CHAPTER 2

Home Agent（HA）の設定プランニング

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

この章は、次の内容で構成されています。

- 「サポート対象プラットフォーム」（P.2-1）
- 「前提条件」（P.2-2）
- 「設定作業」（P.2-2）
- 「必要な基本設定」（P.2-9）
- 「設定例」（P.2-11）
- 「制約事項」（P.2-13）
- 「サポート対象の規格、management information base（MIB; 管理情報ベース）、および Request For Comments（RFC; コメント要求）」（P.2-13）
- 「マニュアルの入手方法およびテクニカル サポート」（P.2-14）

サポート対象プラットフォーム

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

SAMI サポート

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

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

前提条件

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

7600 シリーズ ルータ上の HA

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

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

Cisco HA をインストールする前に、次の考慮事項を確認してください。

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

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

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

設定作業

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

- c7svcsamifeature-mz HA イメージ

SAMI ソフトウェアのアップグレード

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

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

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

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

SAMI イメージをアップグレードする手順は、次のとおりです。

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

次に、**show module** コマンドの例を示します。

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

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

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

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

設定例

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

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

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

ユーザの移行

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

複数の移行シナリオが可能です。

表 2-1　移行シナリオ

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

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

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

表 2-2 に、移行パスをいくつか示します。

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

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

機能の互換性およびシームレスな移行

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

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

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

表 2-3　表 2-2 の移行シナリオに対応する移行手順

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

表 2-3　表 2-2 の移行シナリオに対応する移行手順 （続き）

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

表 2-3　表 2-2 の移行シナリオに対応する移行手順 （続き）

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

SAMI の移行に関する警告および制約事項

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

必要な基本設定

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

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

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

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

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

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

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

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

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

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

HA 環境における AAA の設定

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

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

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

HA 環境における RADIUS の設定

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

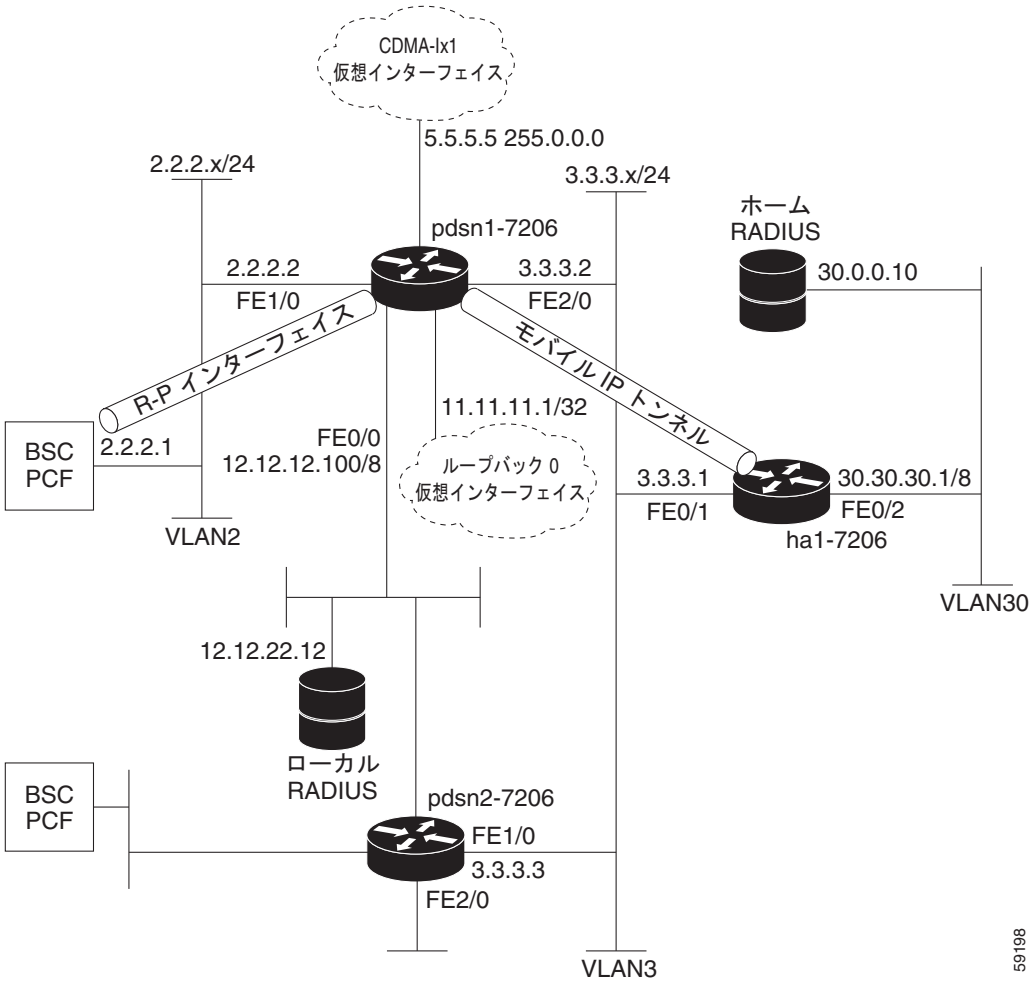
HA 環境で RADIUS を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

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

設定例

図 1 およびそれに続く情報は、Cisco HA の配置と設定の例です。

図 1　　HA：ネットワーク マップ



例 1　　HA の設定

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

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

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

制約事項

同時バインディング

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

セキュリティ

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

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

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

RFC

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

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

規格

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

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

MIB

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

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

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

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

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

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

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

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

マニュアルの入手方法およびテクニカル サポート

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

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

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