CHAPTER 3

単一 IP インフラストラクチャ

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

この章は、次の内容で構成されています。

単一 IP 機能の概要

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

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

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

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

また、シャーシ単位モデルは次の対象機能に適用されます。

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

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

単一 IP インターフェイス

次の機能はブレード単位の単一 IP によって管理されます。

- MIP の単一インターフェイス
- 設定の単一インターフェイス
- SNMP 管理の単一インターフェイス
- トラブルシューティングおよびデバッグの単一インターフェイス
- AAA の単一インターフェイス
  - MIP および AAA の単一インターフェイス
- フェールオーバーの単一インターフェイス

MIP の単一インターフェイス

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

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

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

設定の単一インターフェイス

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

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

SNMP 管理の単一インターフェイス

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

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

トラブルシューティングおよびデバッグの単一インターフェイス

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

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

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

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

AAA の単一インターフェイス

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

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

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

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

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

MIP および AAA の単一インターフェイス

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

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

アクティブ HA での手順

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

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

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

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

次の情報は、バインディング用に CP から TP に更新されます。

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

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

アクティブ HA での MN の登録解除

次のコール フローは、アクティブ HA での MN の登録解除を示します。

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

次の情報は、バインディング用に CP から TP に更新されます。

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

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

次のコール フローは、アクティブ HA での登録失効の手順を示します。

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

次の情報は、バインディング用に CP から TP に更新されます。

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

アクティブ HA の Registration Revocation ACK

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

アクティブ HA で受信された COA

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

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

次の情報は、バインディング用に CP から TP に更新されます。

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

アクティブ HA で受信された POD

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

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

スタンバイ HA 上の手順

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

- ダイナミック同期
- バルク同期

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

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

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

次の情報は、バインディング用に CP から TP に更新されます。

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

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

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

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

次の情報は、バインディング用に CP から TP に更新されます。

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

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

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

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

次の情報は、バインディング用に CP から TP に更新されます。

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

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

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

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

その他の場合

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

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

フェールオーバーの単一インターフェイス

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

操作と管理

ここでは、操作と管理に関連する機能について説明します。

アプリケーション関連パラメータのシャーシ全体の MIB

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

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

シャーシ全体のロードのアプリケーション インスタンス単位での報告

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

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

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

AAA 無応答に対するトラップ生成

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

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

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

この機能をイネーブルにするには、次の作業を実行します。

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

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

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

サブスクライバの表示

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

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

表 3-1 に、この機能のリストを示します。

表 3-1　サブスクライバの表示機能のリスト

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

表 3-1　サブスクライバの表示機能のリスト （続き）

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

使用可能な出力表示形式は次のとおりです。

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

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

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

この機能は SNMP ではサポートされません。

シャーシ間の設定同期

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

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

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

初期化

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

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

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

RF クライアント

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

設定ファイルおよび同期

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

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

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

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

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

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

HA 設定同期機能では次の転送メカニズムを使用できます。

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

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

スタートアップ コンフィギュレーションの同期

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

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

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

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

実行コンフィギュレーションの同期

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

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

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

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

バルク同期

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

初期化中に同期する設定は次のとおりです。

- プライベート コンフィギュレーション
- 実行コンフィギュレーション

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

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

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

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

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

ライン単位の同期

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

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

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

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

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

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

設定の詳細

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

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

次の新しい CLI が導入されました。

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

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

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

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

シャーシ間の設定同期を設定するには、次のコマンドを使用します。

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

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

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

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

次の設定手順は各カードで実行する必要があります。

	コマンド	目的
ステップ 1	`Router#show redundancy states`	冗長性コマンドを実行する前に、両方の SAMI で次のコマンドを実行します。**my state** は両方のカードでアクティブにする必要があります。

ステップ 1	`Router(config)# redundancy inter-device`
	
	`redundancy unit1 slot 9 unit2 slot 6`
	
	`interface GigabitEthernet0/0.2`
	`encapsulation dot1Q 20`
	`redundancy ip address unit1 4.0.0.1 255.255.255.0`
	`unit2 4.0.0.2 255.255.255.0`
	`standby 0 ip 4.0.0.4`
	`standby 0 name hsrp`
		シャーシ間の設定同期をイネーブルにします。
		
		グローバルな冗長装置 / スロットのマッピングを設定します。
		
		HSRP のインターフェイスを設定します。
		
		HSRP ではアクティブ装置とスタンバイ装置に一意の IP が必要です。また、**redundancy ip address** コマンドを使用する必要があります。
		
		（注） このインターフェイスでは **ip address** コマンドを設定しないでください。

ステップ 2	`Router(donfig)# redundancy unit1` *hostname name 1* `unit2` *hostname name2*	同じシャーシ内のピア スロットの特定および設定に使用します。

ステップ 3	`Router(config)# redundancy inter-device scheme standby hsrp`
	
	`ipc zone default`
	`association 1`
	`no shutdown`
	`protocol sctp`
	`unit2-port 5000`
	`unit2-ip 4.0.0.2`
	`unit1-port 5000`
	`unit1-ip 4.0.0.1`
		HSRP スキーム名を RF Interdevice に関連付けます。
		
		RF Interdevice の ipc 情報を設定します。

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

サブスクライバのモニタリング

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

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

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

次の 2 段階のプロセスを実行します。

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

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

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

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

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

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

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

サブスクライバ セッションの表示

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

これは次の 2 段階のプロセスになります。

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

バルク統計情報収集

この機能を使用すると、単一ポイントから次の機能を実行できます。

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

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

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

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

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

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

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

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

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

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

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

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

パフォーマンス要件

単一 IP HA は次のパフォーマンス機能をサポートします。

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

単一 IP サポート - 再利用 CLI と新しい CLI

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

EXEC モード

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

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

Show コマンド

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

設定モード

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

単一 IP HA の分散設定

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

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

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

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

コマンドが TP に送信されると、各 TP で実行されます。

表 3-2　　単一 IP の HA コマンド

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

表 3-2　単一 IP の HA コマンド（続き）

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

表 3-2　単一 IP の HA コマンド（続き）

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

表 3-2　単一 IP の HA コマンド （続き）

router(config-if)#standby [*group-number*] [priority *priority*] preempt [delay [minimum | sync] *delay*]	アクティブ ルータの選択に使用するホットスタンバイ プライオリティを設定します。	あり
router(config-if)# standby name *hsrp-group-name*	スタンバイ グループの名前を設定します。	あり
ip mobile home-agent redundancy *hsrp-group-name*	HSRP グループ名を使用して、HA に冗長性を設定します。	あり
ip mobile home-agent dynamic-address *ip address*	登録応答パケットの Home Agent Address フィールドを設定します。Home Agent Address フィールドを ip address に設定します。	なし
ip mobile home-agent revocation	HA で MIPv4 登録失効のサポートをイネーブルにします。	あり
interface tunnel *10*	トンネル テンプレートを設定します。	なし
ip mobile home-agent template tunnel *10* address *10.0.0.1*	テンプレート トンネルを使用する HA を設定します。	なし
ip mobile home-agent accounting *list*	HA アカウンティングをイネーブルにし、HA の定義済みアカウンティング方式リストを適用します。list は、HA アカウンティング レコードの生成に使用する AAA アカウンティング方式です。	なし
ip mobile home-agent *method* redundancy [virtual-network address *address*] periodic-sync	アカウンティング アップデート イベントを使用して、各バインディングのバイトとパケットのカウントをスタンバイ装置に同期化します。同期が実行されるのは、最後の同期以降、バイト カウントが変更された場合だけです。	なし
ip mobile realm *realm* hotline redirect *redirect-server-ipaddress*	インバウンド ユーザ セッションをイネーブルにして、特定のアトリビュートが表示された場合にセッションを切断します。	なし
ip mobile home-agent dfp-max-weight *dfp-max-weight-value*	HA で許可できる最大 dfp 重み値をイネーブルにします。デフォルトの最大 dfp 重み値は 24 です。	なし
ip mobile home-agent max-cps *max-cps-value*	HA で許可できる最大 cps をイネーブルにします。アカウンティングをサポートする場合のデフォルトの最大 cps 値は 160 cps です。	なし

表 3-2　単一 IP の HA コマンド（続き）

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

表 3-2　単一 IP の HA コマンド（続き）

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

表 3-2　単一 IP の HA コマンド（続き）

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

表 3-2　単一 IP の HA コマンド（続き）

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

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

Distributed Show および Distributed Debug

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

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

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

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

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

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

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

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

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

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

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

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

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

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

シャーシ管理の Show CLI の拡張

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

表 3-4　シャーシ管理に関連する show コマンド

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

表 3-4　シャーシ管理に関連する show コマンド （続き）

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

ネットワーク管理と MIB

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

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

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

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

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

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

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

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

表 3-5 に、サポートされる MIB を示します。

表 3-5　HA Release 5.0 の単一 IP MIB

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

表 3-5　HA Release 5.0 の単一 IP MIB （続き）

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

サポートされない機能

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

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

シャーシ管理

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

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

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

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

制約事項

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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