CHAPTER 16

その他の設定作業

その他の設定作業

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

HA：レルム ケース インセンシティブ オプション

Network Access Identifiers（NAI; ネットワーク アクセス識別子）には、ユーザ名とレルムの 2 つのパラメータが含まれています。ユーザ名 @ レルムの形式で記述されます。HA 5.0 では、ユーザ名とレルムの両方ともがケース センシティブです。Foreign Agent（FA; 外部エージェント）から、NAI とともに Registration Request（RRQ; 登録要求）を受信した場合、HA は設定されたコマンドと照合する必要があります。HA 5.0 は、ユーザ名とレルムの両方にケース センシティブで一致するものを検索します。

レルム ケース インセンシティブ機能によって、ケース インセンシティブのレルム パラメータを使用して、RRQ NAI と設定されたコマンドを照合できます。ただし、その場合もユーザ名はケース センシティブと見なされます。

例 1：

ローカル設定

```
router(config)#ip mobile host nai @sprintpcs.com interface Null0
```

次の NAI （同一のレルムの異なるケース）は、上述の設定に一致します。

- mobile1@sprintpcs.com
- mobile2@sprintPCS.com
- mobile3@sprintPCS.COM
- mobile4@SPRINTPCS.COM
- mobile5@sPrInTpCs.cOm

例 2：

ローカル設定

```
router(config)#ip mobile host nai mobile6@sprintpcs.com interface Null0
```

次の NAI（同一のユーザ名の異なるケース）は、上述の設定 Command-Line Interface（CLI; コマンドライン インターフェイス）に一致しません。

- Mobile6@sprintpcs.com
- MoBiLe6@SPRINTPCS.COM
- MOBILE6@sprintpcs.com

レルム ケース インセンシティブ機能の設定

レルム ケース インセンシティブ機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile options`	モバイル IP オプションを入力するためのサブ コンフィギュレーション モードを開始します。
	`Router(config)# realm case-insensitive`	レルム ケース インセンシティブ機能をイネーブルにします。

次に、例を示します。

```
HA(config)#ip mobile options
HA(config-ipmobile-options)#realm case-insensitive
```

次は、コマンドを確認する方法の例です。

```
router#show ip mobile options
IP Mobility Options information:

Realm (Domain) match is case insenstive
```

制限事項および制約事項

この機能の制限事項および制約事項は次のとおりです。

- レルムがケース インセンシティブである同一の NAI を持つ RRQ は、同一の Mobile Node（MN; モバイル ノード）から送信されたと見なされます。たとえば、"user1@cisco.com" と "user1@CISCO.COM" は、同一の MN から送信されたと見なされます。
- アクティブなセッションが存在するときは、レルム ケース インセンシティブのイネーブルまたはディセーブルを変更できません。
- レルム ケース インセンシティブは、ユーザ名、**debug condition username** *nai* を使用する条件付きデバッグでは機能しません。あるユーザで条件付きデバッグをイネーブルにするには、ケース センシティブ NAI を使用する必要があります。

FA-HA 認証エクステンションの義務化

HA は、HA が Mobile IP（MIP; モバイル IP）RRQ 内で FA-HA エクステンションを要求するか、または、RRQ を拒否することを強制できる必要があります。この機能は、該当する **ip mobile secure foreign-agent** コマンドが設定されていない RRQ を拒否します。現時点で、RRQ を HA に送信し、FA-HA エクステンションを省略し、さらに、その FA IP アドレスに **ip mobile secure foreign-agent** コマンドが設定されていない場合、RRQ は受け入れられます。これはセキュリティ リスクであると考えられます。

現時点で、HA は、**FA Access-Type** コマンドのローカル設定に基づいた、RRQ または失効メッセージで Wimax FA から受信した Foreign-Home Authentication Extension（FHAE）エクステンションを許可します。HA は、Wimax FA の受信 MIP RRQ の FHAE を許可する次のコマンドをサポートします。

ip mobile home-agent foreign-agent *fa-address mask* **access-type wimax {enable-fhae | disable-fhae}**

上のコマンドは、3gpp2 アクセス タイプのために変更され、3gpp2 FA に対するキーワード **enable-fhae** および **disable-fhae** が追加されました。この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent foreign-agent {default | {fa-address mask}} access-type {wimax | 3gpp2} [enable-fhae | disable-fhae]`	Wimax または 3gpp2 FA から RRQ または失効メッセージ内で受信される FHEA エクステンションを設定します。

次は、設定の詳細です。

- 同一のアドレスおよび option-less/enable-fhae から disable-fhae までの FA のマスク値に対するコマンド オプションが変更されるときは必ず、HA はすでに保存されたこれらの FA の FA-HA キーをクリアします。
- 設定されたアドレスおよびマスク値に対する Access-type オプションが変更される場合、HA はすでに保存された FA-HA キーを削除します。

HA 上の RRQ 処理

次のシナリオは、HA がこれらのシナリオの RRQ を処理する方法を示します。

シナリオ -1

次のコマンドでは、FA のアクセス タイプは、**enable-fhae** または **disable-fhae** を使用して設定されません。

```
ip mobile home-agent foreign-agent default access-type 3gpp2
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax.
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2.
```

次のコマンドを使用して、3gpp2 FA の FA-HA キー値を HA 上でローカルに設定します。

ip mobile secure foreign-agent *start-ip end-ip* spi …..

ケース 1 :

3GPP2 FA、RRQ に FHAE がある。

a. FA-HA キーはローカルに設定されます。
RRP は、FHAE とともに正常に送信されます。

b. FA-HA キーはローカルに設定されません。
RRP はエラーコード 132 とともに（FHAE なしで）送信されます。

3GPP2 FA、RRQ に FHAE がない。

a. FA-HA キーはローカルに設定されます。
RRP はエラー コード 132 および FHAE とともに送信されます。

b. FA-HA キーはローカルに設定されません。
RRP は、FHAE なしで正常に送信されます。

ケース 2：

Wimax FA、RRQ に FHAE がある。

a. FA-HA キーは、HA-RK から作成済みであるか、または、HA-RK がすでに存在します。
アクセス要求は HA-RK のためには送信されないが、別の目的で送信される可能性があります。
RRP は FHAE とともに正常に送信されます。

b. FA-HA キーは存在せず、かつ、HA-RK は存在しません。アクセス要求が送信されます。
- HA-RK はダウンロードされます。
- RRP は FHAE とともに正常に送信されます。

c. HA-RK はダウンロードされません。

- RRQ はドロップされ、RRP は送信されません。

Wimax FA、RRQ に FHAE がない。

a. FA-HA キーは、HA-RK から作成済みです。または、この FA からの以前の RRQ に FHAE があります。
RRP は、エラー コード 132 および FHAE とともに送信されます。

b. FA-HA キーが存在しません。この FA からの RRQ に FHAE が 1 つもありません。
RRP は正常に送信されます。

シナリオ -2

FA のアクセス タイプは、次のコマンドで **enable-fhae** を使用して設定されます。

```
ip mobile home-agent foreign-agent default access-type 3gpp2 enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 enable-fhae
```

3gpp2 FA の FA-HA キーを HA 上でローカルに設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	3gpp2 の FA-HA キーを HA 上でローカルに設定します。

ケース 1：

3GPP2 FA、RRQ に FHAE がある。

a. FA-HA キーはローカルに設定されます。
RRP は、FHAE とともに正常に送信されます。

b. FA-HA キーはローカルに設定されません。
RRP はエラーコード 132 とともに（FHAE なしで）送信されます。

3GPP2 FA、RRQ に FHAE がない。

a. FA-HA キーはローカルに設定されます。
RRP には FHAE が追加され、エラー コード 132 とともに送信されます。

b. FA-HA キーはローカルに設定されません。
RRP はエラーコード 132 とともに、FHAE なしで送信されます。

ケース 2 :

Wimax FA、RRQ に FHAE がある。

a. FA-HA キーは、HA-RK から作成済みであるか、または、HA-RK がすでに存在します。
アクセス要求は HA-RK のためには送信されないが、別の目的で送信される可能性があります。
RRP は FHAE とともに送信されます。

b. FA-HA キーは存在せず、かつ、HA-RK は存在しません。
アクセス要求が送信されます。

a.HA-RK はダウンロードされます。
RRP は FHAE とともに送信されます。

b.HA-RK はダウンロードされません。
RRQ はドロップされ、RRP は送信されません。

Wimax FA、RRQ に FHAE がない。

a. FA-HA キーは、HA-RK から作成済みです。この FA からの以前の RRQ に FHAE があります（この結果は、HA-RK ライフタイムの期限が切れたために FA-HA キーが削除される場合でも同様です。この FA に FHAE を 1 回使用するだけで、この条件を満たします）。
RRP は、FHAE なしで送信されます - （FA 認証失敗エラーコード）。

b. FA-HA キーが存在しません。
HA-RK がダウンロードされるかどうかに関係ありません。RRP は、エラー コード 132 とともに、FHAE なしで送信されます。

シナリオ -3

FA のアクセス タイプは、次のコマンドで **disable-fhae** を使用して設定されます。

```
ip mobile home-agent foreign-agent default access-type 3gpp2 disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 disable-fhae
```

FA-HA キー値を HA 上でローカルに設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	FA-HA キーを HA 上でローカルに設定します。

ケース 1 :

3GPP2 FA、RRQ に FHAE がある。

a. FA-HA キーは、ローカルに設定されません。
アクセス要求は（FA-HA 入手のために）送信されません。
RRP は、エラー コード 132 とともに（FHAE なしで）送信されます。

3GPP2 FA、RRQ に FHAE がない。

a. FA-HA キーはローカルに設定されません。
RRP は、（FHAE なしで）正常に送信されます。

ケース 2 :

Wimax FA、RRQ に FHAE がある。

a. FA-HA キーは存在せず、かつ、HA-RK は存在しません。
アクセス要求が送信されます。
a.HA-RK はダウンロードされます。
b.RRP は FHAE なしで送信されます。

b. HA-RK はダウンロードされません。
RRP は FHAE なしで送信されます。

Wimax FA、RRQ に FHAE がない。

a. FA-HA キーが存在しません。
RRP は FHAE なしで送信されます。

失効メッセージの処理および開始

シナリオ -1

次のコマンドでは、FA のアクセス タイプは、**enable-fhae** または **disable-fhae** を使用して設定されません。

```
ip mobile home-agent foreign-agent default access-type 3gpp2
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax.
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2.
```

3gpp2 FA の FA-HA キー値を HA 上でローカルに設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	3gpp2 の FA-HA キーを HA 上でローカルに設定します。

- 3ggp2 FA の場合、HA は FHAE ベースの FA-HA キー設定を使用して（または使用せずに）Registration Revocation メッセージを認証することによって、Registration Revocation メッセージを FA に送信します。
- Wimax FA の場合、HA-RK キー タイマーが期限切れになるか、または HA-RK キーか FA-HA キーが利用できないときは、HA は Registration Revocation メッセージを FA に送信しません。
- Registration Revocation メッセージに FHAE があり、対応する FA の FA-HA キーを HA がローカルに持たない場合、HA は FA から受信した Registration Revocation メッセージをドロップします。これは、3gpp2 FA および Wimax FA の両方に当てはまります。
- 受信メッセージに FHAE がなく、一方で 3gpp2 の FA-HA キーによって HA 上でローカルに設定されているか、または、Wimax の FA-HA キーがすでに生成されている場合、HA は FA から受信した Registration Revocation メッセージをドロップします。
- その他の場合は、HA は Registration Revocation メッセージを処理または開始します。

シナリオ -2

FA のアクセス タイプには、次のコマンドの **enable-fhae** にオプションがあります。

```
ip mobile home-agent foreign-agent default access-type 3gpp2 enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax enable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 enable-fhae
```

3gpp2 FA の FA-HA キーを HA 上でローカルに設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	3gpp2 の FA-HA キーを HA 上でローカルに設定します。

- 3ggp2 FA の場合、HA は FA-HA キーがローカルに利用できない場合、Registration Revocation メッセージを FA に送信しません。
- Wimax FA の場合、HA-RK キー タイマーが期限切れになるか、または HA-RK キーか FA-HA キーが利用できないときは、HA は Registration Revocation メッセージを FA に送信しません。
- 受信メッセージに FHAE がなく、一方で 3gpp2 の FA-HA キーによって HA 上でローカルに設定されているか、または、Wimax のキーがすでに生成されている場合、HA は FA からの受信した Registration Revocation をドロップします。
- その他の場合は、HA は Registration Revocation メッセージを開始します。

シナリオ -3

```
ip mobile home-agent foreign-agent default access-type 3gpp2 disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type wimax disable-fhae
ip mobile home-agent foreign-agent <ip> <mask> access-type 3gpp2 disable-fhae
```

FA-HA キー値を HA 上でローカルに設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile secure foreign-agent start-ip end-ip spi`	FA-HA キー値を HA 上でローカルに設定します。

- HA は Registration Revocation メッセージに FHAE がある場合、FA から受信した Registration Revocation メッセージをドロップします。これは、3gpp2 FA および Wimax FA の両方に当てはまります。
- その他の場合は、HA は Registration Revocation メッセージを開始します。

NAI ごとの絶対タイムアウト

データパス アイドル タイマーの場合、設定されたインターバルの間中アイドル（トラフィックがない）のままであるときは常にユーザが削除されます。しかし、絶対タイマーは開始されたときに、ユーザがアクティブであってもユーザを削除します。

この機能は、ユーザがトラフィックを送信しているかいないかにかかわらず、タイマーが期限切れになったときにユーザのセッションを切断するために、セッションに絶対タイムアウトをローカルにまたは Radius Access Accept を使用して設定します。現時点で、HA はホットラインユーザの場合に Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）アトリビュート、session-timeout（27）をサポートします。絶対タイマーに同じアトリビュートが拡張されます。

絶対タイマーの開始は、登録中だけに限る必要があります。また、絶対タイマーは、バインディングが削除されるまで変更しないでください。絶対タイマーが登録中に受信されず、再登録中に受信された場合、絶対タイマーは開始されません。絶対タイマーは、初期登録に対してだけ意味を持ちます。

絶対タイマーは、ホットライン タイマーからは独立して動作します。絶対タイマーが設定されると、クロックが進み、期限切れになったときにバインディングを削除します。

冗長構成の場合でも使用でき、絶対タイムアウト値は、スタンバイと同期する必要があります。

絶対タイムアウト機能の設定

HA がセッションに対する絶対タイムアウトをセットすることをイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile realm realm absolute-time interval-in seconds`	**absolute-time** を HA 上でローカルに設定します。Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）から Session- Timeout（27）がダウンロードされる場合、より高い優先順位が与えられ、ローカルに設定された **absolute-time** 値が上書きされます。

設定の確認

次に、設定の確認とトラブルシューティングに役立つ複数の例を示します。

3GPP2 バインディングの場合、出力は次のとおりです。

```
# show ip mobile binding

Mobility Binding List:
Total 1
derath5@cisco.com (Bindings 1):
    Home Addr 65.0.0.2
    Care-of Addr 50.1.1.92, Src Addr 50.1.1.92
    Lifetime granted 02:00:00 (7200), remaining 01:59:52
    Flags sBdmg-T-, Identification CD735149.00000005
    Tunnel0 src 14.0.0.2 dest 50.1.1.92 reverse-allowed
    Tunnel0 Output ACL: p1_test - ACL is empty or not configured
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Acct-Session-Id: 0x00000002
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Absolute session time granted 00:01:00 (60), remaining 00:00:52
    Traffic Plane Id:6
```

WiMAX バインディングの場合、出力は次のとおりです。

```
HA-Slot3#show ip mobile binding
Mobility Binding List:
Total 1
sony6@cisco.com (Bindings 1):
    Home Addr 65.0.0.3
    Care-of Addr 50.1.1.90, Src Addr 50.1.1.90
    Lifetime granted 02:00:00 (7200), remaining 01:59:07
    Flags sBdmg-T-, Identification CD7352EA.00000006
    Tunnel0 src 14.0.0.2 dest 50.1.1.90 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: WiMAX(802.16e)
    Acct-Session-Id: 0x00000004
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Absolute session time granted 00:02:00 (120), remaining 00:01:07
    Traffic Plane Id:5
```

ホットライン タイマーおよび絶対タイマーの両方がバインディングに存在する場合、出力は次のとおりです。

```
HA-Slot3#show ip mobile binding
Mobility Binding List:
Total 1
derath5@cisco.com (Bindings 1):
    Home Addr 65.0.0.2
    Care-of Addr 50.1.1.92, Src Addr 50.1.1.92
    Lifetime granted 02:00:00 (7200), remaining 01:59:49
    Flags sBdmg-T-, Identification CD7358E6.00000005
    Tunnel1 src 14.0.0.2 dest 50.1.1.92 reverse-allowed
    Routing Options - (B)Broadcast (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Acct-Session-Id: 0x00000009
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Hotline status Active
    Hotline session granted 00:01:00 (60), remaining 00:00:49
    Radius Disconnect Enabled
    Absolute session time granted 00:01:00 (60), remaining 00:00:49
    Traffic Plane Id:6
```

この機能が設定されている場合、次の新しいデバッグ ステートメントが表示されます。

```
MobileIP: Absolute timer expired for MN derath5@cisco.com
MobileIP: MN id for addr freeing is derath5@cisco.com careof 50.1.1.92
MobileIP: De-allocating AAA ID: 0x00000009
MobileIP: MN derath5@cisco.com Tunnel route deleted for 65.0.0.2/255.255.255.255 via
gateway50.1.1.92
MobileIP: Deleted Tunnel1 src 14.0.0.2 dest 50.1.1.92
MobileIP: Delete database info. for MN 65.0.0.2
MobileIP: MN id for addr freeing is derath5@cisco.com careof 50.1.1.92
MobileIP: MN derath5@cisco.com Tunnel route deleted for 65.0.0.2/255.255.255.255 via
gateway50.1.1.92
MobileIP: Deleted Tunnel0 src 14.0.0.2 dest 50.1.1.92
MobileIP: De-allocating AAA ID: 0x00000007
MobileIP: Delete database info. for MN 65.0.0.2
```

制約事項および制限事項

- HA は、スタンバイ Control Plane（CP; コントロール プレーン）のバインディングを削除しないでください。そうでない場合、アクティブからのバインディングの削除が失敗し、エラー統計情報に表示されます。

  次の特殊なケース/レース コンディションは、個別に処理されます（例、1 レース コンディション）。

  - アクティブ/スタンバイ上にバインディングが作成されます。
  - アクティブおよびスタンバイ上でタイマーが期限切れになります。
  - タイマーが期限切れになったため、バインディングがアクティブから削除されますが、スタンバイからは削除されません。
  - アクティブからスタンバイにバインディング削除イベントが送信される前に切り替えが発生します。
  - スタンバイがアクティブになり、絶対タイマーが期限切れになったバインディングを所持します。

  上のケースを処理するには、スタンバイ上で絶対タイマーを停止し、最初に開始したときのインターバルで再スタートします。このインターバルが終了した後、バインディングは削除されます。

トンネル インターフェイスでのアクセス制御リスト（ACL）のサポート

シスコのトンネル テンプレート機能を使用すると、作成済みのスタティック トンネルの Access Control List（ACL; アクセス制御リスト）設定を Home Agent で起動されたダイナミック トンネルに適用できます。トンネル テンプレートは、Home Agent と PDSN/Foreign Agent の間のトンネルに定義され、適用されます。

モバイル IP トンネル テンプレート機能の設定

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

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

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

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

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

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

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

MN-HA-SPI（26/57）

MN-HA-SHARED-KEY（26/58）

このサポートの手順は次のとおりです。

ステップ 1　HA が PDSN/FA から RRQ を受信します。

ステップ 2　HA が AAA に Access Request を送信します。HA は RRQ の Mobile-Home Authentication Extension（MHAE）Security Parameter Index（SPI; セキュリティ パラメータ インデックス）を MN-HA-SPI（26/57）アトリビュートとして Access Request に追加します。

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

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

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

（注）　MN-HA キーおよび SPI が 3gpp2 アトリビュート（57/58）を使用する AAA からダウンロードされている場合、HA は MD5 アルゴリズムだけを使用して MHAE を認証します。

ユーザ プロファイル

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

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

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

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

Home Agent は最大 200,000 のユーザ プロファイルのローカル設定をサポートしています。Service Application Module for IP（SAMI）では、HA は 6 × 200,000 のユーザ プロファイルをサポートします。ユーザ プロファイルは、NAI で識別され、ローカルに設定することも、AAA サーバから取得することもできます。

モビリティ バインディング アソシエーション

Home Agent は、モビリティ バインディングを次の方法で識別します。

- スタティック IP アドレス割り当ての場合は、NAI + IP
- ダイナミック IP アドレス割り当ての場合は、NAI
- **show ip mobile binding** コマンドを使用すると、各ユーザのモビリティ バインディング情報が表示されます。

バインディング アソシエーションには、次の情報が含まれています。

- Care-of-Address（CoA; 気付アドレス）
- ホーム アドレス
- アソシエーションのライフタイム
- Signaling identification フィールド

アップストリーム パスでのモバイル ステーション（MS）トラフィック リダイレクション

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

HA バインディングのアップデート

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

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

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

（注） Home Agent がバインディング アップデート メッセージをグローバルベースで送信するように設定することもできます。

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

選択的なモバイル ブロッキング

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

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

（注）　"mobileip:prohibited" アトリビュートは 0 と 1 以外の値に設定できません。

移動体識別番号（MEID）のサポート

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

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

Offset=0 による第 1 パケットのフラグメント サイズの設定

この機能を使用すると、ネットワークでの第 2 フラグメントのさらなるフラグメンテーションを避けるために、第 1 フラグメント サイズを設定できます。また、IP フラグメンテーションの発生時には、第 1 フラグメントに内部パケットの L4 ヘッダー情報は含まれません。これが原因となって、L4 までのディープ インスペクションを実施するネットワークのファイアウォールで、第 1 フラグメントがドロップされる可能性があります。

この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Router#**ip fragment first minimum size** *size*	さらなるフラグメンテーションを避けるために第 1 セグメント サイズを設定します。範囲は *8* ～ *560* バイトです。サイズは、ペイロードだけを含み、ヘッダーは含まれません。

（注）　「ペイロード サイズ」は 8 バイトの倍数である必要があります。そうでない場合は、"%% First fragment payload size is not in multiples of 8 bytes" というエラーメッセージとともにコマンドが拒否されます。

これは、IP レベルのコマンドであり、サイズ設定は IP パケットのペイロードだけを考慮に入れます。

たとえば、第 1 フラグメント サイズを 48 バイトと設定すると、20 バイトの IP ヘッダーを含めて、68 バイトのサイズで第 1 フラグメントが作成されます。

IP-IP トンネル パケットの場合、設定されたペイロード サイズは内部 IP ヘッダーを含みます。フラグメンテーション コードの場合、内部 IP は、外部 IP ヘッダーへのペイロードと見なされます。

- コマンド設定は、第 1 フラグメントのペイロードの最小値を示すだけです。Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）の既存のフラグメンテーション メカニズムが、設定値より大きい第 1 フラグメントを選択する場合は、設定は実施されません。そうでない場合は、Broadband Wireless Gateway（BWG）は想定よりも多くのフラグメントを生成します。
- また、設定された第 1 フラグメント サイズが出力インターフェイスの Maximum Transmission Unit（MTU; 最大伝送ユニット）を上回る場合は、設定値は実現されません。

次の例は、IP パケット、および IP-IP トンネルパケットの場合のパケットの状態を示しています。

```
router(config)# ip fragment first minimum size 80
IP Packet:

10:27:59.660 IST Mon Apr 13 2009                Relative Time: 2.990258
Packet 8 of 26                                  In: FastEthernet0/1

Ethernet Packet:  114 bytes
      Dest Addr: 0003.FEAB.D871,   Source Addr: 001F.6C89.0D74
      Protocol: 0x0800

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 100,   ID: 0x0092,   Flags-Offset: 0x2000 (more fragments)
      TTL: 255,   Protocol: 1 (ICMP),   Checksum: 0x582D (OK)
      Source: 50.1.1.200,     Dest: 13.2.2.15

ICMP  Type: 8,   Code: 0  (Echo Request)
      Checksum: 0x1A45 ERROR: C661
      Identifier: 006A,  Sequence: 0000
Echo Data:
    0 : 0000 0000 E794 B5A4 ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   20 : ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   40 : ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD  ..................
   60 : ABCD ABCD ABCD ABCD ABCD ABCD ............


IP-IP tunnel packet:
20:39:40.394 IST Sun Apr 12 2009                Relative Time: 2.967188
Packet 7 of 22                                  In: FastEthernet0/1

Ethernet Packet:  114 bytes
      Dest Addr: 0003.FEAB.D871,   Source Addr: 001F.6C89.0D74
      Protocol: 0x0800

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 100,   ID: 0x8008,   Flags-Offset: 0x2000 (more fragments)
      TTL: 255,   Protocol: 4 (IP-IP),   Checksum: 0xD9F5 (OK)
      Source: 14.0.0.1,     Dest: 50.1.1.150

IP    Version: 0x4,  HdrLen: 0x5,  TOS: 0x00
      Length: 1500,   ID: 0x0086,   Flags-Offset: 0x0000
      TTL: 255,   Protocol: 1 (ICMP),   Checksum: 0x40D0 (OK)
      Source: 50.1.1.200,     Dest: 65.0.0.2

ICMP  Type: 8,   Code: 0  (Echo Request)
      Checksum: 0x72CB ERROR: 7C6A
```

```
      Identifier: 005E,  Sequence: 0000
Echo Data:
    0 : 0000 0000 E49E 6020 ABCD ABCD ABCD ABCD ABCD ABCD
```

FA-HA IP-in-IP トンネルに対する一意の IP ID の保護

この機能は、単一 IP アーキテクチャにおける数十万のセッションをサポートします。これは、パケットがフラグメントする可能性があるときにだけ、IP ヘッダーに一意の ID を設定することで実現されます。そうでない場合は、IP ヘッダーの ID フィールドは **0** に設定されます。

この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	Router#**ip mobile tunnel ip-ip conserve-ip-id threshold** *value*	パケットがフラグメントする可能性があるとき、IP ヘッダーに一意の ID を設定します。しきい値の範囲は *576-1500* であり、外部 IP パケット サイズを示します。 この機能は、IP-IP トンネルの場合にだけサポートされます。

ip mobile tunnel ip-ip conserve ip-id threshold コマンドを設定する場合、パケット サイズが**しきい値**を上回るときは、パケットは、外部 IP ヘッダーに一意の IP ID を設定されて送信されます。そうでない場合は、ID フィールドは **0** に設定されます。しきい値を 1400 バイトに設定すると、サイズが 1401 以上のパケットは、一意の IP ID を設定されて送信されます。

この機能は、デフォルトの動作ではありません。このコマンドを使用してイネーブルにする必要があります。さらに、デフォルトのしきい値はありません。

China Telecom アトリビュートの Vendor-Specific Extensions（VSE）サポート

HA リリース 5.1（単一 IP アーキテクチャである）では、この機能のサポートの一部として、次の点が変更されました。

- アクティブとスタンバイの間のこれらの NVSE / アトリビュートの同期が、HA 5.0 に導入された SR インフラストラクチャを使用して正しく作動することを保証する。
- CP と Traffic Plane（TP; トラフィック プレーン）の間のこれらの NVSE の同期が正しいことを保証する。
- インターフェイスとアカウンティングが正しく動作することを保証する。
- **show ip mobile binding** の出力がこの情報を示すアトリビュートを表示することを保証する。

  次は、出力の例です。

```
Active-HA#sh ip mobile binding
    Mobility Binding List:
Total 1
ct-cisco@cisco.com (Bindings 1):
        Home Addr 60.0.2.1
    Care-of Addr 4.0.2.3, Src Addr 4.0.2.3
    Lifetime granted 00:33:20 (2000), remaining 00:33:15
    Flags sbdmg-t-, Identification C1F3C1D5.0000000F
    Tunnel1 src 40.0.11.20 dest 4.0.2.3 reverse-allowed
```

```
Routing Options -
Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
Acct-Session-Id: 0x00000005
Sent on tunnel to MN: 0 packets, 0 bytes
Received on reverse tunnel from MN: 0 packets, 0 bytes
Radius Disconnect Enabled
Correlation Id cisco-ha(vendor id 20942)
Calling Station Id cisco
Served MDN CT-MDN
Charging Type 0x00000001
Traffic Plane Id:7
```

次のアトリビュートは、この機能の一部としてサポートされます。

- Correlation-Id
- Calling-Station-Id
- Served-MDN
- Charging-Type
- HA-Service-Address

また、この機能のサポートの一部として、FA および AAA サーバとの相互動作が若干変更されました。次のサブセクションに詳細情報を示します。

FA との相互動作

この機能のサポートによって、HA は RRQ で受信される次のアトリビュートを処理します

- **Calling-Station-Id**

  HA は、RRQ で受信される CT NVSE Calling Station ID（CLID; 発信ステーション ID）アトリビュートの処理をサポートします。これによって、PDSN/FA はユーザの IMSI を CT NVSE アトリビュートとして HA に送信できます。

- **Correlation-Id**

  HA は、MobileIP のベンダー固有アトリビュートのために RFC 3115 に定義される形式で、FA から受信した Correlation-Id を処理します。

  HA が再登録中に RRQ で correlation-id アトリビュートまたは calling-station-id アトリビュートの新しい値を受信したとき、HA は MIP セッションの Accounting Stop および Accounting Start を送信します。

AAA との相互動作

HA は、AAA との認証とアカウンティングのための相互動作中に、次のアトリビュートを処理します。

- **Correlation-Id**

  RRQ で受信した Correlation-Id は、Accounting Start/Stop/Interim メッセージで、AAA サーバへ送信されます。このアトリビュートは、AAA との認証中には含められません。

- **Calling-Station-Id**

  RRQ で受信した Calling-Station-Id は、AAA との MN サブスクライバの認証中にアクセス要求で送信されます。このアトリビュートも、Accounting Start/Stop/Interim メッセージで AAA サーバへ送信されます。HA は、Calling-Station-Id を RFC 2865 で定義された標準 RADIUS Attribute（31）の形式で AAA へ送信します。

- **Served-MDN**

  HA は、AAA サーバとの認証の成功後に、Served MDN 値を Access-Accept で受信します。受信したアトリビュートは、Accounting Start/Stop メッセージで、アカウンティングの目的のために AAA にだけ送信されます。

- **Charging-Type**

  HA は、AAA サーバとの認証の成功後に、Charging-Type 値を Access-Accept で受信します。受信したアトリビュートは、Accounting Start/Stop メッセージで、アカウンティングの目的のために AAA にだけ送信されます。

  Charging-Type 値は次を含みます。

  - 0x00000001：ポストペイド アカウンティング
  - 0x00000002：プリペイド アカウンティング
  - 0x00000003：ポストペイド アカウンティングおよびプリペイド アカウンティングの両方

- **HA-Service-Address**

  HA は、ユーザの HA サービス アドレスをアカウンティング開始メッセージの中で AAA に送信します。

表 16-1 は、HA が AAA との相互動作の中でどのように各種の Radius メッセージ（RFC 2865 および 2866）に組み込むかを示しています。

表 16-1　AAA 中の HA アトリビュート Radius メッセージ

アトリビュート	アトリビュート値	Access-Request	Access-Accept	Accounting-Start	Accounting-Stop	Accounting-Interim-Update
Calling-Station-Id	31	0-1	0	0-1	0-1	0-1
Correlation-Id	26/5535/44	0	0	0-1	0-1	0-1
Served-MDN	26/ 20942/ 100	0	0-1	0-1	0-1	0
Charging-Type	26/ 20942/ 101	0	0-1	0-1	0-1	0
HA-Service-Addres	26/5535/7	0	0	0-1	0-1	0

代替 MN ID のサポート

現時点で、Home Agent はサブスクライバの一意な識別に NAI を使用しています。China Telecom オペレータ ネットワークでは、すべてのモバイル ノードが同一の NAI を持ち、発信ステーション ID（CLID）で識別されます。このため、Home Agent は、サブスクライバを一意に識別するために別のアトリビュートを使用するように拡張されます。China Telecom の場合、代替 MN ID は CLID です。

CLID の形式仕様は、NAI 形式のサブセットです。CLID モードでは、HA はシステム内のバインディング識別に CLID を使用します。したがって、NAI には同じ値を持ち、CLID には異なる値を持つ 2 つの RRQ が 2 つの異なるバインディングとして識別されます。

認証、認可、アカウンティングのために、RRQ で受信された NAI のレルム部分がシステム内の設定の識別のために使用されます。

このモードでは、HA が CT CLID NVSE のない RRQ を受信した場合、HA は RRQ を拒否し、該当するカウンタ（Bad Request）が増分されます。

HA は、（グローバル コンフィギュレーションに基づいて）NAI または CLID ベースのバインディング ID のいずれかをサポートします。システムにアクティブ バインディングがある場合、代替 MN ID オプションの動的変更はできません。

この機能を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent options`	（任意）IP Mobile Home Agent オプションの設定をイネーブルにして、IP Mobile Home Agent オプション コンフィギュレーション サブモードを開始します。
ステップ 2	`Router(config-ipmobile-ha-options)#mn-identifier calling-station-id`	（任意）CLID を代替モバイル ノード ID としてイネーブルにします。システムにアクティブなバインディングがある場合は、この CLI をイネーブルまたはディセーブルにできません。

設定を確認するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router# show ip mobile binding`	モビリティ バインディング テーブルを表示します。

次に、例を示します。

```
router#sh ip mob bind
Mobility Binding List:
Total 1
Total VPDN Tunnel'ed 0
111111111111450 (Bindings 1):
    Home Addr 1.1.1.14
    Care-of Addr 10.5.1.2, Src Addr 10.5.1.2
    Lifetime granted 00:08:20 (500), remaining 00:05:17
    Flags sbdmg-t-, Identification CDE8617E.00000008
    Tunnel0 src 86.6.6.6 dest 10.5.1.2 reverse-allowed
    Routing Options -
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Revocation negotiated - I-bit set
    Acct-Session-Id: 0x00000015
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Radius Disconnect Enabled
    Correlation Id 8(vendor id 20942)
    Calling Station Id 111111111111450
    NAI  ctc_user8@ispxyz.com <--- RRQ nai for this binding.
    Traffic Plane Id:4
```

コール アドミッション制御（CAC）のサポート

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

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

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

上記の 2 つのパラメータによる式は、次のようになります。

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

HA での CAC の設定

HA で許可される最大バインディング数を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent max-binding` *max-binding-value*	HA でオープンできるバインディングの数を制限します。max-binding-value のデフォルト値は 235,000 です。

輻輳制御機能

Cisco Mobile Wireless Home Agent Release 5.0 では、輻輳制御機能のために、Home Agent が実施するコール アドミッション制御アルゴリズムを、輻輳状態に到達したと判定したときにアクションを実行するように変更することが必要です。

輻輳が発生したかどうかを判定するために、DFP 重みを設定できます。一般に、DFP 値は輻輳状態の 70% に対応します。デフォルトで、DFP 重みは **0 ～ 24** の範囲内です。値の必須範囲を設定するために、最大重みを設定できます。**0** は、使用される最大リソースに対応し、最大スケール値はリソースが 100 % 使用できることを示します。

使用される DFP 値は、単に、単一 IP モデルのコントロール プロセッサ向けにだけ計算されます。トラフィック プレーン プロセッサ リソース利用が輻輳の一因となることは予想されません。

輻輳状態に到達した場合、次の 4 つのアクションが実行可能です。

- Reject : 新しい発呼をすべて拒否します。エラーコード 130 （不十分なリソース）を含む MIP Registration Reply が送信されることで、拒否が示されます。
- Abort : 新しい発呼をすべて拒否し、「進行中」のコールを打ち切ります。進行中とは、Registration Request が受信され、Registration Reply が送信されていない MIP Registration を意味します。エラーコード 130 （不十分なリソース）を含む MIP Registration Reply が送信されることで、拒否が示されます。
- Redirect : 新しい発呼をすべて拒否し、「進行中」のコールを打ち切ります。進行中とは、Registration Request が受信され、Registration Reply が送信されていない MIP Registration を意味します。エラーコード 136（未知の Home Agent アドレス）を含む MIP Registration Reply が送信されることで、拒否が示されます。Home Agent アドレス フィールドには、発呼のリダイレクト先の Home Agent のアドレスが含まれます。to-be-redirected-to-address は、Home Agent でグローバルに設定されます。
- Drop : 既存のコールがデータ パス アイドル タイマー評価に基づいてドロップされます。設定された値を超えるデータ パス アイドル タイムのあるバインディングは解放されます。このとき、Resource Revocation メッセージが（設定されていれば）送信されます。Resource Revocation が設定されていない場合は、ローカル バインディングのクリアが要求されたときのように、バインディングがメッセージなしに削除されます。

（注）　一度に 1 つのアクションしか設定できません。第 2 のアクションを設定しようとすると、第 1 のアクションが上書きされます。

輻輳制御機能の設定

輻輳トリガーが発生したときのコール アドミッション制御アクションを定義するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent congestion` *dfp_weight* **action | reject | abort | redirect** *HA-address* **| drop data-path-idle** *minutes*	輻輳トリガーが発生したときのコール アドミッション制御アクションを定義します。
ステップ 2	`Router# show ip mobile home-agent congestion`	次の情報を表示します。 • 輻輳状態：混雑しているか、いないか。 • 設定された congestion-threshold 値 = 設定された CLI での dfp_weight。 • 現在の DFP 値。現在の DFP 値とは、最近 5 分間の DFP 値の平均値です。

さらに、CISCO-SLB-CLIENT-MIB には、次の情報が含まれています。

- DFP 輻輳開始しきい値。この値を超えると Congestion On Trap が生成されます。
- DFP 輻輳減少しきい値。輻輳がこの値を下回ると Congestion Off Trap が生成されます。
- 現在の DFP 値。

次は、輻輳制御機能の出力例です。

```
router#show ip mobile home-agent congestion
Home Agent congestion information :
Current congestion level:  Congested
Configured Action : Reject
Configured threshold : 10
Current DFP value = 7
```

Framed-Pool 基準

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

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

Framed-Pool 基準機能を設定するには、次の作業を実行します。

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

次に、例を示します。

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

ローカル プールのプライオリティ メトリック

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

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

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

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

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

Network Manager からアクセスし、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）Management Information Base（MIB; 管理情報ベース）を通じてプライオリティ値を設定し、取得することも可能です。"cIpLocalPoolConfigEntry" テーブルにプライオリティ用の新しい MIB オブジェクトが追加され、プライオリティ値にアクセスできます。新しい MIB オブジェクトを使用すると、既存のローカル プールのプライオリティを変更できます。

ローカル プールのプライオリティ メトリックの設定

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

ステップ 1	router# Router(config)#**ip local pool {default | *poolname*} [*low-ip-address* [*high-ip-address*]] [group *group-name*] [cache-size *size*] [priority *1-255*] [theshold *low-threshold high-threshold*]**	リモート ピアが point-to-point（p2p; ポイントツーポイント）インターフェイスに接続したときに使用され、プール使用率が上限または下限しきい値（パーセント単位）に達したときにトラップを生成するよう、IP アドレスのローカル プールを設定します。 新しいオプション **priority** *1-255* により、プライオリティを新しく作成されたプールに割り当てることができます。このプライオリティは IP アドレスの割り当てに使用されます。
ステップ 2	Router(config)#**no ip local pool** vsa-pool 1.0.0.201 priority 180	プールの設定を解除します。

次に、例を示します。

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

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

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

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

設定の確認

設定の確認作業は次のとおりです。

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

次に、例を示します。

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


router# show ip local pool

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

モバイル IPv4 ホスト設定エクステンション（RFC4332）

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

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

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

次に示す Cisco Vendor-Specific Extensions は、モバイル ノードにホスト設定を提供します。"Host Configuration Request" エクステンションが許可されるのは、Registration Request 内だけです。

その他のエクステンションは Registration Reply に付加されます。

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

（注）　DHCP サーバからダウンロードされる場合は、DNS サフィクスは RRP に付加されません。

WiMAX AAA アトリビュート

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

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

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

- Framed IP Address : **ip mobile home-agent send-mn-address** コマンドが設定されている場合、モバイル IP RRQ で受信されたホーム アドレスはアクセス要求メッセージの Framed-IP-Address アトリビュートの値として送信されます。

（注）　Home Agent Release 4.0 ソフトウェアでは、MIP フロー（Wimax）を開くとき、アクセス要求に Framed-IP-Address アトリビュートはありません。

- WiMAX Capability：このアトリビュートは、HA の WiMax 機能を特定し、すべてのアクセス要求メッセージで送信されます。HAAA による Access-Accept メッセージでも送信されます。このアトリビュートが Access-Accept メッセージ内にある場合、このアトリビュートに含まれるのは Accounting Capabilities sub-TLV だけです。これは、そのセッションに対してサーバが選択したアカウンティング機能を示します。Access-Accept で HAAA が返したアカウンティング機能はアクセス要求で HA が指定した値と一致すると予想されます。HA は現在のところ、Access-Accept で受信した WiMAX Capability VSA を処理せず、アカウンティング機能が一致しているかどうかの確認を実行しません。
- HA-IP-MIP4：このアトリビュートは、要求を作成している HA の IP アドレスを特定します。このアトリビュートは HA からのすべてのアクセス要求メッセージに含まれます。既存のバインディングでは（再登録および削除に対応するアクセス要求）、値はそのバインディングの Home Agent アドレスに設定されます。新しいバインディングでは、このアトリビュートの値は、HA 設定でバインディングに割り当てられた HA IP アドレス（ホームアドレスではない）に設定されます。この値は RRP で Home Agent IP アドレスとして送信されます。「バインディングの Home Agent IP アドレスの設定」セクションを参照してください。
- RRQ-HA-IP：モバイル IP RRQ の Home Agent フィールド内の IP アドレスが HA の IP アドレスとは異なる場合、HA がこのアトリビュートをアクセス要求メッセージに含めます。その場合、値はモバイル IP RRQ 内の Home Agent IP アドレスに設定されます。
- MN-HA-MIP4-KEY：このアトリビュートは、MIP4 手順に使用される MN-HA キーを識別します。このアトリビュートは Access-Accept メッセージに含まれ、MN-HA-SHARED-KEY に類似しています。HA は、WiMAX サブスクライバ用の MN-HA MIP4 キーに基づいて、MN-HA Authentication エクステンションを計算します。
- MN-HA-MIP4-SPI：このアトリビュートは、MIP4 手順に使用される MN-HA SPI を識別します。このアトリビュートはアクセス要求メッセージに含まれ、MN-HA-SPI と類似しています。

表 16-2 に、Home Agent の WiMAX AAA Authorization アトリビュートを示します。

表 16-2　WiMAX AAA Authorization アトリビュート

アトリビュート名	タイプ	説明	Access Request	Access Chall.	Access Accept	Access Reject	HA 4.0 以降でのサポート
Message-Authenticator	80	AAA メッセージの整合性保護のためのメッセージ オーセンティケータ。	1	0	1	0	あり
WiMAX Capability	26/1	HA がサポートする WiMAX 機能を特定します。RADIUS サーバによって選択された機能を示します。	1	0	0-1	0	あり
Chargeable User Identity（CUI）	89	課金ユーザの ID。支払いユーザの固有の一時的ハンドルです。	0-1	0	0-1	0	あり
AAA-Session-ID	26/4	このセッションに対するホーム レルムでの固有の識別子（HAAA で設定）。	0-1	0	1	0	あり

表 16-2　WiMAX AAA Authorization アトリビュート （続き）

HA-IP-MIP4	26/6	この要求を作成している HA の IP アドレス。	0-1	0	0	0	あり
RRQ-HA-IP	26/18	Registration Request または Binding Update に含まれる HA-IP アドレス。	0-1	0	0	0	あり
MN-HA-MIP4-KEY	26/10	MIP4 手順に使用される MN-HA キー。	0	0	1	0	あり
MN-HA-MIP4-SPI	26/11	MN-HA-MIP4-KEY に関連付けられた SPI。	1	0	1	0	あり
RRQ-MN-HA-KEY	26/19	RRQ-HA-IP アトリビュートで報告される HA-IP アドレスとバウンドされる MN-HA-KEY。	0	0	0-1		あり
HA-RK-Key-Requested	26/58	HA-RK-KEY アトリビュートが Access-Accept に含まれる必要があることを示します。	1	0	0	0	あり
HA-RK-KEY	26/15	FA-HA キーの生成に使用される HA-RK キー。	0	0	0-1	0	あり
HA-RK-SPI	26/16	HA-RK と関連付けられた SPI。	0-1	0	0-1	0	あり
HA-RK-Lifetime	26/17	MIP4 操作用の FA-HA キーの生成に使用される HA-RK キー。	0	0	0-1	0	あり
Acct-Interim-Interval	85	この特定のセッションの暫定アップデート間の秒数を示します。	0	0	0-1	0	あり

"ip mobile host/realm" の AAA アトリビュート

次のアトリビュートは、この機能の一部としてサポートされます。

- アトリビュート "data-path-idle" : これは、AAA アトリビュートとして、モバイル単位でデータ パス アイドル タイマーを設定します。これは Cisco の Attribute Value pairs （AV pair; AV のペア）としてダウンロード可能です。値が AAA からダウンロードされ、ローカルにも設定される場合は AAA からダウンロードされた値が優先されます。RSIM サブスクライバ プロファイルでは、config は次のようになります。

  vsa cisco generic 1 string "mobileip:data-path-idle=300"

  変更点：

  - AAA アトリビュート "data-path-idle" を使用してバインディングが作成済みの場合で、後で **ip mobile realm** *realm* **data-path-idle** が設定されるかまたは変更されると、AAA アトリビュートなしで作成されたバインディングだけが更新されます。これによって、AAA 優先順位が維持されることが保証されます。
  - 再登録がデータ パス アイドル タイマーをアップデートする可能性があります。

- アトリビュート "Nexthop" : これは、AAA アトリビュートとして、モバイルごとにネクストホップ IP を設定します。これは Cisco の AV のペアとしてダウンロード可能です。この値が AAA からダウンロードされ、ローカルにも設定される場合は AAA からダウンロードされた値が優先されます。RSIM サブスクライバ プロファイルでは、config は次のようになります。

  vsa cisco generic 1 string "mobileip:nexthop=1.1.1.1"

  変更点：

  - AAA からダウンロードしたネクストホップを使用してバインディングが作成済みの場合で **ip mobile realm** *realm* ***any-traffic nexthop*** *ip* コマンドが設定されると、CLI は受け入れられません。

- バインディングが作成済みで、**nexthop ip** が CLI で設定されるときは、バインディングの削除の確認だけで、値が更新されます。
- 再登録はダウンロードされた nexthop アトリビュートをアップデートしません。

MN および外部エージェント認証

HA は MHAE で受信した SPI を MN-HA-MIP4-SPI アトリビュートとして HA-IP-MIP4 とともにアクセス要求に含めます。モバイル IP RRQ 内の MHAE の検証およびモバイル IP RRP の MHAE の生成には、MN-HA-MIP4-SPI アトリビュート内の HA-IP-MIP4 および SPI 値に対応する AAA からダウンロードされた MN-HA-MIP4-KEY アトリビュート値が使用されます。

次の情報が Registration Request から抽出されます。

- MN-HA Authentication エクステンションの MN-HA SPI
- Home Agent フィールドの HA IP アドレス
- 宛先 IP アドレス フィールドの受信者 IP アドレス
- FA-HA Authentication エクステンションの FA-HA SPI（このエクステンションがメッセージにある場合）

HA は、AAA サーバに送信されるアクセス要求に MN-HA-MIP4-SPI および HA-IP-MIP4 アトリビュート（それぞれに、MN-HA SPI および HA IP アドレスが含まれる）を含めます。AAA サーバからの Access-Accept には、アクセス要求のこの 2 つのアトリビュートに対応する MN-HA-MIP4-KEY アトリビュートが含まれます。HA は、ダウンロードされたキーを使用して MN-HA セキュリティ アソシエーションを設定します。セキュリティ アソシエーションは、Registration Request 内の MN-HA Authentication エクステンションの認証、および Registration Reply でのこのエクステンションの生成に使用されます。

Registration Request の Home Agent フィールドに、ダイナミック HA 割り当てを示す、すべてが 1 または 0 に設定された IP アドレスが含まれることがあります。この場合、HA は、アクセス要求内に Home Agent フィールド値に設定された追加の RRQ-HA-IP アトリビュートを含めます。MN-HA-MIP4-SPI アトリビュートは、前述のとおりです。その代わりに、HA-IP-MIP4 アトリビュートは、受信者 IP アドレスに設定されます。AAA サーバは、追加の RRQ-MN-HA-KEY アトリビュート（RRQ-HA-IP に対応）を Access-Accept に含めます。HA はこのキーを使用して、Registration Request の MN-HA Authentication を認証します。認証に成功したら、HA は Registration Reply を送信するために MN-HA-MIP4-KEY を使用して MN-HA セキュリティ アソシエーションを設定します。後続の登録認証は、このセキュリティ アソシエーションを使用します。

CMIP の場合、RRQ に ALL-ZERO-ONE-ADDR である HA IP 、および、MN-HA-MIP4-SPI と HA-IP-MIP4 が含まれる場合、RRQ-HA-IP も RRQ の HA IP と同じ値に設定され、アクセス要求で送信されます。HA は RRQ-HA-IP の RRQ-MN-HA-KEY 、および、MN-HA-MIP4-SPI に対応する HA-IP-MIP4 の MN-HA-MIP4-KEY をダウンロードします。HA は RRQ-MN-HA-KEY を使用してモバイル IP の MHAE を検証し、MN-HA-MIP4-KEY を使用してモバイル IP の MHAE を生成します。

FA から受信した RRQ に FHAE が含まれている場合は、該当する FA の外部エージェント認証が発生します。また、その FA から受信したすべてのサブ シーケンス RRQ には FHAE が含まれます。HA で FA を認証する場合、HA-RK が HA に存在する必要があります。HA に HA-RK が存在しない場合は、HA は AAA から HA-RK をダウンロードします。

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

HA は AAA から HA-RK をダウンロードする必要がある場合、HA は、アクセス要求で HA-RK-Key-Request VSA の値を 1 に設定して、Access-Accept で HA-RK-KEY アトリビュートを受信することを期待していることを示します。アクセス要求には HA-RK-SPI アトリビュートも含まれ、その値は FHAE で受信された SPI に設定されます。HAAA は、アクセス要求で送信された HA-IP-MIP4 アトリビュートに関連する Access-Accept で、HA-RK-KEY、HA-RK-SPI、および HA-RK-Lifetime アトリビュートを返します。これらのアトリビュートのいずれかが存在している場合は、すべてが存在している必要があります。そうでなければ、HA は Access-Accept を廃棄します。このアトリビュートは、あらゆる Accounting（Start/Stop/Interim）メッセージに含まれます。

HA-RK キー（26/15）、HA-RK SPI（26/16）、HA-RK ライフタイム（26/17）がスタンバイまたは冗長 HA と同期されます。

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

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

上記で

H は HMAC-SHA1 です。RFC 2104 で規定されます。HMAC：Keyed-Hashing for Message Authentication

HA-IPv4 はアクセス要求で送信される HA-IP-MIP4 アトリビュートです（バインディング Home Agent IP など）。

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

FA から受信した MobileIP RRQ に FHAE エクステンションが含まれている場合、このエクステンションの検証には上述のアルゴリズムを使用して生成された FA-HA キーと SPI が使用されます。

次の **show ip mobile secure home-agent ha-rk** *ha-ip* コマンドを使用して、ダウンロードした HA-RK キー、SPI、およびライフタイムを表示できます。

次に、例を示します。

```
router#show ip mobile secure home-agent
HomeAgent HA-RK List:
15.1.1.80:
    SPI 102, Lifetime 00:10:30 (630), Remaining 00:10:24
    Key 31323334353637383930313233343536373839 30
```

show ip mobile secure foreign-agent *fa-ip* コマンドを使用して生成された FA-HA キーを表示できます。

次に、例を示します。

```
router#show ip mobile secure foreign-agent
Security Associations (algorithm,mode,replay protection,key):
14.1.1.28:
    SPI 102,  HMAC-MD5, Timestamp +/- 7, HA-IP 15.1.1.80
    Key b932c46406dcfe411f8bd147103ac53ca0c7fe65
```

HA-RK ライフタイムが期限切れになると、上述のダウンロードされた HA-RK と、生成された FA-HA キーは削除されます。ライフタイムが期限切れになる前に新しい HA-RK キーがダウンロードされると、両方のキーが共存を続け、認証はいずれかのキーを使用して成功します。**clear ip mobile secure all** コマンドを使用して、同一のキーを削除できます。このコマンドはすべてのキー、MN、FA、および（生成された、または AAA からダウンロードされた）HA-RK を削除します。

WiMAX の場合、MHAE または FHAE 検証のために、ローカルに SPI およびキーを設定できません。

バインディングの Home Agent IP アドレスの設定

Home Agent IP アドレスをバインディングに割り当てるために Home Agent を設定する方法が複数あります。次の作業を実行して、この機能をイネーブルにします。

ステップ 1	**ip mobile realm @cisco.com vrf** *vrf-name* **ha-addr** ***vrf-ha-address***	インバウンド ユーザ セッションをイネーブルにして、特定のレルムに対する特定のアトリビュートが存在した場合にセッションを切断します。
ステップ 2	**ip mobile home-agent dynamic-address** *dynamic-ha-address*	Registration Response パケットの Home Agent Address フィールドを設定します。
ステップ 3	**ip mobile virtual-network** *virtual-net-start mask* **address** *virtual-net-ha-address*	仮想ネットワークを定義します。
ステップ 4	**ip mobile home-agent address** *global-ha-address*	仮想ネットワークの IP アドレスをイネーブルにします。
ステップ 5	**HA HSRP redundancy virtual IP address** *hsrp-ha-ip-address*	Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）IP アドレスを指定します。

前述の設定詳細情報を使用して、バインディングの Home Agent IP アドレスが選択されます。同一の Home Agent IP アドレスがアクセス要求で HA-IP-MIP4 として、または、RRP で Home Agent IP が送信されます。次のロジックは、以前に存在したバインディングの RRQ には適用されません。既存のバインディングの場合、現在のバインディングの Home Agent IP アドレスが使用されます。

- RRQ HA IP と RRQ 宛先 IP は同一です。

  HA-IP-MIP4 = RRP HA IP アドレス =

  - *vrf-ha-address*（設定されている場合）
  - RRQ 宛先 IP アドレス

- RRQ HA IP は、RRQ 宛先 IP と等しくありません（ダイナミック HA の場合 true を保持し、RRQ HA IP は 0.0.0.0 または 255.255.255.255 です）。

  HA-IP-MIP4 = RRP HA IP アドレス =

  - *vrf-ha-address*（設定されている場合）
  - **ip mobile home-agent address** *global-ha-address* **unknown-ha accept reply** が設定されている場合、RRQ HA IP（ダイナミック HA ではない場合）
  - *dynamic-ha-address*（設定されている場合）
  - RRQ 宛先 IP アドレス

- RRQ HA IP または RRQ 宛先 IP は、サブネット ダイレクト ブロードキャスト アドレスです（RRQ HA IP は 255.255.255.255 と等しくありません）。HA 検出 !

  HA-IP-MIP4 = RRP HA IP アドレス =

  - MN は物理インターフェイス上にあります（物理インターフェイスに対応する前述の IP）

    hsrp-ha-ip-address（設定されている場合）

    物理インターフェイス IP アドレス

  - MN は仮想ネットワーク上にあります（仮想ネットワークに対応する前述の IP）。これによって、*virtual-net-ha-address* または *global-ha-address* のいずれかが設定されていると推測されます。

    virtual-net-ha-address（設定されている場合）

global-ha-address.

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

AAA Accounting アトリビュートの機能は次のとおりです。

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

表 16-3 に、Cisco HA の WiMAX AAA Accounting アトリビュートを示します。

表 16-3　WiMAX AAA Accounting アトリビュート

名前	タイプ	説明	Start	Int	Stop
Acct-Multi-Session-Id	50	この ID は、認証の成功後に AAA によって生成され、Access- Accept メッセージで Network Access Server（NAS; ネットワーク アクセス サーバ）に配信された AAA-Session-Id の値に設定されます。これは CSN ごとに一意であり、セッション内ですべてのアカウンティング レコードと照合するために使用されます。	1	1	1
Framed-IP-Address	8	MS に割り当てられた IPv4 アドレス。これは、IP セッションを特定します。	0-1	0-1	0-1
Chargeable User Identity（CUI）	89	課金ユーザの ID。支払いユーザの固有の一時的ハンドルです。	0-1	0-1	0-1
HA-IP-MIP4	26/6	Home Agent の IP アドレス。	1	1	1
Event-Timestamp	55	イベント発生時刻。	1	1	1
GMT-Time-Zone-Offset	26/3	NAS または HA での Greenwich Mean Time（GMT; グリニッジ標準時）からのオフセット秒数。	0-1	0-1	0-1

WiMAX サポートの設定

HA はデフォルトで、すべてのバインディングは 3gpp2 アクセス タイプであると推定します。WiMAX の場合、**per foreign-agent access type** コマンドが設定される必要があります（「外部エージェント別アクセス タイプ サポート」セクションを参照）。さらに、WiMAX AAA サポートのイネーブルにするには、次の作業を実行します。

ステップ 1	`Router# radius-server vsa send authentication wimax`	WiMAX VSA が RADIUS メッセージに含まれるように設定します。このコマンドがイネーブルに設定されていると、HA が生成するアクセス要求メッセージに次の RADIUS アトリビュートが含まれます。 • Acct-Interim-Interval（85） • Message-Authenticator（80） • Chargeable-User-Identity（89） • WiMAX Capability（26/1） • HA-IP-MIP4（26/6） • RRQ-HA-IP（26/18） • MN-HA-MIP4-SPI（26/11）
ステップ 2	`Router# radius-server vsa send accounting wimax`	WiMAX VSA が RADIUS メッセージに含まれるように設定します。このコマンドがイネーブルに設定されていると、HA が生成する Accounting メッセージに次の RADIUS アトリビュートが含まれます。 • Acct-Terminate-Cause（49） • Acct-Multi-Session-Id（50） • Acct-Session-Time（46） • Chargeable-User-Identity（89） • Acct-Input-Gigawords（52） • Acct-Output-Gigawords（53） • HA-IP-MIP4（26/6） • GMT-Time-Zone-Offset（26/3）
ステップ 3	`Router# ip mobile home-agent send-mn-address`	標準 IETF アトリビュートが RADIUS メッセージに含まれるように設定します。設定すると、モバイル IP RRQ で受信されたホーム アドレスがアクセス要求メッセージの Framed-IP-Address アトリビュート値として送信されます。
ステップ 4	`Router# radius-server attribute 55 access-request include`	アクセス要求に Event-Timestamp（55）アトリビュートを含めます。
ステップ 5	`Router# radius-server attribute 55 include-in-acct-req`	Accounting メッセージに Event-Timestamp（55）アトリビュートを含めます。

設定の確認

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

ステップ 6	`Router# show ip mob bind`	サブスクライバの認証中に WiMAX 機能のネゴシエーションが実行された場合を示します。

次に、例を示します。

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

使用済みの場合のフレーム化された IP の拒否

AAA から受信したフレーム化された IP アドレスが、すでに既存のバインディングに割り当てられていた場合、HA は現在、設定された IP のプールから別の IP アドレスを割り当てます。リリース 5.2 のこの新しい機能によって、HA は AAA がすでにセッションのバインディングに割り当てられているフレーム化された IP アドレスを返したときに、新しいセッションを拒否できます。

この機能がイネーブルである場合、AAA 応答がバインディングに割り当てられている "Framed IP-Addr" を返したときは、エラーコードに "Insufficient Resources or Admin Prohibited" が設定され、RRQ が拒否されます。

この機能を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)#ip mobile home-agent options`	IP Mobile Home Agent オプションをイネーブルにし、IP Mobile Home Agent オプション コンフィギュレーション サブモードを開始します。
ステップ 2	`Router(config-ipmobile-ha-options)#rrq reject frame-ip in-use`	イネーブルの場合、このサブコマンドは Access-Accept の "Framed IP Address" がすでにバインディングに割り当てられていると、RRQ を拒否します。

Acct-Terminate-Cause のサポート

Home Agent Release 4.0 では、Acct-Terminate-Cause RADIUS アトリビュート（RFC 2866 Radius Accounting で定義されている）がサポートされましたが、常に値 0 が挿入されました。

Home Agent Release 5.0 では、次の一覧にある値がサポートされます。

値のフィールドは、セッションの終了理由を指定する 1 つの整数を含む、4 個の 8 ビットです。終了理由は次のとおりです。

- User Request（1）：サービスの終了を要求したユーザ。たとえば、Link Control Protocol（LCP; リンク コントロール プロトコル）の終了またはログアウトによるなど。- 通常の MIP セッション終了時。
- Lost Service（3）：サービスがこれ以上提供できない。たとえば、ホストへのユーザ接続が中断されたなど。- Resource Revocation が受信されたとき。
- Idle Timeout（4）：アイドル タイマーが期限切れになった。- アイドル タイマーが期限切れになり、MIP セッションが終了されたとき。
- Session Timeout（5）：最大セッション長タイマーが期限切れになった。- MIP セッション登録タイマーが期限切れになったとき。
- Admin Reset（6）：管理者がポートまたはセッションをリセットした。- バインディングがオペレータによってクリアされたとき。
- NAS Error（9）：NAS が、セッションの終了が必要なエラーを検出した（ポートに関するものを除く）。- 再登録の RRQ がエラーであるとき、または、FA-HA AE が確認できないとき。
- NAS Request（10）：NAS が、非エラーの理由でセッションを終了した（特にここでリストされていない限り）。- Terminate-Cause の値以外の定義されていない理由でバインディングが削除されたとき。
- Port Preempted（13）：より優先度の高い使用にポートを割り当てるために NAS がセッションを終了した。- 輻輳のためにセッションが終了したとき。
- User Error（17）：ユーザからの入力がエラーであり、このためセッションの終了が発生した。- 再登録時に MN-HA AE が確認できず、バインディングが削除されたとき。

（注）　この Acct-Term-Cause を Accounting-Stop メッセージに含めるためには、基本的な Accounting 機能が HA でイネーブルにされる必要があります。

外部エージェント別アクセス タイプ サポート

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

外部エージェント アクセス タイプ サポートの設定

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

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

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

AAA サーバの設定

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

表 16-4　AAA サーバの AAA Authentication および Accounting アトリビュート

アトリビュート	説明
アトリビュート 4 *vsa string*	このセッションに対するホーム レルムでの固有の識別子（HAAA で設定）。
アトリビュート 6 *ip address as string*	MIP4 の場合の HA の IPv4 アドレス。要求を作成している HA の IP アドレスです。
アトリビュート 10 *ascii または hex corresponding string*	Proxy Mobile IP（PMIP; プロキシ モバイル IP）の場合に RADIUS サーバが Access Service Network（ASN; アクセス サービス ネットワーク）に送信する MN-HA-KEY。または MIP4（MIP または PMIP）の場合に RADIUS サーバが HA での使用のために送信する MN-HA-KEY。PMIP4 中、ASN が MN-HAAE の計算に使用します。 HA に送信され、MIP バージョン（MIP4 または MIP6）および SPI に基づいて、MN-HA-AE（MIP4）の検証、および MIP4 Registration Response の MN-HAAE または MIP6 Binding Answer の AUTH の計算に使用されます。
アトリビュート 11 *spi hex value* 16 進値 100 ～ FFFFFFFF の範囲	MN-HA-MIP4-KEY に関連付けられた SPI。
アトリビュート 15 *ascii または hex corresponding string*	RADIUS サーバによる EAP 認証中に決定され、EAP 認証成功の場合は NAS に渡される HA-RK-KEY。NAS はこのキーを FA-HA キーの生成に使用します。
アトリビュート 16 *spi hex value* 16 進値 100 ～ FFFFFFFF の範囲	HA-RK に使用された SPI。

表 16-4　AAA サーバの AAA Authentication および Accounting アトリビュート （続き）

アトリビュート 17 *vsa value*	HA-RK および抽出されたキーのライフタイム。
アトリビュート 19 *ascii または hex corresponding string*	HAAA が HA に送信し、モバイル IP Registration Request の MN-HA-AE の検証に使用される MN-HA キー。

外部エージェントの分類

Home Agent は、モバイル IP Registration Request で受信した Proxy Mobile IPv4 Access Technology Type Extension の組み込みをサポートします。Tech-type 値 **3** は、802.16e（WiMax）のサポートを示し、**7** は、1xRTT/HRPD のサポートを示します。エクステンションが受信されない場合は、外部エージェントごとの設定が適用されます。FA ごとの設定がない場合は、グローバル値が適用されます。このデフォルトは 3GPP2 であり、WiMax に設定することもできます。

その他の値はサポートされず、その場合、エクステンションは無視されます。非サポート値とともにエクステンションを受信した回数を示す、単一のカウンタがあります。エクステンションの内容はデバグコマンドで表示されます。このコマンドはモバイル メッセージングの内容を表示します。

tech-type 値 **3** の受領は、モバイル IP 登録が WiMax アクセス用であることを示します。この場合、実行されるアクションは WiMax アクセスをサポートするように外部エージェントがローカルに設定されている場合のアクションと同じです。

tech-type 値 **7** の受領は、1xRTT/HRPD アクセスのモバイル IP 登録があることを示します。この場合、実行されるアクションは 3GPP2 アクセスをサポートするように外部エージェントがローカルに設定されている場合のアクションと同じです。

tech-type 値に基づいて実行されるアクションは、ローカルに設定された外部エージェントごとのアクセス タイプ設定よりも優先されます。たとえば、ローカルに設定された値が 3GPP2 を示し、tech-type 値が WiMax を示す場合、WiMax 用のアクションが実行されます。

（注）　Home Agent が Re-registration で異なる Access Technology Type を受信した場合でも、バインディングのアクセス タイプは同一のままです。

アップストリームでの MS トラフィック リダイレクション

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

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

これまでの設定に加えて、次の作業を実行します。

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

設定の確認

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

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

次に、例を示します。

```
Router#sh ip mobile binding
Mobility Binding List:
Total 1
Total VPDN Tunnel'ed 0
xyz1@xyz.com (Bindings 1):
    Home Addr 11.110.1.1
    Care-of Addr 13.1.1.112, Src Addr 13.1.1.112
    Lifetime granted 00:30:00 (1800), remaining 00:29:52
    Flags sbdmg-T-, Identification CAF62BE1.1
    Tunnel0 src 13.1.254.254 dest 13.1.1.112 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Acct-Session-Id: 0x00000002
    Sent on tunnel to MN: 0 packets, 0 bytes
    Received on reverse tunnel from MN: 0 packets, 0 bytes
    Hotline status Active
    Radius Disconnect Enabled
    Next-hop set for any-traffic to 14.1.1.201
```

Show/Clear バインディング キーとしての MAC アドレス

Cisco Mobile Wireless Home Agent Release 5.0 では、現在、セッションに端末の MAC アドレスが含まれます。この識別子は、モバイル IP シグナリングを通じて学習されます。初期登録要求には MAC アドレスが含まれ、再登録、および、登録解除にも MAC アドレスが含まれます。この機能を使用することで、ネットワーク管理者は、セッションの検索、削除およびデバグのイネーブル化を MAC でのホストベースで実行できます。該当する場合は、デバグ メッセージおよび syslog メッセージに端末の MAC アドレスが含まれます。

MAC アドレスは、Cisco-Mobile-IP-MIB にも追加される必要があります。

（注）　アクセス ネットワーク テクノロジーでは MAC アドレスは一意であり、Proxy Mobile IPv4 Access Network Technology Extension から学習できます。アクセス ネットワーク テクノロジーのデフォルト値はありません。

新しいフィールドを含めるために、次のコマンドが変更されています。

Show コマンド：

show ip mobile binding mac address : 指定された MAC アドレスのホストのバインディング情報を表示します。出力に MAC アドレスが含まれます。

Debug コマンド：

debug ip mobile host mac address : は、指定された MAC アドレスのホストのデバグ イベントを表示します。該当する場合は、メッセージに MAC アドレスが含まれます。

Clear コマンド：

clear ip mobile binding mac address: 指定された MAC アドレスのホストのモビリティ バインディング エントリを削除します。

データ パス アイドル タイマー

Cisco Mobile Wireless Home Agent Release 5.0 では、指定された時間（アイドルタイム）の間にターミナルでデータトラフィックの送受信がない場合、セッションが終了されます。このアイドル タイムは、ドメイン単位またはグローバルのいずれかで設定できます。ドメイン単位の設定が優先されます。バインディングの削除イベントによってトリガーされた失効メッセージングが発生します。

RRQ はデータ パスで受信されないため、再登録はアイドル タイマーをリセットしません。

コントロール プレーンと /データ プレーンの問題を分離するために、トラフィック プロセッサだけがセッションのデータ トラフィックを認識します。アイドル時間に到達したときは、コントロール プロセッサに通知する必要があります。

データ パス アイドル タイマー情報は、中間アカウンティングの同期化機能を使用して Home Agent 間で同期されます。

次の作業を実行して、この機能をイネーブルにします。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile realm` *realm* `data-path-idle` *minutes* `Router(config)# ip mobile home-agent data-path-idle` *minutes*	設定された時間（アイドル時間）の間、指定されたレルムに一致する NAI を持つモビリティ ホストのトラフィックがないとき、ドメイン内のモビリティ バインディングを削除します。範囲は 1 ～ 65535 です。 設定された時間（アイドル時間）の間トラフィックがないとき、モビリティ バインディングを削除します。範囲は 1 ～ 65535 です。

次は、データ パス アイドル タイマー機能の出力例です。

```
cisco-1@cisco.com (Bindings 1):
    MAC Addr 0000.0001.0000
    Home Addr 5.1.0.1
    Care-of Addr 2.2.2.200, Src Addr 2.2.2.200
    Lifetime granted 10:00:00 (36000), remaining 09:52:39
    IdleTime granted 00:10:00 (10 min), remaining 00:09:24
    Flags sBdmg-T-, Identification CCA7F408.1
    Tunnel0 src 81.81.81.81 dest 2.2.2.200 reverse-allowed
    Routing Options - (T)Reverse-tunnel
    Access-tech Type: 3GPP2 (3GPP2 1xRTT/HRPD)
    Revocation negotiated - I-bit not set
```

3GPP2 / WiMAX バインディングの OM メトリック

この機能は、以前のインターバルの Object Identifier（OID; オブジェクト ID）がクエリーされたときに、MaxActiveBindings、MaxActive3GPP2Bindings および MaxActiveWimaxBindings のピーク値を返します。

Cisco HA Release 5.1 は、OM メトリック機能を処理するために、2 つのタイマーを導入しました。タイマーの 1 つは、Network Timing Protocol（NTP）タイムによって最大値と最小値でのインターバル開始をサポートします。2 番目のタイマーは OM メトリックを計算します。1 番目のタイマーは、ルータのブート アップ時またはコマンドが変更された時点で開始します。2 番目のタイマーは、1 番目のタイマーが期限切れになった時点で開始します。このタイマーは、設定された値に基づいて期限切れになります。

デフォルトでこの機能はイネーブルであり、デフォルトのインターバルは 30 分です。実行コンフィギュレーションでは、デフォルト設定は表示されません。

（注）　冗長構成の場合は、OM メトリック機能が使用できません。

OM メトリックの設定

この機能のインターバルを設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# om-metric-interval {15 | 30 | 60 }`	これは、**ip mobile options** コマンドのサブメニューで使用できるサブコマンドです。

次に、設定の確認に役立つ出力例を示します。

3gpp2 バインディングの数や Wimax バインディングの数などのメトリック カウンタは、**show ip mobile binding summary** の下に表示されます。

```
router#sh ip mob binding summary
Mobility Binding List:
Total 1
3gpp2 Bindings 1
Wimax Bindings 0
```

新しいメトリック値は、新しいコマンドの下に表示されます。

```
router#show ip mobile options ommetrics
OM Metric Statistics:

 Peak Active bindings in the elapsed (previous) interval 0
 Peak Active 3GPP2 binding in the elapsed (previous) interval 0
 Peak Active Wimax binding in the elapsed (previous) interval 0
 Elapsed configured interval size is 15 minutes
```

さらに **debug ip mobile** がイネーブルの場合は、次のデバッグ ステートメントが出力されます。

```
%IPMOBILE-6-OMMETRICS_TIMER_INFO: OM Metric Interval Timer will be started after 1170577
milliseconds.
MobileIP:  OM Metric Sleep Timer is Started
MobileIP:  OM Metric Sleep Timer is Stoped
MobileIP:  OM Metrics Interval Timer is Started for 900005 milliseconds
MobileIP:  OM Metrics Interval Timer is Expired
MobileIP:  OM Metrics Interval Timer is Stoped
MobileIP:  System clock has been updated,
                    So Om Metric Timers will restart
%IPMOBILE-4-OMMETRICS_TIMER_WARNING: Clock skew is more, So Om metric timers will restarts
 metrics interval time is 900000.
 deltaOffset is 39599997.
 currentSystemClock is 3599997.
 nextSystemClock is 50400000.
```

MIP/ユーザ データグラム プロトコル（UDP）トンネルの単一インターフェイス記述ブロック（IDB）

MIP/User Datagram Protocol（UDP; ユーザ データグラム プロトコル）RFC 3519 要件は、MN への各 MIP/UDP Collocated Care-of Address（CCoA; コロケーション気付アドレス）バインディングには、個別の MIP/UDP トンネルが必要であると記述しています。HA Release 5.0 では、HA は、それぞれのトンネルに 1 つのハードウェア / ソフトウェア Interface Descriptor Block（IDB; インターフェイス記述ブロック）を使用しました。システムが最大で 16K のハードウェア IDB をサポートできることから、MIP/UDP CCoA バインディングの最大数は 16K に制限されます。

Cisco HA Release 5.1 では、数十万の MIP/UDP CCoA バインディングをサポートできます。この要件をサポートするために、当社はすべての種類のトンネルに対し単一 IDB を使用します。

単一 IDB、つまりトンネル スケーラビリティ機能は MIP/UDP トンネルだけをサポートします。しかし、他の種類のトンネル（IP/IP や Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）/IP など）の機能性には影響ありません。

この機能の一部として、次の項目がサポートされます。

- 他の種類のトンネル（IP/IP、GRE/IP など）が影響されないように、また機能性を維持するように、必要に応じてトンネル Application Programming Interface（API; アプリケーション プログラミング インターフェイス）が変更されます。

- サポートされた MIP/UDP トンネル（CoA または CCoA）の CPS レートは、HA 5.0 と同じままです。
- サポートされた MIP/UDP トンネル（CoA または CCoA）のデータ スループット レートは、HA Release 5.0 と同じままです。
- サポートされる 1GB SAMI カード上の MIP/UDP トンネルの最大数は 80,000 です。この数字を実現するには、I/O メモリを 64MB から 128MB に増やす必要があります。

単一 IDB の SAMI の設定

（注）　I/O メモリを 64MB から 128MB に設定するには、**memory-size iomem 128** コマンドを実行し、I/O メモリの変更後にカードをリブートします。

設定の確認

この機能を実現するための新しい設定作業はありません。次のコマンドは、単一 IDB 機能が機能していることを確認するように変更されました。

show ip mobile tunnel summary コマンドの出力は、次のように変更されました。

```
#show ip mob tunnel sum
Mobile IP tunnels summary:
   One IDB used per tunnel for IP/IP, GRE/IP tunnels
   Single IDB used for MIP/UDP tunnels

   Total mobile ip tunnels 2
```

show ip mobile tunnel コマンドの出力は、MIP/UDP トンネルの場合だけ、若干変更されました。MIP/UDP トンネルに適用される 2 つの変更は次のとおりです。

- すべての MIP/UDP トンネルは、単一 IDB 機能を使用するため、すべての MIP/UDP トンネルのトンネル番号は同一です。
- トンネルの状態は IDB データ構造に保存されます。すべての MIP/UDP トンネルに、単一 IDB を使用するため、MIP/UDP トンネルの各トンネル カウンタが表示されます。一方、新しい show コマンド **show ip mobile tunnel mip-udp aggregate-statistics** を使用すると、すべてのトンネルの集約統計情報が表示されます。

IP/IP トンネルおよび GRE/IP トンネルの出力は同じままです。

```
router#show ip mob tunnel
Mobile Tunnels:
Total mobile ip tunnels 2
Tunnel0:
    src 16.1.2.80, dest 18.1.1.202
    src port 434, dest port 1244
    encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 0, Output ACL users 0
    IP MTU 1468 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Mobile0
    HA created, CEF switching enabled, ICMP unreachable enabled
Tunnel0:
    src 16.1.2.80, dest 18.1.1.202
    src port 434, dest port 1245
    encap MIPUDP/IP, mode reverse-allowed, tunnel-users 1
    Input ACL users 0, Output ACL users 0
```

```
    IP MTU 1468 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Mobile0
    HA created, CEF switching enabled, ICMP unreachable enabled
```

show ip mobile tunnel mip-udp aggregate-statistics 出力は、次のように表示されます。

```
router#show ip mob tunnel mip-udp aggregate-statistics
Tunnel0 Aggregate Counters:
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
    300 packets input, 45600 bytes, 0 drops
    300 packets output, 39600 bytes
```

show ip mobile traffic 出力では、すべてのトンネルで送受信されたキープアライブの数が、既存の show コマンドの下に表示されます。次の例では、新しい行に注目します。

```
router#show ip mob traffic
IP Mobility traffic:
UDP:
    Port: 434 (Mobile IP) input drops: 0
Advertisements:
    Solicitations received 0
    Advertisements sent 0, response to solicitation 0
Home Agent Registrations:
    Register requests rcvd 22961, denied 0, ignored 0, dropped 0, replied 22961
    Register requests accepted 22961, No simultaneous bindings 0
  . . .
  . . .
  . . .
MIP/UDP Tunnel:
    Number of Keepalives received (on all tunnels) 13809
    Number of Keepalives sent (on all tunnels) 13809
```

非 VPN ルーティングおよびフォワーディング（VRF）環境での GRE 鍵 Critical Vendor-Specific Extension（CVSE）

MIPv4 は GRE 鍵を使用しない GRE/IP トンネリングをサポートします。GRE CVSE Extension を使用することで、FA は GRE トンネリングを要求でき、HA と FA の両方が GRE/IP トンネルのアップストリーム/ダウンストリーム キーを交換できます。

次は、この機能が動作する方法を示すコール フローです。

1. FA は GRE 鍵を生成し、GRE 鍵エクステンションを RRQ に付加し、RRQ を HA に転送します。
2. HA は初期登録 RRQ を受信し、GRE 鍵エクステンションを解析します。不十分な構成である GRE 鍵エクステンションを受信した場合、HA は、"unknown CVSE" とともに RRP を送信します。登録が受け入れられると、HA はバインディングを作成し、FA によって提供された GRE 鍵をバインディング内に保存します。リバース トンネルが必要な場合、HA は一意な GRE 鍵も作成し（HA はランダムな番号を生成し、一意性のためにすでに割り当てられた GRE 鍵と比較します）、RRP を GRE 鍵エクステンションとともに返します。HA は FA によって提供された鍵の重複をチェックしません。
3. リバース トンネルがイネーブルである場合、FA は HA へのアップストリーム トラフィック（例：MN から CN へ）をトンネリングし、FA が HA へのパケットをトンネリングする場合は、（RRP で HA によって提供された）GRE 鍵を追加します。トンネルと一致する発信元 IP アドレスおよび宛先 IP アドレスのあるパケットを HA が受信した場合、HA は、カプセル化されたパケット内の GRE 鍵とも一致します。

4. ダウンストリーム トラフィック（例 : CN から MN へ）の場合、CN からのパケットは HA に到達し、HA は HA-FA トンネルを指す MN のルーティング エントリを保持します。MN のバインディングが探索され、バインディングに保存された GRE 鍵がパケットのカプセル化に使用され、FA へトンネリングされます。
5. HA が再登録 RRQ を受信した場合、HA は GRE 鍵エクステンションを解析します。再登録が受け入れられると、HA は再登録 RRQ で受信したダウンストリーム キーを使用してバインディングをアップデートし、FA による使用のために生成されたアップストリーム キーとともに RRP を送り返します。
6. HA が有効な登録解除 RRQ と（存在する場合は）GRE 鍵エクステンションを受信した場合は、HA は以前に生成された GRE 鍵を含む RRP を送り返します。

冗長構成に関する注意 :
冗長構成の場合でも、GRE CVSE 機能が使用できます。

その他の注意 :
受信 RRQ（初期 / 更新 / 登録解除）の GRE 鍵の値がゼロ（0）の場合、

- リバース トンネリング ビット（T）がセットされていない場合でも、HA は GRE 鍵を生成します。
- RRQ で T ビットがセットされている場合、HA によって生成された鍵は、双方向に使用されます。
- GRE CVSE エクステンションが RRQ にある場合は、RRQ の G ビット ステータスに関わりなく、トンネル モードが GRE に設定されます。

非 VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）環境での GRE 鍵の設定

GRE トンネルの GRE 鍵に基づいて各セッションのデータ ストリームを特定するように Cisco Mobile Wireless HA を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent options`	IP Mobile Home Agent オプションをイネーブルにし、IP Mobile Home Agent オプション コンフィギュレーション サブモードを開始します。
ステップ 2	`Router(config-ipmobile-ha-options)#cvse gre-key`	CVSE からの GRE 鍵を使用して GRE トンネリングをイネーブルにします。システムにアクティブなバインディングがある場合は、このコマンドをイネーブルまたはディセーブルにできません。デフォルトの動作では、CVSE からの GRE 鍵を解析しません。

RFC 4917 のサポート

RFC 4917 は、Registration Replies メッセージまたは Registration Revocation メッセージに付加される Message String Extension を指定します。Message String Extension は、表示可能な通知をネットワークからユーザに提供するために端末に送信されます。エクステンションのテキストは、Access-Accept、Access-Reject、または Disconnect（RFC 3576）メッセージで送信される RADIUS Reply-Message アトリビュートを使用して、AAA サーバから入手できます。RADIUS Change of Authorization（COA）によって、Registration Reply メッセージ、または Registration Revocation メッセージの送信は発生しません。したがって、このメッセージはモバイル IP 拡張機能でサポートされません。

モバイル登録メッセージを表示するデバグ出力には、Registration Reply メッセージと Revocation メッセージが表示されます。

この機能をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip mobile home-agent message-string`	AAA サーバからユーザへのテキストの配布をイネーブルに、またはディセーブルにします。

次に、Message String エクステンションのサンプル設定を示します。

```
HA Config

ip mobile home-agent template Tunnel10 address 10.10.10.188
ip mobile home-agent template Tunnel10 address 10.10.10.203
ip mobile home-agent template Tunnel10 address 10.10.10.179
ip mobile home-agent binding-overwrite
ip mobile home-agent message-string
ip mobile home-agent accounting ha-acct
ip mobile virtual-network 2.0.0.0 255.0.0.0
ip mobile host nai @aricent.com address pool local mip-pool-1 virtual
network 2.0.0.0 255.0.0.0 aaa load-sa lifetime 3600
ip mobile secure mn-aaa spi 101 algorithm md5 mode ppp-chap-style

RADIUS Config

simulator radius subscriber 123
  framed address 18.18.0.1
  framed protocol ppp
  vsa cisco generic 1 string "mobileip:static-ip-pool=mip-pool-1"
  vsa cisco generic 1 string "mobileip:spi#0= spi 101 key ascii cisco"
  attribute 18 string "Welcome TO Cisco"

simulator radius subscriber 124
  framed address 18.18.0.1
  framed protocol ppp
  vsa cisco generic 1 string "mobileip:static-ip-pool=mip-pool-1"
  vsa cisco generic 1 string "mobileip:spi#0= spi 101 key ascii cisco"
  reply-message RFC4917 "HA-CHAP Failed"
```