Cisco Mobile Wireless Home Agent 機能ガイド

Cisco IOS Release 12.4(15)XM
Cisco Mobile Wireless Home Agent 4.0

30 January, 2008

Text Part Number: CMWHA-12415-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。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。

CONTENTS

CHAPTER 1

Cisco Mobile Wireless Home Agent の概要

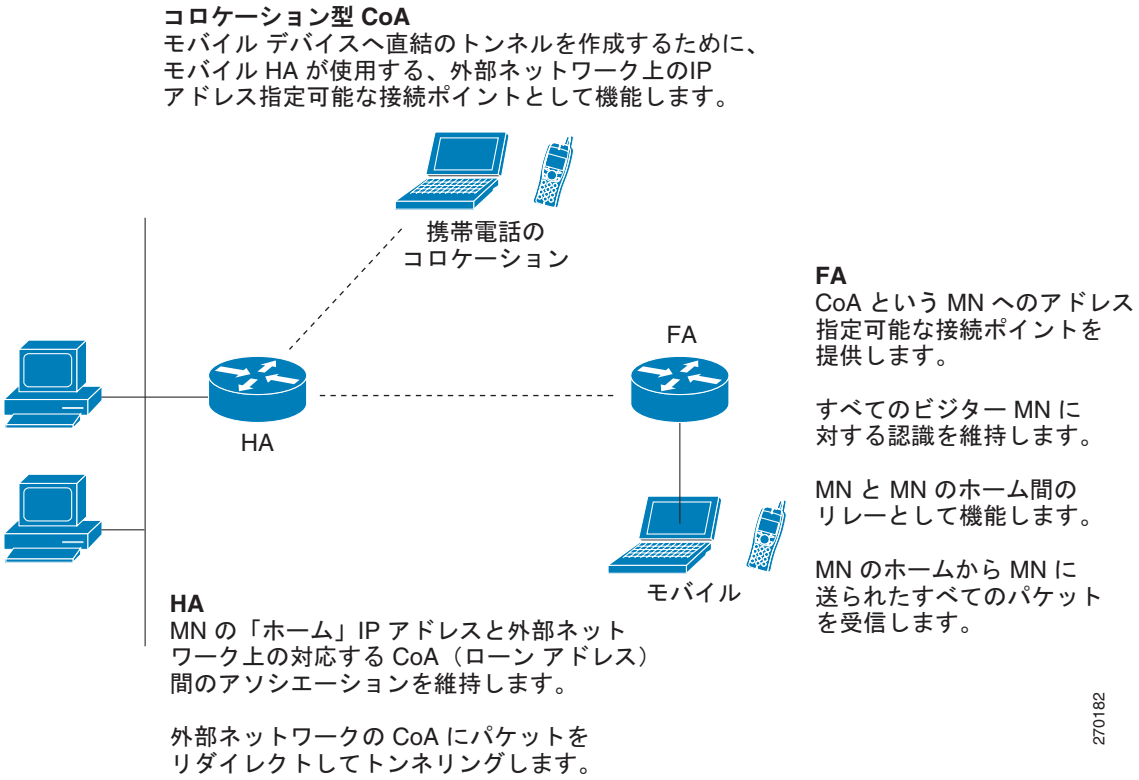
この章では、一般的なモバイル IP パケット データ システムにおける機能要素、このソリューションをサポートする販売中のシスコ製品、さらに Cisco IOS Mobile Wireless Home Agent ソフトウェアでの実装について説明します。

この章の構成は、次のとおりです。

機能の概要

Cisco Mobile Wireless Home Agent は、加入者のアンカー 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、QoS（Quality of Service）機能を提供して、モバイル ユーザ エクスペリエンスを最適化します。Cisco Mobile Wireless Home Agent（HA）は、Foregin Agent（FA; 外部エージェント）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、FA を通じて、またはコロケーション モード（CCOA）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 FA 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 FA 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 DHCP 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、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。

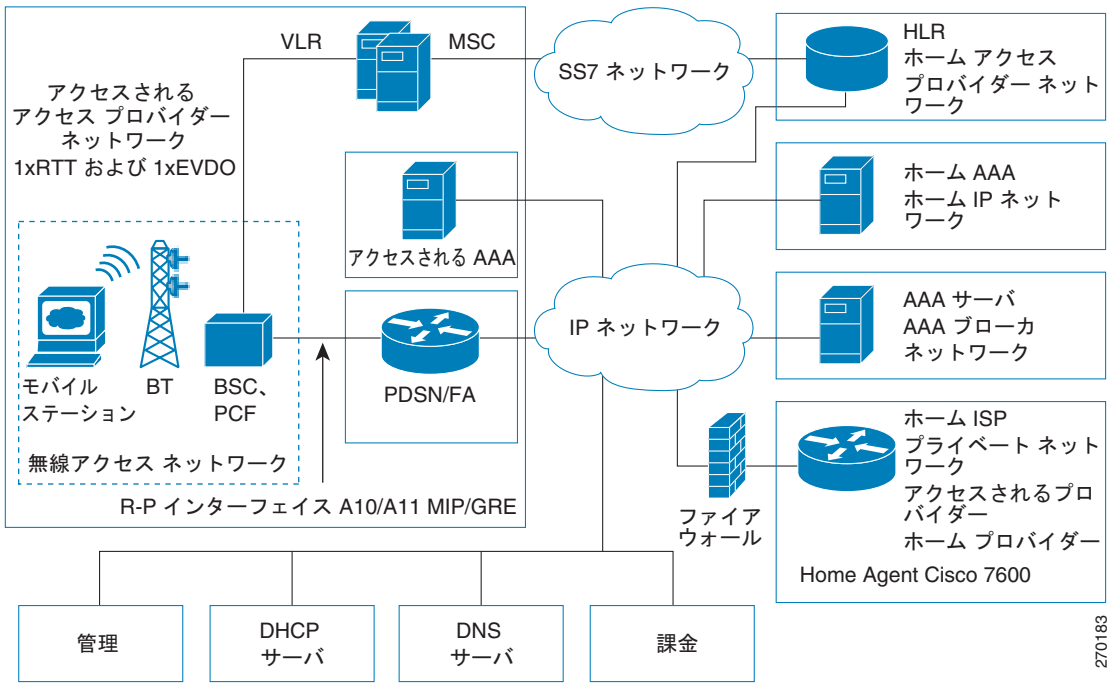
Cisco Mobile Wireless Home Agent は、モバイル端末のアンカー ポイントであり、そこからモバイル端末にモバイル サービスまたはプロキシ モバイル サービスが提供されます。端末に送信されたトラフィックは、HA を使用してルーティングされます。リバース トンネリングによって、端末からのトラフィックも Cisco Mobile Wireless Home Agent 経由でルーティングされます。HA 冗長性、ロード バランシングなどの独自機能が、高度な可用性と信頼性をもたらし、アカウンティングの整合性を維持しながら、地理的分散を可能にします。もう 1 つの独自機能である 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。

CMDA 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 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、FA 機能を備えた Cisco Packet Data Serving Node（PDSN）、CDMA2000 ベースの Cisco Mobile Wireless HA、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 Mobiel Wireless Home Agent を Cisco PDSN FA 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 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 HA 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 BTS 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 BSC 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 RAN-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 SAMI プラットフォーム上でギガ イーサネット（GE）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 FE 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 FA 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/FA 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。

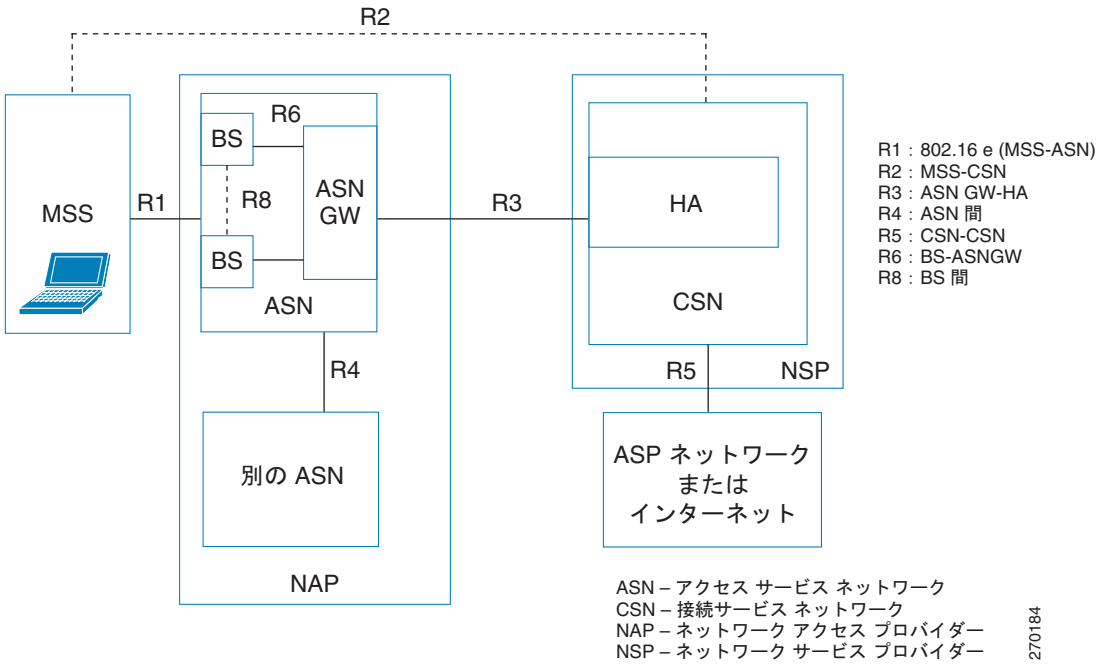
HA は、モバイル端末のアンカー ポイントであり、そこからモバイル端末にモバイル IP サービスまたはプロキシ モバイル IP サービスが提供されます。トラフィックは HA を介してルーティングされ、HA もプロキシ ARP サービスを提供します。リバース トンネリングの場合は、端末からのトラフィックも HA 経由でルーティングされます。

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。

WiMAX 環境における Cisco Mobile Wireless Home Agent

WiMAX（Worldwide Interoperability for Microwave Access）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、モバイル加入者ステーション（MSS）、アクセス サービス ネットワーク（ASN）、およびコア サービス ネットワーク（CSN）です。図 1-3 に、ASN の分解図を示します。ネットワーク リファレンス モデル（NRM）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



ASN

アクセス サービス ネットワーク（ASN）は、WiMAX 加入者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、複数の接続サービス ネットワーク（CSN）間で共有することもあります。

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、加入者識別、およびポリシー実施を実現するための土台になります。シスコでは、シスコの総合的な IP Next Generation Netowork（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（ATM、フレームリレー）、SPA（共有ポート アダプタ）および 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。

プラットフォームの利点

- HA SAMI サービス モジュールは、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

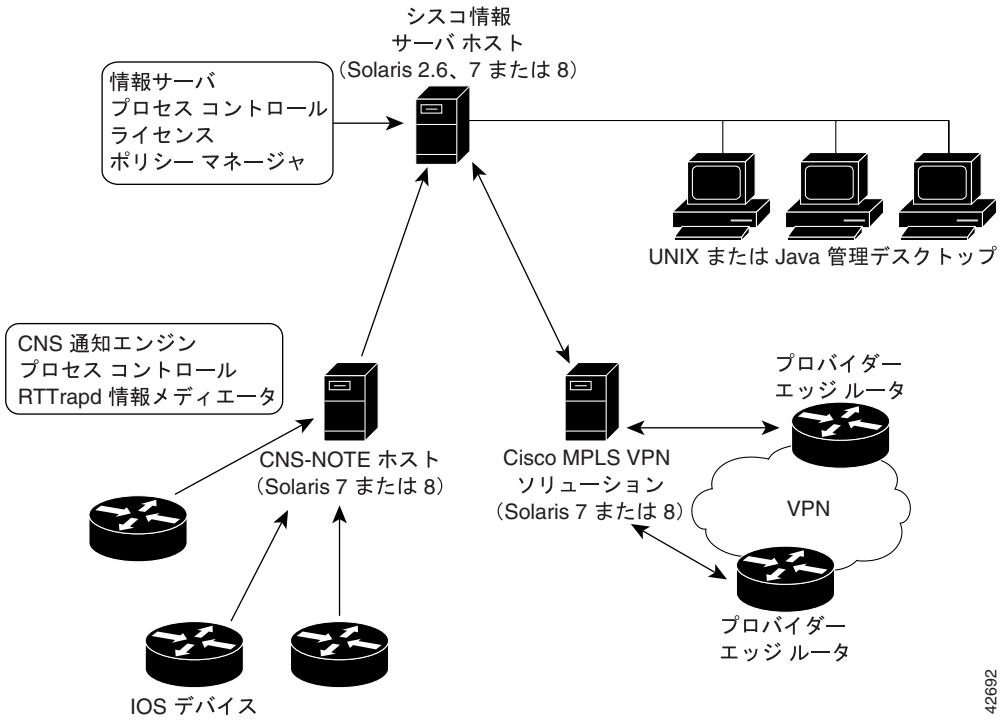
CDMA2000 ネットワークのコンテキストにおいて、Cisco HA は 2 種類のパケット データ サービスをサポートします。モバイル IP サービスおよびプロキシ モバイル IP サービスです。Cisco HA にとって、この 2 種類のサービスは同じです。

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 1-4 に、モバイル IP 環境における Cisco HA の配置を示します。

図 1-4　CDMA ネットワーク — モバイル IP 環境



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（すなわち PDSN）間に PPP リンク、FA と HA 間に IP-in-IP または GRE 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 CoA 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。FA 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 CoA として使用されます。Cisco HA の場合、CoA は常に FA 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 CoA 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 CoA 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、ホーム エージェントでモバイル 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 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（FA 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登録要求（RRQ）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登録応答（RRP）を送信します。
5. FA が 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、すなわち 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 MIP 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 CMWHA-12415-J の新機能

ここでは、Cisco IOS Release CMWHA-12415-J 対応の Home Agent Release 4.0 で追加または変更された機能について説明します。

- SAMI サポート（p.2-1）

  Cisco HA 4.0 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 SLB 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。

（注）　Cisco Mobile Wireless Home Agent は、Cisco 7200 または Cisco 6500 シリーズ ルータ プラットフォームではサポートされなくなりました。

- ホットライニング（p.14-2）の機能拡張
- HA の QoS（p.13-1）の機能拡張
- Framed-Pool 基準（p.15-15）
- WiMAX AAA アトリビュート（p.15-18）
- アップストリーム パスでの MS トラフィック リダイレクション（p.15-4）
- 外部エージェント別アクセス タイプ サポート（p.15-4）
- 最大バインディングのサポート（p.15-6）
- コール アドミッション制御（CAC）のサポート（p.15-6）
- MIP/LAC（PPP 再生成）のサポート（p.15-7）
- ローカル プールのプライオリティ メトリック（p.15-16）
- Mobile IPv4 ホスト設定エクステンション（RFC4332）（p.15-17）

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。

- 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 ― 暫定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
  - 地理的冗長性
  - 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 ACL
- IP 到達可能性
- DNS サーバのアドレスの割り当て
- SNMP、MIB、およびネットワーク管理のモバイル 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 レジストレーションの失効（p.7-2）
- HA サーバ ロード バランシング（p.6-2）
- HA のアカウンティング（p.11-1）
- MN-FA Challenge Extension（MFCE）による HA-CHAP の省略（p.4-3）
- HA での VRF サポート（p.12-2）
- RADIUS 切断（p.7-4）
- 条件付きデバッグ（p.16-5）
- ホーム アドレス割り当て（p.3-2）
- HA の冗長性（p.5-1）
- 仮想ネットワーク（p.5-7）
- ODAP（p.3-6）
- モバイル IP の IPSec（p.10-1）
- トンネル インターフェイスでの ACL のサポート（p.15-1）
- AAA アトリビュート MN-HA-SPI および MN-HA SHARED KEY のサポート（p.15-3）
- 3 DES 暗号化（p.10-1）
- ユーザ プロファイル（p.15-3）
- モビリティ バインディング アソシエーション（p.15-3）
- ユーザ認証および認可（p.4-2）
- HA バインディングのアップデート（p.15-5）
- ユーザ単位パケット フィルタリング（p.9-1）
- セキュリティ（p.10-1）

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 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）
- 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。
- MS 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、対応ノード（CN）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。
- CoA 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有効期間を含めた、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 登録継続時間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加入者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。

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

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。

この章の構成は、次のとおりです。

サポート対象プラットフォーム

Cisco Home Agent（HA）は 7600 シリーズ ルータに搭載する、新しい Cisco Service and 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 and 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。

たとえば、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 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
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 /SLB	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 Foreign Agent（FA; 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 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。既存のモバイル加入者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 R4.0 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 プリエンプト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、QoS（Quality of Service）、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を含め、R4.0 と同じです。
- 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

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 2	`Router(config)# 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。
ステップ 3	`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 サーバ 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。

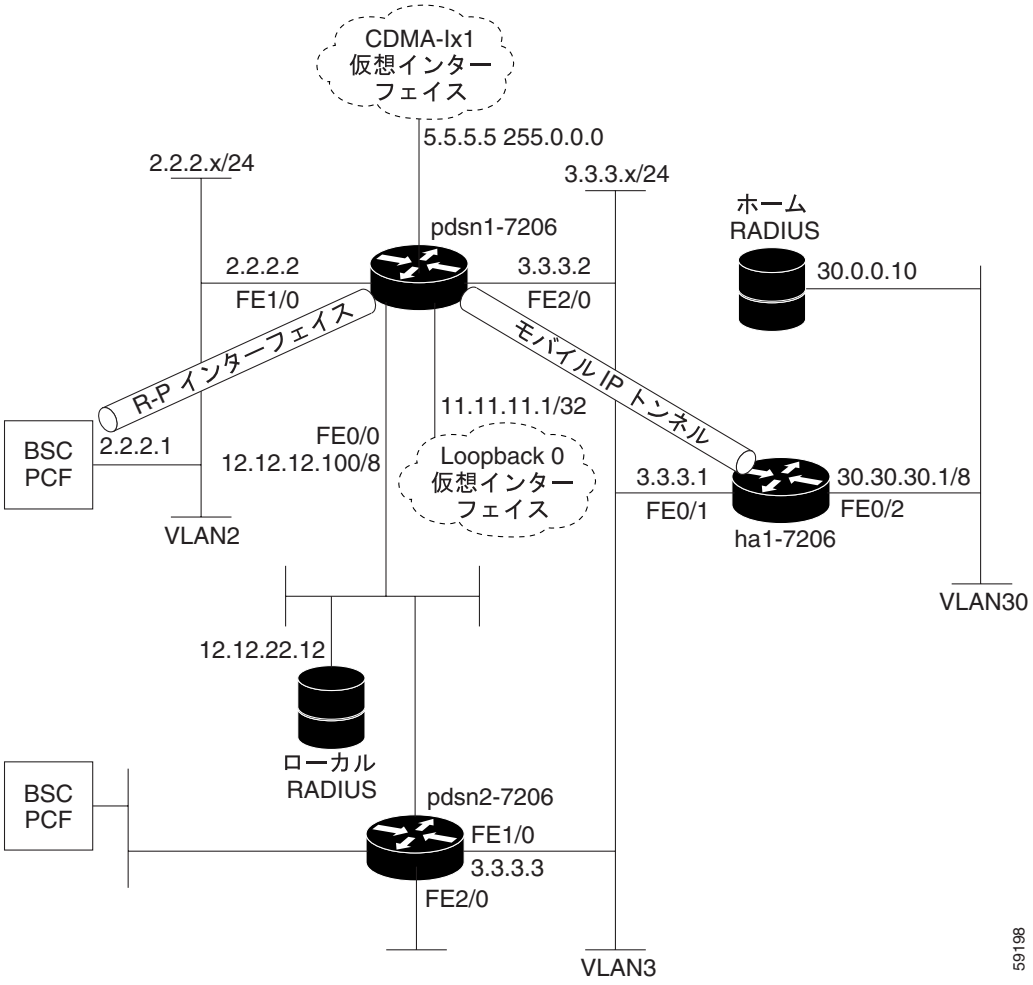
HA 環境で RADIUS を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

	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 2-1 およびそれに続く情報は、Cisco HA の配置と設定の例です。

図 2-1　HA — ネットワーク マップ



例 2-1　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ません。同じ NAI に複数のフローが確立された場合、フローごとに異なる IP アドレスが割り当てられます。したがって、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 アドレスに対して複数のフローを維持するために使用するためのものだからです。

セキュリティ

HA は IS-835-B で必須の IPSec、IKE、IPSec AH（認証ヘッダー）、および IP Encapsulating Security Payload（ESP）をサポートします。HA はコントロールまたはユーザ トラフィック用のセキュリティを別個にサポートすることはしません。両方とも保護するか、両方とも保護しないかのどちらかです。

HA は IS-835-B で定義されているダイナミックに割り当てられた鍵または共有秘密をサポートしません。

サポート対象の規格、MIB、および RFC

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文）、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（Mobile 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 HSRP［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します。
- Radius MIB ― RADIUS 認証クライアント MIB（RFC 2618、1999 年 1 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、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するご意見の送信方法、セキュリティ ガイドライン、さらに推奨エイリアス、一般的なシスコ製品マニュアルについては、毎月公開される『*What's New in Cisco Product Documentation*』を参照してください。ここには、新規および改訂されたシスコ技術マニュアルもすべて記載されています。次の URL にアクセスしてください。

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

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register/

CHAPTER 3

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。

この章の構成は、次のとおりです。

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。

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（認証、認可、アカウンティング）サーバまたは 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、MN 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の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かぎり、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、設定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
```

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かぎり、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”

ODAP

SAMI カードを使用して高密度 HA を実現する場合は、中央のソースから IP アドレスを割り当てることを選択できます。Cisco IOS ODAP（オンデマンド アドレス プール）がこの機能を提供します。ODAP によって HA の設定が簡素化されるので、HA コンフィギュレーションごとにローカル IP アドレス プールを設定する必要はありません。

ODAP を使用すると、大型アドレス プールの管理を中央に集中させ、大型ネットワークの設定を簡素化できます。ODAP 機能は次の 2 つのコンポーネントからなります。

- DHCP ODAP サブネット アロケーション サーバ
- ODAP マネージャ（各 HA に配置）

DHCP ODAP サブネット アロケーション サーバは、サブネット単位で IP アドレス スペースを作成して割り当てる場合に設定します。これらのプールのサイズは設定可能であり、これらのサブネットは HA 上の ODAP マネージャにリースされます。また、ODAP マネージャ が割り当てるためのサブネット アロケーション プールを提供します。DHCP ODAP サブネット アロケーション サーバ機能は、SAMI 上の HA インスタンスの 1 つに配置できます。DHCP ODAP サブネット アロケーション サーバ機能を別の外部 Cisco IOS ルータまたは外部 Cisco アクセス レジスタに配置することもできます。

ODAP マネージャ機能は、各 HA イメージに配置します。HA はローカル IP プールではなく、ODAP マネージャ機能を使用します。ODAP マネージャは、IP アドレスの需要と各 HA のサブネット アベイラビリティに基づいて、ODAP サブネット アロケーション サーバからサブネットをリースします。HA 上の ODAP マネージャは、これらのサブネットからクライアントにアドレスを割り当て、アドレスの使用状況に応じてサブネット プールのサイズをダイナミックに増減します。HA ODAP マネージャがサブネットをリースするときには、HA が受信するサブネットごとに、集約ルートが自動的に追加されます。このルートはスタティック ルートであり、ヌル インターフェイスに追加されます。

HA 上の ODAP マネージャがサブネットを割り当てると、ODAP サブネット アロケーション サーバがサブネット バインディングを作成します。このバインディングは、ODAP マネージャがアドレス スペースを必要とする間、DHCP データベースに保管されます。バインディングが破棄されて、サブネットがサブネット プールに返されるのは、アドレス スペースの使用率が下がり、HA ODAP マネージャがサブネットを解放するときだけです。

DHCP ODAP サブネット アロケーション サーバには、拡張 DHCP 機能があります。この機能は、単一の IP アドレスを返す代わりに、アドレスのサブネットを返します。ODAP マネージャは、HA 上でこの IP アドレス プールを管理します。この機能は、ルーティング プロトコルにとってより効率的なルート集約を行います。

ODAP ベースのアドレス割り当ての設定

HA が ODAP プールをサポートできるようにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile host` *nai* `address pool dhcp-pool` *odap poolname*	HA が ODAP アドレス プールをサポートできるようにします。

例を示します。

```
Router (config)#ip mobile host nai @ispbar2.com address pool dhcp-pool ha-dhcp-pool
```

ODAP の制約事項

ODAP 機能の制約事項は、次のとおりです。

- ピアツーピアの冗長性を使用する ODAP はサポートされません。
- ODAP サーバの最小サブネット リース時間は 10 分にする必要があります。
- rf-interdev サポートを指定したプリエンプトは機能しません。

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みなされます。
- 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 番め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 番め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 番め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みなされます。

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、別々のケースとみなされます。

設定例

ODAP 冗長設定

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
!
redundancy inter-device
 scheme standby cisco
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 500
    local-ip 10.0.0.2
   remote-port 500
    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
!
ip dhcp ping packet 0
ip dhcp pool ha-dhcp-pool
   origin dhcp subnet size initial /30 autogrow /30
ip subnet-zero
ip cef
!
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 min 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 cisco
ip mobile virtual-network 33.0.0.0 255.0.0.0
ip mobile host nai user14@cisco.com address pool dhcp-pool ha-dhcp-pool
virtual-network 10.0.0.0 255.0.0.0 aaa
```

```
ip mobile secure home-agent 10.0.0.3 spi 100 key ascii redundancy
algorithm md5 mode
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
```

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
!
redundancy inter-device
 scheme standby cisco
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 500
    local-ip 10.0.0.3
   remote-port 500
    remote-ip 10.0.0.2
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 dhcp pool ha-dhcp-pool
   origin dhcp subnet size initial /30 autogrow /30
ip subnet-zero
ip cef
!
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 150.2.1.7 255.255.0.0
 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 cisco
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user14@cisco.com address pool dhcp-pool ha-dhcp-pool
virtual-network 10.0.0.0 255.0.0.0 aaa
ip mobile secure home-agent 10.0.0.2 spi 100 key ascii redundancy
algorithm md5 mode
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
```

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 cisco
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 cisco
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 4

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。

この章の構成は、次のとおりです。

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。外部エージェント（FA）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 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加入者を認可するメカニズムがあります。これには「加入者の認可」という機能を使用します。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_chapter09186a0080455cf0.html#wp1056463

（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、モバイル加入者を認可することはありません。

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 4-1 の RADIUS アトリビュートをサポートします。

表 4-1　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	可否	
						アクセス要求	アクセス受諾
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
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

表 4-1　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	可否	
						アクセス要求	アクセス受諾
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、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 5

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。

この章の具体的な内容は、次のとおりです。

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。

次の機能は HA 冗長性ではサポートされません。

- HA のホットラインのサポート
- ODAP/DHCP およびローカル プール アドレッシング スキームは、ピア / ピア冗長性でサポートされません。

モバイル IP レジストレーション プロセス中、HA は、MN 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 SAMI カードに設定されます。

HA 冗長性の機能は、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。

地理的冗長性

冗長ペアの HA は、HA ペアの間の LAN/VLAN ではなく、VPN ソリューション（MPLS に基づいたものなど）を使用して、別々の場所に配置できます。このような配置では、ネットワークで正しいルーティング ロジックを実行し、トラフィックをペアの HA の 1 つにルーティングする必要があります。ネットワークに障害が発生した場合、このような配置で両方の HA は HSRP アクティブ ステートに移行します。HA 冗長性機能は、最小限のバインディングの損失でこの障害から正常に回復します。次のシナリオで障害回復プロセスについて説明します。

1. HA1（高プライオリティ）および HA2（低プライオリティ）は WAN リンク上で、冗長モードで展開されます。HSRP は WAN リンク上の HA の間で動作します。
2. HA1 はアクティブで HA2 はスタンバイです。
3. ネットワーク障害によって HA1 への WAN 接続が切断されると、HA1 と HA2 の間の HSRP リンクが失われます。
4. HA2 は hello パケットを受信しませんが、アクティブに移行します。同じ理由により、HA1 もアクティブのままです（ボックス自体は機能します）。この機能がイネーブルであると、HA1 と HA2 両方ともプライオリティが下がります。
5. モバイル トラフィックおよびシグナリング メッセージは HA2 にルーティングされます。それに応じて HA2 はバインディング テーブルをアップデートし、機能がイネーブルならば、プライオリティを元の値に増やします。ただし、HA2 の変更された HA ステート情報は HA1 と同期化されません（到達不能）。
6. ネットワーク障害が修正されると、hello パケットが HA1 と HA2 の間で交換されます。
7. この機能を使用しないと、HA1 はアクティブのままで、HA2 はスタンバイに移行し、ステップ番号 5 の HA2 で作成された最新のステート情報が失われます。この機能がイネーブルならば、HA1 はスタンバイに移行し、HA2 はアクティブのままです。したがって、HA2 の最新情報は HA1 に同期化されます。ステート情報が複製されると、HA1 は通常のプライオリティに戻ります。これにより、HA1 はアクティブになり HA2 はスタンバイになります。

上記のように、ネットワーク障害が修正されると、最新のステート情報が維持されます。この機能をイネーブルにするには、次のコマンドを HA で設定する必要があります。

track *tracking object id* **application home-agent**

このコマンドは、HA ステートを追跡するトラッキング オブジェクトを作成します。

standby track *tracking object id* **decrement** *priority*

このコマンドは、上記の障害シナリオのステップ番号 4 で必要なプライオリティを下げます。

（注） プリエンプトが設定されている場合、*priority* 値はアクティブおよびスタンバイ HA のプライオリティの差よりも大きい必要があります。

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 に冗長性に提供します。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 RRQ 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 がレジストレーション要求を送信する HA インターフェイスと、反対に HA がレジストレーション要求を受信する 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。

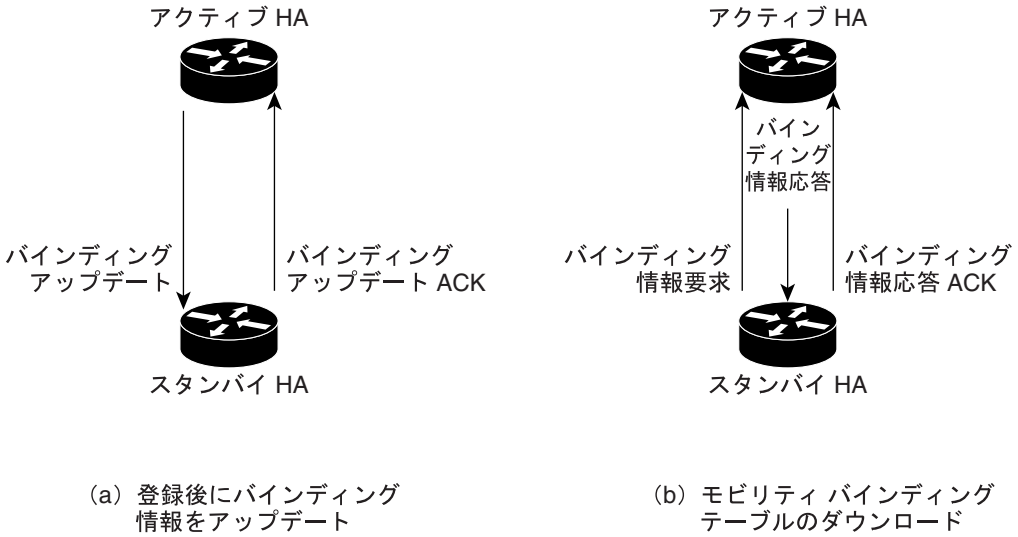
- MN には、MN と同じサブネット上にない HA インターフェイス（HA IP アドレス）があります。
- MN は、MN と同じサブネット上に HA インターフェイスを配置する必要があります。すなわち、HA と MN は同じホーム ネットワーク上にいなければなりません。

物理ネットワークの MN の場合、アクティブ HA は MN からのレジストレーション要求を受け入れ、バインディング アップデートをスタンバイ HA を送信します。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 からのレジストレーション要求を処理し、モビリティ バインディング テーブルをピア HA に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 5-1 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 5-1　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



（a）登録後にバインディング情報をアップデート

（b）モビリティ バインディング テーブルのダウンロード

（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 5-2 および図 5-3 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 つのみで、スタンバイ ステートである HA が 1 つのみであっても、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 5-2　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

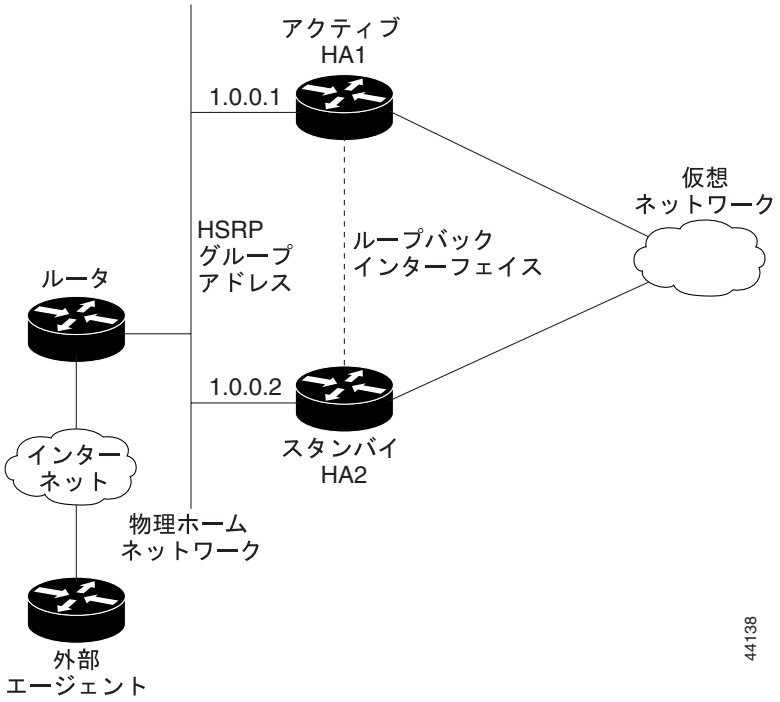
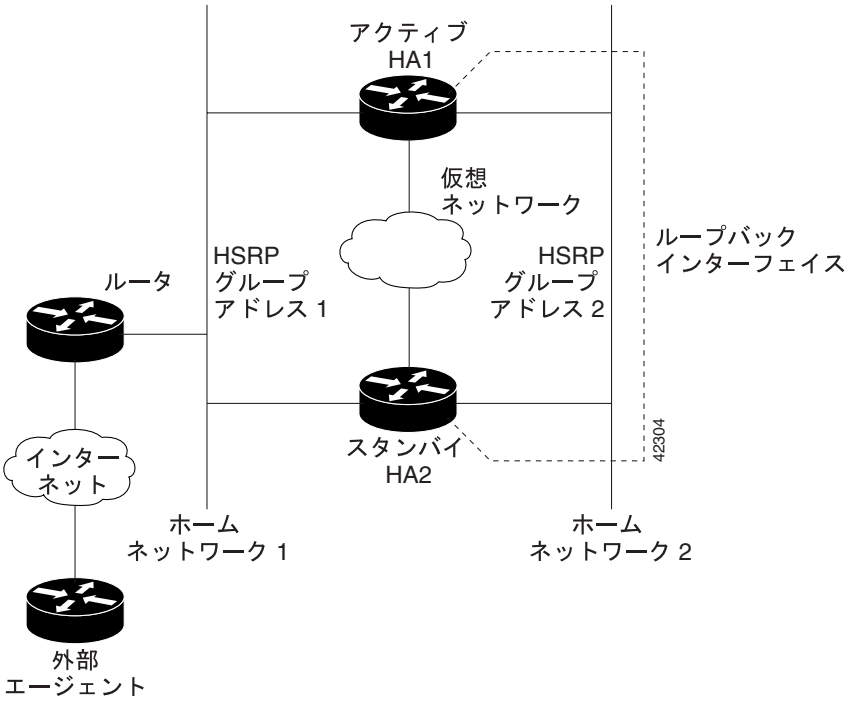


図 5-3　複数の物理ネットワーク（ピア HA/ ピア HA）を使用した仮想ネットワークのサポート



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 デスクリプション 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みなされ、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 1.1.1.250
ip local pool pool1 10.1.2.1 1.1.2.250

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、新しいレジストレーション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 番め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 プールを作成する例を示します。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 番めのプール（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

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*]] または 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、あと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、プリエンプトが設定されます。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ほうのタイマーがタイムアウトすると、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** *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。
ステップ 4	Router(config)#**ip mobile secure home-agent** *address* **spi** *spi* **key hex** *string*	ピア ルータの間に HA セキュリティ アソシエーションを設定します。アクティブ HA で設定されている場合、IP アドレス引数はスタンバイ HA の引数です。スタンバイ HA に設定されている場合、IP アドレス *address* 引数はアクティブ ルータの引数になります。セキュリティ アソシエーションはスタンバイ グループのすべての HA の間で設定する必要があることに注意してください。

地理的冗長性の設定

地理的冗長性を HA で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)# track tracking object id application home-agent`	HA ステートを追跡するトラッキング オブジェクトを作成します。
ステップ 2	`Router(config)# standby track tracking object id decrement priority`	障害シナリオで必要な HA のプライオリティを低くできます。

1 つの物理ネットワークを使用した仮想ネットワークの HA 冗長性のイネーブル化

仮想ネットワークおよび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)#ip mobile home-agent address address`
	または
	`Router(config)#ip mobile home-agent`
		グローバル HA アドレスを定義します。この設定では、アドレスは HSRP グループ アドレスです。モバイル ノードと HA が別のサブネット上にある場合、このコマンドを入力します。
		または
		ルータに対する HA サービスをイネーブルにし、制御します。モバイル ノードと HA が同じサブネット上にある場合、このコマンドを入力します。

ステップ 3	`Router(config)#ip mobile virtual-network net mask [address address]`	仮想ネットワークを定義します。モバイル ノードと HA が同じサブネット上にある場合、[**address** *address*] オプションを使用します。
ステップ 4	`Router(config)# ip mobile home-agent redundancy hsrp-group-name [[virtual-network] address address]`	HSRP グループ名を使用して HA に冗長性を設定し、仮想ネットワークをサポートします。
ステップ 5	`Router(config)# ip mobile secure home-agent address spi spi key hex string`	ピア ルータの間に HA セキュリティ アソシエーションを設定します。アクティブ HA に設定されている場合、IP アドレス *address* 引数はスタンバイ HA の引数になります。スタンバイ HA に設定されている場合、IP アドレス *address* 引数はアクティブ ルータの引数になります。セキュリティ アソシエーションはスタンバイ グループのすべての HA の間で設定する必要があることに注意してください。

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`	レジストレーション応答パケットの Home Agent Address フィールドを設定します。Home Agent Address フィールドは *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
!
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 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 min 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 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 cisco
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface
Ethernet2/0 aaa
ip mobile secure home-agent 7.0.0.3 spi 100 key ascii redundancy algorithm md5 mode
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
```

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 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 cisco
ip mobile host nai mwts-mip-np-user1@ispxyz.com static-address 40.0.0.1 interface
Ethernet2/0 aaa
ip mobile secure home-agent 10.0.0.2 spi 100 key ascii redundancy algorithm md5 mode
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
```

ホットラインの冗長性サポート

Home Agent Release 4.0 では、冗長性はルール ベースとプロファイル ベースのホットライン両方でサポートされます。プロファイル ベースのホットラインでは、アクティブ HA はプロファイル情報のみをスタンバイに同期化します。これはプロファイルで使用可能なルールを同期化しません。

(注)　HA3.1 はホットライン機能の HSRP-HA 冗長性をサポートしません。

ルール ベースのホットラインでは、COA メッセージ コンテンツを受信し、検証したあと、アクティブ HA は COA 関連情報の一部をスタンバイに同期化します。ルールが AAA サーバによって COA コンテンツでアップデートされると、スタンバイで暫定的な同期化が行われます。次の情報がスタンバイに同期化されます。

- User-Name：ルールをスタンバイ HA に同期化しているときの必須アトリビュート
- MN Address：MN セッション（バインディング）がすでに確立されている場合に提供されます。
- Hot-Line Accounting Indication：フェールオーバーが発生してアカウンティング メッセージを送信するときに、このフィールドが使用されます。
- Filter-Id：特定のユーザのホットライン ステータスを指定します。アクティブ HA はユーザごとにたった 1 つの filter-id を受信し、スタンバイ HA に同期化しません。各 filter-id には、対応する profile-id（filter-id）のプロビジョニングされているホットライン プロファイルが含まれます。
- Filter-Rules：IP および HTTP フィルタ ルールが含まれます。複数のフィルタ ルールが存在する可能性があります。
- IP-Redirection-Rules：IP リダイレクション ルールが含まれます。ゼロ以上の IP リダイレクション ルールが存在する可能性があります。
- HTTP-Redirection-Rules：HTTP リダイレクション ルールが含まれます。ゼロ以上の HTTP リダイレクション ルールが存在する可能性があります。
- Accounting-Session-Id：セッションが作成され、ユーザがホットライン化されると提供されます。ユーザがホットライン化されると、新しい「accounting session id」が作成されます。
- Session-Timeout：セッションまたはプロンプトが終了する前にユーザに提供されるサービスの最大秒数を示します。

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、同期化ルールをユーザに適用します。セッションが確立され照合が行われると、ユーザはホットライン化されます。セッションが確立されていない場合、特定のユーザに対するセッションが確立されるまで待機します。

冗長性 / フェールオーバーでは、新しいアクティブ HA は、フェールオーバーする前に同期化された同じ Accounting-Session-Id を使用します。

QoS の冗長性サポート

Home Agent Release 4.0 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のみをサポートするので、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。

CAC の冗長性サポート

現在、コール アドミッション制御（CAC）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。

MIP/LAC の冗長性サポート

冗長性は Release 4 の一部として MIP-LAC 機能ではサポートされません。ただし、できる限り正常にフェールオーバーを実行するよう注意してください。

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 Access-Request 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、暫定的なアカウンティング 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、第 2 章「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 6

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。

この章の具体的な内容は、次のとおりです。

HA サーバ ロード バランシング

HA サーバ ロード バランシング（HA-SLB）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。SLB 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、DFP を使用して各実サーバのヘルスをモニタし、最小ロードを持ったサーバを選択し、アップ状態で稼働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、SAMI でそれぞれ稼働する一連の実 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 はユーザの初期レジストレーション要求を仮想サーバの IP アドレスに送信します。SUP で稼働する HA-SLB はパケットを代行受信し、レジストレーション要求を実 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 Mobile IP RRQ 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、Mobile 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 Mobile 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 Mobile 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）　Mobile 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 を送信したあと MN の電源を再投入する、MN が最初のレジストレーション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 から着信するレジストレーション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 NAI 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 からの以後のレジストレーションは、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 にふたたび割り当てられ、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みなされ、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 番めの RRQ は ServerB に、5 番めと 6 番めの 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.6-4）
- サーバ ロード バランシングの設定（p.6-4）

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`	レジストレーション応答パケットの 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 からのレジストレーション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 モードにのみ必要です。

```
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 モードにのみ必要です。

```
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 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あとに取得されました。

```
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 モードにのみ必要です。

```
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 モードにのみ必要です。

```
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あとに取得されました。

```
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みなされます。各実サーバ（HA）の 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あとに取得されました。

```
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あとに取得されました。

```
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 7

IP レジストレーションの終了

この章では、Cisco Mobile Wireless Home Agent が IP レジストレーションを終了し、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。

この章の具体的な内容は、次のとおりです。

モバイル IPv4 レジストレーションの失効

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 MIP ハンドオフによってレジストレーション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（FA）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 ACK メッセージを HA に送信します。さらに、PDSN/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 のレジストレーション失効をサポートするよう設定された HA には、有効なレジストレーション失効拡張を含んだ PDSN から関連付けられた MIP RRQ 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レジストレーションは、HA によって取り消し可能とみなされます。

次のコール フローでは、モバイル IP リソース失効（レジストレーション フェーズ）を示します。

ステップ 1　MS はコールを発信し、PPP セッションがアップします。

ステップ 2　MIPv4　レジストレーション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 レジストレーション失効サポート 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 MN から MIP RRQ を受信します。これには、FA-CHAP 時の access-request で **2** に設定された 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 MHAE のあとに追加されます。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-AAA 認証）の場合、STC アトリビュート（値 **2**）は、AAA に送信された access-request 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みなされます。

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、レジストレーション失効サポート拡張をモバイル レジストレーション要求に追加し、これを HA に転送します。

ステップ 3　応答として、HA はレジストレーション失効サポート拡張をレジストレーション応答に追加し、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）はレジストレーション要求を HA に送信します。

ステップ 6　HA はレジストレーション応答を PDSN/FA（2）に送信します。

ステップ 7　HA は Mobile 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、レジストレーション失効サポート拡張をモバイル レジストレーション要求に追加し、これを HA に転送します。

ステップ 3　応答として、HA はレジストレーション失効サポート拡張をレジストレーション応答に追加し、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 Mobile 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

レジストレーション失効フェーズ中、モバイル ノード（MN）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。レジストレーション 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 レジストレーション失効の設定

HA で MIPv4 レジストレーション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 レジストレーション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（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することはできません。いずれか 1 つを選択しなければなりません。
- HA MIB はレジストレーション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。

- 複数のフローが同じ NAI に確立されている場合、異なる IP アドレスが各フローに割り当てられます。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。

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 HA 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）VSA 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 NAS-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 pod server** [**clients** *ipaddr1* [*ipaddr2*] [*ipaddr3*] [*ipaddr4*]] [**port** *port number*] [**auth-type** {**any** | **all** | **session-key**}] [**ignore session-key**] {**ignore server-key** | **server-key** *string*}	Cisco IOS の AAA サブシステムで POD サービスをイネーブルにする必要があります。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。
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。
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 Access-Request 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 Access-request 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 のあとに含めます。
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 Access-request 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みなされます。
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 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 に同期化されるときを示します。

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、レジストレーション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 RF 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 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 VLR 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 PCF 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みなし、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）とみなし、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 とみなします。
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。

CHAPTER 8

ダイナミック 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、初回のレジストレーション要求を受信すると、ホーム 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 レジストレーションに成功すると、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 RRQ を受信した場合、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） 再レジストレーション場合は、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 レジストレーション 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 からレジストレーション要求を受信します。
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 にレジストレーション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 レジストレーション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レジストレーション要求を受信します。
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、レジストレーション応答が戻されます。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 レジストレーション応答で、ホーム DNS サーバのアドレスを 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 レジストレーション応答に付加します。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 レジストレーション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。

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 9

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。

この章の内容は、次のとおりです。

パケット フィルタリングでのモバイル ユーザ ACL

Home Agent（HA）は、ユーザ単位のパケット 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、レジストレーション要求が正常に認証された場合、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 ACL 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（FA; 外部エージェント）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`	トンネル テンプレートを設定します。

`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`
	ACL を設定します。

`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。

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
```

CHAPTER 10

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。

この章の内容は、次のとおりです。

3 DES 暗号化

Cisco Home Agent（HA）には、HA 上で 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、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、PDSN 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。

（注） この機能を使用できるのは、Cisco 7200 および 7301 ルータのプラットフォームだけです。

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提供する 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 レジストレーション メッセージ内の認証拡張を処理します。

HA は、IS-835-B の要求に基づいて、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 AAA 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 COA 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。

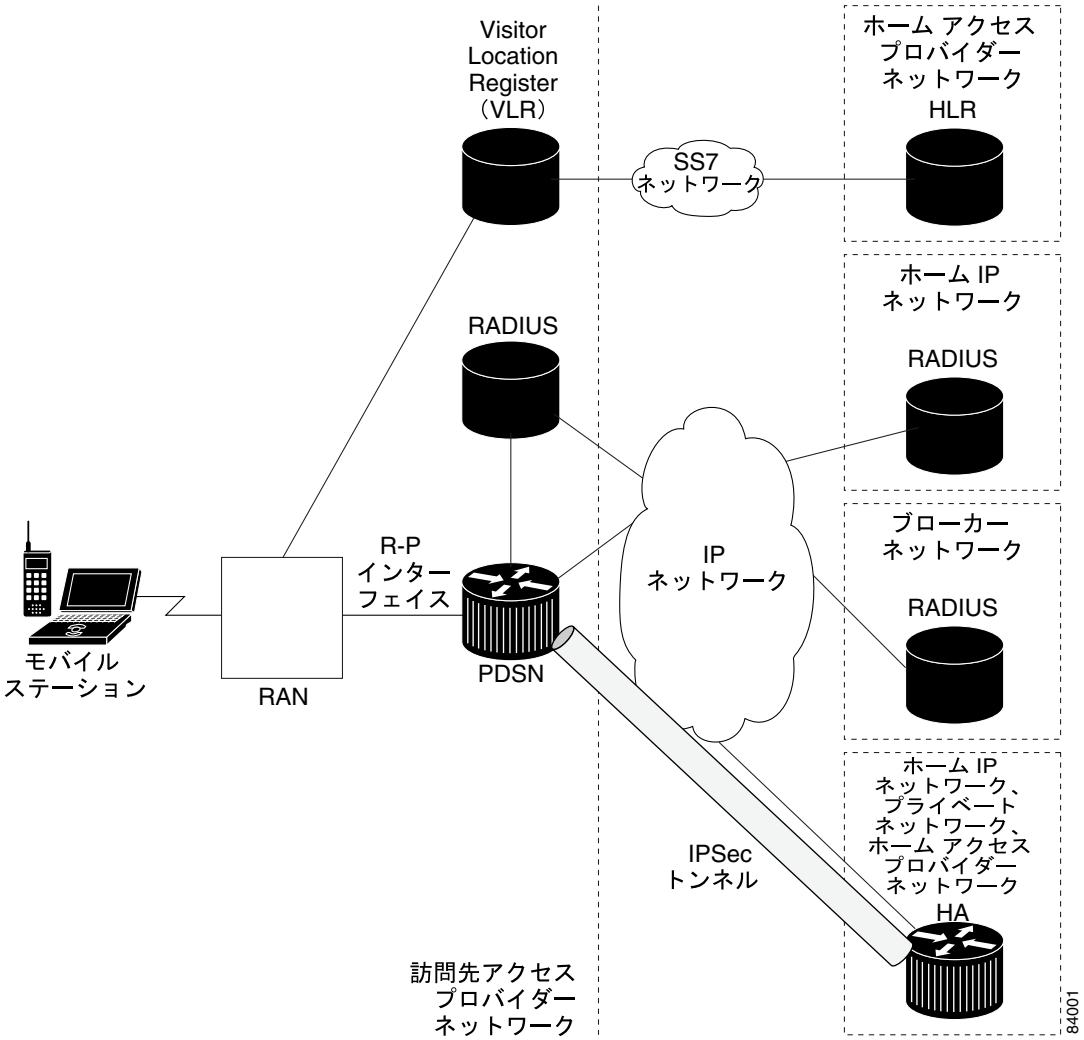
プロキシ モバイル サービスでは、Mobile-Node（MN; モバイル ノード）は簡易 IP によって PDSN/FA に接続し、PDSN/FA が HA への MN のモバイル IP プロキシとして動作します。

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 10-1 に、IS835 の IPSec ネットワーク トポロジを示します。

図 10-1　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。

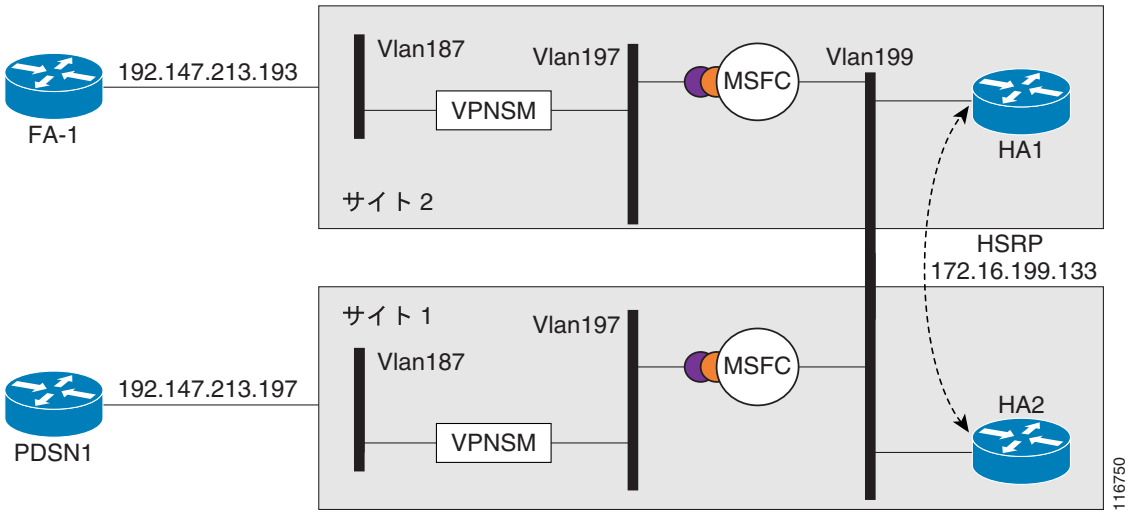
コンフィギュレーションの変更により、HA の IP アドレスへの IPSec 接続と、VPNSM による終端が可能になります。

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 10-2 に、実現可能なコンフィギュレーションを示します。

図 10-2　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 VRF 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 SPI 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 NAI 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 AH、および IP 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

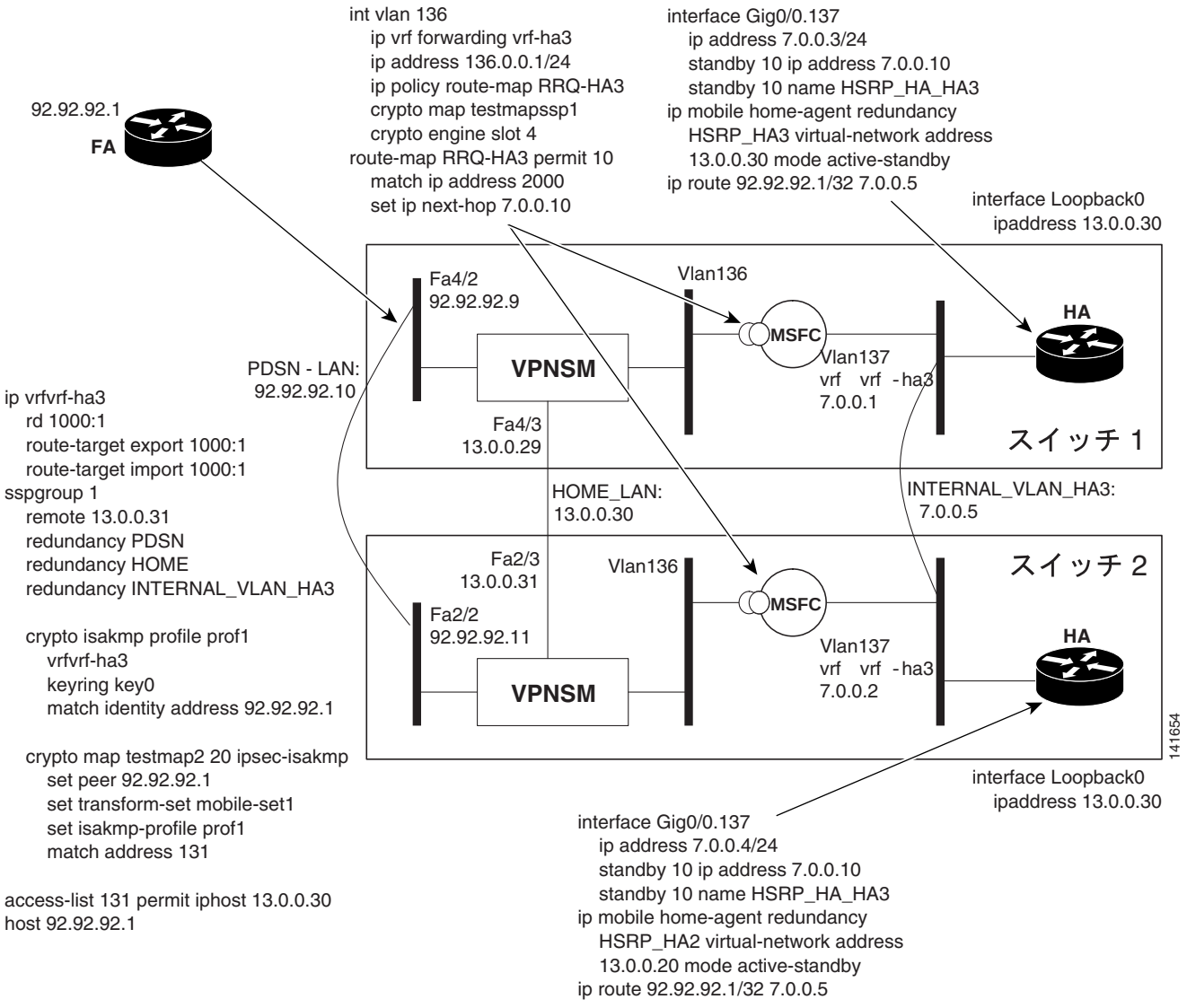
（注）　暗号化するホストおよびサブネットを許可する場合には、必ず、明示的な拒否（deny）ステートメントを指定してください。拒否ステートメントにより、他のすべてのパケットが暗号化されないように設定します。

（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 10-3 を参照してください。

図 10-3　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 11

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。

この章の内容は、次のとおりです。

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 レコードの追加アトリビュート
- 追加のアカウンティング方式 ― 暫定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）について、エラー コードを含むモバイル IP レジストレーション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レジストレーションに失敗すると、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 アトリビュートのレジストレーション フラグ
- 「mobileip:ip-vrf」cisco-avpair アトリビュートの Vrf 名
- 「mobileip:mn-reject-code」cisco-avpair アトリビュート（RRQ が拒否された場合のアカウンティング停止時およびアカウンティング アップデート時のみ）

HA 冗長設定でのアカウンティング カウンタの同期化

冗長設定で HA アカウンティングをイネーブルにし、定期アカウンティングを設定すると、次のコマンドが設定されている場合、アクティブとスタンバイの間でアカウンティング カウンタが定期的に同期化されます。

ip mobile home-agent *method* **redundancy [virtual-network address** *address*] **periodic-sync**

ip mobile home-agent *method* **redundancy periodic-sync** コマンドを設定すると、アカウンティング アップデート イベントにより、各バインディングのバイトおよびパケットのカウントがスタンバイに同期化されます。ただし、最後の同期化以降、バイト カウントが変更されている場合だけです。Time-of-the-day アカウンティングはサポートされません。

次に、例を示します。

aaa accounting update periodic *60* および **ip mobile home-agent** *method* **redundancy update-periodic** を設定して、バインディングを開くと、次のイベントが発生します。

- バインディングを開いたあと、バインディングを通過したデータがない場合、AAA サーバに暫定アカウンティング レコードが送信されていても、スタンバイ装置にバイトカウントは同期化されません。
- 次の暫定レコードが送信される前に、バインディングの各方向に 500 バイトのデータが通過したとします。この場合、アクティブ装置から暫定レコードがトリガーされた時点で、スタンバイにカウンタが同期化されます。
- 次の暫定インターバルでは、フローを通過するデータが存在しなかったとします。この場合、アクティブ装置から前提レコードがトリガーされても、新たにレポートする内容はないので、スタンバイ装置には何も同期化されません。
- この時点でスイッチオーバーが発生した場合、新しいアクティブ装置が保持しているバインディング カウントは、入出力バイト数が 500、入出力パケット数が 5 （各 100 バイトの 5 パケットが通過したと想定した場合）になります。前のアクティブ装置が回復してスタンバイ装置になると、これらのカウンタがスタンバイ装置にバルク同期化されます。

HA は、RADIUS サーバに対して、HA のフェールオーバーを通知できます。この通知には、RADIUS アカウンティング レコードの cisco-avpair radius アトリビュート「mobileip-rfswat=1」が含まれます。このアトリビュートが含まれるのは、フェールオーバー前に作成されていたバインディングで、フェールオーバー後に生成されたそのバインディングの最初のアカウンティング レコードだけです。

たとえば、バインディングが作成され、そのバインディングのアカウンティング開始が送信されます。しばらくして、アクティブに障害が発生し、スタンバイに引き継がれたとします。ここで、スタンバイは RADIUS サーバに、このバインディングのアカウンティング アップデートを送信します。HA は、このアカウンティング レコードに、Cisco-avpair radius アトリビュート「mobileip-rfswat=1」を付加します。

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 redundancy *group* **virtual-network address** *HA address* **swact-notification**

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。
  - MN が初回レジストレーションに成功した場合。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 変更後の再レジストレーション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レジストレーションに失敗した場合、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、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。
- **フレーム化された IP アドレス**：MN の IP アドレスです。通常、レジストレーションに成功すると、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 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、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。
ステップ 2	`Router(config)# 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。
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 サーバに暫定アカウンティング 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# 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。
ステップ 7	`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 8	`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 行めは、COA が変更された場合、アカウンティング アップレード 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 行めで、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 行めで、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 redundancy cisco virtual-network address 7.0.0.2 periodic-sync
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 redundancy cisco virtual-network address 7.0.0.2 periodic-sync
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 mobile 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 12

HA でのマルチ VRF

この章では、マルチ VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）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。

この章の内容は、次のとおりです。

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（すなわち複数のカスタマー）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、必要な機器数を減少し、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 PE 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 にマップされます。

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 12-1　Cisco PDSN/HA アーキテクチャの VRF-Lite

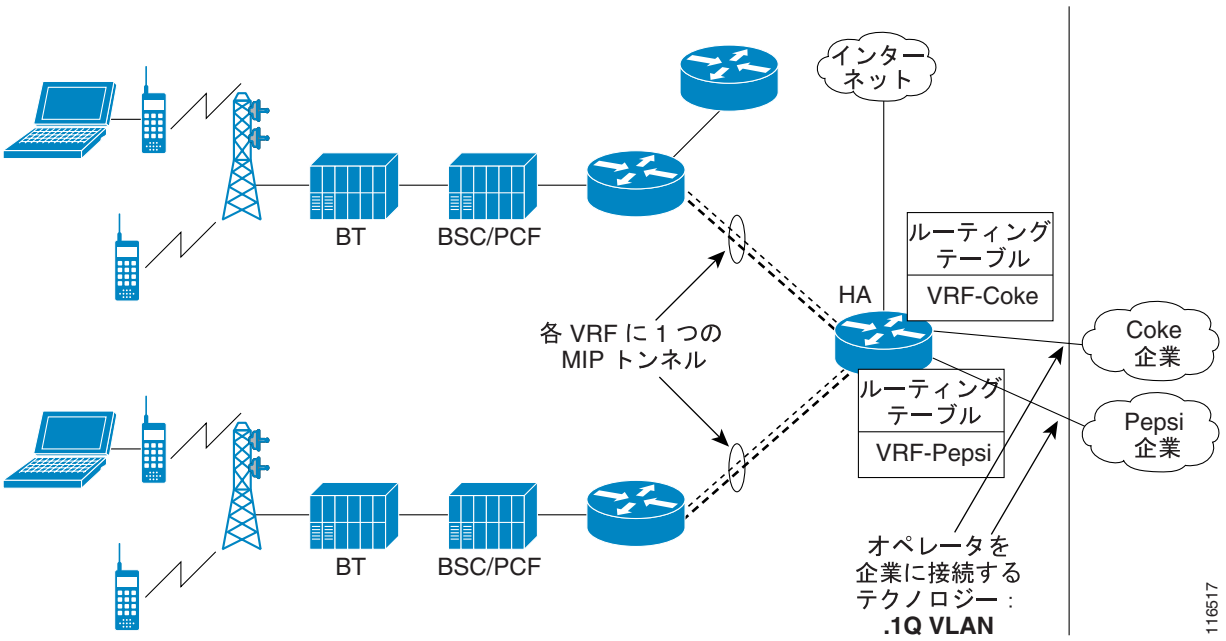


図 12-1 は、PDSN アーキテクチャ、および複数の異なるレルムおよび企業の HA への VRF-Lite ソリューションの適用方法、すなわち、企業間のデータの分離方法を示しています。

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 AAA 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。NAI は、モバイル IP RRQ 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* に登録者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 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「abc.com」企業の HA の IP アドレスとして受信し、LA2 を「xyz.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-SLB 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 レジストレーション要求を受信すると、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 アドレスでレジストレーション応答を送信できるオプションがあります。コード 136 のレジストレーション応答を受信すると、モバイルは新しいアドレスを使用して、もう 1 つのレジストレーション要求を送信します。HA は、この要求を処理し、バインディングを開き、レジストレーション応答（success）を送信することにより、レジストレーション 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 200 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。
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 テーブルを作成します。 **（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、設定すべきではありません。

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 HSRP 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。

```
Active 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 redundancy cisco virtual-network address 192.168.0.0
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

Standby 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 redundancy cisco virtual-network address 192.168.0.0
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 13

HA の 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。

ここで説明する内容は、次のとおりです。

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 Cmmand 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 MN 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 が次のように有効化されます。

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 RRQ 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監視し、これに応じてパケットを許可または廃棄します。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

以下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 ポリシングのみです。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、いったん設定したあとは変更できません。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のみに適用できます。
- 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 コマンドのみを設定できます。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 機能を有効にするには、以下のタスクを実行します。

	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、以下の制限があります。

- 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 つを削除することはできません。
- 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することはできません。

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、以下のタスクを実行します。

	コマンド	目的
ステップ 1	Router#**show ip mobile binding police nai** *@example.com*	QoS ポリシングが有効になっている場合、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 14

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。

ここで説明する内容は、次のとおりです。

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 Release 3.1 では、IP リダイレクションのみ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。Home Agent Release 4.0 では、ルール ベースおよびプロファイル ベースのホットライニングがサポートされ、IS 835-D に準拠したすべてのリダイレクションおよびフィルタ ルールが有効です。

また、Cisco Mobile Wireless Home Agent Release 4.0 は以下の 3 つのフィルタをサポートすることで、IS.835D 標準に準拠します。

- HTTP リダイレクション
- IP リダイレクション
- IP フィルタ

また、Home AAA（HAAA）では、ユーザに対してホットラインが適用されたことを示す、次の 2 つのスタイルが使用されます。

- プロファイルベースのホットライニングでは、Home Agent（HA）のプロファイルとして IP、HTTP、またはその両方のリダイレクション ルールが設定されます。HA は Access-Accept または COA のいずれかによって HAAA から Filter-ID を受信すると、ホットライニングを実行します。HA は hotline capability パラメータを Access-Request メッセージに含めて送信します。

（注） Filter-ID は、HA のいずれかのプロファイルと一致します。

- ルールベースのホットライニングでは、HAAA は登録時に Access-Request によって HA から受信した hotline capability パラメータに基づき、実際のリダイレクション ルール（HTTP または IP）を Access-Accept メッセージまたは COA RADIUS メッセージに含めて送信します。Access-Accept または COA RADIUS メッセージ内で受信したルールが HA によって有効とみなされると、MN パケット データ セッションに対するホットラインが実行され、ユーザのデータ トラフィックにこのルールが適用されます。
- ファイアウォールに対するホットライニングは、ルールベースとプロファイルベースのどちらでも可能です。ルールベースのホットラインでは、HA は Access-Request 内に hotline capability パラメータを含めて送信することで、HAAA から IP-Filter-Rule を受信します（Access-Accept または COA メッセージ内）。

  プロファイルベースのホットラインでは、特定のプロファイルに対し、IP-Filter-Rule が事前に設定されます。HA は Access-Request に hotline capability パラメータを含めて送信することで、HAAA から Filter-Id を受信し（Access-Accept または COA メッセージ内）、ホットライニングを実行します。

（注） Filter-ID は、HA のいずれかのプロファイルと一致します。

その他のホットライニング機能

HA では、HA 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かぎり、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、HA は RRQ を拒否します。

（注） この機能に対しては、MIB サポートは予定されていません。

Home Agent Release 2.0 以上では、Nortel X31-20031013-0xx（2003 年 10 月）に基づき、モバイル ノードに対するホットライニングがサポートされます。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。HAAA 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属性は、HA 上の特定のユーザを識別するための User-Name 属性です。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。

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ニング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 RADIUS Access-Request 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 VSA 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有効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。

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) 属性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 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 ACK 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 NAK 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廃棄を指示します。

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有効にされている場合）、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。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 ルー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かぎりません（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) メッセージのあとには、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。

ホットライニングの HSRP-HA 冗長性サポート

Cisco Home Agent Release 3.1 は、ホットライニング機能の HSRP-HA 冗長性をサポートしていません。Cisco Home Agent Release 4.0 では、ルールベースのホットライニングに対する冗長性のサポートが有効です。しかし、HSRP-HA には Session Redundancy（SR; セッション冗長性）機能がないため、プロファイルベースのホットラインの同期はサポートされません。

ルールベースのホットラインでは、アクティブ HA は COA メッセージを受信して内容を検証したあと、COA 関連情報の一部をスタンバイ HA と同期します。また、AAA サーバによって COA の内容でルールが更新されるたびに、スタンバイとの中間同期が実行されます。

スタンバイと同期できるのは、以下の情報です。

- **User-Name**：ルールをスタンバイ HA に同期する場合の必須属性。
- **MN Address**：MN セッション（バインディング）がすでに確立されている場合に使用。
- **Hot-Line Accounting Indication**：このフィールドは、フェールオーバーが発生した場合にアカウンティング メッセージに含めて送信されます。

- **Filter-Id**：特定のユーザに対するホットライン状態を指定。1 人のユーザに対して複数の filter-id を受信したアクティブ HA は、スタンバイ HA と同期する必要があります。各 filter-id は、IP または HTTP リダイレクション ルールを指定します。
- **Filter-Rules**：IP および HTTP フィルタ ルールを指定。複数のフィルタ ルールを指定することもできます。
- **IP-Redirection-Rules**：IP リダイレクション ルールを指定。複数のリダイレクション ルールを指定することもできます。
- **HTTP-Redirection-Rules**：HTTP リダイレクション ルールを指定。複数のリダイレクション ルールを指定することもできます。
- **Accounting-Session-Id**：セッションが作成され、ユーザに対してホットラインが適用されると指定されます。ユーザに対してホットラインが適用されるたびに、新規の "accounting session id" が作成されます。
- **Session-Timeout**：セッションまたはプロンプトの終了までに、ユーザにサービスの使用が許可される最大秒数を指定。

フェールオーバーが発生し、スタンバイがアクティブに切り替わると、ユーザに対してこの同期ルールが適用されます。セッションが確立し、照合が行われると、ユーザに対してホットラインが適用されます。セッションが確立されない場合は、HA は特定のユーザに対し、セッションの確立まで待機します。

冗長フェールオーバーでは、新たにアクティブとなった HA は、フェールオーバー前に同期されたものと同じ Accounting-Session-Id を使用します。

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、加入者の MIP 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。HA はリレー エージェント機能を使用して、ホットライン ルールを DNS トラフィックおよび DHCP トラフィックに適用します。
   a. MIP 加入者の登録中、HA が無効なホットライン情報を受信した場合は、HA は "HA-CHAP Failure" を示す Registration-Reject を送信することで、この RRQ を拒否できます。
   b. MIP 加入者の再登録中は、HA は Access-Accept によって無効な情報を受信した場合であっても、加入者の MIP セッション、およびホットライン セッションを維持する必要があります。また、“HA-CHAP Failure” を送信してこの RRQ を拒否します。
3. HA は MIP 加入者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 Access-Request メッセージに Hot-line Capability VSA を含める必要があります。
4. HA は以下を含む 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) 属性。または、
   b. RADIUS Filter-Id(11) 属性に加え、Filter-Rule VSA または HTTP/IP Redirection-Rule VSA。または、
   c. デコードできない Filter-Rule（VSA）または HTTP/IP Redirection-Rule（VSA）。

5. RADIUS Filter-Id(11) 属性を含む RADIUS Access-Accept メッセージを受信した HA は、RADIUS Filter-Id(11) 属性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) 属性を含む COA メッセージを受信した HA は、RADIUS Filter-Id(11) 属性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) 属性、HTTP リダイレクション ルール、IP リダイレクション ルール、およびフィルタ ルールをすべて削除し、新たに受信した RADIUS Filter-Id(11) 属性に関連付けられたルールの適用を開始します。HA は Release 3.1 のコール フローのセクションで説明されているように、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) 属性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. HA が受信した RADIUS Access Accept メッセージの中に、適格な（解析可能な）HTTP Redirection-Rule VSA、IP Redirection-Rule VSA、および Filter Rule VSA が含まれている場合は、HA はまず HTTP リダイレクション ルールを適用し（存在する場合）、次に IP リダイレクション ルール（存在する場合）を、最後にフィルタ ルール（存在する場合）を適用します。各タイプのルールは、パケット内に記述されている順序で処理されます。HA はルール（フィルタ ルール、HTTP/IP リダイレクション ルール）を適用する際、すべてのセキュリティ ポリシーに照合して各ルールを検証します。いずれかのセキュリティ ポリシーに違反があった場合は、HA はこのユーザのパケット データ セッションをティアダウンします。
8. 受信した COA メッセージの中に適格な HTTP Redirection Rule VSA、IP Redirection-Rule VSA、または Filter-Rule VSA が含まれている場合は、HA はローカル システム全体のポリシーに対して有効な、ローカルにプロビジョニングされたすべてのフィルタリングを検証します。いずれかのルールがローカル ポリシーに違反している場合、または HA が COA メッセージを受け入れられない場合は、HA は Error-Cause (101) が "Administratively Prohibited" (50) を示す COA NAK メッセージを送信します。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。一方、ローカル セキュリティ ポリシーに対する違反が存在しない場合は、HA は以下を行います。
   a. HA が現在、以前に受信した RADIUS Filter-Id(11) 属性に関連付けられたルールを適用している場合は、HA は以前に受信した RADIUS Filter-Id(11) 属性に関連付けられたルールの適用を中止し、新たに受信した HTTP リダイレクション ルール、IP リダイレクション ルール、またはフィルタ ルールの適用を開始します。HA は HAAA に対して COA ACK で応答し、Release 3.1 のコール フローのセクションで説明されているように、アカウンティング メッセージの送信を開始します。
   b. HA が現在、以前に受信した HTTP リダイレクション ルール、IP リダイレクション ルール、またはフィルタ ルールに関連付けられたルールを適用している場合は、古いルールを同じ種類の新たなルールで上書きします（旧 HTTP に対しては新規 HTTP、旧 IP に対しては新規 IP、旧フィルタに対しては新規フィルタ）。同じ種類の古いルールが存在しない場合は、その種類の新規ルールが適用されます。HA は HAAA に対して COA ACK で応答し、Release 3.1 のコール フローのセクションで説明されているように、アカウンティング メッセージの送信を開始します。
9. Session-Timeout (27) 属性を受信した場合は、HA はセッションに規定されたタイムアウト時間（秒）が経過したあと、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。
10. HTTP-Redirection VSA を受信した HA は、IP フローをモニタします。"src" および "dst" フィールドの一致する IP フローに対しては、HTTP-Redirection VSA に指定されたルールを適用します。ルールに指定されたアクションがリダイレクトである場合は、HA はトラフィックをブロックし、認識したすべての HTTP 要求に対し、一致する HTTP-Redirection Rule VSA の URL を指定した HTTP リダイレクト応答（RFC 2616）を返します。

11. 以下の説明は、ホットラインでの HTTP リダイレクション ルールにおけるループに関するものです。

    a. “ ホットラインでの HTTP リダイレクション ルールにおけるループ ” が生じる状況としては、最初に HA が "redirect www.cisco.com from 10.1.1.0/8 to 192.168.1.0/8" という HTTP リダイレクション ルールを受信します。上記のルール条件と一致した場合、HA は Redirect 302 メッセージを MN 加入者に送信し、www.cisco.com 宛の HTTP パケットをリダイレクトします。MN は、受信したリダイレクト先 URL を含めた新たな HTTP Request Get メッセージを送信します。しかし、リダイレクト URL はサブネット アドレス 192.168.1.0/8 の 1 つ、192.168.1.100 などにマッピングされます。したがって、HA は受信した HTTP-302 メッセージに対し、MN に再度 HTTP-302 メッセージを送信します。この流れは、MN および HTTP サーバ間に HA 経由で TCP セッションが確立されているかぎり、MN と HA 間で繰り返されます。このループ状態を回避するには、HTTP リダイレクション ルールとともに、AAA から以下のルールをダウンロードする必要があります。

    “pass from 10.1.1.0/8 to 192.168.1.100/0”

    “redirect www.cisco.com from 10.1.1.0/8 to 192.168.1.0/8”

    ループ状態を回避するため、“HTTP-Redirection Rule” は常に “HTTP-Pass Rule” に先行します。

12. IP-Redirection rule VSA を受信した HA は、IP フローをモニタします。IP フローがルールと一致した場合、HA は一致したルールに指定されたアドレスにフローをリダイレクトします。

13. IP-Filter rule VSA を受信した HA は、IP フローをモニタします。IP フローがルールと一致した場合、HA は指定されたアクションに従い、フローをブロックするか、または通過を許可します。

14. "flush" というキーワードを含む HTTP Redirection Rule、IP-Filter-Rule、または IP-Redirection-Rule VSA を受信した HA は、このセッションにおいてこれまで受信した、この種類の属性をすべてフラッシュします。

15. HA が受信した Access-Accept または COA に、ホットライン アカウンティング属性は含まれるが、RADIUS FIlter-Id(11) 属性、HTTP Redirection Rule VSA、IP Redirection Rule VSA、Filter Rule VSA のいずれも含まれない場合は、このホットライン アカウンティング属性によってユーザのホットライン状態は影響されません。RADIUS アカウンティング メッセージを生成可能な HA は、以降のすべてのアカウンティング メッセージに、新たに受信したホットライン アカウンティング インジケータを含めます。

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 属性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) 属性を含めるように 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。

ホットライニングの制約事項

ホットライニングには、以下の制限があります。

- アップストリーム トラフィックでは、HA はトラフィックを代行受信し、ユーザに HTTP リダイレクション、IP リダイレクション、または IP フィルタ ルールを適用します。ダウンストリーム トラフィックの場合は、HA は IP リダイレクションおよび IP フィルタ ルールによる検証をサポートします。HA では、ダウンストリーム トラフィックでの HTTP リダイレクションはサポートされません。
- ルータでホットラインを有効にするには、ルータが mobileip および HA 機能をサポートする必要があります。ルータがこれらをサポートしていない場合は、ルータで **router mobile** をイネーブルにし、グローバル コンフィギュレーション モードで **ip mobile home-agent** を設定します。
- 特定のユーザに対するホットライニング機能と設定は、ホットライニング CLI を入力した順序に応じて上書きされることがあります。新たに追加したホットライニング CLI は、以前のものより優先されます。たとえば、プロファイル ベースのホットラインに “mip1@cisco.com” というユーザを設定したとします。このあと、ルールベースのホットラインを設定すると、先の設定は上書きされます。
- 最初にレルムを設定して、このレルム内のすべてのユーザにホットライン機能を適用するとします。あとから特定のユーザに対してホットライン機能を設定すると、このユーザの設定によってレルムの設定が上書きされます。
- IOS では、CLI の設定および設定解除に制限があります。CLI の設定では、使用可能な文字数は最大 249 文字です。CLI の設定解除では、使用可能な文字数は最大 252 文字です。

（注） HA 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 モードで以下のタスクを実行します。

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 番号は 100 ～ 199 および 2000 ～ 2699 となります。
`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 番号は 100 ～ 199 および 2000 ～ 2699 となります。
`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 番号は 100 ～ 199 および 2000 ～ 2699 となります。

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
 	
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
	モバイル ホストのホットライン機能を設定します。
	
	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]

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 属性を使用）。
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、以下のタスクを実行します。

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。

コマンド	目的
router# **show ip mob hot summary**	ホットラインを適用した加入者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
```

CHAPTER 15

その他の設定作業

その他の設定作業

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

トンネル インターフェイスでの ACL のサポート

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

Mobile IP トンネル テンプレート機能の設定

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

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

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

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

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

制約事項

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

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

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

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

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

MN-HA-SPI（26/57）

MN-HA-SHARED-KEY（26/58）

このサポートの手順は次のとおりです。

ステップ 1　HA が PDSN/FA から RRQ を受信します。

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

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

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

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

ユーザ プロファイル

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

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

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

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

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

モビリティ バインディング アソシエーション

HA は、モビリティ バインディングを次の方法で識別します。

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

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

バインディング アソシエーションには、次の情報が含まれています。

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

アップストリーム パスでの MS トラフィック リダイレクション

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

外部エージェント別アクセス タイプ サポート

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

外部エージェント アクセス タイプ サポートの設定

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

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

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

HA バインディングのアップデート

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

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

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

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

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

選択的なモバイル ブロッキング

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

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

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

MEID のサポート

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

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

コール アドミッション制御（CAC）のサポート

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

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

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

上記の 2 つのパラメータによる式は、次のようになります。

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

最大バインディングのサポート

最大バインディングをサポートするために使用できる機能は次のとおりです。

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

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

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

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

最大バインディングのサポートを設定するには、次の作業を行います。

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

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

HA での CAC の設定

HA で許可される最大バインディング数を設定するには、次の作業を行います。

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

MIP/LAC（PPP 再生成）のサポート

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

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

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

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

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

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

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

発生するイベントは次のとおりです。

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

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

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

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

MIP LAC の設定

VPDN 設定をローカルにイネーブルにする手順は次のとおりです。

	コマンド	目的

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

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

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

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

ステップ 3

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

HA に PPP 仮想テンプレート インターフェイスを設定します。

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

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

ステップ 4

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

ローカルに設定された LAC に AAA パラメータを追加します。

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

ステップ 5

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

VPDN と VPDN 検索順序をイネーブルにします。

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

ステップ 6

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

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

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

ステップ 7

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

ローカル設定に基づく LNS ロード バランシングを設定します。

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

ステップ 8

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

ローカル設定に基づく VRF を設定します。

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

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

ステップ 9

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

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

AAA サーバ設定に基づく LNS のロード バランシング

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

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

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

LNS の設定

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

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

AAA の設定

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

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

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

AAA サーバの設定に基づく VRF の設定

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

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

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

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

設定の確認

MIP LAC の設定を確認するには、次の作業を行います。

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

例を示します。

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

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

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

show ip mobile traffic コマンドの例を示します。

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

新しい MIP-LAC 機能に関連して追加されたカウンタは次のとおりです。

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

これらの新しいカウンタについて説明します。

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

制約事項

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

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

Framed-Pool 基準

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

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

Framed-Pool 基準機能を設定するには、次の作業を行います。

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

例を示します。

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

ローカル プールのプライオリティ メトリック

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

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

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

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

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

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

ローカル プールのプライオリティ メトリックの設定

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

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

例を示します。

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

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

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

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

設定の確認

設定の確認手順は次のとおりです。

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

例を示します。

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


router# show ip local pool

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

Mobile IPv4 ホスト設定エクステンション（RFC4332）

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

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

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

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

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

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

WiMAX AAA アトリビュート

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

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

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

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

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

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

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

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

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

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

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

上記で

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

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

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

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

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

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

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

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

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

AAA Accounting アトリビュートの現在の機能は次のとおりです。

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

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

表 15-2　WiMAX AAA Accounting アトリビュート

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

WiMAX サポートの設定

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

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

設定の確認

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

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

例を示します。

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

AAA サーバの設定

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

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

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

アップストリームでの MS トラフィック リダイレクション

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

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

これまでの設定に加えて、次の作業を実行します。

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

設定の確認

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

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

例を示します。

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

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

CHAPTER 16

HA のネットワーク管理、MIB、および 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。

この章の内容は次のとおりです。

Cisco Mobile Wireless Home Agent の運用と管理

ここでは、Home Agent（HA）がサポートしている設定機能、統計情報、MIB について説明します。各 Mobile IP コマンドの詳細については、次の URL を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/1rfmobip.htm

HA は Cisco IOS CLI 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）
- レジストレーション（要求および応答）
- レジストレーション（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 ARP 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 FA-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 GRE）
- 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 Host 単位のほか、NAI または Home 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、MIB、およびネットワーク管理

HA には、プロトコル スイート、RFC 1901 ～ RFC 1908 に指定されている SNMPv2 が実装されています。また、HA 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 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 のリストは、次の URL を参照してください。
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 と Cisco IOS CLI のいずれを使用してもリセットできません。HA CPU と Memory Utilization のカウンタには CISCO-PROCESS-MIB を使用してアクセスできます。

Release 3.0 には、Home Agent Version 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。

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ました。

制限

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。

	コマンドまたは処理	目的
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* の値以下にしなければなりません。 *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* よりも大きい値にしなければなりません。
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 MN 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、AAA と Mobile 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、Mobile 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、各デバッグ文とともに、条件（username/IMSI）も表示されるようになりました。これは、デバッグ文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 Mobile 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。
Router# **debug ip mobile**	IP モビリティ アクティビティを表示します。
Router# **debug ip mobile host**	モビリティ イベント情報を表示します。
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**	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**	VRF 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**	Mobile Agent 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 Mobile IP ホストに関する情報を表示します。
Router#**show ip mobile secure**	Mobile 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。
Router#**show ip mobile traffic**	HA のプロトコル カウンタを表示します。
Router#**show ip mobile tunnel**	Mobile 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

3GP ― P23rd 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 Station Controller（ベース ステーション コントローラ）

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）

FACFA-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（リンク制御プロトコル）

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

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 Mobile 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）