



CHAPTER 3

プロキシ モバイル IP

この章では、Cisco ブロードバンドワイヤレス ゲートウェイ (BWG) のプロキシ モバイル IP 機能について説明します。また、これらの機能の設定方法と、必要に応じて設定例も示します。

概要

BWG の以前のリリースでは、ASN アンカー モビリティの基本機能を実装しました。ASN アンカー モビリティは、MS がデータパス機能間を移動し、ASN ネットワークの北方向のエッジに常駐する同じアンカー FA (BWG) を維持するときに機能します。CSN とデータパス機能間のデータフローは、アンカー FA/BWG でピボットします。CSN は、ASN データプレーン機能間で発生するモビリティを認識しません。ASN アンカー モビリティの典型的な例は、同じ BWG によって制御される BS 間のハンドオーバーです。

CSN アンカー モビリティは主に、R3 リファレンス ポイントを介した ASN と CSN 間のマクロモビリティを処理します。特にモバイル IPv4 の場合、現在の FA から新しい FA に再度位置指定することでバインディングが更新され (または MIP が再登録され)、アップストリームおよびダウンストリームのデータフォワーディングパスが更新されることを意味します。

BWG リリース 2.0 で Proxy Mobile IP (PMIP; プロキシ モバイル IP) 機能が導入されました。PMIP では、MIP クライアントが MS 内ではなく BWG 内に実装されます。

BWG (PMIP クライアント) の基本的な機能は、ユーザの代わりに Mobile IP Registration Request (RRQ; 登録要求) を生成し、それを HA に送信して FA と HA 間にトンネルを確立することです。この作業を完了するには、PMIP クライアントは EAP 認証 (またはシスコが開発した未認証ユーザ用 AAA アクセス) メカニズムを通じて、関連する MIP アトリビュートを収集する必要があります。AAA サーバは、標準のモビリティサービス アトリビュートのセットを BWG に返します。この情報を使用して、BWG/PMIP クライアントは HA に対する MIP RRQ を開始します。HA は MS に割り当てられた IP アドレス (Home Address (HoA; ホーム アドレス)) を含む Registration Reply (RRP; 登録応答) を PMIP クライアントに返します。MIP RRQ/RRP 動作の結果、PMIP クライアントは FA と対話し、逆トンネリング機能を使用して FA と HA 間にデータパスを確立します。

MIP の登録に成功すると、BWG は DHCP または ARP メカニズムを通じて、MS に割り当てられた IP アドレスを通知します。

BWG PMIP 機能には、次の機能があります。

- 簡易 DHCP プロキシサーバ
- 複数の Home Agent (HA; ホーム エージェント) のサポート
- BWG/FA と HA 間の IP-in-IP および GRE トンネリング
- 別のアドレス割り当てメカニズム (DHCP、AAA) と連動するための PMIP クライアント
- HA からの MIP の失効
- FA の位置変更 (ネットワークの再登録)

- MS の背後にある複数ホストに対する PMIP と簡易 IP のハイブリッド（共存）アプローチ
- WiMAX NWG 1.2.2 で規定されたモビリティ サービス（PMIP IPv4）の Radius アトリビュート（IPv4 PMIP 関連）のサポート
- L3-L3（IPCS）および L2-L3（イーサネット CS）での PMIP のサポート
- PMIP クライアント/FA に対するステートフルな冗長性

DHCP プロキシ サーバ

MIP を使用する場合、クライアントの IP アドレスの割り当ては DHCP サーバではなく HA が行います。そのため、BWG は DHCP プロトコルを（リレーではなく）終端させる必要があります。次の DHCP メッセージとオプション がサポートされています。

DHCP Discover

- 53 : DHCP メッセージ タイプ
- 57 : DHCP の最大メッセージ サイズ
- 61 : クライアント ID
- 50 : 要求された IP アドレス
- 12 : ホスト名
- 55 : パラメータ要求リスト（サブネット マスク、DNS、DN）

DHCP Offer

- 53 : DHCP メッセージ タイプ
- 54 : サーバ ID
- 51 : IP アドレス リース期間
- 1 : サブネット マスク（ルータ オプションの前に指定）
- 3 : ルータ
- 6 : DNS
- 12 : ホスト名

DHCP Request :

- 53 : DHCP メッセージ タイプ
- 57 : DHCP の最大メッセージ サイズ
- 61 : クライアント ID
- 54 : サーバ ID
- 50 : 要求された IP アドレス
- 51 : IP アドレス リース期間
- 12 : ホスト名
- 55 : パラメータ要求リスト（サブネット マスク、DNS、DN）

DHCP Ack

- 53 : DHCP メッセージ タイプ
- 54 : サーバ ID
- 51 : IP アドレス リース期間
- 1 : サブネット マスク
- 12 : ホスト名

DHCP Release

- 53 : DHCP メッセージ タイプ
- 61 : クライアント ID
- 54 : サーバ ID

DHCP Decline

- 53 : DHCP メッセージ タイプ
- 61 : クライアント ID
- 54 : サーバ ID

DHCP NAK

- 53 : DHCP メッセージ タイプ
- 61 : クライアント ID
- 54 : サーバ ID

プロキシ DHCP サーバと PMIP との対話

BWG リリース 2.0 では、DHCP プロキシだけがサポートされています。次のデータ フローは、DHCP プロキシ サーバと PMIP クライアント間の対話を示しています。

1. MS がネットワーク内に移動すると、BS と BWG が Pre-Attachment Req/Rsp/Ack 手順の情報を交換します。MS/BS は、認証を要求するかどうかを指定できます。
2. 認証が要求された場合、BWG は Identity Request 手順を開始します。
3. BWG は、AAA Access Request を送信します。
4. AAA と MS は必要に応じて、EAP 交換を開始します。
5. BWG と BS が接続手順を完了します。
6. BWG で、AAA Access Accept を受信します。このメッセージには WiMAX アトリビュート (hHA-IP-MIP4、vHA-IP-MIP4、MN-hHA-MIP4-KEY、MN-vHA-MIP4-KEY、MN-HA-MIP4-SPI、HA-RK-KEY、HA-RK-SPI、および HA-RK-Lifetime) が含まれます。Home アトリビュートは、Visiting アトリビュートよりも優先されます。
7. MSK を受信すると、BWG は MSK から AK コンテキストを抽出して BS に配布し、そこで PKMv2 を使用して MS とキーが交換されます。FA-HA AE を抽出するときは NWG Stage 3 に基づき、適切な SPI を選択します。
8. BWG は DHCP/PMIP プロトコル ステート マシンを起動し、HA に対する MIP RRQ を構築します。RRQ メッセージ用の情報は AAA サーバやユーザ グループの設定から取得し、次の情報が含まれます。
 - Flags : ユーザ グループ設定またはデフォルト値
 - Lifetime : AAA または ユーザ グループの設定のセッション タイムアウト

- HoA : AAA の Framed IP Address またはゼロ
- Home Agent : AAA またはユーザ グループの設定
- Care-of Address : BWG 上のインターフェイス設定
- NAI 拡張を含む
- 失効サポート拡張 (I-bit = 0)
- Host-Config。拡張 (ユーザ グループで設定されている場合)
- MN-HA AE
- GRE-key 拡張 (このリリースでは未対応)
- FA-HA AE

HA の逆トンネリング用仮想アクセス IDB も、作成されていない場合は作成する必要があります。

9. HA は AAA と対話して MIP キーを取得します。
10. HA は AAA から取得した MIP キーを使用して MN-HA AE と FA-HA AE を検証します。
11. HA で認証に成功すると、HA はそのアドレス スキーム (ローカル プール、DHCP、AAA など) を使用し、このモバイル ユーザにホーム アドレスを割り当てます。このアドレスは、BWG への RRP メッセージにも設定されます。BWG は Identification フィールドを確認し、整合性をチェックするために Mobile-Home Authentication Extension を計算します。Foreign-Home Authentication Extension が実装されている場合は、それも検証されます。すべての検証が正常に終了すると、ユーザ データを転送するための逆トンネルが BWG と HA 間に作成されます。
12. BWG と BS が GRE データ パスをセットアップします。このステップは、MIP RRQ/RRP と並行して実行する必要があります。
13. MS/ホストは DHCP DISCOVER を開始して IP アドレスを取得しようとします。
14. BWG は DHCP OFFER を MS/ホストに送信します。
15. 次に MS/ホストは DHCP REQUEST を送信します。
16. BWG が DHCP Ack を返します。



(注)

この手順は多少 NWG 仕様とは異なっており、MIP RRQ が DHCP Discover メッセージによってトリガーされます。MIP RRQ メッセージが DHCP Discover による情報を必要としない限り、このシナリオは正常に動作します。

PMIP Authenticated Network Identifier (PANI)

BWG リリース 2.2 から、BWG は PMIP Authenticated Network Identifier (PANI; PMIP 認証済みネットワーク識別子) をサポートしています。PANI の詳細情報は、AAA サーバから Access Accept メッセージの一部として受信できます。PANI の詳細を受信すると、BWG は HA に対する RRQ を生成する際に、PANI を Network Access Identifier (NAI; ネットワークアクセス識別子) として使用します。

次の表に、PANI の AAA-Authentication アトリビュートを示します。

表 3-1 PANI の AAA-Authentication アトリビュート

アトリビュート	タイプ	説明	Access Request	Access Challenge	Access Accept	Access Reject
PMIP NAI	26/78	AAA によって返される MS の認証済み ID	0	0	0-1	0

複数の HA のサポート

BWG は、複数の HA と通信するよう設計されています。AAA は MS ごとに 1 つの HA IP アドレスを提供できます。AAA を利用できない場合は、ユーザグループの設定から IP アドレスを取得します。

次に設定の例を示します。

```
router(config)#wimax agw pmip profile verizon
    home-agent
        address <home-agent-ip>

router(config)#wimax agw user group-list wimax
    user-group cisco.com
    aaa accounting method-list agw
    sla profile-name silver
    pmip profile-name verizon
!
```

設定できる HA は、ユーザグループごとに 1 つだけです。

FA (BWG) と HA 間のトンネリング

BWG リリース 2.0 から、IP-in-IP と GRE の両方のトンネリング (GRE キーなし) がサポートされています。デフォルトの方式は IP-in-IP トンネリングです (RRQ で G ビットを設定しない)。GRE トンネリングが必要な場合 (RRQ で G ビットを設定する)、ユーザグループ単位で設定できます。

次に設定の例を示します。

```
wimax agw pmip profile verizon
    proxy-mn
        gre-tunneling-enable

wimax agw user group-list wimax
    user-group cisco.com
    aaa accounting method-list agw
    sla profile-name silver
    pmip profile-name verizon
```

MIP ホスト設定拡張

MIP ホスト設定拡張は、RFC 4332 で規定されています。デフォルトはイネーブルです。proxy-mn セクションで no host-config-ext-request コマンドを使用して、明示的にディセーブルにできます。

次の HA のパラメータは、DHCP オプションとしてクライアントに渡すことができます。

- MIP ホーム ネットワーク プレフィクス長 → DHCP サブネット マスク (1)
- MIP デフォルト ゲートウェイ → DHCP ルータ (3)
- MIP DNS サーバ → DHCP DNS (6)

この機能をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	<pre>router(config)# wimax agw pmip profile verizon proxy-mn host-config-ext-request // RFC 4332</pre>	BWG でプロキシ モバイル IP プロファイルをイネーブルにします。
ステップ 2	<pre>router(config)# wimax agw user group-list wimax user-group cisco.com aaa accounting method-list agw sla profile-name silver pmip profile-name verizon</pre>	BWG でユーザ グループ リストを設定します。

DNS とデフォルト ゲートウェイの設定

BWG を使用すると、DNS とデフォルト ゲートウェイをローカルに設定したり、AAA サーバからダウンロードしたりできます。

HA が RFC4332 (ホスト設定拡張) をサポートしていない場合、CLI を使用して BWG で DNS およびデフォルト ゲートウェイを設定できます。または AAA サーバから DNS およびデフォルト ゲートウェイの詳細をダウンロードするように BWG を設定できます。DNS およびデフォルト ゲートウェイの詳細は、DHCP プロキシ応答の一部として CPE に送信されます。

優先順位は次のとおりです。

1. HA から RRP の一部として受信した DNS およびデフォルト ゲートウェイの詳細
2. BWG が AAA から受信した DNS およびデフォルト ゲートウェイの詳細
3. BWG でローカルに設定されている DNS およびデフォルト ゲートウェイ

DNS およびデフォルト ゲートウェイを設定するには、次のコマンドを使用します。

- [no] dns-server primary <ip address> secondary <ip address>
- [no] default-gateway <ip_address>

次に、DNS およびデフォルト ゲートウェイの設定例を示します。

```
wimax agw pmip profile pmip1
proxy-mn
dns-server primary 10.1.1.1 secondary 10.1.1.2
default-gateway 10.1.1.3
```

表 3-2 DNS およびデフォルト ゲートウェイを設定するための AAA-Authentication アトリビュート

アトリビュート	タイプ	説明	Access Request	Access Challenge	Access Accept	Access Reject
Default Gateway	Cisco AVP	デフォルト ゲートウェイの IPv4 アドレス	0	0	1	0
DNS	26/52	DNS サーバの IPv4 アドレス	0	0	1-n	0

クライアントの IP アドレスの割り当て

PMIP は、ダイナミック IP と固定 IP の両方のアドレス割り当てメカニズムをサポートしています。固定 IP アドレスの場合、BWG はモバイルステーションで設定済みの IP アドレスを ARP を通じて学習します。この場合 BWG は、IP アドレスが AAA サーバからダウンロードした IP アドレスプールの範囲内にあることを確認し、IP アドレスを許可します。もう 1 つの固定 IP アドレス方式では、BWG が AAA サーバから取得した IP アドレスを DHCP を通じて MS にリースするという動作に基づきます。どちらのシナリオでも、HA への MIP 登録時に BWG が IP アドレスを提供し、HA が登録を受け入れると、MS がその IP アドレスを使用できます。ダイナミック IP アドレスの場合、MIP 登録時に BWG は IP アドレスを提供せず、HA が固有のアドレス割り当てスキーム（AAA、DHCP、ローカルプールなど）に基づき、登録の応答時に MS/ホストに IP アドレスを割り当てます。

BWG が MIP 動作を呼び出す前に、DHCP リレーメカニズムまたは AAA からの Framed IP Address を通じて既に IP アドレスを取得している場合があります。その場合、BWG はそれらの IP アドレスを固定 IP のシナリオと同様に処理します。つまり、HA への MIP RRQ には、割り当て済みの IP が HoA として設定されます。

HA からの MIP の登録失効

HA からの MIP の失効がサポートされています。セキュリティアソシエーションが RRP メッセージで確認されると、加入者のセッションは破棄されます。

PMIP ホストと簡易 IP ホストの共存

プロトコルの制限により、MIP 加入者が取得できる IP アドレスは 1 つだけです。これは、MS の背後にある複数のホストに対応できる現在の BWG 機能とは対照的です。このため、加入者の（デフォルトの）ホストだけが MIP HoA を割り当てられます。残りのホストは、その加入者用の PMIP が存在しないかのように、引き続き簡易 IP ホストとして機能します。

FA の位置変更

FA の位置変更は、MS が別の FA/BWG を通じてネットワークに再登録するときにトリガーされます。この場合、新しい BWG 内の PMIP クライアントが通常どおり RRQ を開始し、HA は古い FA/BWG の MS の登録を失効させます。

次に、FA の位置変更動作を示します。

1. MS、BS-1、BWG-1、および HA 間でアクティブなセッションが確立されています。
2. MS が BS-2 に移動し、ネットワークへの再登録が必要になります。
3. ネットワークへの再登録の一部として、BWG-2 が HA に対して MIP RRQ を開始します。
4. HA が MS の既存のバインディングを検出し、MS の古い MIP 登録を失効させます。
5. MS のセッションがまだ存在する場合、BWG-1 はそのセッションのクリーンアップを開始します。
6. BWG-1 が MIP の失効を返します。
7. 同じ HoA を使用した MIP RRP が BWG-2 に送信されます。
8. MS が DHCP Discover を送信します。
9. BWG-2 が MS の IP アドレスとして HoA を提供します。
10. MS が DHCP Request を送信します。
11. IP アドレスが割り当てられたことを確認するため、BWG は DHCP Ack を返します。

モバイル IP を使用すると、マクロモビリティの状況では、加入者のホストは同じ HA によって常に同じ IP アドレスを割り当てられます。ただし、マクロモビリティの状況でも、MS の背後にある複数の簡易 IP ホストは同じ IP アドレスを割り当てられない場合があります。これは、関係する 2 つのサービスプロバイダー間の規定によって決まります。BWG-1 と BWG-2 が同じ DHCP サーバを共有する場合は、DHCP サーバで、マクロモビリティ イベント後に確実に同じ IP アドレスを簡易ホストに割り当てるメカニズムを使用できます。一方、BWG-1 と BWG-2 が異なる DHCP サーバを使用する場合、マクロモビリティ イベント後に簡易 IP ホストの IP アドレスが同じであるとは限りません。



(注) R4 ベースのアイドル モードの FA の位置変更は、このリリースではサポートされません。

イーサネット CS L2-L3 または IPCS

MIP プロトコルでは、HA と FA 間でトンネルされるパケットは IP パケットである必要があります。BWG の場合、イーサネット CS L2-L3 または IPCS は、CSN (HA) へのレイヤ 3 IP パケットになります。したがって、BWG の PMIP サポートでは、イーサネット CS L2-L3 および IPCS の両方と連動できるよう設計されています。

一方、ユーザグループでイーサネット CS L2-L2 ブリッジングがイネーブルの場合、それらのユーザに対して PMIP 機能が自動的にディセーブルになります。つまり、L2 ブリッジングのほうが PMIP 機能よりも優先されます。

WiMAX RADIUS アトリビュート

WiMAX Forum NWG 1.2.2 標準のアトリビュートがサポートされます。次の表に、サポートされるアトリビュートの詳細を示します。

WiMAX RADIUS アトリビュート

表 3-3 WiMAX RADIUS アトリビュート

アトリビュート	説明
hHA-IP-MIP4 (26/6)	HA のアドレス
MN-hHA-MIP4-KEY (26/10)	モバイル ノードの作成に使用するアトリビュート : HomeAgent Authentication Extension
MN-HA-MIP4-SPI (26/11)	MN-HA-MIP4 キーに関連付けられた SPI
Session-Timeout	セッションタイムアウト (32 ビット) は登録のライフタイム (16 ビット) に変換されます。最大値は 65534 (秒単位) です。
Framed-IP Address	存在する場合、このアトリビュートは MIP RRQ で HoA として使用されます。
HA-RK-KEY (26/15)	
HA-RK-SPI (26/16)	
HA-RK-Lifetime (26/17)	

ステートフルセッションの冗長性

PMIP クライアント/FA には、セッションの冗長性を実現する独自のスキームが存在しません。そのため、ステートフルデータは BWG のセッションデータの一部として同期されます。スイッチオーバーが発生したときの目標は、新たにアクティブになった BWG が最小の packets 損失でセッションを継続できることです。

PMIP のステートフルセッション情報を BWG セッションデータと共に同期するには、**ip mobile foreign-agent redundancy CLI** をイネーブルにする必要があります。

PMIP プロファイルの設定

次に、HA アドレスおよび GRE トンネリング以外のパラメータの例を示します。

```
router(config)#wimax agw pmip profile verizon
  home-agent
    address <home-agent-ip>
    ha-rk-key <key> spi <spi> lifetime <value>
  proxy-mn
    gre-tunneling-enable
    host-config-ext-request // RFC 4332
    mn-ha-key <key> spi <spi>
    coa <ip_address>
    local-timezone <tz>
```

各ユーザグループは任意で、設定済みの PMIP プロファイルにリンクできます。

```
router(config)#wimax agw user group-list wimax
  user-group cisco.com
  aaa accounting method-list agw
  sla profile-name silver
  pmip profile-name verizon !
```



(注) IP モバイル設定は任意です。必要な加入者ごとのプロビジョニング情報がすべて AAA サーバに存在する限り、加入者に対して PMIP 機能を実行できます。gre-tunneling-enable を除くすべてのユーザグループの設定は、それに対応する加入者の AAA の設定を利用できない場合に、デフォルトとして機能します。

BWG 側で PMIP サポートをアクティブにするには、いくつかの基本的なモバイル IP 設定を行う必要があります。たとえば、インターフェイスイーサネット 1/3 を介して PMIP サービスを有効にするには、次のモバイル IP コマンドを実行する必要があります。

```
interface Ethernet1/3
  ip address 14.1.1.30 255.255.255.0

ip mobile foreign-agent care-of Ethernet1/3
ip mobile foreign-service reverse-tunnel
ip mobile foreign-service revocation retransmit 3
ip mobile foreign-agent redundancy
```



(注) ip mobile foreign-agent redundancy CLI を設定すると、PMIP の冗長性を実現できます。

グローバル コマンドを通じて PMIP サービスをイネーブルにすると、pmip profile を使用するか AAA サーバから提供されるアトリビュートを設定して、WiMAX ユーザグループごとに MIP を設定できます。

BWG では L2-L2 ブリッジングは MIP と連動しません。確立されたセッションが PMIP で、L2 ブリッジングが設定されている場合、L2 ブリッジングはディセーブルになります。セッションが PMIP の場合、L2-L3 オプションはイーサネット CS で使用されます。

L2-L2 ブリッジングをイネーブルにするには、次の手順を実行します。

コマンド	目的
ステップ 1 <pre>router(config)# wimax agw user group-list wimax user-group cisco.com aaa accounting method-list agw sla profile-name silver bridge-group 1 ! Enable L2-L2 for Ethernet CS</pre>	BWG で L2-L2 ブリッジングをイネーブルにします。

IPCS ユーザまたは L2-L3 ユーザの場合、ユーザの PMIP 機能は AAA アトリビュートを通じて指定されます。AAA アトリビュートが存在しない場合は、**pmip profile** を使用してユーザグループの設定で指定されます。

次に、PMIP プロファイルとユーザグループの設定例を示します。

```
router(config)#wimax agw pmip profile pmip1
home-agent
address 14.1.1.80
ha-rk-key ascii rootcisco spi decimal 258 lifetime 6000
proxy-mn
gre-tunneling-enable
no host-config-ext-request
mn-ha-key ascii cisco spi 102 lifetime 3000
coa-address 14.1.1.100
!
```

「host-config-ext-request」はデフォルトでイネーブルです。

```
router(config)#wimax agw user group-list wimax
user-group cisco.com
aaa accounting method-list agw
sla profile-name silver
pmip profile-name pmip1
!
```

デフォルトのフラグは次のとおりです。

S ビット = 0
 B ビット = 0
 d ビット = 0
 M ビット = 0
 G ビット = gre-tunneling-enable を使用して設定
 r ビット = 0
 T ビット = 1
 x ビット = 0
 I ビット = RFC 3543



(注) GRE トンネルは、FA CLI を使用して設定する必要があります。AAA サーバが必要な PMIP 加入者の情報をすべて提供できる場合、ユーザグループの設定はすべて任意です。

セッションの登録ライフタイムは、次のいずれかの方法で取得できます。

- mn-ha-key ライフタイムは未設定、session_timeout は未設定、AAA は session_timeout を送信しない：

この場合、reg_lifetime は無制限（65535）と見なされます。
- mn-ha-key ライフタイムは未設定、session_timeout は 65535 より大きく設定：

この場合、session_timeout 値は 65535 に切り詰められ、reg_lifetime として使用されます。
- mn-ha-key ライフタイムは 0 より大きく、65536 より小さく設定、session_timeout も 0 より大きく、65536 より小さく設定：

この場合、mn-ha-key ライフタイムが reg_lifetime として使用されます。
- AAA が session-timeout を送信：

この値が 0 より大きく、65536 より小さい場合、reg_lifetime として使用されます。この値が 65535 より大きい場合、65535 に切り詰められた値が使用されます。

NAI の設定

EAP 認証コール

認証の初期段階では、BWG は MS の NAI を使用して情報を取得します。

次に、ループバックを使用した FA インターフェイスの冗長性設定の例を示します。

BWG #1

```
interface Loopback0
 ip address 16.1.1.100 255.255.255.255
!
! HSRP redundancy interface
!
interface Ethernet0/0
 description WiMAX Simulator Interface
 ip address 14.1.1.30 255.255.255.0
 standby 2 ip 14.1.1.100
 standby 2 name AGW-IOU
!
```

BWG PMIP の設定

```
wimax agw pmip profile <name>
 home-agent
  address 14.1.1.80
  ha-rk-key ascii rootcisco spi decimal 258 lifetime 7200
 proxy-mn
  host-config-ext-request
  mn-ha-key ascii cisco spi 102 lifetime 7200
  coa-address 16.1.1.100

wimax agw user group-list wimax
 user-group unauthenticated
  aaa accounting method-list agw
  sla profile-name silver
  proxy realm cisco.com
  ip static-allowed
  pmip profile-name <name>
```

モバイル IP の設定

```
router mobile
! tell FA about the loopback interface
ip mobile foreign-agent care-of Loopback0
!
ip mobile foreign-agent redundancy
ip mobile foreign-service revocation
ip mobile foreign-service challenge
ip mobile foreign-service reverse-tunnel
```

BWG #2

```
!
```

PMIP の設定はアクティブおよびスタンバイ BWG の両方で同一ですが、物理インターフェイスは HSRP によって異なります。

HSRP 冗長性インターフェイス

```
interface Ethernet0/0
description WiMAX Simulator Interface
ip address 14.1.1.32 255.255.255.0
standby 2 ip 14.1.1.100
standby 2 name AGW-IOU
```

次に、HSRP グループアドレスを使用した FA インターフェイスの冗長性設定の例を示します。

HSRP 冗長性インターフェイス

```
BWG #1
interface Ethernet0/0
description WiMAX Simulator Interface
ip address 14.1.1.30 255.255.255.0
standby 2 ip 14.1.1.100
standby 2 name AGW-IOU
```

BWG PMIP の設定

```
wimax agw pmip profile <name>
home-agent
address 14.1.1.80
ha-rk-key ascii rootcisco spi decimal 258 lifetime 7200
proxy-mn
host-config-ext-request
mn-ha-key ascii cisco spi 102 lifetime 7200
coa-address 14.1.1.100
wimax agw user group-list wimax
user-group unauthenticated
aaa accounting method-list agw
sla profile-name silver
proxy realm cisco.com
ip static-allowed
pmip profile-name <name>
!
```

モバイル IP の設定

```
router mobile
! tell FA about the loopback interface
ip mobile foreign-agent care-of Ethernet0/0
!
ip mobile foreign-agent redundancy
ip mobile foreign-service revocation
```

```
ip mobile foreign-service challenge
ip mobile foreign-service reverse-tunnel
```

BWG #2

PMIP の設定はアクティブおよびスタンバイ BWG の両方で同一ですが、物理インターフェイスは HSRP によって異なります。

HSRP 冗長性インターフェイス

```
interface Ethernet0/0
description WiMAX Simulator Interface
ip address 14.1.1.32 255.255.255.0
standby 2 ip 14.1.1.100
standby 2 name AGW-IOU
```

設定の確認

BWG 上の PMIP 情報の確認およびトラブルシューティングを行うには、次の手順を実行します。

コマンド	目的
ステップ 1 router# <code>show wimax agw</code>	BWG のソフトウェア バージョン、許可されるベースステーションの数、許可される加入者の数など、各種システムパラメータを表示します。 次の情報が追加されました。 <ul style="list-style-type: none"> • PMIP がイネーブルになっている現在の加入者数
ステップ 2 router# <code>show wimax agw subscriber</code>	BWG 内の PMIP コンテキスト情報を反映するため、出力が拡張されました。PMIP トンネルおよびレジストリ情報は、標準のプロキシモバイル ip コマンドで取得できます。次の情報が追加されました。 <ul style="list-style-type: none"> • PMIP を使用する加入者の機能 • 次の MIP 情報： <ul style="list-style-type: none"> - HA アドレス - ホーム アドレス - // host-config が存在する場合 - ホーム ネットワーク プレフィクス長 - Default Gateway - プライマリ DNS - セカンダリ DNS • ホストの詳細 <ul style="list-style-type: none"> - Host PMIP ステータス (アドレスが PMIP を使用して割り当てられたかどうか) • MIP 登録が完了していないために破棄されたパケット数

	コマンド	目的
ステップ 3	router# show wimax agw subscriber internal	<p>上記の情報以外に、次の情報がこの CLI に追加されました。</p> <ul style="list-style-type: none"> • 次の MIP 情報 : <ul style="list-style-type: none"> – MN-HA キー – MN-HA-Spi – HA-RK-Key – HA-RK-Key-Spi – 要求されたライフタイム – Mip-Flag – AAA-Pmip-Flag – Pmip-Cli-Conf-Flag
ステップ 4	router# show wimax agw statistics internal	<p>次の情報が追加されました。</p> <ul style="list-style-type: none"> • 固定 IP ホストが AAA によって認証されていないために破棄されたパケット数 (以前は、固定 IP ホストが許可されていないために破棄されたパケット数) • 固定 IP ホストが HA によって認証されていないために破棄されたパケット数 • MIP 登録中に受信し、データ パケットが破棄された DHCP パケット • MIP 登録中に受信し、データ パケットが破棄された ARP パケット • MIP 登録中に受信し、データ パケットが破棄された ARP 以外かつ DHCP 以外のパケット • PMIP がイネーブルの加入者の合計作成数 • PMIP がイネーブルの加入者の合計削除数 • MIP 登録が完了していないために破棄されたパケット数
ステップ 5	router# show wimax agw statistics dhcp-relay	<p>このコマンドは、以前は show wimax agw statistics dhcp として知られていました。BWG が DHCP リレーとして機能する際に DHCP サーバとの間で送受信される DHCP メッセージ数を表示します。</p>
ステップ 6	router# show wimax agw statistics dhcp-proxy	<p>このコマンドは、BWG が DHCP プロキシとして機能する際に DHCP クライアントとの間で送受信される DHCP メッセージ数を表示します。</p>
ステップ 7	router# show wimax agw fsm dhcp-proxy	<p>このコマンドは、現在プロキシ ステート マシンのステートと異なる要素の数を表示します。</p>
ステップ 8	<pre>router#show wimax agw statistics internal inc SLB Total SLB sticky update notifications succeeded 0 Total SLB sticky update notifications failed 0 Total SLB sticky delete notifications succeeded 0 Total SLB sticky delete notifications failed 0</pre>	<p>SLB スティッキ性サポートの一部として、4 つのカウンタが追加されました。これらのカウンタは、送信に成功または失敗した、更新通知と削除通知の数を追跡します。</p>

BWG リリース 2.0 では、次のデバッグ コマンドが追加されました。

	コマンド	目的
ステップ 1	router# debug wimax agw switching pmip	PMIP スイッチング デバッグを表示します。
ステップ 2	router# debug wimax agw switching pmip errors	PMIP スイッチング エラー デバッグを表示します。
ステップ 3	router# debug wimax agw switching pmip events	PMIP スイッチング イベント デバッグを表示します。
ステップ 4	router# debug wimax agw switching pmip fsm	PMIP スイッチング fsm デバッグを表示します。
ステップ 5	router# debug wimax agw switching pmip packet	PMIP スイッチング パケット デバッグを表示します。
ステップ 6	router# debug wimax agw switching pmip fsm errors	PMIP スイッチング fsm エラー デバッグを表示します。
ステップ 7	router# debug wimax agw switching pmip fsm events	PMIP スイッチング fsm イベント デバッグを表示します。
ステップ 8	router# debug wimax agw switching pmip packet detail	PMIP スイッチング パケットの詳細を表示します。
ステップ 9	router# debug wimax agw switching pmip packet brief	PMIP スイッチング パケット情報を表示します。
ステップ 10	router# debug ip slb sticky asn msid	SLB スティック情報のデバッグを記録します。

FA 上の PMIP レジストリ テーブルを確認するには、次のコマンドを実行します。

```
BWG#show ip mobile proxy registration
Proxy Mobile Node Registrations:

100022240001@cisco.com:
  Registration accepted 06/13/08 05:18:59
  Next Re-registration 00:01:29
  Registration sequence number 1
  Care-of addr 14.1.1.30, HA addr 14.1.1.80, Home addr 5.1.0.2
  Flags sbdmg-T-, Identification CBFC81C3.1108C374
  Lifetime requested 00:50:00 (3000), granted 00:50:00, remaining 00:26:29
  Revocation negotiated
```

HA のバインディング テーブルを確認するには、次のコマンドを実行します。

```
HA#sho ip mob bind
Mobility Binding List:
Total 4
Total VPDN Tunnel'ed 0
100022230001@cisco.com (Bindings 1):
  Home Addr 5.1.0.1
  Care-of Addr 14.1.1.30, Src Addr 14.1.1.30
  Lifetime granted 00:50:00 (3000), remaining 00:45:16
  Flags sbdmg-T-, Identification CBFC8713.59B6D7F8
  Tunnel0 src 14.1.1.80 dest 14.1.1.30 reverse-allowed
  Routing Options - (T)Reverse-tunnel
  Proxy registration, sequence number 1
  Revocation negotiated - I-bit not set
  Acct-Session-Id: 0x00000004
  Sent on tunnel to MN: 0 packets, 0 bytes
  Received on reverse tunnel from MN: 0 packets, 0 bytes
```

HA と FA 間のモバイル IP トンネルを確認するには、次のコマンドを実行します。

```
BWG#sho ip mobile tunnel
Mobile Tunnels:

Total mobile ip tunnels 1
Tunnel0:
  src 14.1.1.30, dest 14.1.1.80
  encaps IP/IP, mode reverse-allowed, tunnel-users 4
```

```

Input ACL users 0, Output ACL users 0
IP MTU 1480 bytes
Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
outbound interface Ethernet1/3
FA created, fast switching enabled, ICMP unreachable enabled
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
23106 packets input, 2772720 bytes, 0 drops
23106 packets output, 2772720 bytes

```

モバイル ノードの HA ルーティング テーブルを確認するには、次のコマンドを実行します。

```

HA#show ip route mobile
    5.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
M   5.1.0.0/16 is directly connected, Mobile0
M   5.1.0.1/32 [3/1] via 14.1.1.30, 06:24:02, Tunnel0
M   5.1.0.2/32 [3/1] via 14.1.1.30, 06:21:43, Tunnel0
M   5.1.0.3/32 [3/1] via 14.1.1.30, 06:21:40, Tunnel0

```

次に、BWG PMIP 機能のすべての設定例を示します。

```

!
ip vrf voice
  rd 200:1
!
ip vrf sales
  rd 200:1
!
radius-server host 12.12.22.12
radius-server key cisco
!! Start mobile IP process
router mobile

Specify an interface as the COA used by the MN
ip mobile foreign-agent care-of Ethernet1/3
ip mobile foreign-service reverse-tunnel
ip mobile foreign-service revocation retransmit 3
!
interface Ethernet1/0
Description Interface towards voice switch
ip vrf forwarding voice
ip address 15.9.9.1 255.255.0.0
!
interface Ethernet1/3
ip address 14.1.1.30 255.255.255.0
!
interface Ethernet2/0
description Interface towards sales department
ip vrf forwarding sales
ip address 15.9.9.2 255.255.0.0
!
interface Ethernet3/0
description VLAN 10 for Voice
ip address 4.2.4.4 255.255.0.0
encapsulation dot1q 10
!
interface Ethernet4/0
description this interface to be used for FA
ip address 4.3.4.4 255.255.0.0
!
!
Interface VirtualTemplatel
ip address 4.4.4.4 255.255.0.0
encapsulation agw

```



```
!
wimax agw service-flow pak-classify-rule profile sec1-classifier-uplink
  priority 1
    ipv4 permit gre 2.2.2.2 224.0.0.0 any
    ethernet permit any all 0032.00AE.0023 ffff.0000.0000 ethernet-type qinq
    vlan permit any priority 0 7
  !
!
wimax agw service-flow pak-classify-rule profile sec1-classifier-downlink
  priority 1
    ipv4 permit gre 2.2.2.2 224.0.0.0 any
    ethernet permit any all 0032.00AE.0023 all ethernet-type qinq
    vlan permit any priority any
  !
!
wimax agw service-flow profile sec1
  direction downlink
    cs-type eth-cs
      pak-classify-rule sec1-classifier-downlink
    cs-type ip-cs
      pak-classify-rule sec2-classifier-downlink
    qos-info isf-qos-downlink
  !
  direction uplink
    cs-type <eth-cs/ip-cs/vlan-cs>
      pak-classify-rule sec1-classifier-uplink
    qos-info isf-qos-uplink
    set vlan-priority 5
  !
!
wimax agw sla profile silver
  service-flow pre-defined isf profile isf
  service-flow pre-defined secondary 1 profile sec1
!
wimax agw user group-list wimax
  user-group unauthenticated
  aaa accounting method-list agw
  aaa authentication method-list agw
  sla profile-name silver
  proxy realm cisco.com
  ip mobile
  home-agent
    address 14.1.1.80
    ha-rk-key ascii rootcisco spi 102 lifetime 36000
  proxy-mn
    host-config-ext-request
    mn-ha-key ascii cisco spi 102 lifetime 36000
!
```

