or Admin Prohibited" が設定され、RRQ が拒否されます。

この機能を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)#ip mobile home-agent options`	IP Mobile Home Agent オプションをイネーブルにし、IP Mobile Home Agent オプション コンフィギュレーション サブモードを開始します。
ステップ 2	`Router(config-ipmobile-ha-options)#rrq reject frame-ip in-use`	イネーブルの場合、このサブコマンドは Access-Accept の "Framed IP Address" がすでにバインディングに割り当てられていると、RRQ を拒否します。

Acct-Terminate-Cause のサポート

Home Agent Release 4.0 では、Acct-Terminate-Cause RADIUS アトリビュート（RFC 2866 Radius Accounting で定義されている）がサポートされましたが、常に値 0 が挿入されました。

Home Agent Release 5.0 では、次の一覧にある値がサポートされます。

値のフィールドは、セッションの終了理由を指定する 1 つの整数を含む、4 個の 8 ビットです。終了理由は次のとおりです。

- User Request（1）：サービスの終了を要求したユーザ。たとえば、Link Control Protocol（LCP; リンク コントロール プロトコル）の終了またはログアウトによるなど。- 通常の MIP セッション終了時。
- Lost Service（3）：サービスがこれ以上提供できない。たとえば、ホストへのユーザ接続が中断されたなど。- Resource Revocation が受信されたとき。
- Idle Timeout（4）：アイドル タイマーが期限切れになった。- アイドル タイマーが期限切れになり、MIP セッションが終了されたとき。
- Session Timeout（5）：最大セッション長タイマーが期限切れになった。- MIP セッション登録タイマーが期限切れになったとき。
- Admin Reset（6）：管理者がポートまたはセッションをリセットした。- バインディングがオペレータによってクリアされたとき。
- NAS Error（9）：NAS が、セッションの終了が必要なエラーを検出した（ポートに関するものを除く）。- 再登録の RRQ がエラーであるとき、または、FA-HA AE が確認できないとき。
- NAS Request（10）：NAS が、非エラーの理由でセッションを終了した（特にここでリストされていない限り）。- Terminate-Cause の値以外の定義されていない理由でバインディングが削除されたとき。
- Port Preempted（13）：より優先度の高い使用にポートを割り当てるために NAS がセッションを終了した。- 輻輳のためにセッションが終了したとき。
- User Error（17）：ユーザからの入力がエラーであり、このためセッションの終了が発生した。- 再登録時に MN-HA AE が確認できず、バインディングが削除されたとき。

（注）　この Acct-Term-Cause を Accounting-Stop メッセージに含めるためには、基本的な Accounting 機能が HA でイネーブルにされる必要があります。

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、サブスクライバに **3gpp2** または **wimax** のアクセス タイプを選択します。

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。

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 16-4　AAA サーバの AAA Authentication および Accounting アトリビュート

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*	Proxy Mobile IP（PMIP; プロキシ モバイル IP）の場合に RADIUS サーバが Access Service Network（ASN; アクセス サービス ネットワーク）に送信する MN-HA-KEY。または MIP4（MIP または PMIP）の場合に RADIUS サーバが HA での使用のために送信する MN-HA-KEY。PMIP4 中、ASN が MN-HAAE の計算に使用します。 HA に送信され、MIP バージョン（MIP4 または MIP6）および SPI に基づいて、MN-HA-AE（MIP4）の検証、および MIP4 Registration Response の MN-HAAE または MIP6 Binding Answer の AUTH の計算に使用されます。
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。

表 16-4　AAA サーバの AAA Authentication および Accounting アトリビュート （続き）

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、モバイル IP Registration Request の MN-HA-AE の検証に使用される MN-HA キー。

外部エージェントの分類

Home Agent は、モバイル IP Registration Request で受信した Proxy Mobile IPv4 Access Technology Type Extension の組み込みをサポートします。Tech-type 値 **3** は、802.16e（WiMax）のサポートを示し、**7** は、1xRTT/HRPD のサポートを示します。エクステンションが受信されない場合は、外部エージェントごとの設定が適用されます。FA ごとの設定がない場合は、グローバル値が適用されます。このデフォルトは 3GPP2 であり、WiMax に設定することもできます。

その他の値はサポートされず、その場合、エクステンションは無視されます。非サポート値とともにエクステンションを受信した回数を示す、単一のカウンタがあります。エクステンションの内容はデバグコマンドで表示されます。このコマンドはモバイル メッセージングの内容を表示します。

tech-type 値 **3** の受領は、モバイル IP 登録が WiMax アクセス用であることを示します。この場合、実行されるアクションは WiMax アクセスをサポートするように外部エージェントがローカルに設定されている場合のアクションと同じです。

tech-type 値 **7** の受領は、1xRTT/HRPD アクセスのモバイル IP 登録があることを示します。この場合、実行されるアクションは 3GPP2 アクセスをサポートするように外部エージェントがローカルに設定されている場合のアクションと同じです。

tech-type 値に基づいて実行されるアクションは、ローカルに設定された外部エージェントごとのアクセス タイプ設定よりも優先されます。たとえば、ローカルに設定された値が 3GPP2 を示し、tech-type 値が WiMax を示す場合、WiMax 用のアクションが実行されます。

（注）　Home Agent が Re-registration で異なる Access Technology Type を受信した場合でも、バインディングのアクセス タイプは同一のままです。

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 Home Agent 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、次の作業を実行します。

	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。

次に、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
```

Show/Clear バインディング キーとしての MAC アドレス

Cisco Mobile Wireless Home Agent Release 5.0 では、現在、セッションに端末の MAC アドレスが含まれます。この識別子は、モバイル IP シグナリングを通じて学習されます。初期登録要求には MAC アドレスが含まれ、再登録、および、登録解除にも MAC アドレスが含まれます。この機能を使用することで、ネットワーク管理者は、セッションの検索、削除およびデバグのイネーブル化を MAC でのホストベースで実行できます。該当する場合は、デバグ メッセージおよび syslog メッセージに端末の MAC アドレスが含まれます。

MAC アドレスは、Cisco-Mobile-IP-MIB にも追加される必要があります。

（注）　アクセス ネットワーク テクノロジーでは MAC アドレスは一意であり、Proxy Mobile IPv4 Access Network Technology Extension から学習できます。アクセス ネットワーク テクノロジーのデフォルト値はありません。

新しいフィールドを含めるために、次のコマンドが変更されています。

Show コマンド：

show ip mobile binding mac address : 指定された MAC アドレスのホストのバインディング情報を表示します。出力に MAC アドレスが含まれます。

Debug コマンド：

debug ip mobile host mac address : は、指定された MAC アドレスのホストのデバグ イベントを表示します。該当する場合は、メッセージに MAC アドレスが含まれます。

Clear コマンド：

clear ip mobile binding mac address: 指定された MAC アドレスのホストのモビリティ バインディング エントリを削除します。

データ パス アイドル タイマー

Cisco Mobile Wireless Home Agent Release 5.0 では、指定された時間（アイドルタイム）の間にターミナルでデータトラフィックの送受信がない場合、セッションが終了されます。このアイドル タイムは、ドメイン単位またはグローバルのいずれかで設定できます。ドメイン単位の設定が優先されます。バインディングの削除イベントによってトリガーされた失効メッセージングが発生します。

RRQ はデータ パスで受信されないため、再登録はアイドル タイマーをリセットしません。

コントロール プレーンと / データ プレーンの問題を分離するために、トラフィック プロセッサだけがセッションのデータ トラフィックを認識します。アイドル時間に到達したときは、コントロール プロセッサに通知する必要があります。

データ パス アイドル タイマー情報は、中間アカウンティングの同期化機能を使用して Home Agent 間で同期されます。

次の作業を実行して、この機能をイネーブルにします。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile realm` *realm* `data-path-idle` *minutes* `Router(config)# ip mobile home-agent data-path-idle` *minutes*	設定された時間（アイドル時間）の間、指定されたレルムに一致する NAI を持つモビリティ ホストのトラフィックがないとき、ドメイン内のモビリティ バインディングを削除します。範囲は 1 ～ 65535 です。 設定された時間（アイドル時間）の間トラフィックがないとき、モビリティ バインディングを削除します。範囲は 1 ～ 65535 です。

次は、データ パス アイドル タイマー機能の出力例です。

```
cisco-1@cisco.com (Bindings 1):
    MAC Addr 0000.0001.0000
    Home Addr 5.1.0.1
    Care-of Addr 2.2.2.200, Src Addr 2.2.2.200
    Lifetime granted 10:00:00 (36000), remaining 09:52:39
    IdleTime granted 00:10:00 (10 min), remaining 00:09:24
    Flags sBdmg-T-, Identification CCA7F408.1
    Tunnel0 src 81.81.81.81 dest 2.2.2.200 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Revocation negotiated - I-bit not set
```

3GPP2 / WiMAX バインディングの OM メトリック

この機能は、以前のインターバルの Object Identifier（OID; オブジェクト ID）がクエリーされたときに、MaxActiveBindings、MaxActive3GPP2Bindings および MaxActiveWimaxBindings のピーク値を返します。

Cisco HA Release 5.1 は、OM メトリック機能を処理するために、2 つのタイマーを導入しました。タイマーの 1 つは、Network Timing Protocol（NTP）タイムによって最大値と最小値でのインターバル開始をサポートします。2 番目のタイマーは OM メトリックを計算します。1 番目のタイマーは、ルータのブート アップ時またはコマンドが変更された時点で開始します。2 番目のタイマーは、1 番目のタイマーが期限切れになった時点で開始します。このタイマーは、設定された値に基づいて期限切れになります。

デフォルトでこの機能はイネーブルであり、デフォルトのインターバルは 30 分です。実行コンフィギュレーションでは、デフォルト設定は表示されません。

（注）　冗長構成の場合は、OM メトリック機能が使用できません。

OM メトリックの設定

この機能のインターバルを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# om-metric-interval {15 | 30 | 60 }`	これは、**ip mobile options** コマンドのサブメニューで使用できるサブコマンドです。

次に、設定の確認に役立つ出力例を示します。

3gpp2 バインディングの数や Wimax バインディングの数などのメトリック カウンタは、**show ip mobile binding summary** の下に表示されます。

```
router#sh ip mob binding summary
Mobility Binding List:
Total 1
3gpp2 Bindings 1
Wimax Bindings 0
```

新しいメトリック値は、新しいコマンドの下に表示されます。

```
router#show ip mobile options ommetrics
OM Metric Statistics:

 Peak Active bindings in the elapsed (previous) interval 0
 Peak Active 3GPP2 binding in the elapsed (previous) interval 0
 Peak Active Wimax binding in the elapsed (previous) interval 0
 Elapsed configured interval size is 15 minutes
```

さらに **debug ip mobile** がイネーブルの場合は、次のデバッグ ステートメントが出力されます。

```
%IPMOBILE-6-OMMETRICS_TIMER_INFO: OM Metric Interval Timer will be started after 1170577
milliseconds.
MobileIP:  OM Metric Sleep Timer is Started
MobileIP:  OM Metric Sleep Timer is Stoped
MobileIP:  OM Metrics Interval Timer is Started for 900005 milliseconds
MobileIP:  OM Metrics Interval Timer is Expired
MobileIP:  OM Metrics Interval Timer is Stoped
MobileIP:  System clock has been updated,
                    So Om Metric Timers will restart
%IPMOBILE-4-OMMETRICS_TIMER_WARNING: Clock skew is more, So Om metric timers will restarts
 metrics interval time is 900000.
 deltaOffset is 39599997.
 currentSystemClock is 3599997.
 nextSystemClock is 50400000.
```

MIP/ユーザ データグラム プロトコル（UDP）トンネルの単一インターフェイス記述ブロック（IDB）

MIP/User Datagram Protocol（UDP; ユーザ データグラム プロトコル）RFC 3519 要件は、MN への各 MIP/UDP Collocated Care-of Address（CCoA; コロケーション気付アドレス）バインディングには、個別の MIP/UDP トンネルが必要であると記述しています。HA Release 5.0 では、HA は、それぞれのトンネルに 1 つのハードウェア / ソフトウェア Interface Descriptor Block（IDB; インターフェイス記述ブロック）を使用しました。システムが最大で 16K のハードウェア IDB をサポートできることから、MIP/UDP CCoA バインディングの最大数は 16K に制限されます。

Cisco HA Release 5.1 では、数十万の MIP/UDP CCoA バインディングをサポートできます。この要件をサポートするために、当社はすべての種類のトンネルに対し単一 IDB を使用します。

単一 IDB、つまりトンネル スケーラビリティ機能は MIP/UDP トンネルだけをサポートします。しかし、他の種類のトンネル（IP/IP や Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）/IP など）の機能性には影響ありません。

この機能の一部として、次の項目がサポートされます。

- 他の種類のトンネル（IP/IP、GRE/IP など）が影響されないように、また機能性を維持するように、必要に応じてトンネル Application Programming Interface（API; アプリケーション プログラミング インターフェイス）が変更されます。

- サポートされた MIP/UDP トンネル（CoA または CCoA）の CPS レートは、HA 5.0 と同じままです。
- サポートされた MIP/UDP トンネル（CoA または CCoA）のデータ スループット レートは、HA Release 5.0 と同じままです。
- サポートされる 1GB SAMI カード上の MIP/UDP トンネルの最大数は 80,000 です。この数字を実現するには、I/O メモリを 64MB から 128MB に増やす必要があります。

単一 IDB の SAMI の設定

（注）　I/O メモリを 64MB から 128MB に設定するには、**memory-size iomem 128** コマンドを実行し、I/O メモリの変更後にカードをリブートします。

設定の確認

この機能を実現するための新しい設定作業はありません。次のコマンドは、単一 IDB 機能が機能していることを確認するように変更されました。

show ip mobile tunnel summary コマンドの出力は、次のように変更されました。

```
#show ip mob tunnel sum
Mobile IP tunnels summary:
   One IDB used per tunnel for IP/IP, GRE/IP tunnels
   Single IDB used for MIP/UDP tunnels

   Total mobile ip tunnels 2
```

show ip mobile tunnel コマンドの出力は、MIP/UDP トンネルの場合だけ、若干変更されました。MIP/UDP トンネルに適用される 2 つの変更は次のとおりです。

- すべての MIP/UDP トンネルは、単一 IDB 機能を使用するため、すべての MIP/UDP トンネルのトンネル番号は同一です。
- トンネルの状態は IDB データ構造に保存されます。すべての MIP/UDP トンネルに、単一 IDB を使用するため、MIP/UDP トンネルの各トンネル カウンタが表示されます。一方、新しい show コマンド **show ip mobile tunnel mip-udp aggregate-statistics** を使用すると、すべてのトンネルの集約統計情報が表示されます。

IP/IP トンネルおよび GRE/IP トンネルの出力は同じままです。

```
router#show ip mob tunnel
Mobile Tunnels:
Total mobile ip tunnels 2
Tunnel0:
    src 16.1.2.80, dest 18.1.1.202
    src port 434, dest port 1244
    encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 0, Output ACL users 0
    IP MTU 1468 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Mobile0
    HA created, CEF switching enabled, ICMP unreachable enabled
Tunnel0:
    src 16.1.2.80, dest 18.1.1.202
    src port 434, dest port 1245
    encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 0, Output ACL users 0
```

```
    IP MTU 1468 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Mobile0
    HA created, CEF switching enabled, ICMP unreachable enabled
```

show ip mobile tunnel mip-udp aggregate-statistics 出力は、次のように表示されます。

```
router#show ip mob tunnel mip-udp aggregate-statistics
Tunnel0 Aggregate Counters:
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    300 packets input, 45600 bytes, 0 drops
    300 packets output, 39600 bytes
```

show ip mobile traffic 出力では、すべてのトンネルで送受信されたキープアライブの数が、既存の show コマンドの下に表示されます。次の例では、新しい行に注目します。

```
router#show ip mob traffic
IP Mobility traffic:
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 22961, denied 0, ignored 0, dropped 0, replied 22961
    Register requests accepted 22961, No simultaneous bindings 0
  . . .
  . . .
  . . .
MIP/UDP Tunnel:
    Number of Keepalives received (on all tunnels) 13809
    Number of Keepalives sent (on all tunnels) 13809
```

非 VPN ルーティングおよびフォワーディング（VRF）環境での GRE 鍵 Critical Vendor-Specific Extension（CVSE）

MIPv4 は GRE 鍵を使用しない GRE/IP トンネリングをサポートします。GRE CVSE Extension を使用することで、FA は GRE トンネリングを要求でき、HA と FA の両方が GRE/IP トンネルのアップストリーム/ダウンストリーム キーを交換できます。

次は、この機能が動作する方法を示すコール フローです。

1. FA は GRE 鍵を生成し、GRE 鍵エクステンションを RRQ に付加し、RRQ を HA に転送します。
2. HA は初期登録 RRQ を受信し、GRE 鍵エクステンションを解析します。不十分な構成である GRE 鍵エクステンションを受信した場合、HA は、"unknown CVSE" とともに RRP を送信します。登録が受け入れられると、HA はバインディングを作成し、FA によって提供された GRE 鍵をバインディング内に保存します。リバース トンネルが必要な場合、HA は一意な GRE 鍵も作成し（HA はランダムな番号を生成し、一意性のためにすでに割り当てられた GRE 鍵と比較します）、RRP を GRE 鍵エクステンションとともに返します。HA は FA によって提供された鍵の重複をチェックしません。
3. リバース トンネルがイネーブルである場合、FA は HA へのアップストリーム トラフィック（例：MN から CN へ）をトンネリングし、FA が HA へのパケットをトンネリングする場合は、（RRP で HA によって提供された）GRE 鍵を追加します。トンネルと一致する発信元 IP アドレスおよび宛先 IP アドレスのあるパケットを HA が受信した場合、HA は、カプセル化されたパケット内の GRE 鍵とも一致します。

4. ダウンストリーム トラフィック（例 : CN から MN へ）の場合、CN からのパケットは HA に到達し、HA は HA-FA トンネルを指す MN のルーティング エントリを保持します。MN のバインディングが探索され、バインディングに保存された GRE 鍵がパケットのカプセル化に使用され、FA へトンネリングされます。
5. HA が再登録 RRQ を受信した場合、HA は GRE 鍵エクステンションを解析します。再登録が受け入れられると、HA は再登録 RRQ で受信したダウンストリーム キーを使用してバインディングをアップデートし、FA による使用のために生成されたアップストリーム キーとともに RRP を送り返します。
6. HA が有効な登録解除 RRQ と（存在する場合は）GRE 鍵エクステンションを受信した場合は、HA は以前に生成された GRE 鍵を含む RRP を送り返します。

冗長構成に関する注意：
冗長構成の場合でも、GRE CVSE 機能が使用できます。

その他の注意：
受信 RRQ（初期 / 更新 / 登録解除）の GRE 鍵の値がゼロ（0）の場合、

- リバース トンネリング ビット（T）がセットされていない場合でも、HA は GRE 鍵を生成します。
- RRQ で T ビットがセットされている場合、HA によって生成された鍵は、双方向に使用されます。
- GRE CVSE エクステンションが RRQ にある場合は、RRQ の G ビット ステータスに関わりなく、トンネル モードが GRE に設定されます。

非 VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）環境での GRE 鍵の設定

GRE トンネルの GRE 鍵に基づいて各セッションのデータ ストリームを特定するように Cisco Mobile Wireless HA 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(config)# ip mobile home-agent options`	IP Mobile Home Agent オプションをイネーブルにし、IP Mobile Home Agent オプション コンフィギュレーション サブモードを開始します。
ステップ 2	`Router(config-ipmobile-ha-options)#cvse gre-key`	CVSE からの GRE 鍵を使用して GRE トンネリングをイネーブルにします。システムにアクティブなバインディングがある場合は、このコマンドをイネーブルまたはディセーブルにできません。デフォルトの動作では、CVSE からの GRE 鍵を解析しません。

RFC 4917 のサポート

RFC 4917 は、Registration Replies メッセージまたは Registration Revocation メッセージに付加される Message String Extension を指定します。Message String Extension は、表示可能な通知をネットワークからユーザに提供するために端末に送信されます。エクステンションのテキストは、Access-Accept、Access-Reject、または Disconnect（RFC 3576）メッセージで送信される RADIUS Reply-Message アトリビュートを使用して、AAA サーバから入手できます。RADIUS Change of Authorization（COA）によって、Registration Reply メッセージ、または Registration Revocation メッセージの送信は発生しません。したがって、このメッセージはモバイル IP 拡張機能でサポートされません。

モバイル登録メッセージを表示するデバグ出力には、Registration Reply メッセージと Revocation メッセージが表示されます。

この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent message-string`	AAA サーバからユーザへのテキストの配布をイネーブルに、またはディセーブルにします。

次に、Message String エクステンションのサンプル設定を示します。

```
HA Config

ip mobile home-agent template Tunnel10 address 10.10.10.188
ip mobile home-agent template Tunnel10 address 10.10.10.203
ip mobile home-agent template Tunnel10 address 10.10.10.179
ip mobile home-agent binding-overwrite
ip mobile home-agent message-string
ip mobile home-agent accounting ha-acct
ip mobile virtual-network 2.0.0.0 255.0.0.0
ip mobile host nai @aricent.com address pool local mip-pool-1 virtual
network 2.0.0.0 255.0.0.0 aaa load-sa lifetime 3600
ip mobile secure mn-aaa spi 101 algorithm md5 mode ppp-chap-style

RADIUS Config

simulator radius subscriber 123
  framed address 18.18.0.1
  framed protocol ppp
  vsa cisco generic 1 string "mobileip:static-ip-pool=mip-pool-1"
  vsa cisco generic 1 string "mobileip:spi#0= spi 101 key ascii cisco"
  attribute 18 string "Welcome TO Cisco"

simulator radius subscriber 124
  framed address 18.18.0.1
  framed protocol ppp
  vsa cisco generic 1 string "mobileip:static-ip-pool=mip-pool-1"
  vsa cisco generic 1 string "mobileip:spi#0= spi 101 key ascii cisco"
  reply-message RFC4917 "HA-CHAP Failed"
```

CHAPTER 17

Home Agent のネットワーク管理、管理情報ベース（MIB）、および簡易ネットワーク管理プロトコル（SNMP）

この章では、Cisco Mobile Wireless Home Agent のさまざまなネットワーク管理について説明します。

この章は、次の内容で構成されています。

Cisco Mobile Wireless Home Agent の運用と管理

ここでは、Home Agent がサポートしている設定機能、統計情報、Management Information Base（MIB; 管理情報ベース）について説明します。各モバイル IP コマンドの詳細については、http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/1rfmobip.htm を参照してください。

Home Agent は Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）または Cisco Works for Mobile Wireless を使用して管理できます。

Cisco Mobile Wireless Home Agent には、次の設定パラメータがあります。

- ユーザ プロファイル（ローカル ユーザ）の管理
- IP プールのローカル設定
- 通信ノードとのセキュリティ アソシエーションの設定
- 入力/出力フィルタリングの設定
- モバイル バインディングのアップデートの設定
- ルーティング情報の設定

統計情報

Mobile Wireless Home Agent は次のパラメータに関してグローバルベースの統計情報を維持します。

- アドバタイズメント（受信および送信）
- 登録（要求および応答）
- 登録（受諾および拒否）
- バインディング
- バインディングのアップデート
- Gratuitous Address Resolution Protocol（ARP; アドレス解決プロトコル）およびプロキシ ARP
- ルート最適化バインディングのアップデート

Mobile Wireless Home Agent は次のパラメータに関して Foreign Agent（FA）-Home Agent（HA）トンネル単位の統計情報を維持します。

- トンネルの発信元および宛先 IP アドレス
- トンネル タイプ（IpinIP または Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化））
- 許可されたリバース トンネリング
- そのトンネルを使用しているユーザの数
- そのトンネル上の送信トラフィック（パケット数およびバイト数）
- そのトンネル上の受信トラフィック（パケット数およびバイト数）

Mobile Wireless Home Agent は次のパラメータに関して、ホスト単位のほか、Network Access Identifier（NAI; ネットワーク アクセス識別子）またはホーム IP アドレス別の統計情報を維持します。

- ライフタイム
- セッション時間
- そのホストへの送信トラフィック（パケット数およびバイト数）
- そのホストからリバース トンネルを通じて受信されたトラフィック（パケット数およびバイト数）

（注） 統計情報は、CLI を使用してクリアできます。MIB カウンタはクリアできません。

SNMP によるトンネル統計情報

HA Release 5.1 では、**show ip mobile tunnel** コマンドに、セッション ユーザの数およびパケット / バイト統計情報のほかに、IP アドレスのペア（HA-FA）形式でエントリを表示するための新しいコマンド オプションが導入されました。

たとえば、**show ip mobile tunnel brief** のようにコマンドを指定します。

また、CISCO-MOBILE-IP-MIB に新しい MIB テーブル "cmiHaRegTunnelStatsTable" が追加され、この新しく導入されたコマンド オプションで表示される情報が Stats テーブルの各エントリに含められます。

この機能は、IP/IP トンネルおよび GRE/IP トンネルに対してのみ適用できます。

次に、参照用の出力例を示します。

```
show ip mobile tunnel brief
Mobile Tunnels:
```

```
Total mobile ip tunnels 6
SrcAddr         DestAddr        Encap  Users Data Interval           PktRt In/Out
BitRt In/Out        Pkts In/Out        Bytes In/Out
86.6.6.30       10.109.1.82     IP/IP  2     5 minute                 0/0
0/0             0/0               0/0
86.6.6.30       10.109.1.83     IP/IP  1     5 minute                 0/0
0/0             0/0               0/0
86.6.6.30       10.109.1.81     IP/IP  2     5 minute                 0/0
0/0             0/0               0/0
86.6.6.6        10.109.1.62     IP/IP  2     5 minute                 0/0
0/0             0/0               0/0
86.6.6.6        10.109.1.63     IP/IP  1     5 minute                 0/0
0/0             0/0               0/0
86.6.6.6        10.109.1.61     IP/IP  2     5 minute                 0/0
0/0             0/0               0/0
```

SNMP、MIB、およびネットワーク管理

HA はプロトコル スイート RFC 1901 ～ RFC 1908 で規定された SNMPv2 を実装します。Home Agent は、『The Definitions of Managed Objects for IP Mobility Support UsingSMIv2, RFC 2006, October 1995』に定義されている MIB をサポートしています。Cisco MIB である CISCO- MOBILE-IP-MIB の追加により、管理機能が強化されています。そのほかに、『RADIUS Authentication Client MIB, RFC 2618, June 1999』に定義されている Remote Authentication Dial-In User Service（RADIUS）MIB もサポートしています。Cisco 7600 シリーズ プラットフォームでサポートされているすべての MIB のリストについては、http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml を参照してください。

MIB で維持されるセッション カウンタは、SNMP と Cisco IOS CLI のいずれを使用してもリセットできません。Home Agent CPU カウンタおよびメモリ使用率カウンタには、CISCO-PROCESS-MIB を使用してアクセスできます。

Release 3.0 には、Home Agent バージョンの MIB オブジェクトが追加されています。

SNMPv3 がサポートされています。

HA Release 5.0 における MIB の拡張

HA Release 5.0 では、CISCO-MOBILE-IP-MIB は、バインディング単位の変数として追加された Medium Access Control（MAC; メディア アクセス制御）アドレスを持ちます。RADIUS-CLIENT-AUTHENTICATION-MIB には、AAA アクセスのタイムアウトに関するエントリが含まれます。CISCO-RADIUS-MIB には、トラップが追加されています。新しい CISCO-SLB-DFP-MIB も追加されています。

MIB の詳細については、次の URL を参照してください。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

IP-LOCAL-POOL-MIB 用の CLI

Cisco Mobile Wireless Home Agent Release 3.0 では CISCO-IP-LOCAL-POOL-MIB が強化され、プールの利用率が上限または下限のしきい値に達すると、トラップが生成されます。下限および上限のしきい値を定義するのは、オブジェクト "cIpLocalPoolPercentAddrThldLo" と "cIpLocalPoolPercentAddrThldHi" です。

IP ローカル プール内の使用アドレスのパーセンテージが上限しきい値以上になると、"cilpPercentAddrUsedHiNotif" 通知が生成されます。いったん通知が生成されると、その通知は解除され、使用アドレスの数が "cIpLocalPoolPercentAddrThldLo " に指定された値を下回るまで生成されません。

IP ローカル プール内の使用アドレスのパーセンテージが下限しきい値未満になると、"cilpPercentAddrUsedLoNotif" 通知が生成されます。いったん通知が生成されると、その通知は解除され、使用アドレスの数が "cIpLocalPoolPercentAddrThldHi " に指定された値以上になるまで生成されません。

Cisco IOS 12.3(11)YX5 リリースでは、**ip local pool** コマンドに、上限および下限のしきい値を設定する新しい変数が実装されています。

このコマンドの構文は次のとおりです。

ip local pool {**default** | ***poolname***} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**threshold** *low-threshold high-threshold*]

low-threshold 引数は、プール利用率トラップを生成する下限のしきい値です。*high threshold* 引数はプール利用率トラップを生成する上限のしきい値です。

さらに、cilpPercentAddrUsedHiNotif 通知に次の 2 つの変数バインドが追加されています。

- cIpLocalPoolChildIndex：IP プールの名前
- cIpLocalPoolPercentAddrThldHi：IP ローカル プールの上限しきい値のパーセンテージ値

cilpPercentAddrUsedLoNotif 通知にも次の 2 つの変数バインドが追加されています。

- cIpLocalPoolChildIndex：IP プールの名前
- cIpLocalPoolPercentAddrThldLo：IP ローカル プールの下限しきい値のパーセンテージ値

（注）　CISCO-IP-LOCAL-MIB ファイルは、SNMP SMIv2 標準に従って変更されていません。

制約事項

IP ローカル プールしきい値トラップに次の制限が適用されます。

- IP ローカル プール名の長さは、ASCII 文字で最大 240 文字です（使用するパラメータによって異なります）。
- SNMP トラップ名の長さは最大 48 文字に制限されます。SNMP MIB がサポートする最大文字数が 48 文字であるためです。
- プール名が 48 文字を超えていると、トラップは生成されません。

IP オーバーラッピング アドレス プールの設定方法

ここでは、次の手順を説明します。

- ローカル プール グループの設定および確認

ローカル プール グループの設定および確認

ここでは、ローカル プール グループの設定およびその確認に必要な手順を説明します。

手順の概要

1. enable
2. configure terminal
3. **ip local pool** {**default** | ***poolname***} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**threshold** ***low-threshold high-threshold***]
4. **show ip local pool** [*poolname* | [**group** *group-name*]]

手順の詳細

	コマンドまたは処理	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]] [**group** *group-name*] [**cache-size** *size*] [**threshold** ***low-threshold high-threshold***] 例： `Router(config)# ip local pool XYZPool 100.1.1.1 100.1.1.10 group MWG cache-size 50 threshold 50 90`	ローカル IP アドレス プールのグループを設定し、このグループに名前とキャッシュ サイズを指定します。 *low-threshold* は、プール利用率トラップ生成用の下限しきい値です。この値は、*high threshold* の値以下にする必要があります。 *high threshold* は、プール利用率トラップ生成用の上限しきい値です。この値は、*lowthreshold* よりも大きい値にする必要があります。
ステップ 4	**show ip local pool** [*poolname* | [**group** *group-name*]] 例： `Router(config)# show ip local pool group testgroup testpool`	定義済みの IP アドレス プールすべての統計情報を表示します。

条件付きデバッグ

HA は、NAI に基づく条件付きデバッグと Mobile Node（MN; モバイル ノード）のホーム アドレスに基づく条件付きデバッグをサポートしています。条件付きデバッグをサポートしているのは、Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）とモバイル IP のコンポーネントだけです。

CLI を使用して、すべてのユーザまたは NAI で識別される特定ユーザのアクティビティをトレースできます。特定ユーザのアクティビティのモニタリング（条件付きデバッグ）では、モバイル IP メッセージおよび RADIUS メッセージに関連したユーザ アクティビティが表示されます。

Release 3.0 から、各デバッグ ステートメントとともに、条件（username/IMSI）も表示されるようになりました。これは、デバッグ ステートメントをその条件と照合するのに役立ちます。この機能をイネーブルにするには、次のコマンドを使用します。

ip mobile home-agent debug include username

条件付きデバッグでサポートされているモバイル IP デバッグは次のとおりです。

- **debug ip mobile**
- **debug ip mobile host**

条件付きデバッグでサポートされている AAA は、次のとおりです。

- **debug aaa authentication**
- **debug aaa authorization**
- **debug aaa accounting**
- **debug aaa ipc**
- **debug aaa attr**
- **debug aaa id**
- **debug aaa subsys**

条件付きデバッグでサポートされている RADIUS デバッグは次のとおりです。

- **debug radius**
- **debug radius accounting**
- **debug radius authentication**
- **debug radius retransmit**
- **debug radius failover**
- **debug radius brief**

HA のモニタリングとメンテナンス

HA のモニタリングとメンテナンスを行うには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **clear ip mobile binding**	モビリティ バインディングを削除します。
Router# **clear ip mobile host-counters**	各モバイル ステーション固有のモビリティ カウンタをクリアします。
Router#**clear ip mobile secure**	リモート セキュリティ アソシエーションをクリアし、取得します。
Router#**clear ip mobile traffic**	IP モバイル トラフィック カウンタをクリアします。
Router# **debug ip mobile advertise**	アドバタイズメント情報を表示します。
Router# **debug aaa pod**	AAA サブシステム レベルで処理する Radius Disconnect メッセージのデバッグ情報を表示します。

コマンド	目的
Router# **debug ip mobile** ? **advertise** Mobility Agent advertisements **dfp** DFP Agent **host** Mobile host activities **ipc** Distributed HA Mobile activities **local-area** Local area mobility **mib** Mobile MIB Events **redundancy** MobileIP redundancy debugging **router** Mobile router activities **udp-tunneling** UDP Tunneling **vpdn-tunnel** VPDN tunnel	IP モビリティ アクティビティを表示します。次に、debug ip mobile コマンドのさまざまなオプションをすべて示します。 • **advertise** : モビリティ エージェント アドバタイズメント • **dfp** : Dynamic Feedback Protocol（DFP）エージェント • **host** : モバイル ホスト アクティビティ • **ipc** : 分散 HA モバイル アクティビティ • **local-area** : ローカル エリア モビリティ • **mib** : モバイル MIB イベント • **redundancy** : MobileIP 冗長性デバッグ • **router** : モバイル ルータ アクティビティ • **udp-tunneling** : User Datagram Protocol（UDP; ユーザ データグラム プロトコル）トンネリング • **vpdn-tunnel** : Virtual Packet Data Network（VPDN; 仮想パケット データ ネットワーク）トンネル
Router# **debug ip mobile host mac**	モビリティ イベント情報を表示します。HA Release 5.0 で、新しいオプションが導入されました。**mac** キーワードは、MAC アドレスで識別された MN を表示します。
Router# **debug ip mobile redundancy**	IP モビリティ イベントを表示します。
Router# **debug radius**	RADIUS に関連した情報を表示します。
Router#**debug tacacs**	Terminal Access Controller Access Control System（TACACS）に関連した情報を表示します。
Router# **show ip mobile binding**	モビリティ バインディング テーブルを表示します。
Router# **show ip mobile binding vrf**	VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）がイネーブルになっている HA のすべてのバインディングを表示します。
Router#**show ip mobile binding vrf realm**	VRF がイネーブルになっているレルムのすべてのバインディングを表示します。
Router#**show ip mobile globals**	モバイル エージェントのグローバル情報を表示します。
Router# **show ip mobile host**	モバイル ステーションのカウンタおよび情報を表示します。
Router# **show ip mobile proxy**	プロキシ モバイル IP ホストに関する情報を表示します。
Router#**show ip mobile secure**	モバイル IP のモビリティ セキュリティ アソシエーションを表示します。

コマンド	目的
Router#**show ip mobile traffic**	Home Agent のプロトコル カウンタを表示します。単一の IP の場合、このコマンドはすべての冗長性バインディング カウンタを 0 と表示します。これらのカウンタ用に、新しいコマンドである **show ip mobile redundancy statistics** が導入されました。
Router#**show ip mobile redundancy statistics**	HA の冗長性ステータスを表示します。
Router#**show ip mobile tunnel**	モバイル IP トンネルに関する情報を表示します。
Router#**show ip mobile violation**	セキュリティ違反に関する情報を表示します。
Router#**show ip route vrf**	VRF に対応するルーティング テーブル情報を表示します。

APPENDIX A

用語集

3GPP2：3rd Generation Partnership Project 2（第 3 世代パートナーシップ プロジェクト 2）
AAA：Authentication, Authorization and Accounting（認証、認可、アカウンティング）
AH：Authentication Header（認証ヘッダー）
APN：Access Point Name（アクセス ポイント ネーム）
BG：Border Gateway（ボーダ ゲートウェイ）
BSC：Base Station Controller（ベース ステーション コントローラ）
BSS：Base Station Subsystem（ベース ステーション サブシステム）
BSC：Base Transceiver Station（ベース トランシーバ ステーション）
CHAP：Challenge Handshake Authentication Protocol（チャレンジ ハンドシェーク認証プロトコル）
CoA：Care-of Address（気付アドレス）
DSCP：Differentiated Services Code Point（DiffServ コード ポイント）
DNS：Domain Name Server（ドメイン ネーム サーバ）
ESN：Electronic Serial Number（電子シリアル番号）
FA：Foreign Agent（外部エージェント）
FAC（FA-CHAP）：Foreign Agent Challenge（外部エージェント チャレンジ）
HA：Home Agent
HDLC：High-Level Data Link Control（ハイレベル データ リンク コントロール）
HLR：Home Location Register（ホーム ロケーション レジスタ）
HSRP：Hot Standby Router Protocol（ホット スタンバイ ルータ プロトコル）
IP：Internet Protocol（インターネット プロトコル）
IPCP：IP Control Protocol（IP コントロール プロトコル）
IS835：
ISP：Internet Service Provider（インターネット サービス プロバイダー）
ITU：International Telecommunications Union（国際電気通信連合）
L2_Relay：Layer Two Relay Protocol （レイヤ 2 リレー プロトコル）
L2TP：Layer 2 Tunneling Protocol（レイヤ 2 トンネリング プロトコル）
LCP：Link Control Protocol（リンク コントロール プロトコル）
LNS：L2TP Network Server（L2TP ネットワーク サーバ）

MAC：Medium Access Control（メディア アクセス制御）
MEID：Mobile Equipment Identifier（移動体識別番号）
MIP：Mobile IP（モバイル IP）
MS：Mobile Station（モバイル ステーション）（= TE + MT）
MT：Mobile Termination（モバイル ターミネーション）
NAI：Network Access Identifier（ネットワーク アクセス識別子）
NAS：Network Access Server（ネットワーク アクセス サーバ）
P-MIP：Proxy-Mobile IP（プロキシ モバイル IP）
PAP：Password Authentication Protocol（パスワード認証プロトコル）
PCF：Packet Control Function（パケット制御機能）
PDN：Packet Data Network（パケット データ ネットワーク）
PDSN：Packet Data Serving Node（パケット データ サービス ノード）
PPP：Point-to-Point Protocol（ポイントツーポイント プロトコル）
PPTP：Point-to-Point Tunneling Protocol（ポイントツーポイント トンネリング プロトコル）
SLA：Service Level Agreement（サービス レベル契約）
TE：Terminal Equipment（ターミナル装置）
TID：Tunnel Identifier（トンネル識別子）
VPDN：Virtual Packet Data Network（仮想パケット データ ネットワーク）