Cisco IOS リリース 12.4(24)YG2 向け Cisco ブロードバンド ワイヤレス ゲートウェイ リリース 2.2

Cisco Broadband Wireless Gateway Release 2.2 for Cisco IOS Release 12.4(24)YG2

Cisco IOS リリース 12.4(24)YG2
2010 年 4 月 9 日

Text Part Number: OL-14679-02-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco IOS リリース 12.4(24)YG2 向け Cisco ブロードバンド ワイヤレス ゲートウェイ リリース 2.2

© 2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2010, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

CHAPTER 1

Cisco ブロードバンド ワイヤレス ゲートウェイの概要

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）の概要について説明します。また、エンドツーエンド固定またはモバイル IP ネットワーク内での機能についても説明します。

概要

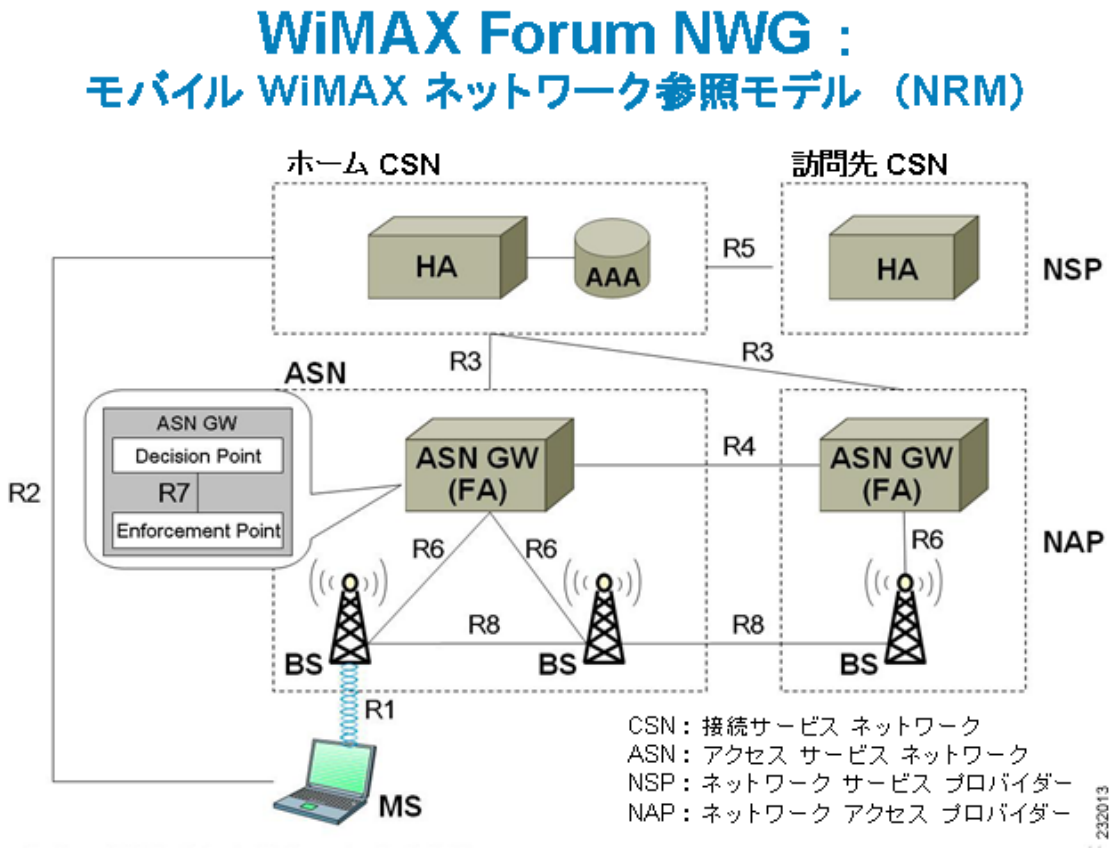
Cisco BWG は WiMAX ネットワークでゲートウェイの役割を果たします。また、エンドツーエンド IP アーキテクチャの一部として設計されています。WiMAX は規格準拠のワイヤレス テクノロジで、長距離でも高い水準のスループット ブロードバンド接続を実現できます。WiMAX はさまざまなアプリケーションで使用できます。たとえば、「ラスト マイル」ブロードバンド接続、固定および携帯電話サービス、ホットスポットおよびセルラー バックホール、業務用高速エンタープライズ接続があげられます。

WiMAX は固定ワイヤレスについては IEEE 802.16d 規格、モバイル ワイヤレスについては 802.16e 規格にそれぞれ準拠しています。この規格によりチップセットの大量生産が可能となり、CPE コストの削減、ベンダー間の相互運用性、使用者の投資リスクの抑制を実現できるため、顧客にとっては魅力的です。

WiMAX ネットワークの構造的枠組みは、Access Service Network（ASN; アクセス サービス ネットワーク）と Core Service Network（CSN; コア サービス ネットワーク）で構成されています。固定 / モバイル市場を対象とした新しい、または小規模な展開については、このリリースでは独立した ASN のみが可能です。リリース 1.0 以上では、スタンドアロンの ASN のみを対象としています。

図 1-1 に WiMAX ネットワーク参照モデルを示します。

図 1-1　WiMAX ネットワーク参照モデル



アクセス サービス ネットワーク

アクセス サービス ネットワークは、WiMAX 加入者が無線アクセスできるようにするためのネットワーク機能の集合です。ASN では通常、ネットワークの検出および選択、MSS とコア サービス ネットワーク（CSN）の間の接続サービス、ラジオ リソース管理、マルチキャストおよびブロードキャスト制御、イントラ ASN モビリティ、ページング、位置管理などの機能を使用できます。

WiMAX アーキテクチャはモバイル加入者と固定加入者、ASN と CSN で構成されています。ASN とこれらの加入者の間のインターフェイスは、IEEE 802.16（固定加入者の場合「d」、モバイル加入者の場合「e」）に準拠しています。ASN はベース ステーション（1 つまたは複数のベース ステーション クラスタ）で構成されています。ASN は複数の Connectivity Service Network（CSN; 接続サービス ネットワーク）で共有できます。

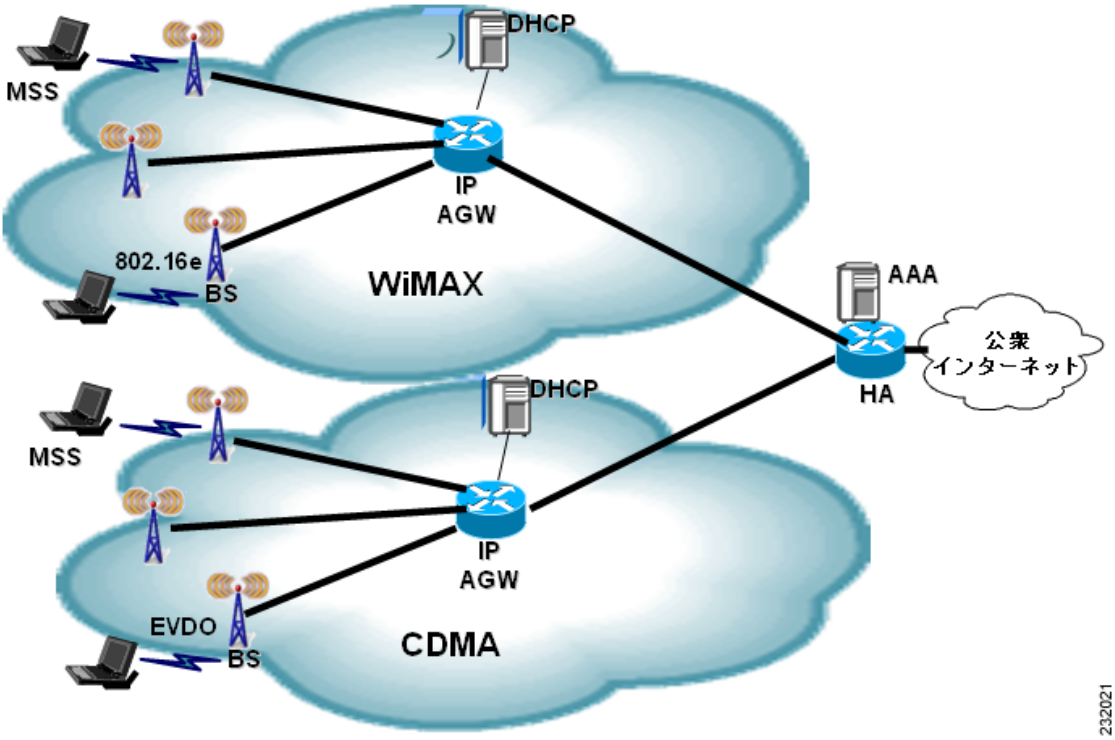
Network Access Provider（NAP; ネットワーク アクセス プロバイダー）は、WiMAX 無線アクセス インフラストラクチャを 1 件または複数の WiMAX Network Service Provider（NSP; ネットワーク サービス プロバイダー）に提供する事業者です。NAP は 1 つ以上の ASN を使用してこのインフラストラクチャを実装します。

接続サービス ネットワーク（CSN）は、IP 接続サービスを WiMAX 加入者に提供するためのネットワーク機能の集合です。CSN を構成するネットワーク要素として、ルータ、ホーム エージェント、AAA プロキシ/サーバ、ユーザ データベース、ポリシー サーバ、コンテンツ サービス ゲートウェイ、サービス セレクション ゲートウェイ、インターワーキング ゲートウェイ デバイスなどがあげられます。

完全 IP エンドツーエンド モバイル ネットワークの登場により、完全 IP ブロードバンド アクセス ゲートウェイが必要となっています。IP アクセス ゲートウェイは無線に依存せず、モビリティとセキュリティに対応します。また、無線ネットワークで IP サービスを使用できるようにします。つまり、BWG はベース ステーション（BS）と IP ネットワークの間で情報を共有するために使用されます。無線に依存しない制御はすべて BWG の一部であり、無線に依存する制御はすべて BS の一部です。

図 1-2 は WiMAX ネットワークの要素を示しています。

図 1-2　　WiMAX ネットワークの要素



Cisco BWG

Cisco BWG は 802.16e ワイヤレス ドメインと IP ネットワークの間でアクセス ゲートウェイの機能をはたします。ユーザ側から見れば最初のホップ IP ルータであり、AAA サーバとのインタラクションのための NAS およびアカウンティング クライアント機能を使用できます。

BWG ではアクセス ネットワーク認証およびセキュリティ機能を使用できます。

BWG にはローカル モビリティ アンカー機能があり、ユーザはベース ステーション間で移動することができます。BWG は認証およびセキュリティ ID をキャッシュし、ベース ステーション間または BWG 間での高速ローミングに対応できるようにしています。

BWG は IP モビリティ スキームの重要な部分を占めています。ベース ステーション間のモビリディ機能や、外部エージェント機能を終了させることができます。BWG は無線ベアラを IP ネットワークにマッピングします。BWG は CSN およびポリシー サーバとあわせて動作することにより、ユーザにかわってポリシーを制御します。さらに、BWG はベース ステーションに配置される IP ホスト機能の IP ゲートウェイとして機能します。BWG では、エンドツーエンド QoS、モビリティ、セキュリティなどの、アクセス ネットワークのための IP 機能が統合されています。

Cisco IOS リリース 12.4(24)YG2 は、Cisco 6500 Catalyst Switch プラットフォームおよび 7600 シリーズ ルータの SAMI カードの Cisco BWG 機能用に最適化されています。

Cisco BWG リリース 2.0 以降は次のプラットフォームに対応しています。

- Cisco Catalyst 6500 シリーズ スイッチ プラットフォーム（SAMI ブレードがインストール済み）：設置と設定については次の URL を参照してください。

  スイッチ シャーシの設置

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Chassis_Installation/Cat6500/6500_ins.html

  スイッチ シャーシ モジュールの設置

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Module_Installation/Mod_Install_Note/78_15767.html

  リリース ノート

  http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_notes_list.html

- Cisco Catalyst 7600 シリーズ ルータ プラットフォーム（SAMI ブレードがインストール済み）：設置と設定については次の URL を参照してください。

  http://www.cisco.com/en/US/products/hw/routers/ps368/prod_installation_guides_list.html

  - 7600 シリーズのスーパーバイザ モジュール（Sup720-3BXL、SUP IOS リリース 12.2(33)）は IOS-SLB 機能に対応しています。また、機能拡張により BWG 選択機能を使用できるようになっています。
  - シャーシごとに最大 8 個のブレードを使用できます。
  - BWG はまとめて配置されているブレード上で CSG2 および HA と共存できます。

Supervisor 720 はシングル モードでもリダンダント モードでも使用できます。Supervisor 720 は 3B と 3BXL の両方のバージョンが使用できますが、3BXL の方が推奨バージョンであり、テストも完了しています。

このリリースでは Supervisor 32 はサポートされていません。

表 1-1　6500 Catalyst スイッチおよび 7600 インターネット ルータでの Cisco SAMI のメモリ要件

Cisco 6500 Catalyst スイッチ	BWG ソフトウェア フィーチャ セット	Sup720-3BXL、SUP IOS リリース 12.2(33)	256 MB	512 MB	RAM
Cisco 7600 インターネット ルータ	BWG ソフトウェア フィーチャ セット	Sup720-3BXL、RSP720-3C-GE、RSP720-3CXL-GE SUP、IOS リリース 12.2(33)	256 MB	512 MB	RAM

SUP の下位互換性

Cisco 7600 ハードウェア プラットフォームの BWG リリース 2.2 では、SUP ソフトウェア バージョン SRE が必要です。しかし、古い SUP ソフトウェア バージョン SRD では BWG リリース 2.2 で使用できる機能が限られます。

BWG 2.2 が SUP-SRD で動作するようにするには、次の非表示 CLI をグローバル コンフィギュレーション モードで設定する必要があります。

	コマンド	目的
ステップ 1	`router(config)# wimax agw sup-backward-compatible`	BWG が SRD スーパーバイザ イメージで動作するよう指定します。

SUP-SRD では、BWG リリース 2.2 は主に Cisco-R6、PMIP などの BWG1.x 機能のために使用されます。

（注）　SUP-SRD イメージを使用する場合、次の BWG リリース 2.2 の機能は使用できません。

- L2-L2 ブリッジングのサポート
- SLB スティッキ性のサポート
- SLB モードでの NWG R6
- SLB モードでの MS アイドル モード

CHAPTER 2

Cisco ブロードバンド ワイヤレス ゲートウェイの構成

このフィーチャ モジュールでは、Cisco ブロードバンド ワイヤレス ゲートウェイ（BWG）の機能セットについて説明します。また、これらの機能を設定する方法について説明し、設定の例を適宜示します。

この章では、次の機能について説明します。

リリース 2.2 の新機能

リリース 2.2 では、次の機能が追加されました。これらは、メインの機能リストで相互参照にもなっています。

- L2-L2 ブリッジング
- ハンドオフ時の中間アカウンティングの更新
- Network Access Identifier（NAI）としての PMIP Authenticated Network Identifier（PANI）
- ローカル設定または AAA サーバから DNS およびデフォルト ゲートウェイ設定を送信するための PMIP DHCP プロキシ サポート

リリース 2.0 の新機能

リリース 2.0 では、次の機能が追加されました。これらは、メインの機能リストで相互参照にもなっています。

- 「プロキシ モバイル IP」のサポート
- 「DSCP マーキング」（P.2-8）
- 「WiMAX NWG 仕様（1.2.2）への準拠」（P.2-9）
- 「Accounting Start 応答」（P.2-60）
- 「AAA ベースのホットライン」（P.2-64）
- 「AAA パケット オブ ディスコネクト メッセージ（PoD）」（P.2-69）
- 「AAA ベースの固定 IP アドレスのプロビジョニング」（P.2-70）
- 「SLB スティッキ性のサポート」（P.2-94）
- 「合法的傍受」（P.2-96）
- 「ヒットレス ソフトウェア アップグレード」（P.2-116）

イーサネット コンバージェンス サブレイヤ（CS）

Wimax イーサネット Convergence Sublayer（CS; コンバージェンス サブレイヤ）を使用すると、WiMAX ネットワークでイーサネット サービスをお客様に直接提供できます。IP CS と比較した場合、イーサネット CS では IEEE 802.3 フレーム（上位レイヤの IP データグラムを伝送する）を 802.16 PDU でカプセル化できます。Cisco BWG 1.1 リリースでは、BS ローカル スイッチ（企業カスタマーの場合）と L2-L3 ブリッジング コンバージョン（ホームカスタマーの場合）というイーサネット CS の 2 つのオプションのみが実装されています。

イーサネット CS の要件として、BWG では Customer Premises Equipment（CPE; 顧客宅内機器）/MS/ホストに静的に割り当てられた IP アドレスをサポートします。BWG の次のサブ機能が含まれます。

- 加入者/CPE あたり最大数（8）のアクティブ ホストを強制使用します。
- ARP またはホストからのアップリンク パケットを通じて、ホストの L2/L3 の詳細を自動学習します。
- AAA からの Framed-Route による静的ホスト IP 検証
- アイドル ホストをエージングする/追い出すメカニズム

イーサネット CS：R6 コントロールのみ

Cisco 12.4(15)XL1 リリースでは、BWG と Base Station（BS; ベース ステーション）との間で WiMAX R6 インターフェイスがシグナリング目的のみで使用されます。BWG はトラフィックをローカルでスイッチするように BS に指示します。Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）によるカプセル化を行わないと、BWG は BS からのベアラ トラフィックを受信しません。ただし BS はイーサネット フレームを外部に接続されている L2 スイッチに切り替えまたは転送する必要があります。

（注） R6 コントロール プレーン専用の機能は、Cisco BWG R1.1 リリースのイーサネット CS のみで使用してください。

この設定ではデータ パケットが BWG を通過しなくなるため、BWG には次の調整が必要です。

- セッション アイドル タイマー：BWG は、パケットを受信しない場合や加入者に送信しない場合であっても、セッションが開いたままであるようにする必要があります。
- AAA でセッション タイマーが 0 に設定されている場合、無限であることを意味します。
- アカウンティング：BWG では、「Accounting Start」と「Accounting Stop」のみを実行します。これらはサービス フローの作成と削除に対応します。定期的な中間アカウンティング アップデートは実行されません。この場合、BWG はベアラ トラフィックを受信しないためです。

BWG が BS から登録解除要求を受信しない場合、ハングしているセッションを取り除くために、絶対セッション タイマーを使用して BWG 上の MS が登録解除されます。

R6 コントロール専用の機能におけるイベントのシーケンスを次の手順に示します。

ステップ 1　SS は登録メッセージを BS に送信します。BS は登録メッセージを BWG に転送します。

ステップ 2　BWG は user_name が「*MSID*@プロキシレルム」であるプロファイルを AAA サーバに要求します。プロキシレルムは、ユーザ グループで設定されます。

ステップ 3　AAA は、次の情報とともに SLA プロファイルを送り返します。

- SS は、SLA プロファイルに基づいて、ビジネスとして識別されます（BWG で **encap-type none** として設定）。この場合、そのトラフィックは BS でローカルにスイッチされ、エンタープライズとして識別されます。
- VLAN ID（同じ BS に接続するビジネス SS ごとに一意）。たとえば VLAN ID = 250 です。

ステップ 4　BWG はサービス フロー プロファイル情報を VLAN ID およびパケット分類ルールとともに BS に送信します。さらにアップリンク パケット分類ルールを SS に送信します。

ステップ 5　アップストリーム トラフィックが開始されます。たとえば CPE ルータがアップリンク .1q タグ付きトラフィックを次の VLAN で送信するとします。

- VLAN 10（営業）
- VLAN 20（音声）

ステップ 6　SS が VLAN 10 からのトラフィックをサービス フロー 1 に送るように PCR が設定されている場合、このサービス フローのタイプは BE です。SS が VLAN 20 からのトラフィックをサービス フロー 2 に送るように PCR が設定されている場合、このサービス フローのタイプは UGS です。SS はトラフィックを BS に送信します。

ステップ 7　BS は別の .1q タグをエンタープライズ x の着信トラフィック（たとえば VLAN ID = 250）に割り当てます。内部タグは変更されません。トラフィックは L2 ネットワークへスイッチされ、BWG へは転送されません。

ステップ 8　ダウンストリーム トラフィックの場合は、次のようになります。

- BS は L2 スイッチド ネットワークからトラフィックを受信します。
- エンタープライズ トラフィックは BWG を通過しません。
- PCR は、送信された SF トラフィックについて BS に通知します。
- BS は外部タグをすべて取り除き、残りのパケット トラフィックを SF1（BE）または SF2（UGS）として無線で転送します。

ステップ 9　SS はトラフィックを受信して、スイッチに転送します。内部タグは変更されません。

また、このシナリオでは BWG ではなく BS がアップリンク / ダウンリンク サービス フローを終了します。BWG はダウンリンク分類子を BS に送信して、BS がパケットの適切なダウンリンク サービス フローを選択できるようにします。BS は、ダウンリンク分類子で 802.16e エアーリンク接続 ID/ サービス フローを選択する必要があります。また、BWG はアップリンク トラフィックに使用する VLAN タグを BS に通知します。

BWG の設計にはフロー単位で BS ローカル スイッチングを実行できる柔軟性がありますが、リリース 1.1 では、すべてのサービス フローがすべてを BS ローカルでスイッチするのか、または特定の加入者に対して BWG でスイッチするのか設定されている必要があります。

R6 コントロール専用の設定

この項では、Cisco BWG で R6 コントロール専用機能を設定する方法について説明します。R6 コントロール専用を有効にするには、次の作業を行います。

	コマンド	目的
ステップ 1	`router(config)# wimax agw sla profile gold`	BWG で Service Level Agreement（SLA; サービス レベル契約）を指定します。BWG は、各 SLA プロファイルでサービス フローの数を 4 に制限します。この条件を超えようとするとエラーが発生します。
ステップ 2	`router(config)# service-flow pre-defined isf profile isf encap-type none vlan 10`	VLAN ID が 10 に設定されている場合に、最初のサービス フローが BS でローカルにスイッチされることを指定します。
ステップ 3	`service-flow pre-defined secondary profile sec1 encap-type none vlan 10`	BWG は、R6 DP 登録要求メッセージのデータ パスの暗号化タイプ（NONE）とデータ パス ID（プライオリティ + VLAN ID）を使用して、BS のローカル スイッチングを制御します。ここで定義されている VLAN ID は、AAA から上書きされる可能性があることに注意してください。

（注）　BWG リリース 1.1 では、VLAN が同じ場合は同じ SLA プロファイルで設定しなければなりません。

（注）　VLAN が AAA からダウンロードされると、すべてのサービス フローでローカルに設定された VLAN がその VLAN で上書きされます。

BWG は、R6 DP 登録要求メッセージのデータ パスの暗号化タイプ（NONE）とデータ パス ID（プライオリティ + VLAN ID）を使用して、BS のローカル スイッチングを制御します。ここで定義されている VLAN ID は、AAA から上書きされる可能性があることに注意してください。VLAN プライオリティ（VLAN タグで最上位 3 ビット）は、サービス フローに定義された DSCP/優先度が使用されます。DSCP/優先度がローカルで定義されていない場合は、サービス フローに使用される WiMAX QoS データ デリバリ サービス タイプを基に計算されます。

イーサネット CS：R6 でデータとコントロールの両方

WiMAX Forum の NWG 規格に合わせるため、Cisco の R6 インターフェイスではデータとコントロールでイーサネット CS をサポートします。前述のとおり、このリリースでは、BWG の L2-L3 ブリッジング オプションのみがサポートされています。

L2 アップリンク トラフィックは CPE/MS の背後にあるホストから送られます。パケットは 802.16 PDU でカプセル化され、R1 インターフェイスを介して CPE によって BS に送信されます。BS はイーサネット フレームを GRE パケットにカプセル化し（GRE トンネルは R6 シグナリング交換時に確立されている）、BWG に送信します。BWG は、R6 データ パスを介して GRE パケットを受信します。GRE ヘッダーと L2 ヘッダーが取り除かれたら、内側の IP パケットが目的の VRF で設定された適切なインターフェイスに転送されます。

BWG は、ダウンリンク パケットを受信すると、特定ホストに関する L2 情報が保存されているホストを探します。L2 情報は、パケットで伝送される L3 情報とともに、設定された分類子と比較するために使用されます。その結果、適切なサービス フローが選択されます。サービス フローが選択されると、保存されているホストの L2 情報を使用して、受信した IP パケットがカプセル化されます。

BWG では、次のメカニズムによって、ホストの L2/L3 情報を動的に学習します。

- ホストからの DHCP 手続き
- ホストからの ARP 要求
- ホストからのアップリンク パケット

L2-L3 ブリッジングの VLAN - VRF マッピング

この機能では、特定の VLAN ID を持つアップリンク L2 トラフィックが VRF ルーティング ドメインにマッピングして、IP パケットを転送できます。一方、特定の VRF からのダウンリンク IP トラフィックは、同じ VLAN ID でカプセル化された MS に送信されます。MS の背後にあるホストごとに多くても 1 つの VLAN ID をサポートするように設計されていることに注意してください。

パケット フラグメンテーションの処理

BWG 上のバーチャル テンプレート インターフェイスは、R6 データ パスで GRE フラグメンテーションが不要になるような MTU を使用して設定される必要があります。推奨される MTU 値は 1440 未満です。

バーチャル テンプレート インターフェイス用に設定された MTU よりも大きいダウンリンク パケットの場合、IOS によってパケットが断片化されます。このとき、IOS は元のパケットの DF ビットをクリアすることが予想されます。その場合、BWG は 2 つの IP パケットを受信します。2 つの IP パケットは別々に GRE でカプセル化されて、BS に送信されます。BS は、2 つのパケットを構成してアプリケーションに渡すホストに対して、これらのパケットを透過的に渡します。

大規模なアップリンク パケットの場合、BS は DF ビットをクリアし、2 つのパケットに分割して BWG に送信します。BWG はパケットを再構成しませんが、別々に転送します。

ジャンボ フレームのサポート

この機能では、BWG がペイロードで最大 2000 バイトのジャンボ フレームをサポートできます。これまでは、1500 バイトがパケット断片化の上限でした。この機能により Maximum Transfer Unit（MTU; 最大伝送ユニット）は 2000 に高まります。

- BWG アプリケーションの mtu は 2000 に設定されています。バーチャル テンプレート インターフェイスで設定することにより、mtu の設定を変更できます。しかしバーチャル アクセス インターフェイスに反映されるのは BWG に対して 2000 です。
- バーチャル テンプレート インターフェイスにおいてデフォルトの mtu と ip mtu はそれぞれ 2000 と 1500 です。そのため、どちらも BWG の起動時に設定されていないと、running-config のバーチャル テンプレート インターフェイスの設定は次のようになります。

```
Router#sh run | sec Virt
interface Virtual-Template1
 mtu 2000
 ip address 3.3.3.3 255.255.255.0
 ip mtu 1500
 encapsulation agw
```

- mtu が設定されると、ip mtu は mtu 以下に設定でき、バーチャル アクセス インターフェイスで動的に反映されます。

no ip mtu により、バーチャル アクセス インターフェイスの **ip mtu** は mtu（2000）に設定されます。**ip mtu** に他の値を設定する場合は、バーチャル テンプレート インターフェイスで明示的に設定する必要があります。

DHCP Option 82 機能拡張

BWG がダウンリンク DHCP パケットの L2 ヘッダーを構成できるように、L2 ヘッダー全体が Option 82 内にコーディングされます。Option 82 は、DHCP サーバから反映されます。このサブオプションは、BWG と DHCP サーバとの間のみに適用されます。

DSCP の計算 / マーキング / シグナリング

ダウンリンク トラフィックの場合、DSCP マーキングが BWG によって実行されます。外側 IP の DSCP 値は、優先度順に次から取得されます。

- フローに設定された DSCP/ 優先度
- SF のデータ デリバリ サービス タイプから計算（次表）

表 2-1

WiMAX QoS	DSCP	コメント
UGS	46	
ERT-VR	38	
RT-VR	30	
NRT-VR	22	
BE	0	

（注） 内側 IP の DSCP 値は、外側 IP の DSCP をマーキングするために使用できなくなりました。

（注） 内側 IP 値もマークされます。

（注） SF QoS から DSCP のマッピング テーブルは、DSCP が SF 向けに設定されていないときのみ使用されます。

アップリンク トラフィックの場合、BWG はダウンリンク サービス フローと同様の方法で DSCP 値を取得します。アップリンク DSCP 値は、データ パス情報 TLV で BS に通知されます。

内側のユーザ（アップリンク）パケットの DSCP マーキングは信頼できないことに注意してください。そのため、サービス フローについて BS に通知される同じアップリンク DSCP 値も R3 アップリンク パケットを再マーク付けするために使用されます。

DSCP マーキング

リリース 2.0 では、次の 2 つの方法で、BWG で外側 IP の DSCP 値をダウンリンク データ トラフィック用にマーキングできます。

- ダウンリンクのサービスフロー プロファイルで指定された DSCP 値を使用する

  router(config-gw-sf-dir)#set dscp *value*

- インバウンド R3 IP パケットの DSCP 値を使用する

  router(config-gw-sf-dir)#set dscp r3

次の 3 つの方法で、BWG で R3 IP の DSCP 値をアップリンク データ トラフィック用にマーキングできます。

- 内側 IP の DSCP 値を使用する（デフォルト）
- 外側 R6 IP の DSCP 値を使用する

  router(config-gw-sf-dir)#set r3 dscp r6-outer

- アップリンクのサービスフロー プロファイルで指定された DSCP 値を使用する

  router(config-gw-sf-dir)#set r3 dscp *value*

イーサネット フレームのサポート

BWG では、異なるホストに対して Ethernet II、LLC（802.2）、Ethernet SNAP フレーム タイプに対応できます。ただし、1 つのホストはセッション中に同じフレーム タイプを使用する必要があります。つまり、そのホストは同じイーサネット フレーム タイプを使用した場合のみ、パケットを送信できます。

イーサネット VLAN のサポート

VLAN タグ（具体的には 802.1Q および Q-in-Q）を使用したイーサネット パケットもサポートされます。

イーサネット FCS（CRC）

GRE から BWG へのアップリンクとダウンリンクの両方のパケットで CRC を使用しないでください。

制限事項

Cisco BWG リリース 1.1 以上では、CS イーサネットに次のような制限があります。

- ARP と DHCP 以外の MS から送信されるレイヤ 2 ブロードキャスト/マルチキャスト パケットは、BWG でドロップされます。

WiMAX NWG 仕様（1.2.2）への準拠

BWG では、Cisco R6 と NWG 仕様の両方を同時にサポートします。この機能を使用するに当たって、特別な設定は必要ありません。BWG はメッセージ ヘッダーの「Version」フィールドを使用して Cisco R6 と NWG R6 を区別します。この区別は、BWG の登録者単位で行われます。セッションの最初の WiMAX R6 メッセージの Version が 1 の場合、NWG R6 として指定されます。同様に、最初のメッセージで Version が 0x81 の場合は、Cisco R6 です。セッションではそのライフ スパンを通じて同種の R6 を使用する必要があります（ハンドオーバーを除く）。

異種の R6 による 2 つの BS からのハンドオーバーもサポートされます。

L2-L2 ブリッジング

リリース 2.2 以降の BWG では L2-L2 ブリッジングをサポートします。BWG で L2-L2 ブリッジングを設定するには、IOS の Integrated Routing and Bridging（IRB）機能に関する知識が必要です。

L2-L3 ブリッジングに比べて L2-L2 ブリッジングでは、BWG でイーサネット CS パケットをそのまま通過させることができます。

L2-L2 ブリッジングは、ユーザ グループごとに個別にイネーブルです。L2-L2 機能があるユーザ グループに対してイネーブルの場合、そのユーザ グループに対して L2-L3 機能は自動的にディセーブルになります。

Wimax ユーザ グループでブリッジングをイネーブルにするには、グループをブリッジ グループに追加しておく必要があります。ユーザ グループがブリッジ グループに追加されると、仮想 Wimax インターフェイス（Wimax<bridge-group>）が作成されます。この仮想 Wimax インターフェイスは、ブリッジ グループ内のユーザ グループを表します。複数のユーザ グループを同一のブリッジ グループには追加できません。

ブリッジ グループを作成するには、**bridge-group** コマンドを使用します。

次に、ブリッジ グループを設定する例を示します。

```
bridge irb
!
interface Ethernet1/1
  description Interface belong to bridge-group 1
  bridge-group 2
  no bridge-group 2 source-learning
  no ip address
!
bridge 2 protocol ieee
!
wimax agw user group-list wimax
 user-group any
  aaa authentication method-list agw
  aaa accounting method-list agw
  sla profile-name silver
  bridge-group 2
  no bridge-group 2 source-learning
  bridge-group 2 transparent-vlan vlan-tag
```

イーサネット IP ホスト

イーサネット IP ホストでは、パススルー ARP パケットまたは他のアップリンク データ パケットに基づいて、BWG ホスト エントリが作成されます。ホストの IP アドレスは、BWG 内にある加入者のホスト エントリ テーブルに収集されます。

MS またはホストに送信される ARP パケットは、BWG（プロキシ ARP）によって応答されます。Wimax に送信される ARP パケット以外のパケット （ダウンリンク ブロードキャストまたはマルチキャスト L2 パケットなど）はドロップされます。

BWG は、ホストで生成される DHCP 要求に対してレイヤ 2 DHCP リレー エージェントとして動作します。BWG は、circuit-id および remote-id を含む DHCP Option 82 をアップストリーム DHCP パケットに追加します。ただしブリッジングでは、BWG にレイヤ 3 ネットワーク ID がないため、giaddr フィールドが設定されません。

PPPoE ホスト

PPPoE ホストでは、BWG は PPPoE Discovery（シグナリング）パケットを代行受信します。代行受信されるパケットは次のとおりです。

- PPPoE Active Discovery Initiation（PADI）
- PPPoE Active Discovery Offer（PADO）
- PPPoE Active Discovery Request（PADR）

- PPPoE Active Discovery Session-confirmation（PADS）
- PPPoE Active Discovery Terminate（PADT）

PADS に対応する BWG ホスト エントリは、BWG がネットワークからクライアントに送信された PADS を検出した後で作成されます。

加入者ごとに最大で 20 の PPP0E ホストを作成できます。新しいホストが受け入れられるのは、少なくとも 1 つの既存ホストのアイドル期間がしきい値を超えた場合のみです。アイドル時間が最も長かったホストが新しいホストに置き換わります。ホストのアイドルしきい値は、セッション アイドル タイマーの 75% です。

BWG では、ベンダー固有タグとリレー セッション ID タグも各 PADI および PADR パケットに追加します。ベンダー固有タグには、回線 ID（SF ID）およびリモート ID（MSID）サブオプションがあります。リレー セッション ID タグは、SFID を挿入するときに使用されます。BWG ではこれらのタグを PADO および PADS パケットから削除してから、PPPoE クライアントに転送します。

透過 VLAN

L2-L2 ブリッジングを使用すると、BWG では L2VPN を設定できます。

エンタープライズで L2VPN 機能をイネーブルにするために、BWG は ARP、DHCP、PPPoE の代理受信機能をディセーブルにし、アップリンクおよびダウンリンク方向で変更なしですべての L2 パケットをパススルーできるようにします。ARP、DHCP、PPPoE の代理受信機能がディセーブルになると、BWG は ARP プロキシ機能を実行できないため、ホスト情報を学習できません。そのため、BWG では、パケットが CPE からのものなのか、その背後にあるホストからのものなのかを特定できません。

VLAN ID とブリッジ グループの組み合わせは、BWG コンテキスト内の加入者ごとに一意でなければなりません。モバイル環境では、MS のモビリティ イベントが関連するときにこの一意性を保証するため、AAA VLAN と BWG の加入者のブリッジ グループ割り当てを設定するときは注意が必要です。

トランスペアレント ブリッジングがイネーブルの場合、BWG には加入者からのすべてのアップリンク トラフィックをブリッジ グループに送信する前に VLAN タグを設定できます。VLAN ID は、Cisco AVP である AAA から取得されます。VLAN 優先度値は、R6 アップリンク サービス フローの QoS データ デリバリ サービス タイプ（BE、UGS など）から明示的に設定またはマッピングされます。AAA が VLAN ID を提供しない場合は、セッションが拒否されます。

ダウンリンク パケットの場合、加入者はブリッジ グループ ID と VLAN ID の組み合わせで特定されます。外側の VLAN タグとそのイーサネット ヘッダーは、設定済みのパケット分類ルールに合わせ、R6 ダウンリンク サービス フローを選択するときに使用されます。このとき、アップリンク トラフィックが BWG によって VLAN タグが設定されている場合は、外側の VLAN タグが取り除かれます。

トランスペアレント ブリッジングがイネーブルであり、BWG の VLAN タギングがディセーブルの場合、加入者からのすべてのトラフィックは同じ VLAN ID を使用する必要があります。

次に、BWG でトランスペアレント ブリッジングをイネーブルにする例を示します。

```
wimax agw user group-list wimax
 user-group unauthenticated
  aaa accounting method-list agw
  sla profile-name silver
bridge-group 2
bridge-group 2 source-learning
bridge-group 2 transparent-vlan [vlan-tag]
 !
!
```

CPE 管理

CPE 管理機能では、AAA を使用して Cisco WiMax ソリューション全体で加入者/CPE を集中管理できます。実際の導入では輻輳が発生する可能性や複数の AAA プロキシがあることを考慮すると、RADIUS Access Accept メッセージを AAA から受信するには最大で 10 秒かかります。そのため、特定 R6 プロトコル ステート マシンは、この AAA 応答遅延を許容するように設計されていなければなりません。

未認証 CPE 管理機能は、AAA と BWG に移動しました。具体的には、次の機能が含まれます。

- ユーザ ドメイン グループの再割り当て
- サービス レベル契約（SLA）
- VLAN ID
- モバイル機能（ホーム BS リストによる非移動性、および移動性）
- 静的 IP の許可（### CPE で静的 IP が許可されるか）
- CPE タイプ
- CPE 設定
- CPE 自動プロビジョニング
- CPE サービス ステート（CPE がブラックリストに載っているかどうか）

この項では、次の機能について説明します。

未認証加入者の AAA アクセス

EAP ベース認証をサポートしないベース ステーション/CPE の場合、BWG は RADIUS を使用した PPP/PAP 認証方式を提供します。このような CPE は、一般に未認証の CPE として分類されます。また、未認証ユーザの場合、CPE からユーザ名を取得しません。

この場合、次の CLI に基づいてユーザ名、レルム、パスワードが作られます。

```
wimax agw user group-list wimax
 user-group unauthenticated
  aaa authentication method-list xxxx
  proxy realm sprint.com passwd ciscoway
  sla profile-name silver
 !
```

（注）　**aaa authentication method-list xxxx** コマンドは、RADIUS Access Request がグループの BWG から開始するかどうかを示します。CLI が設定されていない場合、AAA クエリーは必要ありません。それぞれの認証方式リストはタイプ PPP であり、BWG は PAP ベースの認証を実行できます。

（注）　PAP ユーザに対する再認証はサポートされていません。CPE/MS によって再認証が試みられると、セッションは登録解除されます。

（注）　**proxy realm** *sprint.com* **password** *ciscoway* コマンドは、RADIUS Access Request メッセージの設定方法を BWG に指示します。設定された場合、ユーザ名は *mac@realm*（たとえば *mac @sprint.com*）のように構成されます。レルムが構成されていない場合のユーザ名は *mac* です。構成されていない場合、パスワードとして *cisco* が使用されます。**aaa authentication method-list** *xxxx* を使用して設定された方式リストは、Access-Requests で使用されません。PAP 認証では **aaa authentication ppp default** コマンドでグローバルに設定された **default** 方式リストを使用するためです。

（注）　これら 2 つの CLI は、他のユーザ グループ（EAP ユーザ）にも適用できます。ただし EAP ユーザに **proxy-realm** を設定しても影響はありません。

AAA サーバからの応答には、ユーザの実際のドメイン名が含まれます。このドメイン名は、ローカル ユーザ グループを選択するために使用されます。前述のスキーマでは、EAP 認証ユーザを対象外にしないでください。つまり、BWG では EAP および非 EAP 認証されたユーザが共存できなければなりません。認証済みユーザの場合、ユーザ名は EAP 識別情報要求を通じて CPE から取得されます。EAP では、AAA に対するアクセス要求で NAI を使用します。AAA からの応答に SLA プロファイル名、および EAP ユーザのユーザ ドメイン名が含まれる場合、AAA からの結果が先に決定された情報を上書きします。

新しい AAA アトリビュート

CPE 管理をサポートするために、次の新しい AAA アトリビュートが導入されました。これらの新しいアトリビュートは、RADIUS Access-Accept メッセージで返される可能性があります。これらのアトリビュートはすべてオプションであり、cisco_vsa 下の AVP です。

表 2-2　新しい AAA アトリビュート

アトリビュート	形式 / 長さ	コメント
User Domain Name （name_string "User-Name"）	ストリング /253	返された場合、加入者は対応するユーザ グループに再割り当てされます。
SLA Profile Name （name_string "sla-profile-name"）	ストリング /253	返された場合、この名前に対応する SLA プロファイルによって、BWG 内のユーザ グループ内にローカルで定義された SLA プロファイルが上書きされます。
VLAN ID （name_string "vlan-id"）	整数 /2	L2 トラフィックにタグ付けするときに使用されます。SF のローカル定義を上書きします。BS ローカル スイッチの場合は、BS に通知されます。 （注）　このアトリビュートは、R6 コントロール専用セッションに適用されます。

表 2-2　新しい AAA アトリビュート（続き）

CPE Type （name_string "cpe-type"）	ストリング /253	診断用であり、BWG によって使用されません。ただし「show wim agw sub」CLI によって表示されます。
CPE Mobility （name_string "cpe mobility"）	整数 /2	CPE で可能なモビリティの程度を定義します。 0：ホーム BS リストによる非移動性 1：移動性 デフォルトは移動性です。
CPE Settings （name_string "cpe-settings"）	整数 /4	これらの CPE 切り替え設定は、AAA で設定され、BWG にダウンロードされます。BWG では、R6 コントロール プロトコルをさらに使用して、BS に通知し、さらに BS は情報を CPE に渡します。 - ビット 31：IngressACL Toggle：イネーブルにすると、CPE は、学習していないソース IP アドレスを持つホストからのアップリンク トラフィックをブロックします。 - ビット 30：Broadcast Filtering Toggle：イネーブルにすると、CPE はアップリンク ブロードキャスト トラフィックをブロックします。 - ビット 29：Rate Limiting Toggle：イネーブルにすると、CPE はアップリンク トラフィック（ICMP や ARP など）にレート制限を課します。 - ビット 0 ～ 28：予約済み。0 に設定されています。 Cisco R6 仕様を参照してください。
Base Station List （name_string "bs-list"）	バイナリ 16 進 /253 BSID1:BSID2	CPE のモバイル機能が「非移動性」である場合、このリストはホーム BS リストとして解釈されます。BSID は、IPv4 アドレスまたは 802.16（6 バイト）形式です。 BSID1 = 1A.01.23.BC

表 2-2　新しい AAA アトリビュート （続き）

Static IP Allowed （name_string "static-ip-allowed"）	整数 /4	BWG が CPE/ ホストの固定 IP アドレスを学習できるようにするかどうかを指定するために使用します。これは主にセキュリティ上の理由からです。 0：未許可 1：許可 このアトリビュートがない場合のデフォルトは未許可です。
CPE Service State （name_string "cpe-service-state"）	ストリング /253	CPE がブラックリストに載るかどうかを示します。 このアトリビュートに定義されている値は次のとおりです。 0：アクティブ 1：滞納 2：盗難報告 3：要注意ユーザ 4：サービスの一時停止

（注）　上記の AAA アトリビュートは、PAP ユーザの場合ですが、EAP ユーザの場合も同様に機能します。

SLA プロファイルの設定

BWG でサービス レベル契約を設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config)# wimax agw sla profile eth_vlan_pri_sla`	BWG でサービス レベル契約（SLA）を設定します。 SLA プロファイルには、すべてのフローが含まれます。BWG は、各 SLA プロファイルでサービス フローの数を 4 に制限します。この条件を超えようとするとエラーが発生します。 Cisco BWG リリース 1.1 では、VLAN が同じ場合は同じ SLA プロファイルで設定しなければなりません。 異なるサービス フローが 1 つの SLA プロファイルの下にリストされます。サブコマンド **sla profile** *profile name* を設定することにより、SLA とユーザ グループを関連付けできます。SLA をプロビジョニングすると、サービス フローの管理が向上します。

	コマンド	目的

ステップ 2	`router(config)# service-flow pre-defined isf profile dfault_vlan_sf`
	`  service-flow pre-defined secondary 1 profile vlan_pri_01_sf`
	`  service-flow pre-defined secondary 2 profile vlan_pri_02_sf`
	`  service-flow pre-defined secondary 3 profile vlan_pri_03_sf`
		異なるサービス フローが 1 つの SLA プロファイルの下にリストされます。

ステップ 3	`router(config)#wimax agw user group-list wimax`
	` user-group unauthenticated`
	`  aaa accounting method-list agw`
	`  sla profile-name silver`
		BWG でユーザ グループ リストを設定します。BWG のプロセッサ 1 つにはユーザ グループ リスト 1 つのみ使用できます。
		コマンドで **no** を使用すると、ユーザ グループ リストが削除されます。このコマンドは、user-group-list サブ コンフィギュレーション モードに入り、作成したユーザ グループ リストの下に複数のユーザ グループを作成します。

上述の設定では、ユーザ グループの SLA プロファイルがデフォルトとして使用されます。AAA が返す SLA プロファイル名が優先されます。

加入者あたり複数 SLA プロファイルのサポート

これまで BWG での SLA プロファイル設定では、サービス パッケージを定義した WiMax サービス プロバイダーがサービス オファリング（フロー タイプ）を適切なプロファイル数に効率的に分類していました。

たとえば次のフロー（flow-voice、flow-data、flow-video、flow-hd-video、flow-premium-voice、flow-premium-data）は、2 つのパッケージに定義してパッケージ単位で加入者に販売できました。

SLA-regular

- flow-voice
- flow-data

SLA-premium

- flow-premium-voice
- flow-premium-data
- flow-hd-video

しかし、サービス プロバイダーが前記のフローで考えられるすべての組み合わせでサービスを提供するには、BWG に同数の SLA プロファイルを設定する必要がありました。

この機能を使用すると、サービス プロバイダーは次のように SLA プロファイルを設定して、希望する組み合わせで顧客にサービスをパッケージ化できます。

SLA-regular data

- Flow-data

SLA-regular voice

- Flow-voice

SLA premium video

- Flow-hd-video

SLA-premium data flow

- Flow-premium-data

BWG では、単一の SLA プロファイル名に対する既存のサポートに加えて、AAA から受信した複数の SLA プロファイル名に基づいてフローを作成できます。AAA は、カンマ、スペース、またはセミコロンで区切った SLA プロファイル名のリストを送信できます。

- BWG はこのリストを解析して、有効な設定済み SLA プロファイルを選択し、セッションのサービス フローを作成します。
- BWG は次のイベント シーケンスを使用してフローを作成します。
- BWG は、設定済み SLA プロファイル名のみをリストから選択します。
- BWG は、SLA プロファイル名のリスト全体から一意のフローのみを選択します。たとえば受信した SLA プロファイル名の下で定義されているすべてのフローから「Union」を選択します（ISF の例外あり）。
- 現在の実装では、フローの作成に成功するには、ISF が 1 つだけ必要です。その結果、BWG は、AAA から受信した SLA プロファイル名のリストにおける SLA プロファイル名の順序に基づいて ISF を選択します。受信した SLA プロファイルで別の ISF プロファイルが設定されている場合でも、受信したリストで最初に有効な設定済み SLA プロファイルから ISF を選択します。
- サービス フローの最大許容数の制限に達した場合、BWG は残りの SLA プロファイルと SF プロファイルをすべて破棄します。
- BWG は、AAA から受信したリストを解析するときに、SLA プロファイルの下にある SF の有効性（たとえば SF が正しく設定されているかどうか）を確認しません。その結果、BWG が SF を開こうとしたときに SF が無効または未設定であることが判明した場合、その SF はドロップされ、BWG は残りの SF プロファイルで処理を続けます。
- AAA から受信した SLA プロファイルに ISF が存在しない場合、セッションはクリアされます。

次に設定の例を示します。

```
wimax agw sla profile silver
service-flow pre-defined isf profile isf
wimax agw sla profile platinum
      service-flow pre-defined secondary 1 profile sec4

wimax agw sla profile gold
      service-flow pre-defined isf profile isf2
      service-flow pre-defined secondary 1 profile sec
      service-flow pre-defined secondary 2 profile sec2
      service-flow pre-defined secondary 3 profile sec3
```

AAA から受信した SLA リストが「silver, gold, or platinum」である場合、セッションの SLA プロファイル名は「silver, or gold」に設定され、BWG で次のような 4 つのフローが作成されます。

- isf
- sec4
- sec
- sec2

AAA から受信した上記の設定 SLA リストが「platinum, unconfigured, gold」の場合、セッションのプロファイル名は「platinum, gold」に設定され、次のような 4 つのフローが作成されます。

- isf2
- sec
- sec2
- sec3

「unconfigured」SLA は、BWG によって破棄されます。

別の例を示します。

```
wimax agw sla profile silver
     service-flow pre-defined isf profile isf
wimax agw sla profile platinum
      service-flow pre-defined secondary 1 profile sec
wimax agw sla profile gold
      service-flow pre-defined isf profile isf2
      service-flow pre-defined secondary 1 profile sec
      service-flow pre-defined secondary 2 profile sec2
      service-flow pre-defined secondary 3 profile sec3
```

AAA から受信した SLA リストが「platinum, unconfigured, gold」の場合、セッションのプロファイル名は「platinum, gold」に設定され、次のような 4 つのフローが作成されます。

- isf2
- sec（SLA を受信した順序に基づいて、このフローは SLA platinum から採用されています）
- sec2
- sec3

「unconfigured」SLA は、BWG によって破棄されます。

AAA からの SLA がない場合、BWG はセッションのユーザ グループの下に定義された SLA プロファイルに従って、フローを作成します。これまでどおり BWG では AAA から送信された単一 SLA プロファイルもサポートします。

ユーザ自動プロビジョニング

AAA がユーザに対してプロビジョニングしない場合でも、短時間だけユーザがネットワークに参加できることがあります。この機能をイネーブルにするには、関連する未認証グループが正しく設定されていなければなりません。イネーブルにするときは、ユーザがネットワークを自由に使用できないように、ユーザ グループのセッション タイマーが小さい値に設定されている必要があります。

自動プロビジョニングを設定するには、次のタスクを実行します。

	コマンド	目的

ステップ 1	`router(config)# wimax agw user group-list wimax`
	` user-group unauthenticated`
	`  aaa accounting method-list agw`
	`  sla profile-name silver`
	`  **user auto-provisioning**`
	`  timeout session **600**`
		AAA がユーザに対してプロビジョニングしない場合でも、指定した時間（設定可能）でユーザがネットワークに自動プロビジョニングできるようにします。

（注）　自動プロビジョニングは、EAP ユーザに対応していません。未認証以外のユーザ グループで設定しても影響はありません。

（注）　固定 IP および IPCS のホストに対する自動プロビジョニングは対応していません。

セッション キャッシング メカニズム

MS と BS との間でエアーリンクの障害が発生し、CPE/MS の背後にあるホストが見つからなくなることがあります。エアーリンク障害時は、CPE に代わって元の BS が R6 登録解除を送出することもしないこともあります。エアーリンク障害後に、CPE が同じ BS または異なる BS に再接続する可能性があります。これまではどちらの場合でも BWG 内のセッションが削除されて再作成されていたため、セッションとホストの情報が失われていました。セッション キャッシング メカニズムでは、CPE 障害時にセッションを保存（つまりキャッシュ）します。この機能には、2 つのシナリオがあります。

- 元の BS は、CPE 障害時に、R6 登録解除要求を BWG に送信します。この場合、BWG のセッションは、CACHED ステートになります。セッションが CACHED ステートのときに CPE が BWG に再参加すると、元のセッションはそのホストとともに保存されます。
- BWG のセッションが準備ステートになると、CPE は（Pre-Attachment Request を通じて同じまたは異なる BS 経由で）BWG に再参加します。この場合、セッションはホスト情報を失わずに再初期化され、再参加が許可されます。

CACHED ステートに入る前に、両方のフローとホストに対する課金は停止します。R6 Pre-Attachment Request を受信すると、CACHED セッションは以前のホストとともに復元されます。この時点でホストの課金は再開されます。その後、通常の手順に従って、加入者に事前定義済みのサービス フローを作成します。

（注）　BWG CLI を使用してセッションをクリアすると、CACHED ステートにはなりません。

セッション キャッシュ タイマーの値は、**user-group** サブコンフィギュレーション モードで指定します。次のように指定できます。

- セッション キャッシュ タイムアウトの値は、1 ～ 259200 秒（3 日間）です。
- サブオプション **follow-dhcp-lease** は、セッション キャッシュ タイムアウトの値をすべてのダイナミック ホストにおける DHCP リースの最大残り時間に設定します。これがデフォルトのオプションです。

Session_Cache_timeout = MAX (ダイナミック ホスト [0] の DHCP リース残り時間 ,
ダイナミック ホスト [1] の DHCP リース残り時間 ,
……..
ダイナミック ホスト [n] の DHCP リース残り時間)

前述のとおり、デフォルトでは **follow-dhcp-lease** オプションによって、セッション キャッシング機能がイネーブルです。詳細な **show-subscriber** コマンドは、セッションの CACHED ステートを表示します。

セッション キャッシングはデフォルトでイネーブルです。以下のいずれかのタスクで次の **user-group** コマンドを使用して、セッション キャッシュ機能をイネーブル/ディセーブルにします。

	コマンド	目的
ステップ 1	`router(config-gw-ugl)# [no] timeout cache-session [1-259200]`	セッション キャッシュ タイマーを秒単位で指定します。範囲は 1 ～ 259200 です。

またはこのオプションを使用します。

ステップ 1	`router(config-gw-ugl)# timeout cache-session follow-dhcp-lease`	セッション キャッシュ タイムアウトの値をすべてのダイナミック ホストにおける DHCP リースの最大残り時間に設定します。

加入者あたり 20 ホストのサポート

Cisco BWG リリース 1.3 以上では、CPE に最大で 20 のホストを使用できます。ただし、BWG に対するホストの合計数は、サポートされる加入者の合計数の 4 倍を超えないようにしてください。

CPE におけるホストのモビリティ

BWG リリース 1.2 では、ユーザはホット スポットと呼ばれる BWG を導入していました。各ホット スポットには WiMAX CPE があり、個人用のホスト/コンピュータは CPE の周辺を移動していました。これらのホストは DHCP ホストです。CPE から離れたホストは DHCP RELEASE を実行できませんでした。ホストが移動してしまったとしても BWG はそのホストに関する情報を保持していて、DHCP リース タイマーが期限切れになるまで情報は BWG から削除されませんでした。これまでの DHCP リースは 3 日間に設定されていました。そのため、BWG から見てホストの最大数に達してしまうと、BWG は新しいホストを拒否していました。

この新しい機能では、次のシナリオに対応します。

- 同じ DHCP ホスト（MAC アドレスに基づく）が CPE1 から CPE2 に移動した。

  このような状況になると、ホストは CPE1 経由で DHCP リリースを実行できない可能性があります。そのため、BWG は CPE1 に関連付けられたこのホストを記憶し続けます。これまでは、BWG でこのホストが CPE1 に関連付けられていると記憶し続けている限り、このホストが CPE2 からアクセスしようとしても拒否されていました。

  このリリースでは、同一のホストが別の CPE2 経由でネットワークに参加しようとしていることが BWG によって検出されると、そのホストと CPE1 の関連付けが削除されます。同一ホストがネットワークに再参加するときは、同じ IP アドレスでも異なる IP アドレスでもかまいません。また、同一ホストは同じ VRF でも異なる VRF でもネットワークに再参加できます。この手法を使用する場合、ホストの MAC アドレスはネットワーク全体で一意でなければなりません。

  この機能の悪影響としては、スプーフされたホスト（有効な MAC と同じ MAC を持つ）が別の CPE から参加すると、有効なホストの通常サービスが中断される可能性があります。

- あるホストが同じ VRF と IP アドレスを持つ別のホストを追い出した

  この場合、ホスト 1 はすでに BWG 内にあり、CPE と関連付けられています。ホスト 2（ホスト 1 と MAC が異なる）は同じまたは異なる CPE から BWG に参加します。ネットワーク（AAA サーバのユーザ レルム→ユーザ グループ→ VRF、および DHCP サーバ）はホスト 2 に同じ VRF と IP アドレスを割り当てます。このような状況は、通常は起こりません。DHCP サーバがホスト 1 で既に使用されている IP アドレスを割り当て直すことはないからです。しかし、DHCP サーバが情報を失った場合（非グレースフル リスタートの場合や、オペレータのミスでリースが意図せず削除された場合）は、このような状況になる可能性があります。

この新しい機能を使用すると、ネットワークの不整合や IP ルーティングの混乱を回避するために、ホスト 1 が削除されます。DHCP 手続きをもう一度実行しない限り、削除されたホストのサービスは復帰できません。

固定割り当て IP の MS/ホストのサポート

イーサネット CS に対する BWG の DHCP メカニズムは、IPCS の場合と似ていますが、Option 82 に追加のサブオプション（L2 ヘッダー）がある点が異なります。BWG は DHCP 手続きを通じてホストの L2 ヘッダー（フレーム タイプなど）と IP アドレスを収集できます。DHCP メカニズムだけでなく、IP アドレスが固定割り当てされた MS/ホストもサポートします。

固定 IP アドレスの処理は、IPCS とイーサネット CS のどちらを使用しているのかによって異なります。

IP CS

認証済み加入者

認証済み加入者に対しては、AAA 応答からの Framed-Route を使用してダウンリンク トラフィックのルーティングが可能です。この機能は BWG ですでにサポートされています。

BWG は、IP CS の場合の静的ホストをアップリンク データ パケット経由で学習します。BWG には L2 ヘッダー情報がないため、これらの静的ホストは MAC ID なしで作成されます。「イーサネット CS」で後述するエージング メカニズムは、IP CS の静的ホストにも当てはまります。

（注）　未認証の加入者はサポートされません。

イーサネット CS

BWG が静的に設定されたホストから L2 ヘッダー情報と IP アドレスを学習するメカニズムは 2 つあります。BWG は、ホスト エントリ（テーブル ID（VRF と IP アドレス）でインデックス化）と L3 ルーティング エントリを作成します。BWG で作成される静的ホストは、加入者あたり 8 つのアクティブ ホストに制限されます。ただし、既存の静的ホストの 1 つでアイドル期間がしきい値を超えると、9 番目のホストが受け入れられます。この場合、アイドルだった時間が最も長い静的ホストが新しいホストによって追い出されます。ホストのアイドルしきい値は、セッション アイドル タイマーの 75% です。固定アイドル ホストが BWG から削除されるのは、新しいホストが BWG で検出された場合のみです。DHCP ホストは期限切れになりません。

学習されたすべての固定 IP は、AAA からの Framed-Route によって検証されます。現在のところ、BWG では CPE あたり 1 つの Framed-Route をサポートします。

（注）　ユーザ グループに対してルート アグリケーション機能はディセーブルにしないでください。ルーティング テーブルで静的ホスト ルートを過剰に作成または削除することが避けられます。過剰に行うと、パフォーマンス低下の原因となります。

ホストからの ARP 要求

BWG は、ホストの IP および L2 ヘッダー情報（フレーム タイプを含む）を学習するために、ARP 要求パケットを常に代行受信できます。静的ホストを作成すると、加入者あたりのアクティブ ホスト数に制限が発生します。BWG がホストを許可できない場合、ARP 要求は応答を受信しません。

BWG は、DHCP メッセージの場合と似た ARP パケットを処理します。ARP 応答パケットは、要求元と同じサービス フローに返されます。BWG の MAC アドレス（ARP 要求を受信したインターフェイス）は、MS に対する ARP 応答メッセージで使用されます。

BWG は、自身に過剰な負担がかからないように ARP レート処理制限機能も実装しています。ARP パケットは、その到着レートが BWG の処理能力を超えると、ドロップされます。現在のところ、BWG のスロットリング メカニズムでは、5 秒ごとにアップストリーム ARP パケット 1 つが可能です。

本来の ARP プロキシになるために、BWG はパススルー ARP 要求パケットを代行受信できる必要があります。これらのパケットには、BWG の IP とは異なる Target Protocol Address（TPA）が設定されます。ARP 応答パケットでは、要求パケット内の TPA が使用されます。

ホストからのアップリンク パケット

アップリンク パケットが Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）パス内のホスト エントリなしで BWG によって受信されると、プロセス パスへ再ルーティングされて処理されます。その結果、新しいホストが作成される可能性があります。ホストを作成できない場合（8 つのアクティブ ホスト制限による）、パケットは自動的にドロップされます。

BWG に実装されたスロットリング メカニズムは、パケットをプロセス パスに再ルーティングして BWG に過剰な負荷がかからないようになっています。現在のところ、BWG のスロットリング メカニズムでは、5 秒ごとに 1 パケットを再ルーティングします。

制限事項

- ネットワークから追い出されたホストは、最初にアップリンク トラフィックを送信しないとダウンリンク トラフィックを受信できません。このような場合、CPE は実際にはその背後に 9 以上のホストを保持しています。
- BWG はアップストリーム gratuitous ARP をドロップし、これらのパケットから学習しません。

その他の機能拡張

Cisco BWG リリース 1.1 以降の機能をサポートするために、R6 プロトコル、MIB、統計情報、SR、CLI に関して BWG が強化されました。

R6 プロトコルの機能拡張

イーサネット CS 要件を満たすように、既存の R6 プロトコルの機能が拡張されました。

R6 Attachment Request

CS 機能

メッセージの Registration コンテキストにおける CS 機能は、BS または BS シミュレータによるイーサネット CS を示すように、適切な値に設定する必要があります。

（注）　このメッセージに含まれる CS 機能では、MS がサポートするビットマップで単一の CS タイプまたは一連の CS タイプを示すことができます。どのような場合でも、MS の機能を表します。CS 機能の定義については、802.16 を参照してください。

R6 Attachment Response

このメッセージは BWG から BS に送信されます。このメッセージに対する変更は、R6 Attachment Request メッセージと同等です。

このメッセージ内の CS 機能ビットマップは、BWG が IPCS とイーサネット CS の両方をサポートしていることを示すようにエンコードされています。

R6 Data Path Registration Request

このメッセージは、通常の R6 データ パス設定で BWG から BS に送信されます。MSINFO TLV には、次のサブ TLV が含まれます。

- Anchor GW/DPF ID = ASN ゲートウェイの IPv4 アドレス
- CPE Settings：（任意）
- SF INF
  - SFID
  - CS Type：フローに IP CS、Eth CS、または VLAN CS を指定します。
  - Packet Classification Rule

    Classifier Rule Priority

    Ethernet Src MAC：（任意）アップリンク SF 用。コントロールのみの場合は、ダウンストリーム用に送信されます。

    Ethernet Src MAC Mask

    Ethernet Dest MAC：（任意）アップリンク SF 専用

    Ethernet Dest MAC Mask

    EtherType IP

    VLAN-ID

    VLAN Priority Range
  - Data Path Info

    Data Path ID：GRE Key または VLAN ID

    Data Path Encap.Type

    DSCP

CS Type は、特定のサービス フローに適用されます。これは、MS の指定された CS 機能（Attachment Request 内）と BWG のサービス フロー CLI 設定の共通部分です。CPE と BWG の両方が IPCS とイーサネット CS の両方をサポートし、BWG で両方が同じ手順で設定されている場合は、IPCS が選択されます。

Ethernet Src MAC と Ethernet Dest MAC アドレスは、対応する BWG CLI 設定で **any** として設定されていない場合は含めてください。新しいタグ値は、Cisco R6 仕様に準拠しています。

イーサネットおよび VLAN 関連の分類子は、IPCS サービス フローでは通知されません。イーサネット CS の場合は、分類子 VLAN-ID および VLAN Priority Range がローカルで設定されている場合は、それらが BS に通知されます。

「Data Path ID」は既存の TLV です。VLAN タグの VLAN Priority 値（VLAN タグで最上位 3 ビット）は、フローに設定された DSCP/ 優先度、またはフローに設定された QoS データ デリバリ サービスから取得されます。

「Data Path Encapsulation Type」TLV は、カプセル化タイプが R6 ベアラ トラフィックを転送するために使用されるかどうかを指定します。

0 = なし

1 = GRE（デフォルト）

2 = IP-in-IP

3 = VLAN

「Data Path Encap Type」のタグ値は、Cisco R6 仕様に準拠する必要があります。イーサネット CS の R6 コントロール専用の場合、この TLV は「none」に設定してください。「Data Path Encap.Type」が「none」に設定されると、BS は Data Path ID を VLAN ID として解釈します。設定がない場合、データ トラフィックを転送するために GRE で R6 データ パスを使用します。

アップリンク SF 用に BS に通知される DSCP 値は、SF 用にローカル設定された BWG から取得されるか、BWG が存在しない場合はフローに設定された QoS データ デリバリ サービスから取得されます。

また AAA を介して BS を利用できる場合は、ISF Path Registration Request によって新しく定義された CPE Settings TLV を BS に通知します。CPE 設定は、MS INFO TLV の下にあります。

R6 Data Path Registration Response

このメッセージは、通常のデータ パス設定時に BS から BWG に送信されます。メッセージに対する変更は、R6 Data Path Registration Request メッセージと同等です。Data Path Registration Request メッセージに定義される新しい TLV はすべて Path Registration Response メッセージで利用できます。

その他の R6 の変更

一貫性を持つために、すべての R6 シグナリング UDP パケット には DSCP 値 0x48 が設定されます。また、リリース 1.0 以上では、UDP チェックサムがすでに計算されています。

BWG は、サービス フローの数を 4、アクティブ ホストの数を加入者あたり 20 に制限します。上限を超えそうになると、BWG は失敗します。

（注）　BWG では、SLA プロファイルあたり 4 つまでサービス フローを使用できます。

EAP 認証

BWG は、EAP リレーとして動作し、EAP 方式は問いません。BWG とベース ステーションの間では、コントロールの交換として EAP 転送が行われます。ベース ステーションは EAP リレーとして動作し、Pair-wise Master Key version 2（PKMv2）から BWG への EAP メッセージへと変換します。BWG は EAP パススルーであり、EAP 方式を生成するすべての鍵がサポートされます。

PKMv2 は、無線によるユーザ認証を実行するために使用されます。PKMv2 は、IEEE 802.16 エアー インターフェイスを使用して EAP を MS とベース ステーションの間で転送します。ベース ステーションは、EAP メッセージを BWG のオーセンティケータにリレーします。オーセンティケータ上の AAA クライアントは、EAP メッセージを AAA プロトコル パケットにカプセル化し、1 つ以上の AAA プロキシ経由でホーム NSP の CSN にある AAA サーバに転送します。ローミングの場合、AAA プロキシを使用する 1 つ以上の AAA ブローカがオーセンティケータと AAA サーバの間に存在する可能性があります。すべてのセッションは常にオーセンティケータと AAA サーバの間に存在し、オプションの AAA ブローカによって NAI レルムベースのルーティング用コンジットを提供します。

認証済みユーザのネットワーク許可

次の一連のイベントでは、ネットワークが認証済みユーザを許可する方法を示します。

1. オーセンティケータ（BWG 内）は、Pre-Attachment-Ack メッセージをベース ステーションから受信すると MS による EAP 認証手順を開始します。
2. オーセンティケータは、Authentication Relay プロトコル（AuthRelay-EAP-Transfer）を使用して EAP Request/Identity メッセージを BS に送信します。
3. BS は、PKMv2 EAP-Transfer/PKM-RSP メッセージで EAP Request/Identity ペイロードを MS にリレーします。
4. MS は、NAI を提供する EAP Response/Identity メッセージで応答します。このメッセージは、PKMv2 EAP-Transfer/PKM-REQ メッセージを使用して BS に転送されます。
5. BS は、Authentication Relay プロトコル（AuthRelay-EAP-Transfer メッセージ）を使用して、PKMv2 EAP-Transfer で受信した EAP ペイロードをオーセンティケータにリレーします。
6. EAP ペイロードは、訪問 AAA サーバ経由で MS のホーム AAA サーバに転送されます（オーセンティケータは、提供された NAI を分析して、ホーム AAA サーバの場所を解決します）。オーセンティケータは、Authentication Relay プロトコル（AuthRelay-EAP-Transfer）を使用して EAP Request/Identity メッセージを BS に送信します。
7. BS から受信した EAP ペイロードを AAA サーバに伝送するために、オーセンティケータは RADIUS Access-Request メッセージを使用し、コロケート AAA クライアントを介して EAP メッセージを転送します（EAP ペイロードが RADIUS の「EAP message」アトリビュートにカプセル化されます）。
8. EAP 認証プロセス（トンネリング EAP 認証方式）は、BWG のオーセンティケータを介して MS と認証サーバとの間で実行されます。
9. RADIUS Access-Challenge メッセージ内で AAA サーバから返された EAP ペイロードは、AuthRelay-EAP-Transfer メッセージでベース ステーションに転送されます。Mobile Subscriber Station に位置する EAP サプリカントと、AAA サーバに位置する EAP Authentication Server との間で、複数の EAP メッセージ交換が行われる可能性があります。
10. オーセンティケータは、Key Change Directive メッセージをベース ステーションに送信して、EAP 認証プロセスが完了したことを通知します。鍵は、AAA から Access Accept で受信した Master Secret Key（MSK）を使用して BWG が計算します。Key Change Directive には、AK Context のサブ TLV で MSINFO TLV が含まれ、EAP 成功を示す EAP Payload TLV も含まれます。
11. 認証が失敗した場合、加入者が Normal Mode Network-Initiated Network Exit の手順を使用してネットワークから登録解除されたことが AAA サーバから受信されます。
12. ベース ステーションは、Key Change Acknowledgement メッセージを使用して Key Change Directive メッセージの受信を確認します。
13. ベース ステーションは、PKMv2 EAP-Transfer メッセージを使用して、認証の結果を Mobile Subscriber Station に送信します。

未認証ユーザのサポート

次のような状況では、未認証ユーザのサポートが必要です。その場合は、プリペイド システムや緊急通話で使用できます。

- ヌル認証を通知するように Mobile Subscriber（MS）を選択できます。これは、緊急通話に限定された MS のように、特定タイプの MS にできます。このようなタイプの MS は、SBC_REQ でヌル認証サポートを通知します。BS は、NetEntry MS State Change Request を介してこの情報を BWG にリレーします。

- BWG はローカル ポリシーに基づいて、認証をスキップするように選択でき、加入者がネットワークに参加することを許可します。
- CLI を使用してヌル認証をイネーブルにするように BWG が設定されている場合、ヌル認証を要求する Subscriber Station（SS）/MSS が NULL-AUTH ユーザ グループにマッピングされます。これらの SS/MSS からの DHCP 要求は、設定済みの DHCP サーバにのみ送信されます。これにより、オペレータは未認証ユーザに対するアドレス割り当てを制御したり、そのようなユーザに対する制約事項を適用したりできます。また、SS/MSS からのトラフィックを特定の宛先のみに制限するようにアクセス コントロール リストを設定できます。

Cisco BWG リリース 1.1 では、EAP 認証をサポートします。BS/CPE が EAP 認証をサポートしない場合、その CPE は未認証として分類されます。BWG では、MAC ID とパスワードに基づいて認証される CPE に対して、非常に基本的な PAP タイプの認証をサポートします。RADIUS サーバは、CPE をプロビジョニングするようにあらかじめ設定してください。

BWG で PAP 認証をイネーブルにする AAA の設定

PPP/PAP 認証をイネーブルにするために BWG を設定するには、グローバル コンフィギュレーション モードで次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config)# aaa authentication ppp default group {WORD | radius}`	PPP を実行しているシリアル インターフェイスで使用する Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）認証方式を指定します。

次に例を示します。

```
router(config)#aaa authentication ppp default group radius
```

設定を検証する show 出力の例を示します。

```
Router#show running-config | include aaa
    aaa new-model
    aaa authentication ppp default group radius
    aaa authorization config-commands
    aaa authorization network default group radius local
    aaa authorization configuration default group radius
    aaa accounting update periodic 1
    aaa accounting network agw start-stop group radius
    aaa session-id common
```

PAP 認証を使用した CPE の AAA アクセス

RADIUS サーバに対する未認証ユーザ グループの PAP Access-Request を BWG で開始するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config-gw-ug)#aaa authentication method-list {WORD | default}`	RADIUS Access Request がユーザ グループの BWG から開始するかどうかを示します。コマンドが設定されていない場合、Access-Request は RADIUS に送信されません。

次に設定の例を示します。

```
router#wimax agw user group-list wimax
```

```
user-group unauthenticated
aaa authentication method-list xxx
sla profile-name gold
timeout idle 100000
!
```

PAP 認証を使用した CPE のプロキシ レルム

未認証ユーザの場合、BWG は CPE からユーザ名を受信しません。この場合、BWG はプロキシ レルムとパスワードを指定するメカニズムを提供します。

ユーザ名、レルム、パスワードを設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config-gw-ug)#proxy realm {WORD} password {WORD}`	BWG は、PAP Access-Request 内のユーザ名とパスワードとして、**proxy realm** と MACID の組み合わせ、およびパスワードを使用します。その後、要求を RADIUS サーバに送信します。

次に設定の例を示します。

```
router#wimax agw user group-list wimax
    user-group unauthenticated
    aaa authentication method-list agw
    proxy realm cisco.com password cisco
    sla profile-name gold
    timeout idle 100000
```

この設定では、BWG は *MACID@cisco.com* に設定されたユーザ名と *cisco* に設定されたパスワードを使用して、RADIUS サーバに Access-Request を送信します。

プロキシ レルムが設定されていない場合、BWG は *MACID* に設定されたユーザ名と *cisco* に設定されたパスワード（デフォルトのパスワード）を使用して、Access-Request を RADIUS サーバに送信します。

PAP 認証を使用した未認証 CPE 自動プロビジョニング

自動プロビジョニングを使用すると柔軟性が得られるほか、BWG で設定した場合は、AAA で CPE に対してプロビジョニングしない場合でも、CPE はネットワークに参加できます。

（注） 自動プロビジョニングは、PAP 認証を使用した CPE に限定されます。

未認証のユーザ グループに対する自動プロビジョニングを設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config-gw-ug)#user auto-provisioning`	未認証のユーザ グループに対して自動プロビジョニングを設定します。イネーブルにするときは、ユーザがネットワークを自由に使用できないように、ユーザ グループのセッション タイマーが小さい値に設定されている必要があります。

次に設定の例を示します。

```
router(config)#wimax agw user group-list wimax
    user-group unauthenticated
    aaa authentication method-list agw
```

```
proxy realm cisco.com password cisco
sla profile-name gold
timeout idle 100000
user auto-provisioning
```

認証の設定

この項では、Cisco BWG で認証および認可を設定する方法について説明します。BWG と加入者の間で認証されたコールをイネーブルにするには、BWG で次のタスクを実行します。

- 「AAA でアカウンティング タイプの設定」
- 「認可の設定」
- 「認証の設定」
- 「RADIUS サーバ」

AAA でアカウンティング タイプの設定

BWG でアカウンティング タイプを設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config)# aaa session-id {common | unique}`	異なるアカウンティング タイプに対して、共通または一意のセッション ID を指定します。
ステップ 2	`router(config)# aaa new-model`	新しいアクセス コントロール コマンドと機能をイネーブルにします（古いコマンドをイネーブルにします）。コマンドで **no** を使用すると、古いコマンドと機能を再開できます。

認可の設定

BWG で認可を設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config)# aaa authorization network default group {server-group-name | radius}`	特定の認可リストに対して AAA サーバから設定をダウンロードする server-group を指定します。コマンドで **no** を使用すると、server-group の使用を取り除くことができます。

認証の設定

BWG で認証を設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config)# aaa authentication dot1x {authentication-list-name | default} group {server-group-name | radius | tacacs+}`	使用する認証方式を指定します。dot1x キーワードは、WiMAX 固有のキーワードで置き換えます。

AAA サーバから設定のダウンロードを指定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	router(config)# **aaa authorization configuration default group** {**WORD** | **radius**| **tacacs+**}	AAA サーバから設定のダウンロードを指定します。

次に設定の例を示します。

```
router(config)#aaa authorization ?
  auth-proxy       For Authentication Proxy Services
  cache            For AAA cache configuration
  commands         For exec (shell) commands.
  config-commands  For configuration mode commands.
  configuration    For downloading configurations from AAA server
  console          For enabling console authorization
  exec             For starting an exec (shell).
  ipmobile         For Mobile IP services.
  multicast        For downloading Multicast configurations from an AAA server
  network          For network services. (PPP, SLIP, ARAP)
  prepaid          For diameter prepaid services.
  reverse-access   For reverse access connections
  template         Enable template authorization

router(config)#aaa authorization conf
router(config)#aaa authorization configu
router(config)#aaa authorization configuration ?
  WORD     Named authorization list (max 31 characters, longer will be rejected).
  default  The default authorization list.

router(config)#aaa authorization configuration de
router(config)#aaa authorization configuration default ?
  group  Use server-group.

router(config)#aaa authorization configuration default gr
router(config)#aaa authorization configuration default group ?
  WORD     Server-group name
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.

router(config)#aaa authorization configuration default group radius
```

RADIUS サーバ

BWG で RADIUS サーバ ホストを設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	router(config)# **radius-server host** {*host-name* | *ip-address*} {**auth-port** | **acct-port**} **key**	RADIUS サーバを設定します。 *ip-address* : RADIUS サーバの IP アドレス **auth-port** : RADIUS 認証サーバの UDP ポート（デフォルトは 1645） **acct-port** : RADIUS アカウンティング サーバの UDP ポート（デフォルトは 1646） **key** : サーバごとの暗号化鍵

ユーザ グループの設定

BWG でユーザ グループを設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config)# wimax agw user group-list` *user-group-list-name*	BWG ルータでユーザ グループ リストを設定します。BWG のプロセッサ 1 つにはユーザ グループ リスト 1 つのみ使用できます。コマンドで **no** を使用すると、ユーザ グループ リストが削除されます。このコマンドをイネーブルにすると、ユーザ グループ リスト サブ コンフィギュレーション モードに入り、作成したユーザ グループ リストの下に複数のユーザ グループを作成します。
ステップ 2	`router(config)# user-group {any | unauthenticated | domain` *domain-name*`}`	ユーザ グループ リストの下に **user-group** を設定します。ユーザ グループ サブ コンフィギュレーション モードに入り、ユーザ グループの各種パラメータを設定します。3 種類のユーザ グループがサポートされています。 • ドメイン ベースのユーザ グループ：ユーザが認証済みの場合、BWG は受信した NAI のドメイン名部分に基づいてユーザを検出します。受信した NAI の形式は *userpart@domain* です。ユーザ グループ *abc@cisco.com* に一致するには、**user-group domain** *cisco.com* を設定し、このユーザ グループの下にドメインごとの設定をすべて置きます。 • any ユーザ グループ：ドメインに基づくユーザ グループに認証済みのユーザが見つからない場合、このカテゴリにユーザを分類することがデフォルトの動作です。たとえば NAI が *abc@cisco2.com* であるユーザを受信し、*cisco2.com* のユーザ グループ ドメインがない場合、このユーザは **any** ユーザ グループ カテゴリに分類されます。 • Un-Authenticated ユーザ グループ：すべての未認証ユーザは、このカテゴリのユーザ グループに分類されます。コマンドで **no** を使用すると、ユーザ グループを削除します。 **（注）** BWG リリース 1.0 以上では、ユーザ グループ **any** および **unauthenticated** が存在するかどうかは任意です。
ステップ 3	`router(config)# aaa {authentication | accounting} method-list {`*method-list-name* `| default}`	ドメインに使用する認証またはアカウンティング方式を設定します。コマンドで **no** を使用すると、ユーザ グループを削除します。

（注） AAA サーバ グループは方式リストの設定とリンクして、さまざまな AAA サーバを設定でき、その結果、さまざまなユーザ グループにマッピングできます。

設定の確認

加入者の認証方式では、コールが EAP で認証されたかそれぞれのユーザ グループ（**any**、**unauthenticated**、**domain** に固有）に対して未認証であったかどうかを表示します。

認証されたユーザの場合は、Auth Policy および AK Context も表示されます。

認証設定を確認するには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	router# **show wimax agw subscriber msid**	加入者の認証情報を表示します。

設定例

未認証のコールに対する加入者情報の出力例を示します。

```
Router#show wimax agw subscriber msid 1000.0003.0000
 Connection time 000:01:05
 Auth policy 0X0(0)
 Subscriber address 2.2.0.9, type IPv4, organization IETF
 Subscriber address method Dynamic, source DHCP relay
 Subscriber address assigned on flow downlink ID 17
 Subscriber address prefix len allocated 32, aggregate 32
 Subscriber address traffic sent 0 packets, 0 bytes
 Subscriber address traffic received 0 packets, 0 bytes
 Subscriber address DHCP XID 2391, server 0.0.0.0, htype 1
 Subscriber address DHCP client ID 1000.0003.0000, length 6
 Subscriber address DHCP Refresh time 86400 seconds
Number of sessions 1
  Session details:
   FSM in state Ready(7) on last event Rx Attach Ack(14)
   Authentication method unauthenticated
Associated user group **unauthenticated**
Signalling address local 2.2.2.2, remote 10.1.1.82
   Signalling UDP port local 2231, remote 2231
   Idle for inbound 00:01:10, outbound 00:01:10
   Ingress Address filtering 0 packets, 0 bytes
   Number of flows 1
    Flow details ISF(0)
     FSM in state SF Ready(4) on last event Up(1)
     Transaction ID used 0X8001(32769)
     Data ID local 0x9(9), remote 0x2(2)
     Data address local 2.2.2.2, remote 10.1.1.82
     Data traffic sent 2 packets, 656 bytes
     Data traffic received 2 packets, 1208 bytes
     Accounting last record sent Interim(3)
     Idle for inbound 00:01:10, outbound 00:01:10
     Service Flow information Downlink:
      Identifier 17
QoS information:
       Data-delivery-service real-time-variable-rate
       Minimum traffic-rate-reserved 4, Maximum latency 1
```

認証済みのコールに対する加入者情報の出力例を示します。

```
Router>sh wimax agw subscriber msid 1000.0002.0001MSID 1000.0002.0001
 Connection time 000:01:08
 Auth policy 0X12(18), Single-EAP, CMAC
  AK Ctx method C-MAC(1), Lifetime 65535
  AK Ctx Seq No. AK 0, PMK 0
  AK Ctx C-MAC key count 1
 Number of TIDs 1
```

```
 TID Key 10.1.1.82/2.2.2.2/1000.0002.0001
  Peer TID 0X4(4)
    FT MS State Change(9), MT Attachment Request(8)
  Our TID 0x8004(32772)
 Subscriber address 2.2.0.8, type IPv4, organization IETF
 Subscriber address method Dynamic, source DHCP relay
 ….
 Subscriber address DHCP Refresh time 86400 seconds
 Number of sessions 1
  Session details:
   FSM in state Ready(7) on last event Rx Attach Ack(14)
   Username eap-md5-u@eap-md5.com
   Authentication method EAP
AAA session-id length 7, 0x30313233414243
   AAA termination-action 1
   Reauthentication attempts from subscriber 0, ASNGW 0
   Associated user group **any**
   Signalling address local 2.2.2.2, remote 10.1.1.82
   Signalling UDP port local 2231, remote 2231
   Idle for inbound 00:01:09, outbound 00:01:09
   Absolute timeout 1500, remaining 00:23:49
   Idle timeout 600 (both), remaining 00:08:50
   Ingress Address filtering 0 packets, 0 bytes
   Number of flows 1
    Flow details ISF(0)
     FSM in state SF Ready(4) on last event Up(1)
     Transaction ID used 0X8004(32772)
     Data ID local 0x8(8), remote 0x1(1)
     Data address local 2.2.2.2, remote 10.1.1.82
     Data traffic sent 2 packets, 705 bytes
     Data traffic received 2 packets, 1208 bytes
     Accounting last record sent Interim(3)
     Idle for inbound 00:01:09, outbound 00:01:09
     Service Flow information Downlink:
      Identifier 15
```

セキュリティ鍵交換

加入者の EAP 認証後、BWG はベース ステーションごとの Access Key（AK; アクセス鍵）を計算します。また、BWG は認証時に PMK をキャッシュし、SS/MSS が別の BS に移動したときに追加の AK を再計算します。

リリース 1.0 以上では、モバイルからトリガーされた Re-Authentication をサポートし、新しい PMK を生成します。

DHCP を使用した IP アドレス割り当て

Cisco BWG リリース 1.0 以上では、外部の Dynamic Host Configuration Protocol（DHCP）サーバ ベースのアドレス割り当てをサポートします。

（注）　アドレスを SS/MSS に割り当てる唯一のメカニズムは、DHCP に基づいています。

SS/MSS は DHCP を使用して IP アドレスを割り当てできます。リリース 1.0 以上では、MIP や PMIP はありません。BWG は固定 IP とポータブル IP のみを対象にしているからです。DHCP リレーは BWG 内にあり、ユーザ グループが異なる VRF 上にある場合は DHCP サーバと相互作用します。

VRF の場合のみ、ユーザ グループとアドレスが重複してもかまいません。

最初のサービス フローの認証と設定に成功したら、MS が DHCP を開始して IP アドレスを取得します。DHCP サーバは、BWG でユーザ ドメイン グループごとに設定されます。DHCP メッセージは、BS と BWG の間で R6 データ パス上を透過的に転送されます。アドレスは、ユーザ ドメイン グループに関連している対応 DHCP サーバによって割り当てられることがあります。異なるユーザ グループにまたがってアドレスが重複してもかまいません。ループ バックを使用することが理想的な方法ですが、「dhcp gateway address」が設定されていない場合は、バーチャル テンプレートの IP が gi-address として使用されます。

最初のサービス フローでは、DHCP パケット以外のデータ トラフィックを許可しません。アドレス割り当てが正常に完了したら、SS/MSS に割り当てられた IP アドレスに対応する適切な分類子がインストールされます。

Subscriber Station の背後にある複数のホストをサポートするため、Subscriber Station からの複数の DHCP 要求がサポートされます。これらの要求は、同じまたは別のサービス フローで受信できます。

IP アドレス割り当ての設定

外部の DHCP サーバを使用して IP アドレスを設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	router# interface Loopback102 ip address 102.0.0.1 255.255.255.0 ! user-group domain eaptls.com2 aaa accounting method-list AAA-ACC1 aaa authentication method-list AAA-AUTHN1 **dhcp gateway address 102.0.0.1** **dhcp server primary 27.0.0.8** sla profile-name silver vrf VRF_2	IP アドレスを割り当てるように外部の DHCP サーバを設定します。 デフォルトの IP アドレス割り当て時間は 300 秒です。 （注）　DHCP サーバのアドレスは、ゲートウェイのローカル インターフェイスのアドレスと一致しないようにしてください。

次に設定の例を示します。

```
interface Loopback102
  ip address 102.0.0.1 255.255.255.0
 !
 user-group domain eaptls.com2
  aaa accounting method-list AAA-ACC1
  aaa authentication method-list AAA-AUTHN1
  dhcp gateway address 102.0.0.1
  dhcp server primary 27.0.0.8
  service-flow pre-defined isf profile sf3
  service-flow pre-defined secondary 1 profile sf4
  vrf VRF_2
```

（注）　DHCP サーバとゲートウェイは、ユーザ グループの下に設定することもできます。ユーザ グループの下に DHCP サーバまたはゲートウェイのアドレスを設定しない場合は、グローバル コンフィギュレーション方式が使用されます。DHCP サーバのアドレスは、ゲートウェイのローカル インターフェイスのアドレスと一致しないようにしてください。

複数ホストのサポート

SS の背後にある複数ホストは、IPCS で DHCP リレー Option 82 または Option 82 加入者 ID を使用した場合にサポートされます。

Option 82 の Subscriber-id サブオプションは MS/SS の MSID に、Circuit-id サブオプションはダウンリンク サービス フロー識別子に設定できます。リモート ID は SS/MSS の認証済みユーザのユーザ名、VPNID はユーザの VRF 名に設定できます（設定済みの場合）。これには、L2 ヘッダーの新しいサブオプション 200 が含まれます。

たとえばマルチホストをサポートするように、DHCP サーバは各 MAC に一意の IP アドレスを割り当てることができます。

加入者 ID にはユーザ名、リモート ID にはユーザの MACID が使用されます。

（注）　リリース 1.0 以上では、リレー カスケーディングはサポートされていません。

（注）　MS の背後で使用できるホストの最大数は 8 です。

SS の背後にある複数ホストのサポート

単一 SS/MSS で複数のホストもサポートします。

ステップ 1　CPE（SS）が最初のネットワーク参加と認証を実行すると、ベアラ パスが作成されます。

ステップ 2　BS と BWG の間には、基本的な R6 ベアラ パスが作成されます。基本的な R6 は、アップリンク / ダウンリンク用の GRE 鍵を共有します。この GRE 鍵は SFID と対応するエアーリンク接続にマッピングされることがあります。

ステップ 3　BWG で同じサービス フロー（R6 ベアラ）上のすべてのホストに対して、すべてのアップリンク パケットとダウンリンク パケットは CPE によって送受信されます。

DHCP Option 82

DHCP Option 82 は、加入者とホストに適用できます。このオプションは、任意のホストまたは加入者の DHCP メッセージで送信されます。

複数のホストは、DHCP Option 82 を使用してサポートできます。リレー エージェント情報オプションは、クライアントから発信された DHCP パケットが DHCP サーバに転送されるときに DHCP リレー エージェントによって挿入されます。リレー エージェント情報オプションを認識するサーバは、この情報を使用して IP アドレスまたはその他のパラメータ割り当てポリシーを実装できます。また、イーサネット CS の場合の L2 ヘッダーも Option 82 で挿入されます。

DHCP Options 82 は、加入者 ID、リモート ID、回線 ID を付加します。そして、すべての DHCP メッセージでサーバに送信されます。VRF の場合は、VPN ID も送信されます。DHCP サーバが Option 82 に対応しておらず、Option 82 をエコー バックしない場合、BWG はメッセージを DHCP サーバからドロップします。

次の操作が可能なため、有用な機能です。

- 各加入者を特定する
- 加入者管理を実行する
- 加入者情報に基づいて IP アドレスを割り当てる
- アクセス コントロール、QoS、およびセキュリティ ポリシーを設定する

DHCP Option 82 機能で発生するイベントのシーケンスは次のとおりです。

ステップ 1　ホストは、クライアントの識別情報フィールドに DHCP メッセージ内の MAC アドレスを設定します。

ステップ 2　CPE の IP アドレスを取得するために、DHCP メッセージのやりとりが ISF でのみ行われます。ホストの IP アドレスを取得する場合は、任意のフローで行えます。BWG からの DHCP パケットは、ホストからの着信 DHCP メッセージと同じフローで送出できます。

ステップ 3　BWG は、DHCP サーバが使用する Option 82 フィールドを挿入します。Option 82 は、DHCP サーバに対するすべての DHCP メッセージに挿入される必要があります。挿入するオプションのリストについては、表 2-3 を参照してください。

ステップ 4　DHCP サーバは、着信 DHCP パケットの Option 82 フィールドの任意のオプションを使用して、IP アドレスを割り当てることができます。IP アドレスが割り当てられると、BWG では応答をモニタして割り当てられた IP アドレスを学習し、R6 ベアラにマッピングします。このプロセスはホストごとに繰り返され、アドレスが追跡されて同じ R6 ベアラにマッピングされます。

ステップ 5　BWG はすべての DHCP メッセージをモニタし、Option 82 フィールドが挿入されていることを確認します。

表 2-3 に、DHCP サーバのオプションを示します。

表 2-3　DHCP サーバのオプション

サブオプション	コード	長さ	サブ値
回線 ID	1	可変	ダウンリンク サービス フロー ID
加入者 ID	6	可変	MSID（SS/MSS の MAC アドレス）
リモート ID	2	6	SS/MSS のユーザ名（認証済みのユーザの場合）
ベンダー固有のリレー情報（イーサネット ヘッダー）	200		イーサネット CS L2 ヘッダー
VPN-ID	151	可変	VRF 名（ユーザが VRF に属している場合）

リリース 1.1 における DHCP Option 82 の機能拡張

BWG がダウンリンク DHCP パケットの L2 ヘッダーを構成できるように、L2 ヘッダー全体が Option 82 内にコーディングされます。Option 82 は、DHCP サーバから反映されます。このサブオプションは、BWG と DHCP サーバとの間のみに適用されます。

加入者単位の DHCP ホスト オーバーフロー メカニズム

この機能が実装されるまで、加入者単位で DHCP ホストの数は厳格にコントロールされていました。最大数に達すると、加入者宛の後続ホストはすべて拒否されていました。このような厳格なコントロールは、負荷の高いホットスポットには適切ではありません。この問題は、DHCP リース時間が長く、CPE を離れたホストが DHCP リリースを実行しなかった場合には、さらに深刻になります。

Least Recently Used（LRU; 最低使用頻度）に基づく新しいホスト オーバーフロー メカニズムは、ホストの数が CPE の上限（20）を超えることがある問題に対処するために使用されます。新しいホストが加入者に参加するとき、その最大数に達している場合は、LRU ホストが選択されます（トラッシングを避けるため、最小のアイドル時間が適用されます）。このホストはアクティブ リストから削除されてオーバーフロー リストに移り、新しい加入者のために空きを用意します。オーバーフロー リストのホストからアップリンク データまたは DHCP メッセージを受信すると、そのホストはアクティブ リストに昇格します。

CLI を使用して、この機能をイネーブルにし、ホスト オーバーフロー リストのサイズを設定できます。デフォルトのサイズは 50 です。新しく追加されるホストは、常にリストの末尾に追加されます。オーバーフロー リストがいっぱいになると、最も古いオーバーフロー ホスト（リストの先頭）が削除され、新しい加入者を受け入れます。

アクティブ リストの LRU ホストがオーバーフローに押し出されると、そのホストのアカウンティングが停止します（アカウンティングがイネーブルの場合）。ダウンリンク ホスト ルートも削除され、オーバーフロー ホストはダウンリンク データを受信できないようになります。また、オーバーフロー ホストに対しては DHCP タイマーが実行されません。

メモリを節約するために、オーバーフロー ホストは、後でアクティブ リストに復帰するために必ず必要な情報のみを保存します。アクティブ ホストは約 300 バイトのメモリを確保するのに対して、オーバーフロー ホストが使用するメモリは 40 バイトにもなりません。

オーバーフロー ホストに対するアップリンク データまたは DHCP Renew メッセージを受信すると、BWG はオーバーフロー ホストをアクティブ ホストに復帰させようとします。しかしこの処理の結果は、2 つの要因に依存します。

- アクティブ リストの容量に達した場合、または
- アクティブ リストがいっぱいの場合、BWG は別の認定済み LRU ホストをアクティブ リストから見つけ出せるか。認定済みホストは LRU ホストは、最小アイドル要件を満たさなければなりません。

復帰に成功すると、ホストはオーバーフロー リストから削除されて、アクティブ リストに追加されます。まるでずっとアクティブであったかのように、そのホストの残りライフタイムに対して DHCP リース タイマーが再開します。さらに、ホスト ルートが復元され、このプロセスにおけるホストのアカウンティングが再開します。アクティブ リストへの復帰に失敗すると、ホストはキャッシュ リストに残ります。

つまり、ホストがオーバーフロー リストから削除されるのは、次の 2 つの状況下です。

- アクティブ リストへの復帰に成功した場合。
- 最古（リストの先頭）になり、かつリストがいっぱいのときに、別の加入者によって削除された場合。この場合、DHCP リリースが DHCP サーバに送信されます。キャッシュ リストから削除されたホストは、DHCP 手続きがホストでもう一度開始されるまでデータを送受信できなくなります。

冗長設定の場合は、オーバーフロー ホストのリスト自体はアクティブ BWG からスタンバイ BWG に同期されません。ただし、アクティブ ホストの追加や削除に関する情報は、動的に同期されます。この情報はスタンバイ側でオーバーフロー ホスト リストを再構築するために使用できることを想定しています。バルク同期を行うと、スタンバイ側のホスト オーバーフロー リストは再構築できなくなります。アクティブ ホストがリスト内のその位置を占めるに至った履歴が失われるためです。

BWG のホスト オーバーフロー機能は、DHCP クライアントにも DHCP サーバにも認識されません。これは新しい機能であり、CPE がアクティブ リストを超える数のホストにサービスを提供できます。

利用可能なメモリを効率的に使用できるようにするため、この機能はユーザ グループ単位で提供されます。ホットスポットのような CPE のユーザ グループでは、明示的にこの機能をイネーブルにする必要があります。デフォルトでは、この機能はイネーブルではありません。

加入者単位の DHCP ホスト オーバーフロー メカニズムを設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(usr-grp)#`**`host-overflow`** [**`size`** *`1-100`*] [**`min-idle`** *`1- 60`*]	DHCP ホスト キャッシング機能をイネーブルにし、キャッシュ リストのサイズ（デフォルトは 50）とアイドル タイマー（デフォルトは 5）を設定します。**min-idle**：加入者をアクティブ リストからオーバーフロー リストに移動する基準を確立します。**min-idle** により、BWG がホストをアクティブ ホスト リストからオーバーフロー リストに頻繁に移動することを防止します。**min-idle** 値は分数で指定します。

- データ パケットを受信した場合は MAC アドレスがないため、レコード配列は IP のみに基づいて突き合わせが行われます。動的ホストとスプーフした固定ホストを区別できません。推定される影響としては、スプーフしたホストがだましている間も、本物の DHCP ホストとスプーフしたホストの両方が、リースを更新している DHCP ホストとのトラフィックを送信し続けます。ただし、既存の動作に変更はなく、この問題は現在でも残っています。本物の IP ホストが CPE に接続されている場合、スプーフされた CPE もその CPE と同じアドレスを使用して開始できます。
- 固定 IP を使用できる場合、CPE から削除された DHCP ホストのレコードも配列から削除されます（別のレコードによって上書きされます）。DHCP ホストが復帰すると、代理受信した最初のデータ パケットによって固定ホストが開きます（固定 IP が許可されているため）。ホストが DHCP 更新を送信しない場合、そのホストは固定として扱われ、リストから追い出されるまで削除されません。ただし、これはユーザが選択した場合のことであり、既存の動作はまったく同じです。
- ホストのアカウンティングがイネーブルの場合、ホストに対するアカウンティングの開始/終了がオーバーヘッドになる可能性があります。
- ネットワークでホット スポット CPE の使用状況が高い場合、セッションあたりのメモリ要件が高くなります。

オーバーフロー ホストを表示するには、次のタスクを実行します。

ステップ 1	`router#` **`show wimax agw subscriber internal`** `router#` **`show wimax agw subscriber msid`** *`msid`* **`overflowed-host`**	オーバーフロー ホストを表示します。

サービス フローの作成と管理

802.16 では、任意の SS に対して複数のサービス フローをサポートします。サービス フローは、一連の分類規則をパケット ベアラに対してマッピングすることで識別されます。サービス フローはそれぞれ一方向のフローであり、エアーリンクとネットワークの両方で、QoS（Quality of Service）の扱いを個別に変えることができます。

Cisco BWG リリース 1.0 以上では、サービス フローの作成は、ネットワークによって開始した場合のみサポートされています。サービス フローを作成すると、SS/MSS 上の分類子もプロビジョニングされます。

また、事前にプロビジョニングされたサービス フロー テンプレートは、BWG のローカルに設定されます。AAA でのサービス フロー プロファイル ID のダウンロードは、BWG ではサポートしていません。

サービス フロー

BWG では、SS/MSS ごとにサービス フローを管理します。リリース 1.0 以上では、ネットワークでトリガーされたサービス フローのみをサポートします。BWG は各サービス フローの SFID を割り当て、サービス フローの作成をトリガーします。サービス フローにはそれぞれのデータ パスもあります（たとえば GRE 鍵、および各サービス フローに対応するパケットは、それに従って転送されます）。

事前にプロビジョニングされたすべてのフローは、SS/MSS セッションのライフタイム中は利用可能であることが想定されていて、削除されません。

サービス フローの複数作成

コントロール プレーンが開始すると、BWG はベース ステーションによる最初のサービス フローの作成を要求します。DHCP IP アドレスの割り当てとフローの作成は、BWG リリース 1.1 では並行して行われます。

ISF で発生した DHCP 割り当てと並行して、フローが次々に作成されます。サービス フロー作成が成功した後でのみ、その次のサービス フローの作成が開始します。サービス フローの作成に失敗したときに、その前に次のサービス フローの登録要求をリトライしていると、そのサービス フローの作成も失敗します。サービス フローの作成に失敗した場合、それがセカンダリ サービス フローの場合はそのサービス フローがバイパスされ、最初のサービス フローの場合はセッションが破棄されます。

リリース 1.0 以上の場合、BWG では最初のサービス フローと 3 つのセカンダリ サービス フローの合計 4 つのサービス フローを作成できます。

セカンダリ サービス フローの作成に失敗すると、次のフローが試され、失敗したサービス フローなしでセッションが続行します。

BWG サービスの設定

BWG サービスをイネーブルにするには、グローバル コンフィギュレーション モードを開始して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)# service wimax agw`	WiMAX BWG サービスをイネーブルにします。
ステップ 2	`router(config-if)# encapsulation agw`	カプセル化タイプ「ASNGW」でバーチャル アクセス インターフェイスのクローンを作成します。このコマンドは、バーチャル テンプレート コンフィギュレーション モードで設定します。

設定例

仮想アドレスのクローンを作成する例を示します。

```
!
interface Virtual-Template1
ipaddress 2.2.2.2 255.255.0.0
encapsulation agw
ip mtu 1440
no keepalive !
```

Gi アドレスは、デフォルトで仮想アドレスから使用されます。Gi アドレスを上書きするように **user-group** 設定を使用できます。

設定の確認

BWG サービスがイネーブルであることを確認するには、および MS State Change および Data Path 統計情報を表示するには、特権 EXEC モードで **show wimax agw statistics** コマンドを使用します。

```
Message type Deregistration Request(4/0x4)
   Number of messages sent 1
   Number of messages received 11
   Number of messages resent 0
  Message type Deregistration Response(5/0x5)
   Number of messages sent 6
   Number of messages received 1
   Number of messages resent 10
  Message type Deregistration Ack(6/0x6)
   Number of messages sent 1
   Number of messages received 5
   Number of messages resent 0
  Message type Registration Request(12/0xC)
   Number of messages sent 6
   Number of messages received 0
   Number of messages resent 0
  Message type Registration Response(13/0xD)
   Number of messages sent 0
   Number of messages received 6
   Number of messages resent 0
  Message type Registration Ack(14/0xE)
   Number of messages sent 6
   Number of messages received 0
   Number of messages resent 0

Message function type Context Delivery(4/0x4)
  Message type Context Delivery Request(1/0x1)
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Context Delivery Report(2/0x2)
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0

Message function type Auth Relay(8/0x8)
  Message type EAP Start(1/0x1)
   Number of messages sent 0
   Number of messages received 2
   Number of messages resent 0
  Message type EAP Transfer(2/0x2)
   Number of messages sent 56
   Number of messages received 56
```

```
    Number of messages resent 0
  Message type Key Change Directive(5/0x5)
    Number of messages sent 8
    Number of messages received 0
    Number of messages resent 0
  Message type Key Change Confirm(6/0x6)
    Number of messages sent 0
    Number of messages received 2
    Number of messages resent 0
Message type Key Change ACK(7/0x7)
    Number of messages sent 2
    Number of messages received 8
    Number of messages resent 0
  Message type CMAC Key Count Update(8/0x8)
    Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0
  Message type CMAC Key Count Update Ack(9/0x9)
    Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0

Message function type MS State Change(9/0x9)
  Message type Attachment Response(7/0x7)
    Number of messages sent 6
    Number of messages received 0
    Number of messages resent 0
  Message type Attachment Request(8/0x8)
    Number of messages sent 0
    Number of messages received 6
    Number of messages resent 0
  Message type Attachment ACK(9/0x9)
    Number of messages sent 0
    Number of messages received 6
    Number of messages resent 0
  Message type Pre Attachment Request(15/0xF)
    Number of messages sent 0
    Number of messages received 6
    Number of messages resent 0
  Message type Pre Attachment Response(16/0x10)
    Number of messages sent 6
    Number of messages received 0
    Number of messages resent 0
  Message type Pre Attachment ACK(17/0x11)
    Number of messages sent 0
    Number of messages received 6
    Number of messages resent 0

Message function type Keepalive(20/0x14)
  Message type Keepalive Request(1/0x1)
    Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0
  Message type Keepalive Response(2/0x2)
    Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0

Handoff Statistics
  Message type Successful Handoff
    Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0
  Message type Handoff Registration Request
```

```
    Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0
  Message type Handoff Registration Response
    Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0
  Message type Handoff Registration Ack
    Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0
Message type Handoff Deregistration Request
  Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0
  Message type Handoff Deregistration Response
    Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0
  Message type Handoff Deregistration Ack
    Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0

Undefined Message Function / Message Type
    Number of messages sent 0
    Number of messages received 0
    Number of messages resent 0
```

サービス フローから DiffServ クラスへのマッピング

BWG は、個別のサービス フローを Diffserv クラスにマッピングします。マッピング規則は、ルータで設定されます。マッピング規則を表 2-4 に示します。

表 2-4　各サービス フローから Diffserv クラスへのマッピング

サービス フロー：QoS クラス	適用	ネットワークの Diffserv クラス
Unsolicited Grant Service（UGS）	音声 / ビデオ	EF
Real Time Polling Service	音声 / ビデオ	EF
Non-Real Time Polling Service	インタラクティブ サービス	AF
Best Effort	Web トラフィック	BE

サービス フローに相当するパケットのマーキング

各パケットは、関連するサービス フローに従って特定され、グループ化されます。そのパケットに対応するトランスポート ヘッダーは、BWG によって、前掲の表に基づき関連する Diffserv Code Point（DSCP; Diffserv コード ポイント）でマークされます。

BWG でサービス フローの設定

サービス フローを作成するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config)# wimax agw service-flow profile service-flow-profile-name`	BWG 上のサービスフロー プロファイルを指定します。コマンドで **no** を使用すると、プロファイルを削除します。*service-flow-profile-name* は大文字と小文字を区別しません。このコマンドを設定すると、サービス フロー コンフィギュレーション モードが開始します。
ステップ 2	`router(config-gw-sf)# direction {uplink | downlink}`	設定を行うサービスフローの方向を指定し、サービス フロー コンフィギュレーション サブモードを開始します。コマンドで **no** を使用すると、指定した方向から対応する設定を削除します。デフォルト値は **best** effort です。
ステップ 3	`router(config-gw-sf)# cs-type {ethernet-cs | ip-cs}`	対応する方向における CS タイプ プロファイルを指定します。コマンドで **no** を使用すると、対応する方向から CS タイプ情報を削除します。コマンドを設定すると、各種の CS タイプ コマンドを設定するサブ コンフィギュレーション モードが開きます。
ステップ 4	`router(config-gw-sf-dir-cstype)# precedence 1-2`	設定する方向における CS タイプの **precedence**（優先度）を指定します。優先度は、MS が複数の CS タイプをサポートできるときに、差を付けるために使用されます。コマンドで **no** を使用すると、対応する CS タイプから優先度情報を削除します。
ステップ 5	`router(config-gw-sf-dir-cstype# vlan {2-4095 | range 2-4095 2-4095} vrf vrf-name`	VLAN から VRF へのマッピングを指定します（特定 VLAN-ID フレームがその VRF 名にマッピングされます）。VRF 名にマッピングされる VLAN-ID の範囲を指定するプロビジョニングもあります。 **（注）** この VLAN-VRF マッピングは、アップリンク方向のみのイーサネット CS に対して設定できます。
ステップ 6	`vrf default vrf-name`	オプションのコンフィギュレーション コマンドです。デフォルトの VRF マッピングを指定します。アップリンク フレームが VLAN-ID を持たない場合、または VLAN-VRF マッピングが設定されたこの CS タイプでは設定されていない VLAN-ID を持つ場合、このコマンドを使用して設定された VRF 名にアップリンク フレームがマッピングされます。 **（注）** **vrf-default** は、アップリンク方向のみのイーサネット CS および IP CS に対して設定できます。
ステップ 7	`router(config-gw-sf-dir)# qos-info qos-profile-name`	対応する方向において関連付けられている QoS 情報プロファイルを指定します。コマンドで **no** を使用すると、対応する方向から QoS 情報を削除します。

	コマンド	目的
ステップ 8	router(config-gw-sf-dir)# **set {dscp | precedence}** {*precedence-value* | *dscp-value*}	ダウンストリーム方向で加入者パケットに適用する必要のある DSCP または TOS マーキングを指定します。デフォルトでは、マーキングは行われません。
ステップ 9	router(config-gw-sf-dir-cstype)# **pak-classify-rule**	対応する方向において関連付けられているパケット分類規則プロファイルを指定します。コマンドで **no** を使用すると、対応する方向からパケット分類規則を削除します。

設定例

次に、サービス フロー コンフィギュレーション コマンドの例を示します。

```
wimax agw service-flow profile isf
 direction downlink
  cs-type ip-cs
   pak-classify-rule isf-classifier-downlink
   precedence 1
  cs-type ethernet-cs
   pak-classify-rule isf-classifier-downlink
   precedence 2
  qos-info isf-qos-downlink
 !
 direction uplink
  cs-type ip-cs
   pak-classify-rule isf-classifier-uplink
   precedence 1
  cs-type ethernet-cs
   pak-classify-rule isf-classifier-uplink
   precedence 2
   vlan 2 vrf vrf_1
   vlan range 3 10 vrf vrf_2
   vrf-default vrf_1
  qos-info isf-qos-uplink

wimax agw service-flow profile 2sf
 direction downlink
  cs-type ip-cs
   pak-classify-rule dn-secondary-01
   qos-info downlink-qos-02
   set dscp ef
   set precedence immediate
  !
 direction uplink
  cs-type ip-cs
   pak-classify-rule up-secondary-01
   qos-info uplink-qos-02
  !
!
```

サービス フロー パケット分類の設定

BWG でサービスフロー パケット分類規則プロファイルを設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	router(config)# **wimax agw service-flow pak-classify-rule profile** *profile-name*	BWG 上のサービスフロー パケット分類規則プロファイルを指定します。これらは、加入者に対して開かれている事前定義のサービス フローにおいて設定します。 設定すると、このコマンドはパケット分類規則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-gw-pak-classify-rule-pr)# **priority** *0-255* **IPv4 classifiers===>** ip **permit {***0-255* **| gre | tcp | icmp | udp | ip}** **{***src-address src-mask* **| any | host** *src-address***}** **[range** *src-port-low* **[***src-port-high***]** {*dst-address dst-mask* **| any | host** *dst-address***} [range** *dst-port-low* **[***dst-port-high***] [tos** *tos-low tos-mask tos-high***]** **Ethernet related classifiers ===>** **ethernet permit** {*src_mac src_mac_mask* | **any**} {*dst_mac dst_mac_mask* | **any**} {*0-FFFF* | **any** | **arp** | **ipv4**}] **VLAN related classifiers ===>** **vlan permit** {*2-4095* | **any** } **priority** {*0-7* | **any** | **range** *#start #end*}	プロファイルでパケット分類規則を設定します。各パケット分類規則には、一意の優先度が関連付けられていなければなりません。 現在のところ BWG では IPv4、イーサネット、および VLAN に関連した規則をサポートします。

設定例

サービス フロー パケット分類コンフィギュレーション コマンドの設定例を示します。

```
wimax agw service-flow pak-classify-rule profile sec1-classifier-uplink
 priority 0
  ipv4 permit ip any any
  ethernet permit any any any
  vlan any priority any
 !
 priority 1
  vlan 300 priority 4 7
 !
 priority 2
  ethernet permit 0032.00AE.0023 ffff.ffff.ffff any arp
 !
 priority 3
  ipv4 permit ip 2.2.2.2 /24 192.168.102.0 /24 tos 0 255 100
 !
 priority 4
  ethernet permit any 0032.00AE.0023 ffff.ffff.ffff 8100
  vlan permit 900 priority 4
 !
 priority 5
  ipv4 permit ip 2.2.2.2 /24 192.168.102.0 /24 tos 0 255 100
  ethernet permit 001C.B046.041B ffff.ffff.0000 0032.00AE.0023 ffff.0000.0000 ipv4
  vlan permit 300 priority range 4 7
```

（注）　パケット分類子は、指定されたユーザおよび各パケットのフロー方向に対して合計して表示されます。最高のマッチング優先度規則が適用されます（255 が最高の優先度です）。分類子が一致しない場合、選択されたデフォルトの フローがダウンリンク方向の ISF になります。

クリティカル サービス フロー

1 つ以上のセカンダリ フローの作成に失敗し、加入者が必要としているよりもフローの数が少ないまま加入者セッションが存続する場合があります。このような状況では、セッションを登録解除し、加入者が必要とするすべてのクリティカル フローでセッションを再作成できるようにしてください。たとえば、加入者にすべてのフロー（音声、ビデオ、およびデータ）を使用させたり、まったく使用させないようにしたい場合があります。この機能では、Service Flow（SF; サービス フロー）を加入者にとってクリティカルであるとマークできます。BWG は、「クリティカル」であるとマークされている各 SF が作成された場合に限り、加入者セッションを正常に作成します。

BWG では、SLA プロファイル設定において SF を追加するときに、その SF をクリティカルとマークできます。SF がクリティカルとマークされている場合、そのクリティカル SF の作成に失敗すると、セッションを開けません。重要なのは、セッションを開くには各クリティカル フローを正常に作成する必要があるということです。SF がクリティカルとマークされていない場合、または ISF である場合は、既存の動作に変更はありません。

コントロールされたハンドオーバー時にターゲット BS がクリティカル フローを含めることに失敗している場合、BWG はハンドオーバーに失敗します。ポイントは、「すべてのフローかそれともなしか」という考え方が加入者に常に適用されるようになることです。

デフォルトでは、SLA プロファイルで「クリティカル」であると指定されていない限り、SF はクリティカルではありません。

BWG でサービス フローをクリティカルとマークするように設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	Router(config)#**wimax agw sla profile** *bronze* Router(config-gw-sla)#**service-flow pre-defined secondary** 2 **profile** sec2 critical	BWG が SLA プロファイルでサービス フローを「クリティカル」であるとマークできるようにします。

SR 設定では、アクティブ BWG とスタンバイ BWG で同一の SF クリティカル設定にしている必要があります。

show wimax agw subscriber によるフローの詳細情報では、フローがクリティカルであるかどうかが示されます。

次に例を示します。

```
Router#sh wim agw subs msid <>

MSID 1000.22BA.0001
 CPE is nomadic
 Static IP addresses not permitted
 Subscriber Age 000:00:23
 Base Station ID 0x0A01194B00
....
…
    Flow details Secondary(2)(Critical)
     SF Profile name sec2
     FSM in state SF Ready(4) on last event Up(1)
     Transaction ID used 0X8003(32771)
     Data ID local 0x3(3), remote 0xD(13)
     Data address local 11.1.25.2, remote 10.1.25.75
```

```
Data traffic sent 0 packets, 0 bytes
Data traffic received 0 packets, 0 bytes
Accounting disabled
Idle for inbound 00:00:31, outbound 00:00:31
Service Flow information Downlink:
 Identifier 5
 Set DSCP (DDS) 30
 QoS information:
  Data-delivery-service real-time-variable-rate
  Minimum traffic-rate-reserved 0, Maximum latency 0
  Unsolicited interval-polling 0, Traffic-priority 0
  Maximum traffic-rate-sustained 0, Request/Transmission-policy 0
  Maximum traffic-burst-rate 0
  Reduced-resources-code 0
  Media-flow-type 05abcd
 Classifier information:
  priority 2
   ethernet permit any 1000.2223.0003 FFFF.FFFF.FFFF any
 CS Type information:
  イーサネット CS
```

BWG から Attachment Response の遅延

Navini 製独自モデムの一部タイプでは、最初の電源オフ時に同期してネットワークに接続します。このプロセスにおいて、Surfer モデムのネットワーク ID が 0xFFFF（出荷時デフォルト）の場合、REG-RSP メッセージ時に新しいネットワーク ID をモデムのフラッシュに書き込みます。この ID は、書き込み後に変更できず、モデムが参加できるネットワークは、BS が同じネットワーク ID に属しているネットワークのみです。

Profile C では、未認証モデム（Surfer など）を使用する場合は AAA 認証（Accept）に時間がかかることがあり、BWG は AAA から Radius Accept を受信する前に MS Attachment Response を BS に送信できます。このとき、BS は成功 REG-RSP を Surfer モデムに送信し、その後そのモデムは AAA 認証に失敗する可能性があります。現在の実装では、認証に失敗したことを BWG 経由で AAA から学習したときに、BS がモデムをリセットします。モデムをリセットするのは、モデムがほかの BS にアクセスできるようにするためです。

この問題が与える影響は、次のとおりです。

- 新しい独自モデムは、モデムを販売したネットワーク オペレータに属していない BS にロックされます。この場合、モデムは使用不可能であり、オペレータに返送してプログラミングしなおしてもらう必要があります。
- 同じオペレータにアクティブ ネットワークとテスト ネットワークがあり、2 つの異なるネットワーク ID を使用している場合、新しいモデムは、初めて電源が入った場所によっては誤ったネットワークにロックされることがあります。その後、そのモデムはそのネットワークのみで動作します。ロックされた最初の BS は、意図したネットワークではない可能性があります。

この問題を解決するため、BWG は新しい CLI に基づいて Attachment Response の伝送を遅らせるように設計されています。このコマンドを使用すると、Attachment Response のタイムアウト値を設定できます。デフォルト値は 4 秒です。

ユーザグループにおいてタイムアウト値を設定すると、BWG はタイマーを設定し、適切な処理を実行します。次に、さまざまな状況について説明します。

1. このタイムアウトの前に AAA の応答を受信した場合、および
   - CPE が認証済み（受け入れ済み）であり、サービス ステートの値が CPE がアクティブであることを示している場合、BWG は MS Attachment Response の処理を直ちに続行します。
   - CPE が認証済みであり、サービス ステートの値が CPE がブラック リストに載っていることを示している場合、BWG は Deregistration Reason TLV で Path Deregistration Message を送信します。

2. このタイムアウトの前に AAA の応答を受信しない場合
   - BWG は MS Attachment Response を送信して、（要求に TLV エラーがあるにもかかわらず）成功したことを通知します。
   - AAA の応答を受信して Service Type アトリビュートが CPE がブラック リストに載っていることを示している場合、BWG は Deregistration Reason TLV で適切な Reason Code とともに Deregistration を送信します。
   - AAA の応答を受信して Service Type アトリビュートが CPE がアクティブである（ブラックリストに載っていない）ことを示している場合、BWG は BS に対する Path Registration Request を続行します（現在の実装と同様）。

両方の場合とも、BWG は「Access-Reject」を受信すると、ユーザが自動プロビジョニングされた場合はセッションを開いたままにします。ユーザが自動プロビジョニングされていない場合、セッションは登録解除されます。

デフォルトでこの BWG は Attachment Response を遅延するように設計されています。BWG では、PAP 認証済みユーザに対してのみこの機能をサポートします。

Attachment Response の遅延を設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config)# user-group unauthenticated` `timeout authentication` *[1-20]*	Attachment Response の遅延時間を設定します。デフォルト値は 4 秒です。このコマンドは、「unauthenticated」ユーザ グループでのみ設定可能です。

QoS サポート

QoS のサポートは、エアーリンク QoS とネットワーク上のマッピングの両方を意味します。BWG は、適切なサービス フローを作成するために使用する BS に対して、QoS パラメータを送信する責任があります。

ホストによっては、追加の QoS パラメータが与えられていることがあります。

ホストの IP アドレスに対応する新しい R6 ベアラ（サービス フロー）が作成されます。複数のホストがこのサービス フローを使用できます。

ホストから新しい R6 サービス フローへのマッピングが作成され、RR-Request を介して BS/MS に通知されます。

BWG リリース 1.0 以上では、次のサポートがあります。

- CLI を使用した事前プロビジョニング済み QoS のサポート
- 個別クラスとしてマークされたシグナリング トラフィックのサポート
- Diffserv クラスは、分類子に基づく各サービス フローに対応するように、BS および BWG によってマッピングされ使用されます。
- すべての QoS サービス クラスのサポート

QoS の設定

BWG で QoS の設定を行うには、次のタスクを実行します。

	コマンド	目的
ステップ 1	router(config)# **wimax agw service-flow profile qos-info** *service-flow-qos-info-profile-name*	BWG でユーザがサービス フローの QoS 情報のプロファイルを設定できるようにします。これらのプロファイルは、加入者に公開されている定義済みのサービス フローに関連付けられます。サブ コンフィギュレーション モードをオープンするコマンドを設定し、各種パラメータを設定します。
ステップ 2	router(config-gw-sf-qos-info)# **data-delivery-service {unsolicited-grant|real-time-variable-rate|non-real-time-variable-rate|best-effort| extended-real-time-variable-rate}**	特定の QoS 関連のサービス フロー パラメータの定義済みのセットに関連付けられたデータ配信サービスを設定します。デフォルト値は unsolicited-grant です。
ステップ 3	router(config-gw-sf-qos-info)# **maximum-latency** *maximum-latency-value*	ネットワーク インターフェイス上の BS または MS によってパケットが受信されてからピア デバイスの RF インターフェイスにパケットが配信されるまでの時間の範囲を設定します。定義されている場合、このパラメータは BS または MS でのサービスのコミット（またはアドミッション基準）を表し、BS または MS で保証されます。BS または MS は、最小予約レートを超えるサービス フローに対してこのサービスをコミットする必要はありません。デフォルト値は 0 です。
ステップ 4	router(config-gw-sf-qos-info)# **maximum-traffic-burst** *maximum-traffic-burst-value*	サービスに対応する最大バースト サイズを定義するパラメータを設定します。入力および出力ポート、エアー インターフェイス、およびバックホールの物理的な速度は、サービスの最大継続トラフィック レートのパラメータを上回るため、このパラメータはサービスが現在使用可能なリソースを使用していない場合にシステムがサービスに対応する最大継続バーストを表します。デフォルト値は 0 です。
ステップ 5	router(config-gw-sf-qos-info)# **maximum-traffic-rate-sustained** *maximum-traffic-rate-sustained-value*	サービスの最大情報レートを定義するパラメータを設定します。
ステップ 6	router(config-gw-sf-qos-info)# **media-flow-type** *media-flow-type-hex-string*	アドミッションの決定のヒントとして使用されるアプリケーション タイプを指定します。たとえば、VoIP、ビデオ、PTT、ゲームなどです。
ステップ 7	router(config-gw-sf-qos-info)# **policy-transmission-request** *policy-transmission-request-value*	関連するサービス フローのポリシー送信要求の値を指定します。この値には、PDU の形成およびアップリンク サービス フローのオプション、および使用される可能性のある帯域幅要求オプションのタイプの制約が含まれています。対応するビット位置を 1 に設定すると、アトリビュートがイネーブルになります。
ステップ 8	router(config-gw-sf-qos-info)# **minimum-traffic-rate-reserved** *minimum-traffic-rate-reserved-value*	平均超過時間に達した場合にサービス フローの代わりに転送される最小データ サイズをビット/秒で指定します。指定したレートが採用されるのは、スケジューリングに十分なデータが使用できる場合だけです。十分なデータがない場合、使用可能なデータがすぐに送信されます。

	コマンド	目的
ステップ 9	router(config-gw-sf-qos-info)# **sdu-size** *sdu-size-value*	固定サイズの SDU のバイト数を指定します。データ プレーンの IP パケット長が固定で既知の場合、このパラメータが UGS サービス フローに使用されます。これは通常、フローが特定のコーデックで生成されている場合に該当します。デフォルト値は 49 です。
ステップ 10	router(config-gw-sf-qos-info)# **tolerated-jitter** *tolerated-jitter-value>*	接続の最大遅延変動（ジッタ）を指定します。
ステップ 11	router(config-gw-sf-qos-info)# **traffic-priority** *traffic-priority-value*	サービス フローに割り当てられるプライオリティを指定します。プライオリティ以外が同一であるサービス フローの場合、プライオリティが高いほうのサービス フローの遅延を短くし、バッファリング プリファレンスを高くします。異なるサービス フローの場合、プライオリティ パラメータは競合するサービス フローの QoS パラメータよりも優先されることはありません。このパラメータを強制する特定のアルゴリズムは必要ありません。
ステップ 12	router(config-gw-sf-qos-info)# **unsolicited-interval-grant** *unsolicited-interval-grant-value*	このサービス フローに与えられる一連のデータ間の公称間隔を指定します。データ プレーンの IP パケットの到着間隔が既知の場合、このパラメータは UGS および ERT-VR サービス フローに使用されます（通常、フローが特定のコーデックで生成されている場合に該当します）。
ステップ 13	router(config-gw-sf-qos-info)# **unsolicited-interval-polling** *unsolicited-interval-polling-value*	このサービス フローに与えられる一連のポーリングの最大公称間隔を指定します。

設定例

次に QoS の設定例を示します。

```
wimax agw service-flow qos-info profile isf-qos-downlink
 data-delivery-service real-time-variable-rate
 maximum-latency 1
 maximum-traffic-burst 2
 maximum-traffic-rate-sustained 3
 media-flow-type 012041424344
 minimum-traffic-rate-reserved 4
 policy-transmission-request 5
 sdu-size 6
 tolerated-jitter 7
 traffic-priority 1
 unsolicited-interval-grant 8
 unsolicited-interval-polling 9

wimax agw service-flow qos-info profile isf-qos-uplink
 data-delivery-service unsolicited-grant
 maximum-latency 11
 maximum-traffic-burst 21
 maximum-traffic-rate-sustained 31
 minimum-traffic-rate-reserved 41
 policy-transmission-request 51
 sdu-size 61
 tolerated-jitter 71
 traffic-priority 3
 unsolicited-interval-grant 81
```

```
 unsolicited-interval-polling 91
!
wimax agw service-flow qos-info profile downlink-qos-02
 data-delivery-service real-time-variable-rate
 media-flow-type 05abcd
```

設定の確認

BWG の QoS 値を確認するには、**show wimax agw subscriber** コマンドを使用します。QoS の統計情報の出力の例は、次のとおりです。

```
Router>sh wimax agw subscriber
MSID 1000.2228.0001
  Connection time 000:00:14
  Auth policy 0X0(0)
  Number of TIDs 1
  TID Key 10.1.1.70/2.2.2.2/1000.2228.0001
   Peer TID 0X2(2)
     FT MS State Change(9), MT Attachment Request(8)
   Our TID 0x8001(32769)
QoS information:
      data-delivery-service real-time-variable-rate
      minimum-traffic-rate-reserved 4, maximum-latency 1
      unsolicited-interval-polling 9, traffic-priority 1
      maximum-traffic-rate-sustained 3, policy-transmission-request 5
      maximum-traffic-burst-rate 2
      reduced-resources-code 0
     Classifier information:
      priority 0 permit ip host 0.0.0.0 host 0.0.0.0

Service Flow information Uplink:
      Identifier 4
     QoS information:
      data-delivery-service unsolicited-grant
      minimum-traffic-rate-reserved 41, maximum-latency 11
      tolerated-jitter 71, sdu-size 61
      unsolicited-interval-grant 81, policy-transmission-request 51
      reduced-resources-code 0
     Classifier information:
      priority 0 permit ip host 0.0.0.0 host 0.0.0.0
```

表 2-5 および 表 2-6 に 802.16 の QoS クラスおよびサービス パラメータを示します。

表 2-5　802.16 の QoS クラス

QoS パラメータ	BE ベスト エフォート サービス フロー	ERT-VR	UGS	RT-VR	NRT-VR
トラフィック プライオリティ 0 ～ 7 デフォルト : 0	オプション	オプション *[a]*		オプション *[a]*	オプション *[a]*
最大持続レート 0 ～ 4294967295 ビット / 秒	オプション	オプション *[b]*		オプション *[b]*	オプション *[b]*
最小予約レート 0 ～ 4294967295 ビット / 秒		**X**	**X**	**X**	**X**

表 2-5　802.16 の QoS クラス （続き）

QoS パラメータ	BE ベスト エフォート サービス フロー	ERT-VR	UGS	RT-VR	NRT-VR
最大トラフィック バースト 0 ～ 4294967295 ビット / 秒		オプション		オプション	オプション
ジッタ許容値 0 ～ 4294967295 msc		オプション *[c]*	オプション *[c]*		
最大遅延許容値 0 ～ 4294967295 msc		**X**	**X**	**X**	
非送信請求許可間隔 0 ～ 65535 msc		**X**	**X**		
SDU サイズ 0 ～ 255 バイト デフォルト：49			オプション *[d]*		
非送信請求ポーリング間隔 0 ～ 65535 msc				**X**	
DSCP					

表 2-6　802.16 の QoS クラスおよびサービス パラメータ

QoS クラス	説明	QoS 仕様サービス パラメータ
非送信請求許可サービス（UGS）	**VoIP** リアルタイムでは、パケットは固定サイズで定期的に送信されます（たとえば、ボイス コーデック、ATM CBR、E1/T1 over ATM）。	最大持続レート 最大遅延許容値 ジッタ許容値
リアルタイム ポーリング サービス（rtPS）	**ストリーミング オーディオ、ビデオ** リアルタイムでは、パケットは可変サイズで定期的に送信されます（たとえば、MPEG ビデオ、VoIP、ストリーミング）。	最小予約レート 最大持続レート 最大遅延許容値 トラフィック プライオリティ
拡張リアルタイム パケット サービス（ErtPS）	**VoIP（VAD 機能付き）**	最小予約レート 最大持続レート 最大遅延許容値 ジッタ許容値

表 2-6　802.16 の QoS クラスおよびサービス パラメータ

QoS クラス	説明	QoS 仕様サービス パラメータ
非リアルタイム ポーリング サービス（nrtPS）	**FTP** 非リアルタイム サービス フローでは、可変サイズ、通常のデータ許可バーストが必要とされます（たとえば、インターネット アクセス、ATM GFR）。	最小予約レート 最大持続レート トラフィック プライオリティ
ベスト エフォート サービス フロー（BE）	**データ転送、Web、参照**	最大持続レート トラフィック プライオリティ

ユーザ グループ管理

BWG でユーザ グループを設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config)#` **`wimax agw user group-list`** *`user-group-list-name`*	BWG ルータでユーザ グループ リストを設定します。コマンドで **no** を使用すると、ユーザ グループ リストが削除されます。このコマンドを有効にすると、ユーザ グループ リストのサブ コンフィギュレーション モードに入ることができます。サブ コンフィギュレーション モードでは、作成されたユーザ グループ リストに複数のユーザ グループを作成できます。
ステップ 2	`router(config-gw-ug)#` **`service-flow pre-defined {isf | secondary`** *`secondary-index`*`}` **`profile`** *`sf-profile-name`*	加入者に公開される定義済みのサービス フローの数を指定します。**ISF** キーワードが設定されている場合、サービス フローは初期サービス フローであると想定されます。**secondary** キーワードは、加入者の補助サービス フローを表します。現在、加入者ごとに 1 つの初期サービス フローと 3 つ以内の補助サービス フローが許可されています。
ステップ 3	`router(config-gw-ug)#` **`ip static-allowed`**	このユーザ グループの一部であるセッションのスタティック ホストの作成を許可します。デフォルトでは、スタティック ホストは許可されていません。

設定例

次に、ユーザ グループを設定する例を示します。

```
!
wimax agw user group-list wimax
 user-group any
  aaa accounting method-list agw
  sla profile-name gold
  dhcp server primary 12.1.1.2
!
user-group domain cisco.com
  aaa accounting method-list agw
  sla profile-name gold
  ip static-allowed
  ip route aggregate auto
```

```
!
user-group unauthenticated
  aaa accounting method-list agw
  aaa authentication method-list agw
  sla profile-name gold
  ip static-allowed
  user auto-provisioning
  proxy realm cisco.com password ciscoway
```

アイドル タイマーのサポート

BWG では、ユーザ グループのアイドル タイマーが設定できます。タイマーの時間内にデータ トラフィックがない場合、SS/MSS が登録解除されます。認証フェーズ中に AAA サーバからアイドル タイムアウトがダウンロードされます。

次に設定の例を示します。

```
wimax agw user group-list wimax
 user-group any
  aaa accounting method-list agw
  dhcp server primary 11.1.1.93
  service-flow pre-defined isf profile isf
  timeout idle 30
  timeout session 30
 !
 user-group unauthenticated
  aaa accounting method-list agw
  dhcp server primary 11.1.1.93
  service-flow pre-defined isf profile isf
  service-flow pre-defined secondary 1 profile 2sf
 !
!
```

アイドル タイマーは、ASN のインバウンド トラフィックでサポートされます。

AAA および ASN のユーザ グループでアイドル タイマー値が設定されている場合、AAA が優先されます。

ユーザ グループベースのメンテナンス モード、表示、および消去

特定のユーザ グループに関連付けられたすべてのユーザを消去し、AAA アトリビュートを更新したい場合があるとします。その場合、ユーザ グループ レベルの表示および消去コマンドが必要とされます。メンテナンス モードを使用すると、オペレータが必要に応じてすべての加入者を消去できるようにするために、新しい CPE が特定のユーザ グループに入らないようブロックできます。

ユーザ グループはセッション ハンドルのリストを保持しているため、内部でセッションを追跡できます。このハンドル リストが表示および消去に使用されます。

セッションがユーザ グループに割り当てられるたびに、ユーザ グループのメンテナンス モードが確認されます。セッションは常に 1 つのユーザ グループにしか割り当てられませんが、セッションは有効期間内に複数のユーザ グループを受け入れることができます。これは非 EAP セッションが本来、未認証のユーザ グループに割り当てられるものであり、AAA の応答によって BWG が他のユーザ グループをセッションに再割り当てできるようにするためです。この場合、受け入れたユーザ グループのいずれかのメンテナンス モードがオンになっている場合、CPE が拒否されます。

デフォルトでは、メンテナンス モードはディセーブルです。非 EAP の場合、各着信 CPE は最初に未認証のユーザ グループに割り当てられます。したがって、メンテナンス モードが未認証のユーザ グループでイネーブルになっている場合、新しい非 EAP の CPE が BWG に入ることはありません。

メンテナンス モード機能をイネーブルにするには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router(config-gw-ugl)# service mode maintenance`	ユーザ グループのメンテナンス モード機能をイネーブルにします。

次に設定の例を示します。

```
User group domain name unauthenticated
 User-Group overwritten Counter 0
 Service mode operational
 Sessions 2 associated
 IP-GRE Traffic Sent 0 packets, 0 bytes
 IP-GRE Traffic Received 0 packets, 0 bytes
 Eth-GRE Traffic Sent 18 packets, 6138 bytes
 Eth-GRE Traffic Received 18 packets, 10872 bytes
 Ingress Address filtering 0 packets, 0 bytes
 Traffic Received redirected 0 packets, 0 bytes
 Sessions rejected due to service mode not operational 0   // new line
```

ユーザ グループに割り当てられたセッションを表示するには、次のタスクを実行します。

ステップ 1	router#**show wimax agw user-group name** *user-group-name* [brief] #**show wimax agw user-group any** [**brief**] #**show wimax agw user-group unauthenticated** [**brief**]	メンテナンス モード中に BWG によって拒否されたユーザ グループの新しいセッションを表示します。

ユーザ グループに関連付けられたセッションを表示するには、次のように入力します。

```
router#sh wim agw sub user-group name cisco.com br
MSID           Address         Age       Flows Hosts Pkts-Tx    Pkts-Rx
0003.1238.5678 0.0.0.0         000.07.47 1     0     3          3
0003.123A.5678 11.1.0.5        000.02.32 1     0     2          2
0003.123B.5678 11.1.0.6        000.02.00 1     0     2          2
0003.123C.5678 11.1.0.7        000.01.40 1     0     2          2
0003.123D.5678 11.1.0.8        000.01.40 1     0     2          2
0003.123E.5678 11.1.0.9        000.01.40 1     0     2          2
```

セッションを消去するには、次のタスクを実行します。

ステップ 1	router#**clear wimax agw subscriber user-group name** *group-name* [**local**] router#**clear wimax agw subscriber user-group any** [**local**] router#**clear wimax agw subscriber user-group unauthenticated** [**local**]	ユーザ グループに関連付けられたセッションを消去します。

セッション タイマーのサポート

BWG では、ユーザ グループのセッション タイマーまたは絶対タイマーを設定できます。タイマーの期限が切れると、加入者が登録解除されます。認証フェーズ中に AAA サーバからセッション タイムアウトがダウンロードされます。

Mobile Subscriber Station の登録解除

Cisco BWG リリース 1.0 以降では、Path Deregistration メッセージングの結果として Network Exit がサポートされます。

Mobile Subscriber Station を登録解除するには、次の 2 つの方法があります。

Mobile Subscriber Station による登録解除

ステップ 1　SS が DREG-REQ メッセージを BS に送信し、登録解除プロシージャを開始します。

ステップ 2　BS が Data Path De-Reg Request を BWG に送信します。

ステップ 3　BWG が、アクション コード（0x04 に設定）を持つ Data Path De-Reg Response を BS に送信し、登録解除プロシージャを許可します。

ステップ 4　BS が DREG-CMD を SS に送信し、SS を登録解除します。

ステップ 5　BS が Data Path De-Reg Ack を BWG に送信し、トランザクションを完了します。

ネットワークによる登録解除

ステップ 1　MS が削除されるよう指示する Data Path De-Reg Request メッセージを BWG が BS に送信します。

ステップ 2　BS がエアーリンク経由で DSD-REQ を送信し、特定のサービス フローを登録解除します。

ステップ 3　BS が SS からサービス フローの終了を指示する DSD-RSP を受信します。

ステップ 4　BS がサービス フローの終了を指示する Data Path De-Reg Response を BWG に送信します。

ステップ 5　BWG が Data Path De-Reg Acknowledgement を送信し、トランザクションを終了します。

登録解除要求での Deregistration Reason TLV

リリース 1.4 では、Path Deregistration Request が拡張され、次の論理に基づいた Registration Type TLV に加えて、追加の TLV である Deregistration Reason TLV が含まれています。

- 認証の失敗（つまり、Access-Reject の自動プロビジョニングがないか、AAA に到達できません）
- Access-Accept で受信された CPE サービス状態のアトリビュートによって、CPE がブラックリストに載るよう指示（非アクティブ）
- 内部エラー（つまり、保護タイマーのタイムアウト、セッション タイマーのタイムアウトなど）

表 2-7 に Deregistration Reason TLV の値の詳細を示します。

表 2-7　Cisco R6 Deregistration Reason TLV

タイプ	1010
オクテット長	4

表 2-7　Cisco R6 Deregistration Reason TLV （続き）

値	列挙型。値は次のとおりです。 0：予約済み 1：未払い（サービス許可の失敗） 2：盗難報告あり（ブラックリスト） 3：不正なユーザ動作（ブラックリスト） 4：サービスの一時中断（CPE の一時中断） 5：保護タイマーの終了（BWG 内部エラー） 6：アドレス割り当てタイマーの終了（BWG 内部エラー） 7：AAA サーバに到達不能 8 ～ 127：予備 128：認証の失敗（AAA で CPE が見つからないか、自動プロビジョニングがイネーブルではありません） 129：オペレータによる CPE 登録解除の指示（BWG からのネットワークの退出） 130：オペレータによる CPE リセットの指示 131：認証セッション タイマーの終了 132：アイドル セッション タイマーの終了 133：非ホーム BS 経由のアクセス 134：ISF 作成の失敗 135：メンテナンス モードのユーザ グループ
説明	Deregistration Reason を示します。
この TLV を使用するメッセージの根源	Path Deregistration Request メッセージ

BWG は、EAP および PAP で認証された両方のユーザに対してこの機能をサポートします。

（注） Deregistration Reason TLV はオプションであり、6 および 130 以外の値に一致する場合に限り含まれます。

（注） アドレス割り当てのタイムアウトは、登録解除理由コードの「6：アドレス割り当てタイマーの終了」および「130：オペレータによる CPE リセットの指示」が使用されないため、BWG でサポートされません。

AAA Accounting Start-Stop-Interim

BWG は各サービス フローのアカウンティング情報をサポートします。時間ベースの Interim アカウンティングの更新だけがサポートされます。BWG は各サービス フローをサポートし、各サービス フローのタプル（Acct-Session-Id + Acct-Multi-Session-Id + PDFID）のアカウンティング レコードの一意のセットを生成します。各サービス フローは、GRE キーによって一意に識別されます。指定した MS には複数のサービス フローを作成できます。

（注）　セッションごとのアカウンティングはこのリリースではサポートされていません。

BWG によって送信されるすべてのアカウンティング レコードでは、トラフィックの送信先のモバイルの背後にどのホストがあるかにかかわらず、Framed-IP-Address フィールドがモバイルの IP アドレスに設定されます。

BWG は次のメッセージを AAA サーバに送信します。

- Accounting Start：新しいサービス フローが作成されたときに BWG がこのメッセージを AAA サーバに送信します。冗長 BWG 設定の場合、スタンバイ BWG がアクティブになったときに限り Accounting Start メッセージを送信します。Accounting Start がトリガーされるのは、サービス フローの作成が成功したときです。初期サービス フローの場合、アカウンティング開始レコードが送信されるのは IP アドレスがユーザに割り当てられた後です。補助サービス フローの場合、フローが BS で正常にオープンされるとすぐにアカウンティング レコードが送信されます。

  BWG リリース 2.2 以降では、アカウンティング開始レコードの Framed-IP-Address フィールドの送信の遅延を設定できます。Framed-IP は多くの場合、フロー アカウンティングのアカウンティング開始レコードに含まれていません。初期サービス フローの場合、フローの作成時にアカウンティング開始レコードが送信されてから加入者のホストが作成されます。BWG リリース 2.2 以降では、ホストが作成されるまでアカウンティング開始レコードの送信を遅延させることができます。遅延を設定するには、**[no] aaa accounting flow start include-framed-ip [delay]** コマンドを使用します。デフォルトでは、この機能はディセーブルです。イネーブルの場合、デフォルトの遅延は 3 秒に指定されています。遅延に指定できる値の範囲は 1 ～ 20 秒です。

- Accounting Interim Update：定期的なアカウンティング更新メッセージが設定されている場合、BWG は Accounting Update メッセージを生成します。アカウンティングの更新は、時間に応じてトリガーされるか、設定時に行われます。タイマーに指定できる最小の値は 1 分です。

- Accounting Stop：BWG は、サービス フローが削除されるか、MS が削除を完了したときに Accounting Stop メッセージを送信します。

アカウンティング レコードで送信されるアトリビュートを表 2-8 に示します。

表 2-8　BWG-AAA 認証アトリビュート

アトリビュート	タイプ	説明	Access Request	Access Challenge	Access Accept	Access Reject
User-Name	1	EAP-Response Identity（Outer-NAI）から NAI を取得します。	1	0	0-1	
Service-Type	6	最初の認証では「Framed」に設定され、再認証では「Authenticate-Only」に設定されます。前納割り当ての中間セッションを取得するのに使用された場合は、「Authorize-Only」に設定される場合もあります。	1	0	0-1	0

表 2-8　BWG-AAA 認証アトリビュート （続き）

アトリビュート	タイプ	説明	Access Request	Access Challenge	Access Accept	Access Reject
Framed-MTU	12	RFC3579 に準じ、EAP 認証中の Access-Request で WiMAX によって使用されます。このアトリビュートは、EAP 交換中に PKMv2 の最大ペイロード サイズ（2008 バイト）を超えないように、適切な MTU サイズを提供します（EAP アプリケーション レイヤの認証サーバには、適切なフラグメンテーションがあると見なされます）。このアトリビュートの値は 1020 ～ 2000 バイトの間で設定される必要があります（推奨値は 1400 バイトです）。 Access-Accept での使用は、RFC2865 に準じます。	0-1[m]	0	0-1[m]	0
EAP-Message	79	EAP メッセージ	1-n	1-n	1-n	1-n
Message-Authenticator	80	[RFC3579] の規定に従って、RADIUS パケットの整合性保護機能を提供します。	1	1	1	1
WiMAX-Capability	26/1	NAS でサポートされる WiMAX 機能を識別します。RADIUS サーバによって選択される機能を示します。	1	0	0-1[k]	0
NAS-ID	32	NAS の FQDN	1[b]	0	0	0
NAS-Port-Type	61	要求が関連付けられるポートのタイプを示します。WiMAX ASN からの場合は WiMAX に設定されます。HA からの場合は MIPv4 または MIPv6 に設定されます。	1	0	0	0
Calling-Station-Id	31	デバイス（MS）の MAC アドレスに設定します。	1	0	0	0
Device-Authentication-Indicator	26/2	デバイス認証が実行されたかどうか、およびその結果を示します。	0-1[i]	0	0	0
GMT Timezone-Offset	26/3	NAS での GMT からのオフセットを秒単位で示します。	1	0	0	0
NAS-IP-Address	4	NAS IP アドレス。または NAS-IP-Address。	0-1[b]	0	0	0
Error-Cause	101	アクセス認証 [RFC3576] の間に生成されるエラー コード。	0	0-1	0	0-1
Class	25	認証をアカウンティングにバインドするのに使用するサーバによって設定される、不透明な値。	0	0	0-1[h][k]	0
Framed-IP-Address	8	MN に割り当てられる MIPv4 ホーム アドレス。	0	0	0-1[c][k]	0
Session-Timeout	27	セッションの終了までにユーザに提供されるサービスの最大秒数。キーのライフタイムに関連付けられます。	0	0	0-1[d][k]	0
Termination-Action	29	サービスの完了時に NAS が実行するアクションを示します。	0	0	0-1[d][k]	0

表 2-8　BWG-AAA 認証アトリビュート （続き）

アトリビュート	タイプ	説明	Access Request	Access Challenge	Access Accept	Access Reject
AAA-Session-ID	26/4	このセッションに対するホーム レルムの一意の識別子。	0-1[e]	0-1	1	0
BS-ID	26/46	メッセージの配信時の NAP-ID および BS-ID を示します	0-1[n]	0	0	0
MSK	26/TBD	EAP 認証の成功によって取得される、マスター セッション キー。	0	0	1[f]	0
Session-Timeout	27	セッションの終了までにユーザに提供されるサービスの最大秒数。EAP 認証から取得されるキー（つまり、MSK、EMSK、および EMSK から取得されるキー）のライフタイムに関連付けられます。 Access-Challenge パケットの Session-Timeout は、RFC3579 に準じて EAP 再送信タイマーの設定に使用されます。	0	0-1	0-1[d][k]	0
CPE-service-state	Cisco VSA	CPE がブラックリストに載るかどうかを示します。	0	0	0-1	0

[b] NAS-ID は Access-Request に表示される必要があります。NAS-IP-Address が表示される場合もあります。**radius-server attribute 32 include-in-access-req** コマンドを使用して CLI で NAS-ID を設定できます。

[c] このアトリビュートが存在する場合、モバイルに割り当てられるホーム アドレスは、このアトリビュートの指定どおりにする必要があります。このアトリビュートがない場合、ホーム アドレスは MIP プロシージャまたは他の手段（たとえば DHCP など）で取得されます。

[d] Session-Timeout および Termination-Action の両方が存在する必要があります。Termination-Action が「RADIUS-Request」（1）に設定される必要があります。これにより、Session-Timeout が切れたときに NAS が再認証を行います。

[f] RFC2868 のセクション 3.5 のプロシージャを使用してアトリビュートが暗号化される必要があります。

[h] Access-Accept メッセージ内に複数のクラス アトリビュートが見つかった場合、NAS はすべてのクラス アトリビュートを保存し、アカウンティング要求パケットでそれらを返信します。

[i] ダブル EAP デバイスのユーザ認証フェーズ（ユーザ認証プロシージャ）に関連付けられた Access-Request に表示する必要があります。表示しない場合は、アトリビュートが Access-Request メッセージに存在することはできません。

[k] アトリビュートは、ダブル EAP のデバイス認証フェーズに関連付けられて送信された Access Accept に表示することはできません。

[m] Access-Authentication 中にフレーム化された MTU が Access-Request に表示されている場合、そのフレーム化された MTU は NAS と MS 間のリンク上の MTU を意味します。RFC3579 に準じて、連結されている場合、Framed-MTU 値で指定された長さを超える値の EAP-Message アトリビュートを含む EAP カンバセーションで RADIUS が後続のパケットを送信することはできません。

[n] BS-ID または NAP-ID のいずれかが提供されます。この両方が提供された場合、受信側は NAP-ID アトリビュートを無視します。リリース 1.0 以降では、NAP_ID は AAA に送信されません。NAP-ID は、48 ビット BSID の 24（MSB）ビットです（その後 BS が NAP-ID を送信する場合）。

Cisco BWG リリース 1.4 では、AAA からの Service State アトリビュートのサポートが追加されています。アトリビュート タイプは「Cisco-VSA」で、フォーマット タイプは「string」です。このアトリビュートは、CPE がブラックリストに載っているかどうかを示します。

このアトリビュートに定義されている値は次のとおりです。

0：アクティブ

1：滞納

2：盗難報告

3：要注意ユーザ

4：サービスの一時停止

BWG は、Access-Accept に Service State アトリビュートが含まれていると見なします。BWG でこの実装を支援するために、AAA は Access-Accept だけを持った Service State アトリビュートを返すように設定されています。Access-Reject が送信されたときに Service Attribute は含まれていません。BWG は、EAP と PAP 認証済みユーザの両方に対してこのアトリビュートをサポートします。

デフォルトでは、CPE は BWG でアクティブであると見なされます。

AAA アカウンティングの設定

BWG でアカウンティング機能をイネーブルにするには、次のタスクを実行します。

	コマンド	目的
ステップ 1	router(config)# **aaa accounting network** {*accounting-list-name*} **{none|start-stop|stop-only} {broadcast|group}** {*server-group-name*|**radius**}	ネットワーク サービスのアカウンティングをイネーブルにします。WiMAX では、アカウンティング方式のリスト名が必要です。
ステップ 2	router(config)# **aaa accounting update {newinfo|periodic}** {*periodic intervals to send accounting updates in minutes*}	アカウンティングの更新を定期的な間隔でイネーブルにします。コマンドで **no** を使用すると、アカウンティングの更新の送信をディセーブルにします。
ステップ 3	router(config)# **wimax agw user group-list** *user-group-list-name*	BWG ルータでユーザ グループ リストを設定します。BWG の単一プロセッサで許可されるのは、1 つのユーザ グループ リストだけです。コマンドで **no** を使用すると、ユーザ グループ リストが削除されます。このコマンドによってユーザ グループ リストのサブ コンフィギュレーション モードに入り、作成された *user-group list* の下に複数のユーザ グループを作成します。
ステップ 4	router(config-gw-ug)# **aaa accounting method-list** {*method-list-name*| **default**}	ドメインで使用されるアカウンティング方式のリストを指定します。

Accounting Start 応答

現在、アカウンティング応答メッセージは BWG で処理されません。BWG リリース 2.0 では、フローアカウンティングがイネーブルになっている場合、Accounting Start 応答が受信されないかぎり、フローはトラフィックの処理を開始しません。

この機能はユーザ グループ単位でイネーブルになります。デフォルトでは、この機能はイネーブルではありません。この機能をイネーブルにするには、次のタスクを実行します。

	コマンド	目的
ステップ 1	router(config)# **wimax agw user group-list wimax** **user-group unauthenticated** **aaa accounting method-list agw** **aaa accounting host enable** **aaa accounting start wait-response**	Accounting Start 応答が受信されたあとに BWG をイネーブルにしてフロー アカウンティングのトラフィックを処理します。

イネーブルにすると、AAA からのアカウンティング応答が受信されなかった場合、セッションが削除されます。

設定例

次に、ユーザ グループの設定例を示します。

```
wimax agw user group-list wimax
  user-group any
   aaa accounting method-list agw
   aaa authentication method-list agw
!
  user-group domain cisco.com
   aaa accounting method-list agw
   aaa authentication method-list agw
!
  user-group unauthenticated
   aaa accounting method-list agw
```

次に、AAA および RADIUS の設定例を示します。

```
aaa new-model
!
aaa accounting update periodic 15
aaa accounting network agw start-stop group radius
aaa authorization network default group radius
aaa authentication dot1x agw group radius
!
radius-server attribute 32 include-in-access-req format %h.%d.%i
radius-server attribute 55 access-request include
radius-server attribute 25 accounting prefer-preauth
radius-server vsa send accounting wimax
radius-server vsa send authentication wimax
radius-server host 172.19.25.8 auth-port 1645 acct-port 1646 key cisco
radius-server host 1.8.91.8 auth-port 1645 acct-port 1646 key cisco

!
```

設定の確認

次に、アカウンティング設定を確認するのに使用される、**show wimax agw subscriber** コマンドの例を示します。

```
Router#sh wimax agw subscriber msid 1000.0002.0001
 Connection time 000:01:08
 Auth policy 0X12(18), Single-EAP, CMAC
 Number of TIDs 1
 TID Key 10.1.1.82/2.2.2.2/1000.0002.0001
  Peer TID 0X4(4)
    FT MS State Change(9), MT Attachment Request(8)
  Our TID 0x8004(32772)
 Subscriber address 2.2.0.8, type IPv4, organization IETF
 Subscriber address method Dynamic, source DHCP relay
 Subscriber address assigned on flow downlink ID 15
 Subscriber address prefix len allocated 32, aggregate 32
 Subscriber address traffic sent 0 packets, 0 bytes
 Subscriber address traffic received 0 packets, 0 bytes
 Subscriber address DHCP XID 2390, server 0.0.0.0, htype 1
 Subscriber address DHCP client ID 1000.0002.0001, length 6
 Subscriber address DHCP Refresh time 86400 seconds
 Number of sessions 1
  Session details:
   FSM in state Ready(7) on last event Rx Attach Ack(14)
   Username eap-md5-u@eap-md5.com
   Authentication method EAP
```

```
AAA session-id length 7, 0x30313233414243
   AAA termination-action 1
   Reauthentication attempts from subscriber 0, ASNGW 0
   Associated user group **any**
   Signalling address local 2.2.2.2, remote 10.1.1.82
   Signalling UDP port local 2231, remote 2231
   Idle for inbound 00:01:09, outbound 00:01:09
   Absolute timeout 1500, remaining 00:23:49
   Idle timeout 600 (both), remaining 00:08:50
   Ingress Address filtering 0 packets, 0 bytes
   Number of flows 1
    Flow details ISF(0)
     FSM in state SF Ready(4) on last event Up(1)
     Transaction ID used 0X8004(32772)
     Data ID local 0x8(8), remote 0x1(1)
     Data address local 2.2.2.2, remote 10.1.1.82
     Data traffic sent 2 packets, 705 bytes
     Data traffic received 2 packets, 1208 bytes
     Accounting last record sent Interim(3)
     Idle for inbound 00:01:09, outbound 00:01:09
     Service Flow information Downlink: Identifier 15
```

次に、AAA のアカウンティング開始の RADIUS の出力例を示します。

```
*Aug 11 02:27:21.143: RADIUS(00000006): Send Accounting-Request to
 1.8.91.8:1646 id 1646/61, len 165
*Aug 11 02:27:21.143: RADIUS:  authenticator C4 F4 3F A3 00 1C 01 66 - 78
 DD A4 B4 68 37 F9 5B
*Aug 11 02:27:21.143: RADIUS:  Acct-Session-Id     [44]  10  "00000006"
*Aug 11 02:27:21.143: RADIUS:  Framed-Protocol     [7]   6   noval0
 [0]
*Aug 11 02:27:21.143: RADIUS:  Called-Station-Id   [30]  9   "2.2.2.2"
*Aug 11 02:27:21.143: RADIUS:  Framed-IP-Address   [8]   6   2.2.0.76
*Aug 11 02:27:21.143: RADIUS:  Calling-Station-Id  [31]  19  "10-00-22-
 25-00-01"*Aug 11 02:27:21.143: RADIUS:  Acct-Input-Octets   [42]  6   1208
*Aug 11 02:27:21.143: RADIUS:  Acct-Output-Octets  [43]  6   666
*Aug 11 02:27:21.143: RADIUS:  Acct-Input-Packets  [47]  6   2
*Aug 11 02:27:21.143: RADIUS:  Acct-Output-Packets [48]  6   2
*Aug 11 02:27:21.143: RADIUS:  Vendor, Wimax       [26]  13
*Aug 11 02:27:21.143: RADIUS:   GMT-Time-Zone-Offse[3]   7
*Aug 11 02:27:21.143: RADIUS:   00 00 00 00 00
 [?????]
*Aug 11 02:27:21.143: RADIUS:  Vendor, Wimax       [26]  11
*Aug 11 02:27:21.143: RADIUS:   Packet-Data-Flow-ID[26]  5
*Aug 11 02:27:21.143: RADIUS:   00 00 00
 [???]
*Aug 11 02:27:21.143: RADIUS:  Acct-Session-Time   [46]  6   1630
*Aug 11 02:27:21.143: RADIUS:  Acct-Status-Type    [40]  6   start
 [3]
*Aug 11 02:27:21.143: RADIUS:  NAS-Port-Type       [61]  6   802.16e Wimax
 [27]
*Aug 11 02:27:21.143: RADIUS:  NAS-Port-Id         [87]  11  "WiMAX-AGW"
*Aug 11 02:27:21.143: RADIUS:  Service-Type        [6]   6   Framed
 [2]
*Aug 11 02:27:21.143: RADIUS:  NAS-IP-Address      [4]   6   2.2.2.2
*Aug 11 02:27:21.143: RADIUS:  Acct-Delay-Time     [41]  6   0
*Aug 11 02:27:21.175: RADIUS/ENCODE(00000007):Orig. component type = AGW
*Aug 11 02:27:21.175: RADIUS/ENCODE: NAS PORT sending disabled
*Aug 11 02:27:21.175: RADIUS(00000007): Config NAS IP: 0.0.0.0
*Aug 11 02:27:21.175: RADIUS(00000007): sending
*Aug 11 02:27:21.175: RADIUS/ENCODE: Best Local IP-Address 2.2.2.2 for
 Radius-Server 1.8.91.8
```

次に、AAA のアカウンティング停止の RADIUS の出力例を示します。

```
*Feb 18 15:30:29.011: RADIUS(00000006): Send Accounting-Request to
 172.19.25.8:1646 id 1646/24, len 252
*Feb 18 15:30:29.011: RADIUS:  authenticator 6D FC 9B 49 59 28 56 41 - 3F 2E A5
 3C 7B 7A 3A B1
*Feb 18 15:30:29.011: RADIUS:  Acct-Session-Id     [44]  10  "00000008"
*Feb 18 15:30:29.011: RADIUS:  Framed-Protocol     [7]   6   noval0
[0]
*Feb 18 15:30:29.011: RADIUS:  Called-Station-Id   [30]  9   "2.2.2.2"
*Feb 18 15:30:29.011: RADIUS:  Framed-IP-Address   [8]   6   2.2.0.2
*Feb 18 15:30:29.011: RADIUS:  Calling-Station-Id  [31]  19  "06-76-22-24-22-22"
*Feb 18 15:30:29.011: RADIUS:  Vendor, Wimax       [26]  10
*Feb 18 15:30:29.011: RADIUS:   AAA-Session-ID     [4]   4
*Feb 18 15:30:29.011: RADIUS:   00 00
[??]
*Feb 18 15:30:29.011: RADIUS:  User-Name           [1]   23  "eap-md5-u@eap-
 md5.com"
*Feb 18 15:30:29.011: RADIUS:  Acct-Input-Octets   [42]  6   0
*Feb 18 15:30:29.011: RADIUS:  Acct-Output-Octets  [43]  6   0
*Feb 18 15:30:29.011: RADIUS:  Acct-Input-Packets  [47]  6   0
*Feb 18 15:30:29.011: RADIUS:  Acct-Output-Packets [48]  6   0
*Feb 18 15:30:29.011: RADIUS:  Multilink-Session-ID[50]  10  "30313233"
*Feb 18 15:30:29.011: RADIUS:  Class               [25]  21
*Feb 18 15:30:29.011: RADIUS:   63 6C 61 73 73 2D 77 69 6D 61 78 2D 63 68 61 6E
[class-wimax-chan]
*Feb 18 15:30:29.011: RADIUS:   67 65 64
[ged]
*Feb 18 15:30:29.011: RADIUS:  Vendor, Wimax       [26]  13
*Feb 18 15:30:29.011: RADIUS:   GMT-Time-Zone-Offse[3]   7
*Feb 18 15:30:29.011: RADIUS:   00 00 00 00 00
[?????]
*Feb 18 15:30:29.011: RADIUS:  Vendor, Wimax       [26]  17
*Feb 18 15:30:29.011: RADIUS:   BaseStation-ID     [46]  11
*Feb 18 15:30:29.011: RADIUS:   00 0A 01 01 46 00 00 00 00
[????F????]
*Feb 18 15:30:29.011: RADIUS:  Vendor, Wimax       [26]  11
*Feb 18 15:30:29.011: RADIUS:   Packet-Data-Flow-ID[26]  5
*Feb 18 15:30:29.011: RADIUS:   00 05 01
[???]
*Feb 18 15:30:29.011: RADIUS:  Acct-Session-Time   [46]  6   25
*Feb 18 15:30:29.011: RADIUS:  Acct-Terminate-Cause[49]  6   none
[0]
*Feb 18 15:30:29.011: RADIUS:  Acct-Status-Type    [40]  6   Stop
[2]
*Feb 18 15:30:29.011: RADIUS:  NAS-Port-Type       [61]  6   802.16e Wimax
[27]
*Feb 18 15:30:29.011: RADIUS:  NAS-Port-Id         [87]  11  "WiMAX-AGW"
*Feb 18 15:30:29.011: RADIUS:  Service-Type        [6]   6   Framed
[2]
*Feb 18 15:30:29.011: RADIUS:  NAS-IP-Address      [4]   6   172.19.24.88
*Feb 18 15:30:29.011: RADIUS:  Acct-Delay-Time     [41]  6   0
*Feb 18 15:30:29.019: RADIUS: Received from id 1646/23 172.19.25.8:1646,
Accounting-response, len 20
*Feb 18 15:30:29.019: RADIUS:  authenticator 4D 1A 1B 4D C5 0E 39 FD - 36 6B 90 FF 96 21
66 64
*Feb 18 15:30:29.019: RADIUS: Received from id 1646/24 172.19.25.8:1646,
Accounting-response, len 20
*Feb 18 15:30:29.019: RADIUS:  authenticator EB 25 42 F1 48 2C BF 13 - 43 B0 0A 3A 7A 04
F4 1F
```

WiMAX 固有の VSA

次に、WiMax に固有の VSA を示します。

- Wimax 機能：WiMAX リリース、アカウンティング機能指定、ホットライン機能、および Access Request における AAA への BWG のアイドル モード通知機能を表します。
- GMT タイムゾーン オフセット：GMT 時間に対して、NAS でのローカル時間の現在のオフセットを秒単位で表します。
- Packet Data Flow-Id（PDFID）：このアトリビュートの値は、同じパケット データ フローからのすべての記録に一致します。PDFID は CSN によって割り当てられ、すべての引き継ぎのシナリオを通じて変更されません。リリース 1.0 以降では、BWG はセッションでフローの PDFID を生成します。
- ベース ステーション ID：NAP およびその NAP 内のベース ステーションを一意に識別します。BWG はこのアトリビュートで R6 BS ID を転送します。
- AAA セッション ID：ネットワークに入るときにホーム ネットワークによって WiMAX セッションに割り当てられる、一意のレルム単位の ID。そのセッションのすべての後続の AAA パケットに値が含まれます。

AAA ベースのホットライン

ホットラインは、パケット データ サービスへのアクセスが認証されなくなる可能性のある問題をユーザに知らせる機能です。ユーザがホットラインを受信すると、パケット データ サービスがホットライン アプリケーション（Cisco ISG など）にリダイレクトされ、ユーザに理由が通知されます。ホットラインの理由がユーザに通知されると、通常のパケット データ サービスは再開されます。

ユーザがホットラインを受信できるのは、パケット データ サービスの開始時、または AAA ベースの Change of Authorization（CoA）があるセッションの途中です。セッションの起動時には、ユーザのセッションにホットラインを通知するのに AAA Access Accept が使用されます。セッションの途中でセッションがホットライン プロファイルの詳細を持つ AAA CoA を受信した場合、ユーザのデータ トラフィックがリダイレクトされます。同様に、現在ホットラインを受信しているセッションのホットラインを停止することができます。

次のリストにホットライン機能のサポートを示します。

- BWG による、AAA Access Accept アトリビュートに基づいた新しいセッションのホットラインのサポート
- BWG による、AAA CoA に基づいたアクティブ セッションのホットラインのサポート
- アップリンク トラフィックとダウンリンク トラフィックのホットラインの使用時の、BWG によるパケット リダイレクションのサポート
- プロファイル ベースのホットラインのサポート
- BWG による AAA からの加入者単位でのホットラインのサポート
- トラフィックのリダイレクションは、データ パケットだけに適用。DHCP などのシグナリング パケットはリダイレクションの対象外
- IP リダイレクションおよび HTTP リダイレクションのこのリリースでのサポート

（注）　ホットライン中のダイナミック QoS およびパケット フィルタリングは、このリリースではサポートされません。

ホットラインのトリガー

次にユーザがホットラインを受信していることを HAAA が示す 2 つの方式を説明します。

プロファイル ベースのホットライン：
HAAA が RADIUS メッセージにホットラインのプロファイル ID を送信します。ホットラインのプロファイル ID は、事前に割り当てられた一連のルールを選択します。これにより、ユーザのパケット データ セッションがリダイレクトおよび（または）ブロックされます。プロファイル ベースのアプローチは、このリリースでサポートされています。

ルール ベースのホットライン：
HAAA は RADIUS メッセージに実際のリダイレクション ルール（HTTP または IP）およびフィルタ ルールを送信します。これにより、ユーザのパケット データ セッションがリダイレクトおよび（または）ブロックされます。

上記の 2 つのアプローチの違いは、ネットワーク インテリジェンスが置かれている場所にあります。AAA プロファイル ベースのホットラインは、BWG がホットラインに関するほとんどのネットワーク インテリジェンスを保持することを指示し、AAA サーバは単にトリガーするためにプロファイルを使用します。

また、AAA はルール ベースのアプローチのホットライン中に BWG が実行する詳細アクションを指定する必要があります。このシナリオでは、BWG は AAA が指示することをただ実行するだけです。

（注） ルール ベースのホットラインは、このリリースではサポートされていません。

（注） 上記の 2 つの方式は、混在させることはできません。

プロファイル ベースのホットラインでは、次の条件が適用されます。

アップストリーム フロー
ホットラインがイネーブルの場合、アップストリーム パケットではデフォルトでパケットをドロップします。アップストリーム方向のホットライン プロファイルの下にフィルタ ルールが設定されていない場合、すべてのアップストリーム パケットがドロップされます。ホットラインがイネーブルの場合であっても、特定のパケットが BWG を通過することを許可できます。これらのパケットは、ホットライン サーバ自身、HTTP、DNS パケットなどを宛先とするパケットを含みます。URL を指定し、パケットが通過する必要のあるサーバを示すことができます。

アップストリーム パケットのフィルタ ルールは、IP パススルー、HTTP リダイレクトの順で適用されます。

ダウンストリーム フロー
ホットラインがイネーブルの場合、ダウンストリーム パケットではデフォルトでパケットをドロップします。ダウンストリーム方向にフィルタ ルールが設定されていない場合、すべてのパケットがドロップされます。

AAA サーバからの Change of Authorization（CoA）メッセージでサポートされている必須アトリビュートは、User-Name、Calling-Station-Id、および AAA-Session-Id の各アトリビュートです。Calling-Station-Id アトリビュートは、BWG 上の特定のユーザを一意に識別するために使用します。

AAA アトリビュート

次にホットライン機能の AAA Access Accept に関連付けられた新しいアトリビュートを示します。これらのアトリビュートは、新しいセッションでのホットラインをサポートするために使用します。

表 2-9

アトリビュート	タイプ	説明	Access Request	Access Challenge	Access Accept	Access Reject
Hotline-Profile-ID	26/53	ユーザのホットライン プロファイルを一意に識別する ID	0	0	0-1[a]	0
Hotline-Session-Timer	26/56	ホットラインのセッションをユーザが維持できる時間を秒単位で指定します。	0	0	0-1	0
Hotline-Indication	26/24	フローおよびホストがホットラインを受信していることを示します。	0	0	0-1[b]	0

[a] Hotline-Profile-ID が含まれている場合、HTTP-Redirection-Rule、IP-Redirection-Rule、および Filter-Rule は含まれません。これらが存在する場合、受信側が自動的にアトリビュートを破棄します。

[b] セッションがホットラインを受信し、このアトリビュートが指定されている場合、NAS はアカウンティング メッセージにこのアトリビュートを含んでいます。

次にホットライン機能の AAA CoA に関連付けられた新しいアトリビュートを示します。これらのアトリビュートは、アクティブなセッションでのホットラインをサポートするのに使用されます。

表 2-10

アトリビュート	タイプ	説明	COA	COA-ACK	COA-NAK
User-Name	1	アクセス認証時に受信した MS の NAI	1	0	0
Calling-Station-Id	31	MS のバイナリ形式の MAC アドレス	1	0	0
AAA-Session-ID	26/4	User-Name および AAA-Session-ID に含まれている NAI は、NAS で一意のセッション ID を作成します。	1	0	0
Hotline- Profile-ID	26/53	ユーザのプロファイルを一意に識別する ID	0-1[a]	0	0
Hotline Session Timer	26/56	ホットラインのセッションをユーザが維持できる秒単位の時間を含みます。	0-1	0	0
Hotline- Indication	26/24	フローおよびホストがホットラインを受信していることを示します。	0-1[b]	0	0

[a] Hotline-Profile-ID が含まれている場合、HTTP-Redirection-Rule、IP-Redirection-Rule、および Filter-Rule は含まれません。これらが存在する場合、受信側はアトリビュートを破棄します。

[b] HAAA によって認識されている場合、MS の IP アドレスが含まれます。

プロファイル ベースのホットラインの設定

BWG がプロファイル ベースのホットラインを実行するよう設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router# wimax agw hotline profile` *profile-name* `ip access-group` *number in | out* `passthru` `http access-group` *number* `redir-url` *url*	
ステップ 2	`router(config-gw-hotline)# ip access-group` *number in | out* `passthru`	ACL によって定義されたフィルタ ルールをパケットがパスするのを許可します。in/out は、次のことを意味します。 *in*：アップストリーム パケットのフロー *out*：ダウンストリーム パケットのフロー
ステップ 3	`router(config-gw-hotline)# http access-group <num> redir-url` *url*	フィルタ ルールをパスするパケットがドロップされ、URL が指定されているダウンストリームの HTTP パケットが MS に送信されます。

次に例を示します。

```
router#show run | inc hotline
wimax agw hotline profile XYZ
   ip access-group 101 in passthru
   http access-group 102 redir-url www.hotlined.com
   ip access-group 101 out passthru
```

SLA プロファイルと同様に、AAA サーバはホットライン プロファイルを選択するだけです。ホットラインをディセーブルにするには、AAA サーバが「hotlining-exit」（大文字と小文字は区別されません）という特別なプロファイル名を選択します。この特別なプロファイル名を受信すると、BWG は加入者の通常のトラフィックを再開します。混乱を避けるため、この特別なプロファイル名を通常のホットライン プロファイル名に使用しないでください。

BWG で CoA ハンドリング機能をイネーブルにするには、次のタスクを実行します。

	コマンド	目的
ステップ 1	`router# aaa server radius dynamic-author` `server-key cisco`	

ユーザのホットライン状態を適切に考慮するには、ユーザのホットライン状態がアカウンティング ストリームに記録されている必要があります。AAA から受信された「Hotlining Indication」アトリビュートがアカウンティング開始/終了の記録の一部として含まれる必要があります。

アクティブ/中間セッション ホットライン

中間セッション ホットラインのフローを次に示します。

1. セッションの起動中に BWG が AAA Access Request を指示します。
2. AAA が Access Accept で応答します。
3. アクティブ セッションが起動し、AAA が加入者にホットラインを送信しようとします。
4. AAA からホットラインのプロファイル ID が必要とされていることを示す COA 要求が送信されます。
5. AAA に CoA Ack が送信されます。
6. BWG が各フローおよびホストの AAA に Accounting Stop を送信します。
7. BWG が各フローおよびホストのホットライン ID を持つ AAA に Accounting Start を送信します。

8. ホットライン セッション タイマーが開始されます。AAA から Session-Timeout の値が送信されていない場合、この値はデフォルトで 3600 秒に設定されます。Session-Timeout アトリビュートで指定された期間が経過し、セッションがホットライン化されているままの場合、セッションのティアダウンが開始します。
9. BWG により、コンフィギュレーションで指定された所定のフィルタ ルールがアップストリームまたはダウンストリーム トラフィックに適用されます。
10. AAA が変更され、加入者の通常のトラフィック フローが再開されます。
11. Hotline Profile ID = hotlining-exit であることを示す COA 要求が AAA から送信されます。
12. AAA に対し CoA Ack が送信されます。
13. BWG は各フローおよびホストについて Hotlining Indication を含む Accounting Stop を AAA に送信します。
14. BWG は各フローおよびホストについて Accounting Start を AAA に送信します。
15. BWG で加入者の通常のトラフィックが再開します。

新しいセッションのホットライン化

1. 特定の加入者をホットライン化するため AAA がプロビジョニングされます。
2. BWG は AAA Access Request を AAA サーバに送信します。
3. AAA は Access Accept で応答し、ホットライン プロファイルを強制適用します。
4. Accounting Start によりセッションのホットライン化が指示されます。
5. BWG が、コンフィギュレーションで指定された所定のフィルタ ルールによりアップストリームまたはダウンストリーム トラフィックへのセッションを確立します。
6. AAA が、COA によるセッションのホットライン化を終了するよう指示します。
7. BWG から COA-ACK が返されます。
8. BWG がアカウンティングのホットライン化を停止します。
9. BWG が通常のフロー / ホストのアカウンティングを開始します。
10. ユーザの通常のトラフィックが再開します。

（注）　ホットライン セッションの通常の Accounting Start を最初から開始しないでください。

AAA パケット オブ ディスコネクト メッセージ（PoD）

この機能により、接続済みのセッションを終了することができます。PoD（パケット オブ ディスコネクト）メッセージは RADIUS Access Request パケットで、セッションが RADIUS Access Accept パケットにより許可された後に AAA サーバがユーザとの接続を切断する場合に使用されます。

PoD メッセージのデータ パラメータは、次の RADIUS アトリビュートです。

表 2-11　PoD メッセージのパラメータ

アトリビュート	タイプ	説明	DR	DR-ACK	DR-NAK
User-Name	1	アクセス認証時に受信した MS の NAI	1	0	0
Calling-Station-Id	31	MS のバイナリ形式の MAC アドレス	1	0	0
AAA-Session-ID	26/1	User-Name と AAA-Session-ID に含まれる NAI により、NAS でセッションの一意の識別子が形成されます。	1	0	0
WiMAX-DM-Action-Code	26/60	登録解除アクション コードを AAA から NAS に伝送します。RADIUS Disconnect メッセージに WiMAX-DM-Action-Code がない場合はアクション コード 0xffff が使用され、NAS ではアクションコード 6 が使用されます。最終結果としては、BS が MS に RES-CMD を送信することになります。			

RADIUS Disconnect-ACK メッセージの送信時には、追加のパラメータは使用されません。

RADIUS Disconnect NACK メッセージのアトリビュートを次に示します。

アトリビュート	ID	AR	説明	ソース
Error-Cause	101	1		

PoD を受信するとセッションは終了し、R6 Data Path De-registration Request メッセージによりデータパスが BS に対してクリアされます。Disconnect-Request パケットは UDP ポート 3799 に送信され、識別属性により NAS（および終了するユーザ セッション）を識別します。NAS は RADIUS サーバにより送信された Disconnect-Request パケットに対して、関連付けられたすべてのセッション コンテキストが破棄されている場合（かつ、ユーザ セッションの接続が解除されている場合）には Disconnect-ACK、セッションの接続解除および関連付けられたすべてのセッション コンテストの破棄を NAS が実行できなかった場合には Disconnect-NAK で応答します。

BWG で PoD 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# aaa server radius dynamic-author server-key string`	BWG で PoD 機能をイネーブルにします。 **server-key**：共有秘密テキスト ストリングを設定します。 *string*：ネットワーク アクセス サーバとクライアント ワークステーションの間で共有する共有秘密テキスト ストリングです。この共有秘密ストリングは両方のシステムで同じである必要があります。

PoD 機能の検証とトラブルシューティングを行うには、次の作業を行います。

	コマンド	目的
ステップ 1	`router# debug aaa pod`	

AAA ベースの固定 IP アドレスのプロビジョニング

この機能を使用すると、MS ホストで使用できる固定 IP アドレスを指定できます。Framed-Route アトリビュートは変更されません。Framed-Route が AAA からダウンロードされると、固定 IP も検証されます。また、固定 IP ホストを許可するには、ユーザ グループで **ip static-allowed** コマンドを設定する必要があります。

固定 IP アドレスのアトリビュートを次に示します。

表 2-12

アトリビュート	形式/長さ	コメント
Static IP Address List	ストリング/253	加入者のホストはリストで指定されたアドレスに対してのみ割り当てられます。 A0.B0.C0.D0;A1.B1.C1.D1 リストには最大 10 件の固定 IP アドレスを指定できます。IP アドレスはドット形式または 16 進形式で指定できます。IP アドレスはセミコロン（;）、カンマ（,）、スペース（ ）のいずれかで区切られます。
Static IP Allowed	整数/4	この BWG 1.1 アトリビュートは、AAA から BWG へは送信されません。BWG 2.0 では、送信されても無視されます。

BWG では、複数のホストに同じ IP アドレスが割り当てられないようにする必要があります。AAA プロビジョニング エラーが発生した場合、同じ VRF コンテキストで IP アドレスの重複がないか確認されます。

固定 IP アドレス リストが AAA からダウンロードされ、**ip static-allowed** コマンドがユーザ グループで設定されている場合、**show wimax agw subscriber** コマンドを実行すると次のように表示されます。

```
MSID 0000.1005.1000
 CPE Type: 201
 CPE is non-nomadic
 Static IP allowed by user-group config
 Static IP address list downloaded
 Subscriber Age 000:17:55
...
```

固定 IP アドレス リストが AAA からダウンロードされ、**ip static-allowed** コマンドがユーザ グループで設定されている場合、**show wimax agw subscriber internal** コマンドを実行すると次のように表示されます。

```
MSID 0000.1005.1000
 CPE Type: 201
 CPE is non-nomadic
 Static IP allowed by user-group config
 Static IP address list downloaded
 Static IP address list:
  11.11.2.3       11.11.3.4       11.11.1.2       10.1.19.71      11.175.237.86
 Subscriber Age 000:18:24
```

ハンドオフ

WiMax では、ベース間と BWG 間の 2 種類のハンドオフを使用できます。BWG リリース 1.0 以降では、ベース間ステーション ハンドオフしか使用できません。

BS 間ハンドオフには、非制御ハンドオフと制御ハンドオフがあります。制御ハンドオフでは、ターゲット BS はハンドオフが実際に発生する前に R8 インターフェイス経由で稼動 BS からセッションの情報を取得します。非制御ハンドオフは、ターゲット BS が BWG でハンドオフを発生させる前にベース ステーション間で情報を交換できない場合に発生します。非制御ハンドオーバーは初期ネットワーク エントリと同様に扱われますが、このハンドオーバーについては、BWG は可動ベース ステーションで登録されたパスの登録を解除します。リリース 1.0 以降では、登録解除メッセージを稼動 BS に送信するための試行が 1 回行われると、ASN と SBS の間の登録解除ハンドシェイクが完了しているかどうかにかかわらず、ハンドオフが実行されます。

ハンドオフ時の中間アカウンティングの更新

リリース 2.2 以降では、ハンドオフ時に中間アカウンティングの更新を行うように BWG を設定できます。モバイル ステーション（MS）が他のベース ステーションに対してハンドオーバーを行うと、アカウンティングの更新が AAA サーバに送信されます。

中間アカウンティングの更新機能が有効になっていると、BWG によりフローベースのアカウンティングとホストベースのアカウンティングの両方についてアカウンティングの更新が送信されます。

中間更新の一部として送信されるアトリビュートは、ハンドオフ時に送信されるアカウンティングの更新の一部でもあります。また、新しい Cisco VSA 「Handover-Indicator =1」が含まれています。BS ID はターゲット ベース ステーション IP アドレスの BS ID に対応するように更新されます。

中間アカウンティングの更新は、次の機能については行われません。

- ホットライン化
- PoD

aaa accounting update handover コマンドを使用すると、中間アカウンティング機能が有効になります。

ハンドオフ時の中間アカウンティングの更新を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	router#**aaa accounting update handover**	ハンドオフ時のアカウンティングの更新をイネーブルにします。 このコマンドの no 形式を使用すると、アカウンティングの更新がディセーブルになります。 デフォルトでは、このコマンドはイネーブルです。
ステップ 2	router(config)#**aaa accounting update newinfo**	中間アカウンティングの更新をイネーブルにします。デフォルトでは、このコマンドはディセーブルです。
ステップ 3	router(config)#**aaa accounting update newinfo periodic 3**	中間アカウンティングの定期更新をイネーブルにします。 このコマンドは **update handover** コマンドと **update newinfo** コマンドが設定されている場合のみ実行コンフィギュレーションに表示されます。

次の表は、中間アカウンティングの更新の AAA-Authentication アトリビュートを示しています。

表 2-13　ハンドオフ時の中間アカウンティングの更新の AAA-Authentication アトリビュート

アトリビュート	タイプ	説明	開始	中間	停止
ハンドオーバー インジケータ	Cisco AVP	ハンドオーバーにより中間アカウンティングの更新が発生していることを示します。	0	0-1	0
BS-ID	26/46	UDR の生成時に MS を提供する NAP-ID ベース ステーションを一意に識別するオクテット ストリング。アカウンティングの更新がハンドオフにより発生している場合は、ターゲット BS に置き換えられます。	0-1	0-1	0-1

非制御ハンドオフ

非制御ハンドオーバーを示す信号はパス登録要求メッセージを使用して BS から BWG に送信されます。このメッセージには、ソース BS で確立済みの各サービス フローに関する情報が格納されています。また、ダウンリンク フローに使用する DP-IP も格納されています。

（注） セッションは同じ BWG で維持されるため、デバイスや加入者の再認証は必要ありません。

（注） 非制御ハンドオフでは、ターゲット BS はMS ネットワーク エントリを発生させます。このエントリで MS の認証が行われます。

BWG は以前の BS のパスの登録解除を開始します。この登録解除は BWG によりスケジュール設定されます。新しい BS へのハンドオフが正常に完了した直後に発生するとは限りません。

ハンドオフ時にベアラ パス データをバッファに入れる必要はありません。ハンドオーバー時に BWG で受信したダウンリンク データは破棄されます。

BWG がハンドオフのトリガーを受信する前にデバイスはすでにターゲット BS のサービス領域に移動しているため、以前のパスを通過中のトラフィックはすべて失われます。

ターゲット BS と BWG の間のハンドオフ処理が完了する間にデバイスが新しい BS に移動している場合があります。ハンドオーバーは制御されていないため、新しいハンドオフ イベントが処理される前に現在のターゲット BS へのハンドオフが完了します（必要に応じて R6 メッセージの再送信も行われます）。

ハンドオーバー交換は次の 3 種類のメッセージで構成されます（制御ハンドオフの場合のみ）。

- Path Registration Request（ターゲット BS から BWG に送信）：次の項目があります。
  - Registration Type
  - SF INFO（SFID を含む）、Reservation Action（[Create] に設定）、Direction、QoS パラメータ、Data Path Info、GRE Key（ダウンリンク フロー用）
  - BS INFO（BSID を含む）
- Path Registration Response（BWG からターゲット BS に送信）：次の項目があります。
  - Registration Type
  - SF INFO（SFID を含む）、Reservation Action（[Success] に設定）、Direction、Data Path Info、GRE Key（アップリンク フロー用）
  - BS INFO（BSID を含む）
- Path Registration Acknowledgement（ターゲット BS から BWG に送信）：次の項目があります。
  - Registration Type

BWG がハンドオーバーを許可しない場合、BWG は応答として「reject cause code TLV」を送信します。

BWG が目的のサービス フローのサブセットに対してのみハンドオーバーを許可した場合、このハンドオーバーは拒否されます。

セカンダリ フローが欠落していてもハンドオフは拒否されませんが、プライマリ フローが欠落している場合は拒否されます。

SBS に送信される登録解除要求と ACK の Registration Type は [Handover] となりますが、SBS からの登録解除応答は [Network exit] となります。これは予期された動作です。このメッセージを受信しても、BWG は「reject cause code TLV」が設定された ACK を送信しません。

制御ハンドオフ

制御ハンドオフが発生するのは、ターゲット BS が BWG でハンドオフをトリガーする前に、現在の BS とターゲット BS が情報を伝達し、サービス フロー、分類子などの詳細情報を交換できる状態になっている場合です。つまり、BWG ハンドオフ トリガーを送信する前に、ターゲット BS にはモバイル デバイスに関連するすべての情報が存在することになります。このトリガーは、モバイル デバイスが 802.16e の手順によりターゲット BS に接続済みの場合に発生します。制御ハンドオフが BWG で発生した場合、BS から Path Registration Request メッセージが送信されます。この場合、事前に認証交換は行われません（認証交換はネットワーク エントリ イベントで発生します）。

次のフロー シーケンスは、制御ハンドオフ時に発生するイベントを示しています。

ステップ 1　ターゲット ベース ステーションは Path Registration Request を BWG に送信します。このメッセージには、稼動ベース ステーションから受信したサービス フロー情報が格納されています。

ステップ 2　BWG は Path Registration Response で応答します。これにより、ターゲット ベース ステーションでのデータ パスの登録が許可されます。

ステップ 3　ターゲット ベース ステーションは Path Registration Acknowledgement で応答します。

ステップ 4　BWG は稼動ベース ステーションに Path Deregistration Request を送信します。

ステップ 5　稼動ベース ステーションは Path Registration Acknowledgement で応答します。

ステップ 6　BWG は Path Deregistration Acknowledgement でこの応答を確認します。

ステップ 7　ターゲット ベース ステーションは BWG に Context Report を送信します。

ステップ 8　BWG は Context Acknowledgement で確認します。

ステップ 9　ターゲット BS は CMAC Key Count Update メッセージを送信し、BWG は CMAC Key Count Ack メッセージで応答します。

設定の確認

BWG のハンドオフ統計情報を表示するには、**show wimax agw statistics section handoff** コマンドを使用します。

次に設定の例を示します。

```
Router#show wimax agw statistics section handoff
Message type Successful Handoff
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Handoff Registration Request
   Number of messages sent 0
   Number of messages received 2
   Number of messages resent 0
  Message type Handoff Registration Response
   Number of messages sent 2
   Number of messages received 0
   Number of messages resent 0
  Message type Handoff Registration Ack
   Number of messages sent 0
   Number of messages received 2
   Number of messages resent 0
  Message type Handoff Deregistration Request
   Number of messages sent 2
   Number of messages received 0
   Number of messages resent 0
  Message type Handoff Deregistration Response
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Handoff Deregistration Ack
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
```

セキュリティ コンテキスト交換

BS でエアーリンクをセキュリティ保護するには、BWG からキー関連情報を取得する必要があります。BS やデバイスの観点から見れば、データ パスの登録が完了し、BS がキー関連情報を受信するまで、ハンドオフを正常に実行することはできません。BS は両方の処理の実行を担当しています。BWG は BS とのコンテキスト交換を、ハンドオーバーとはまったく別のイベントとして処理します。

コンテキスト交換はどの時点でも発生します。BS へのキー関連情報の転送には、AK 転送プロトコルが使用されます。この情報は AK、AKID、AK ライフタイム、AK シーケンス番号、EIK で構成されています。

PMK の有効期間が経過した場合、新しい PMK を作成する必要があります。

セキュリティ コンテキスト交換には 2 つのメッセージが使用されます。

- Context Request（ターゲット BS から BWG に送信）：次の項目があります。
  - Context Purpose Identifier
  - BS Info
  - Target BS ID
- Context Report（BWG からターゲット BS に送信）：次の項目があります。
  - MS Info
  - AK Context
  - AKID
  - AK lifetime
  - AK SN
  - CMAC Key count
  - Target BS Info
  - Target BS ID

R6 インターフェイスでのキープアライブのサポート

キープアライブ メカニズムは BWG と Base-Station（BS; ベース ステーション）の間の R6 インターフェイス経由で使用します。これにより、各ネットワーク要素（NE）は障害の検出やピアの再起動ができるようになります。NE は障害の検出やピアの再起動を行う場合に所定の処理（対応する MS コンテキストを規定の方法で消去するなど）を行う場合があります。キープアライブ メカニズムでは、ベース ステーションと BWG の間で Keepalive-Req メッセージと Keepalive-Rsp メッセージが定期的に送信されます。

キープアライブ メッセージの送信は、ベース ステーションと BWG の双方で個別にイネーブルまたはディセーブルにできます。

（注）　BWG または BS が R6 Keepalive-Req メッセージを受信すると、ベース ステーションに加入者がない場合でも Keepalive-Rsp 応答を送信する必要があります。

各 R6 インスタンスについて、ベース ステーションと BWG には次のパラメータが保存されています。

Tk：キープアライブ タイマー

N：連続して発生しているキープアライブ障害の件数。初期値は 0 です。

M：連続して発生するキープアライブ障害の最大許容件数

Pm：セッションの有効期間。ピアの再起動の検出時にセッションを消去する場合に使用します。

R：最終リセット時刻（LRT）。初期値はノードの再起動時刻です。

キープアライブ機能をイネーブルにするには、ベース ステーション グループ サブモードで次の作業を行います。

	コマンド	目的
ステップ 1	router# router(config-wimax-agw-bs)#[no] reference-point r6 keepalive	BWG でキープアライブ機能をイネーブルにします。
	router(config-wimax-agw-bs)#reference-point r6 keepalive timeout <Tk-value>	*Tk* はベース ステーション グループで設定できます。範囲は 30 ～ 65535 秒です。デフォルト値は 60 です。
	BWG(config-wimax-agw-bs)#reference-point r6 keepalive max-failures-allowed <M-value>	*M* はベース ステーション グループで設定できます。範囲は 2 ～ 255 です。デフォルト値は 5 です。
	router(config-wimax-agw-bs)#reference-point r6 session-maturity-period <Pm-value>	*Pm* はベース ステーション グループで設定できます。範囲は 1 ～ 30 秒です。デフォルト値は 5 秒です。

N と R は以下の説明で使用する変数です。

キープアライブ統計情報は次のコマンドで表示されます。

```
router#show wim agw path

Path type Sig-UDP
 State current Ready, old Purging
 Number of sessions connected 1
 Number of old sessions connected 0
 Address local 11.1.27.1(AF_INET), remote 10.1.27.1(AF_INET)
 UDP port local 2231(0x8B7), remote 2231(0x8B7)
 Identification Peer 0x0A011B010000, Our 0x0B011B01
 R6 Version CISCO
 Keepalive Last Reset Time Peer 1244845152, Our 1245156882
 Keepalive timer expires in 00:00:20, timeout 30 secs
 Keepalive consecutive failures max allowed 5, current 0
 Keepalive Request received valid 0, invalid 0
 Keepalive Response received valid 1, invalid 0
 Keepalive Request sent success 2, fail 0
 Keepalive Response sent success 0, fail 0
 IP-GRE traffic sent 18 packets, 2601 bytes
 IP-GRE traffic received 14 packets, 1629 bytes
```

キープアライブ機能の動作

キープアライブ機能の内容は、次のとおりです。

1. ベース ステーションまたは BWG が Keepalive-Req を送信し、タイマー Tk を開始します。
2. Keepalive-Rsp の受信時に N の値が 0 になります。
3. Tk の有効期間が経過すると、ノードは次の Keepalive-Req を送信します。最後の Keepalive-Req メッセージが、タイマー Tk の有効期間が経過する前に受信されなかった場合、**N** の値が増加します。
4. **N** の値が **M** と等しい場合、**N** は **0** にリセットされ、リモート ノードで確立されているすべての R6 セッションが、ネットワーク主導 MS ネットワーク終了と同じ手順で終了されます。

BWG キープアライブ送信者機能は次のように機能します。

- 最初の加入者（MS）が BS からのネットワーク エントリを実行すると、BWG は Keepalive-Req メッセージを BS に送信します。

- BS からのすべての加入者が登録解除しネットワークを終了すると、BWG は BS への Keepalive-Req メッセージの送信を停止します。
- BWG は上記の手順で定期的に Keepalive-Req を BS に送信します。
- BWG は BS に送信するすべての Keepalive-Req メッセージと Keepalive-Rsp メッセージに LRT TLV を記録し、最終再起動時刻を通知します。

BWG キープアライブ受信者機能は次のように機能します。

- BWG は BS から Keepalive-Req を受信し、BS に Keepalive-Rsp で応答します。
- BWG から BS に対して送信されるすべての Keepalive-Req について､BWG は上記のように BS から Keepalive-Rsp を受信します。
- BWG は BS からの Keepalive-Req メッセージまたは Keepalive-Rsp メッセージから LRT 値を抽出します。BWG は最初に LRT 値を取得した時点で LRT 値を保存します。
- それ以降に BS から Keepalive-Req と Keepalive-Rsp を受信すると、BWG は受信した LRT 値を保存済みの値と比較します。受信した LRT 値が保存済みの値と異なる場合、BWG は BS が再起動されていると判断してすべての加入者セッションをクリアし、BS の新しい LRT 値を保存します。新しいセッションがクリアされないようにするため、Pm より古いセッションはすべてクリアされます。

LRT 値は SR アクティブと SR スタンバイの間で同期されます。SR スタンバイがアクティブになると、キープアライブ機能は中断されることなく同じ LRT 値で再開されます。

reset-bs オプションによる CLI ベースのキープアライブ

従来は、BS と BWG はセッションで同期されない場合がありました。この問題を解決するには BWG をリロードするしかないものと考えられていました。BWG を再起動すると、キープアライブを送信してすべての BS をリセットできます。しかし、BWG をリロードするとすべての BS や CPE に影響が生じるため、この操作は乱暴な操作であると考えられています。

現在は、BWG と BS が同期状態にない場合、該当する BS をリセットできます。

BWG が特定の BS を再同期できるようにするには、次の作業を行います。

	コマンド	目的
ステップ 1	router#**clear wim agw path** 10.10.10.10 [**reset-bs**] router#**clear wim agw path** 10.10.10.10 **local** [**reset-bs**]	BWG が特定の BS をリセットできるようにします。

上記の設定では、10.10.10.10 が BS の IP アドレスです。**reset-bs** キーワードを使用すると、BWG はその特定の BS のセッションをすべて消去します（セッションが存在する場合）。さらに、BWG はキープアライブ メッセージを（現在のリセット時刻で）その BS に送信して BWG が再起動したことを通知し、これにより BS は確実にすべてのセッションを消去します。この特殊なキープアライブは、定期的なキープアライブがディセーブルの場合でも必ず送信されます。この場合再送信は実行されないため、コマンドは必要があれば複数回実行できます。

BWG に BS への加入者セッションがない場合、BS のパスは存在しません。BS のパスがない状態で CLI がトリガーされると、BWG は KA 要求を BS に送信しません。

show brief コマンドによるスタティック ホストとダイナミック ホストの識別

ハッカーは一般的に固定 IP を使用してネットワークのぜい弱性を探り当てます。このため、BWG にはすべてのホストとその固定 IP アドレスのリストを表示するコマンドが必要です。

この機能は、既存の **show wimax agw sub brief host** コマンドを強化したものです。出力結果の各行の末尾には「D」または「S」が追加されます。これはそれぞれダイナミック ホストとスタティック ホストを表します。

次に例を示します。

```
Router#sh wim agw sub br host
MSID           Index HostID         Address         DwnLk-SFID Idle Time
1000.2223.0001 1     1000.2223.0002 4.4.0.2         1          00:01:54 D
1000.2223.0001 2     ----.----.---- 4.4.0.3         3          00:00:18 S
```

ホスト キャッシング機能では、ダイナミック ホストは [Idle Time] が「*xxx*」になっています。現在は、ダイナミック ホストが LRU アルゴリズム用にアイドル時間を記憶する必要があるため、このような形にはなっていません。

セッション冗長性

BWG セッション冗長性アーキテクチャでは、1:1 冗長性モデルのユーザ セッション フェールオーバー機能があり、すべてのアクティブ BWG に対してスタンバイ BWG が存在します。アクティブ BWG は必要に応じて状態同期のための状態情報をスタンバイ BWG に送信します。アクティブ BWG で障害が発生した場合、既存のすべてのセッションにサービスを提供するために必要な状態情報はスタンバイ BWG にあります。その後、スタンバイ BWG がアクティブ BWG となり、ユーザ セッションのサービスを開始します。これによりセッション冗長性が実現されます。元のアクティブ BWG がオンライン状態に戻ると、この BWG は現在のアクティブ BWG に対するスタンバイ BWG となり、現在のアクティブ BWG から既存のすべてのセッションの状態情報を取得します。

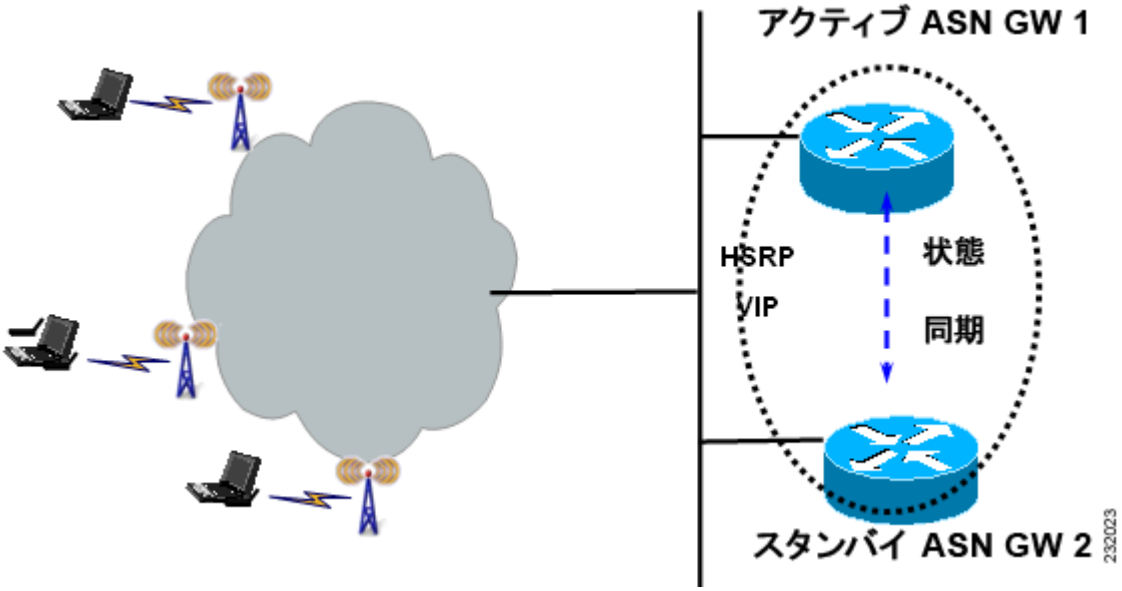
BWG は SAMI ブレードにホストされており、カードツーカード冗長性がサポートされています。つまり、SAMI で 1 つのプロセッサ ユニットの障害が発生すると、カード全体が切り替えられます。

（注） Cisco BWG リリース 1.1 では、セッション冗長性は引き続きサポートされています。しかし、各サービス フロー方向の分類子情報と CS の種類の情報の設定が、スタンバイ側とアクティブ側の両方で同一である必要があります。ホスト データ構造に新しく導入されたフィールドは、アクティブ側からスタンバイ側に同期されます。

BWG セッション冗長性とハイ アベイラビリティ インフラストラクチャ

BWG セッション冗長性は、Cisco IOS Hot Standby Routing Protocol（HSRP）、Cisco IOS Check-point Facility（CF）、Redundancy Framework（RF）、Stream Control Transmission Protocol（SCTP）に基づいて、デバイス間の冗長性とハイ アベイラビリティを実現する機能です。図 2-1 に、IOS HA インフラストラクチャにおける BWG SR のシステム概要図を示します。

図 2-1　BWG でのセッション冗長性



加入者管理

加入者情報には、加入者コンテキストに関連するセッションとフローがあり、作成やアップデートが行われる他、最終的には削除されます。

加入者情報は次の詳細情報で構成されています。

- 認証情報（方式、キー入力情報など）
- アドレッシング情報（MS MAC、割り当てられた DHCP アドレスなど）
- VRF 名
- ユーザ名
- セッション情報（シグナリング アドレス、関連するタイマーなど）
- セッションごとのフロー情報（および関連するフローごとの QoS 情報）

DHCP と AAA

BWG は DHCP リレー モードをサポートしており、DHCP サーバにより割り当てられたクライアントの IP アドレスを追跡しています。これにより、将来の DHCP メッセージがクライアントからサーバにリレーされるようになります。クライアントの IP アドレスと DHCP サーバの IP アドレスは加入者コンテキストに保存され、スタンバイ側と同期されます。スタンバイ側がアクティブになると、引き続き DHCP メッセージをクライアントから所定のサーバにリレーします（プライマリとセカンダリの 2 つのサーバが設定されている場合があります）。

IOS AAA はこの時点では HA に対応していないため、AAA 関連情報の同期はセッション レプリケーションの一部として実行されます。

ダイナミック同期

アクティブ側で障害が発生した場合にアクティブ側の処理をスタンバイ側が引き継げるようにするため、アクティブ側のすべてのセッションとフローに関する情報は明確な同期ポイントでスタンバイ側にダイナミックに同期されます。セッション、フロー、パスに関連する情報の同期には、個別の TLV が使用されます。新しいセッションまたはフロー イベントのダイナミック同期が実行されるのは、スタンバイ側がホット スタンバイ状態になった後と、バルク同期が完了した後です。

次のリストは、現在の同期ポイントを示しています。

- 初期ネットワーク エントリ時にセッションとフローの情報がスタンバイ側に同期されるのは、Initial Service Flow（ISF; 初期サービス フロー）が作成された後のみです。
- ISF が起動すると、アクティブ側で作成された新しいフローはそれぞれ個別にスタンバイ側に同期されます。
- サービス フローに何らかのアップデートが行われると、フローはスタンバイ側に同期されます。
- アドレスの割り当てが発生するたびに、フローはスタンバイ側に同期されます。
- アクティブ側のパスに対する変更はすべてスタンバイ側に同期されます。
- ハンドオフ時には、フロー情報はハンドオフの完了後に限りスタンバイ側に同期されます。クローニングされたフローは同期されません。ハンドオフの結果アクティブ側で新規作成されたフローは、FLOW UPDATE メッセージによりスタンバイ側に同期されます。このメッセージにより、ハンドオフの結果変更されたパラメータが伝送されます。
- アクティブ側からの中間アカウンティング要求の送信後のフロー同期。これにより、FLOW UPDATE メッセージがアクティブ側からスタンバイ側に送信され、中間アカウンティングのアップデートの一部として AAA に送信されるアカウンティング カウンタが所定のメッセージにより伝送されます。

セッション冗長性の設定

セッション冗長性を設定する前に、次の設定作業が必要です。

- インターフェイスで HSRP を設定する。
- デバイス間の冗長性を設定する。
- RF チェック ポイント用の SCTP を設定する。
- Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバを設定する。
- アクティブ BWG とスタンバイ BWG で AAA を設定する。

BWG でセッション冗長性を設定するには、次の作業を行います。

	コマンド	目的

ステップ 1	`Router#interface FastEthernet0/1`
	`  description BS-If`
	`  ip address 9.11.44.147 255.255.255.0`
	`  standby 100 ip 9.11.44.100`
	`  standby 100 name CORE`
		インターフェイスに HSRP を設定します。

ステップ 2	`Router# redundancy inter-device` `  scheme standby CORE`	デバイス間コンフィギュレーション モードを有効にし、Stateful Switchover（SSO）トラフィックをイネーブルにして保護できるようにします。

	コマンド	目的
ステップ 3	Router#ipc zone default association 1 no shutdown protocol sctp local-port 5000 local-ip 9.11.44.147 remote-port 5000 remote-ip 9.11.44.159	RF チェック ポイント用の SCTP を設定します。
ステップ 4	Router#config terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#ntp server 129.237.32.2 Router(config)#^Z	（推奨）**ntp server** コマンドの後に NTP サーバの IP アドレスまたはホスト名を入力すると、ルータが既存の NTP サーバを使用するよう設定されます。
ステップ 5	Router(config)#ip radius source-interface Loopback *Loopback number* さらに、ルータのループバック インターフェイスを次のように設定します。 interface Loopback0 ip address 192.168.0.250 255.255.255.255	両方の BWG で **ip radius source-interface Loopback** を設定すると、AAA サーバが 2 つの BWG を 1 つのまとまりとして表示できるようになります。
ステップ 6	Router(config)# **wimax agw redundancy**	BWG でセッション冗長性をイネーブルにします。
ステップ 7	Router(config)# **subscriber redundancy rate 500 1**	SR の同期率を指定します。

設定例

この設定を行うのは AAA のみです。

アクティブ BWG

```
------------------------------------------------------------

!
interface Loopback192
 ip address 192.168.0.70 255.255.255.255
!
!
aaa group server radius car-sg
 server 1.8.70.99 auth-port 1812 acct-port 1813
!
aaa authentication dot1x car_auth_list group car-sg
aaa accounting network car_acct_list start-stop group car-sg
!
!
ip radius source-interface Loopback192
radius-server host 1.8.70.99 auth-port 1812 acct-port 1813
radius-server key r6AAA
radius-server vsa send accounting wimax
radius-server vsa send authentication wimax
!
```

スタンバイ BWG

```
------------------------------------------------------------


!
interface Loopback192
 ip address 192.168.0.70 255.255.255.255
```

```
!
!
aaa new-model
!
!
aaa group server radius car-sg
 server 1.8.70.99 auth-port 1812 acct-port 1813
!
aaa authentication dot1x car_auth_list group car-sg
aaa accounting network car_acct_list start-stop group car-sg
!
!
ip radius source-interface Loopback192
radius-server host 1.8.70.99 auth-port 1812 acct-port 1813
radius-server key r6AAA
radius-server vsa send accounting wimax
radius-server vsa send authentication wimax
```

BWG の設定の例（アクティブ側）

```
           interface GigabitEthernet0/0.70
              description to AAA/DHCP
 encapsulation dot1Q 70
 ip address 1.8.70.147 255.255.255.0
 standby 70 ip 1.8.70.70
 standby 70 follow P7_REDUNDANCY
```

（注） タイムゾーンが変更される場合は BWG をリロードします。

次の設定例には、DHCP に関する情報が含まれています。

```
interface Loopback102
    ip address 102.0.0.1 255.255.255.0
  !
   user-group domain eaptls.com2
   aaa accounting method-list AAA-ACC1
   aaa authentication method-list AAA-AUTHN1
   dhcp gateway address 102.0.0.1
   dhcp server primary 27.0.0.8
   service-flow pre-defined isf profile sf3
   service-flow pre-defined secondary 1 profile sf4
   vrf VRF_2
```

認証

加入者は、セッションまたはフローがスタンバイ側で再作成される前に、アクティブ側で EAP により認証されます。関連付けられた MSK、AK コンテキスト、その他の証明書をセッション ステートフル データとあわせてスタンバイ側に転送する必要があります。地理的冗長性が導入されている場合、このデータを保護する必要があります。スタンバイ側がスイッチオーバーの後にアクティブになり、同じ加入者が新しいアクティブ側で再認証される場合、元のアクティブ側での認証と同じ手順で認証が行われます。

アカウンティング

アカウンティングの開始、停止、中間アップデートはアクティブ側からのみ送信されます。スタンバイ側は、アクティブになった場合を除き、アカウンティング レコードを送信することはありません。

スタンバイ側でのセッションまたはフローの再作成の一部として、IOS AAA データベースに各セッションおよびフローのアカウンティング レコードが登録されます。たとえば、「class」アトリビュートとアカウント セッション ID はアクティブ側からスタンバイ側に同期され、関連するアカウンティング レコードに保存されます。これにより、スタンバイ側がアクティブになると、正しい情報が記録されたアカウンティング レコードを送信できるようになります。

アカウンティング カウンタの同期は、AAA 中間アカウンティング アップデート機能の一部です。AAA 中間アカウンティング アップデート機能がイネーブルの場合、アクティブ BWG はアカウンティング レコードを AAA サーバに送信します。さらに、同じイベントを使用して FLOW UPDATE イベント（AAA サーバに送信されたものと同じアカウンティング カウンタが使用されます）が開始されます。逆に、アクティブ側でこの機能がディセーブルの場合、AAA に対するアカウンティング アップデートがないため、アカウンティング アップデート同期メッセージがスタンバイ側に送信されることはありません。BWG SR 機能単独ではアカウンティング カウンタの同期を実行しません。

アカウンティング セッション ID はアカウンティング イベント（開始、停止、中間）で使用される重要なアトリビュートで、AAA サーバでレコードの生成に使用します。これは 4 バイトの未使用の整数で、ASNWG 内で一意に割り当てられます。さらに、ロールオーバーするまで順番に値が増加していきます。新しいアクティブ側でスイッチオーバー時に一意のアカウンティング セッション ID の生成を継続できるようにするため、新しいアカウンティング セッション ID は元のアクティブ側での最後のアカウンティング セッション ID から始まります。

加入者 IP アドレス

現在、加入者 IP アドレスは DHCP サーバによって割り当てられ、ホスト ルートが挿入されています。スタンバイ側が加入者セッションを再作成すると、同じホスト ルートがスタンバイ側にも挿入されます。スタンバイ側はアクティブになるまで DHCP クライアントとサーバの間での DHCP メッセージのリレーを実行しません。

QoS

BWG リリース 1.0 以降では、フローが作成されてそのフローの QoS パラメータが BS に送信された後に、アクティブ BWG がすべての QoS パラメータをスタンバイ側に同期します。これらのパラメータのうち、スタンバイ BWG に同期されたフローの DSCP コードは、スタンバイ BWG がアクティブになった時点でパケットのマーク付けに使用されます。

統計情報とカウンタ

統計情報とカウンタはスタンバイ側には同期されません。かわりに、スタンバイ側はアクティブ側からのステートフル データの処理時にこれらの情報を再構築し、セッションやフローの作成、変更、削除を行います。たとえば、スタンバイ側でセッションやフローの作成と削除を行うと、スタンバイ側でのセッションやフローの数がアップデートされます。スタンバイ側で受信した R6 メッセージの数は、スタンバイ側がアクティブになり R6 メッセージの受信を開始した時点から累積されていきます。

BWG ロード バランシング

ロード バランサを実行する場合、ロード バランサはすべての BWG の負荷情報を使用して、いずれかの BWG を選択し、BS から受信した NetEntry メッセージ（SS/MS に関連するもの）を選択した BWG に転送します。

Dynamic Feedback Protocol（DFP）が設定されている場合、アクティブ BWG は定期的に負荷情報をロード バランサに送信します。スタンバイ BWG は R6 メッセージの処理やユーザ トラフィックの処理を行わないため、スタンバイ BWG はフィードバックを送信せず、正確な負荷情報も保有していません。スタンバイ側がアクティブになると、スタンバイ側が R6 メッセージの処理とユーザ トラフィックの処理を進めるにつれ、正確な負荷情報が構築されていきます。そのため、現在の正確な負荷についてフィードバックを送信できるようにするための調整期間があります。

データ パスと GRE

フローのデータ パスはスタンバイ側で再作成されます。フローのアップストリームとダウンストリームの両方の GRE キーがスタンバイ側に同期されます。スイッチオーバー時に、新しいアクティブ側は、ローカルで割り当てられたすべての新しい GRE キーが、元のアクティブ側で割り当てられた使用中の GRE キーと競合しないようにします。

バージョン制御

上位のバージョンへのアップグレードは、直前のソフトウェア バージョンからであれば可能です。ソフトウェア バージョンのダウングレードはできません。たとえば、BWG の冗長ペアがバージョン A で実行されていて、次のソフトウェア バージョンがバージョン B である場合、バージョン A から B へのアップグレードは可能です（B から A へのバージョン変更はできません）。この場合、下位のバージョンから同期されたステートフル データを上位のバージョンが理解できることが必要になります。

制限事項

BWG のセッション冗長性には、次の制限事項があります。

- アカウンティング カウンタの同期

  これは設定可能であり、イネーブルにする AAA 中間アカウンティング アップデート機能により設定が異なります。AAA 中間アカウンティング機能がディセーブルの場合、BWG SR はデフォルトではアカウンティング データ/ペイロード カウンタの同期は行いません。これにより十分な処理が行われない場合があります。たとえば、2 件の連続した中間アップデートの間にスイッチオーバーが発生した場合、新しい中間アップデートでは新しいアクティブ側でのカウントのみが送信されるため、前回の中間アップデート以降に累積されたカウントは失われます。また、スイッチオーバーの直前に STOP が失われる場合があります。

（注） シグナリング カウンタは同期されません。

（注） スタンドアロン システムの場合、現在の AAA/Radius カウンタは正確に動作します。しかし、セッション冗長性がイネーブルの場合、フロー（Radius の場合はセッション）の経過期間を現在のカウンタにもとづいて算出していると、この経過期間の値が正確でない場合があります。そのため、特定のフローが開始されてから経過した秒数を表す「session_elapsed_time」という ASN-GW から別のアトリビュートが送信されます。

- スタンバイ側でのセッションの消失

  SCTP では確実な転送が行われますが、輻輳が発生したり、再試行回数が最大に達したりすると、セッションのレプリケーションに使用するステートフル データが失われる場合があります。この場合、スタンバイ側でのセッションの再作成は実行されません。スイッチオーバーが発生している場合、このセッションは喪失します。

- スタンバイ側での古いセッション

  上記と同じ理由で、セッション削除のためのステートフル データが消失した場合、アクティブ側でセッションが削除されてもスタンバイ側では削除されません。

  - 同じ加入者の次のセッションが作成される前にスイッチオーバーが発生しない場合、同じ加入者に対するセッションの新規作成の次回の同期時に、この古いセッションが消去されることになります。
  - スイッチオーバーが発生する場合、手動操作やアイドル/セッション タイムアウトなどの機能により消去されるまで、古いセッションが停止します。

- コール中の打ち切り

  コール設定が進行中で、最初の同期ポイントに達していない状態でスイッチオーバーが発生すると、コール設定が打ち切られるため、加入者はコールを再試行する必要があります。

スイッチオーバー

スイッチオーバーが発生すると、トラップが生成されて NMS システムに送信され、アクティブ ユニットで障害が発生し、スタンバイ側がアクティブになったことを通知します。次の動作が想定されています。

- ローカルで割り当てられたすべての新しい GRE キーが、元のアクティブ側で割り当てられた使用中の GRE キーと競合しないようにする必要があります。
- ローカルで割り当てられたすべての新しいアカウンティング セッション ID キーが、元のアクティブ側で割り当てられた使用中のアカウンティング セッション ID キーと競合しないようにする必要があります。
- 新しいセッションの DHCP リレーは設定済みの DHCP サーバに転送されます。
- 一部の統計情報は再生成されます。
- DFP の負荷情報が再構築され、ロード バランサに送信されます。

次のリストは、スイッチオーバーの原因となるイベントを示しています。

- ソフトウェアのクラッシュや CPU の負荷増大などによるルータのリロードやクラッシュ。
- HSRP が設定に基づきインターフェイスを追跡する場合。インターフェイス フラップ <on-off transition> を検出すると、HSRP は現在のアクティブ側を強制的にリロードし、これによりアクティビティのスイッチオーバーが発生します。
- 手動操作で、アクティビティを現在アクティブなルータから冗長ホット スタンバイ側に切り替えた場合。この操作は次のコマンドで行います。

  - **redundancy switch-activity force**

    このコマンドは、アクティビティを現在のアクティブ側から現在のホット スタンバイ側に切り替える場合に使用します。このコマンドを実行すると現在のルータがリロードし、現在のホット スタンバイ側がアクティブになります。また、現在アクティブなルータが再起動すると、ホット スタンバイ状態になります。

  - **reload**

    これは通常のルータ リロード コマンドで、スイッチオーバーが発生します。現在アクティブなルータがリロードし、現在のホット スタンバイ側がアクティブになります。

BWG ロード バランシング

ロード バランシングの目的は、ベース ステーション間の情報伝達を妨げずに BWG のスケーラビリティを確保することです。このスケーラビリティは BWG 間でのロード バランシングによって実現できます。ロード バランシングでは、BS から見るとクラスタが単一の BWG として表されます。これにより、ベース ステーションの接点は 1 か所となります。また、システムに新規に追加されたどの BWG もベース ステーションのプロビジョニングには影響しません。

（注） サーバ ロード バランシングとセッション冗長性は Cisco 7600 SAMI プラットフォームでのみ使用できます。

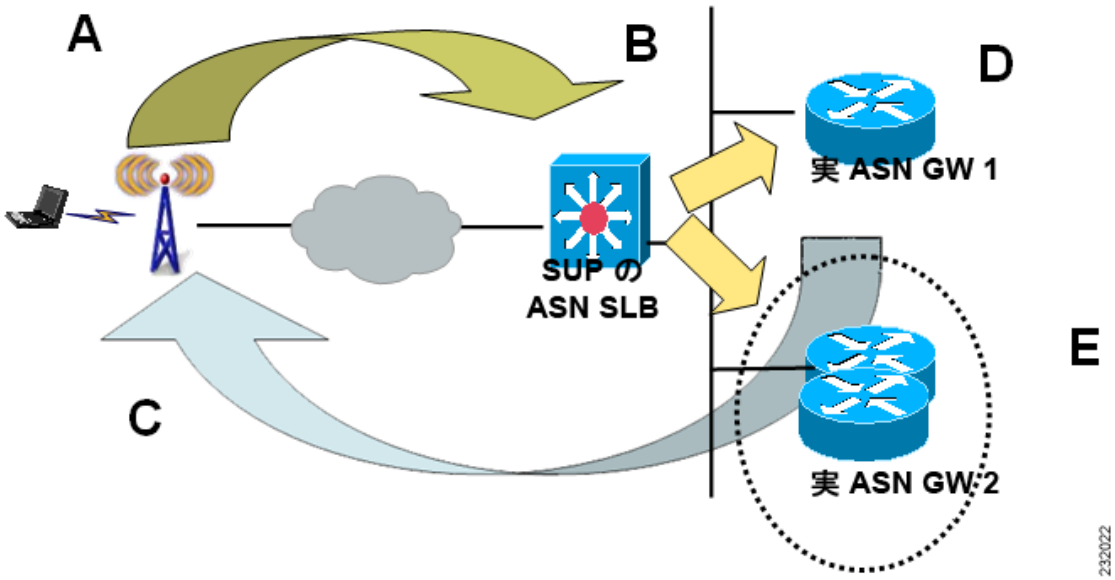
BWG のロード バランシングは、IOS サーバ ロード バランシング（SLB）機能に基づいています。BS には SLB のバーチャル IP アドレスが BWG ID として設定されています。ロード バランシングの BWG 選択フローを次に示します。dispatch モードと directed モードの両方を使用できます。SLB では DFP により実 BWG の負荷を検出できます。

（注） リリース 1.0 以降では、SLB スティッキ機能と BWG ハンドオーバー コール フローは使用できません。

初期コンテキスト要求が処理されると、SLB で作成されたセッションは再送信のため維持されます。維持する時間は設定可能です。この時間内に特定の MS/SS についてコンテキスト要求の再送信が検出されると、SLB はこの再送信された要求を同じ実 BWG に転送します。これは最初のコンテキスト要求で選択された BWG です。

SLB では DFP により実 BWG の負荷を検出できます。実 BWG にはそれぞれ確立できるセッション数の上限があります。実 BWG の負荷は、現在存在するセッション数と、確立可能なセッション数の上限、メモリの使用状況、帯域体の使用状況に基づき、この BWG 自体により計算されます。この負荷情報は SLB に送信されます。SLB は、ラウンドロビン方式または最小接続方式で初期コンテキスト要求を実 BWG のいずれかに転送します。DFP により計算された負荷が 100% の場合、BWG はそれ以上のセッションを許可しません。このため、この方式では CAC も使用できます。

図 2-2　BWG でのサーバ ロード バランシング



BWG の選択

- 初期ネットワーク エントリ段階で、BS は SS/MSS に対応する NetEntry MS Pre-Attachment Request をデフォルトとして設定されている BWG に送信します。
- BWG は NetEntry MS Pre-Attachment Response を BS に送信します。この応答には、代替オーセンティケータ ID の IP アドレスが含まれている場合があります。これにより、これ以降の SS/MSS に対応するトランザクションを処理できるようになります。BS は NetEntry MS Pre-Attachment Response を受信すると、NetEntry MS State Change Ack を送信してトランザクションを完了します。
- これ以降の SS/MSS に対応するトランザクションはすべて、BS と NetEntry MS Pre-Attachment Response メッセージで指定された BWG との間で発生します。

動作モード

BWG には次の 2 つの動作モードがあります。

- dispatched モード：このモードでは、パケットは実サーバに送信され、元のパケットは変更されません。実サーバではバーチャル IP と同じ IP でループバックが設定されています。実サーバは送信元アドレスとしてバーチャル IP アドレスを使用して応答します。
- directed モード：パケットの送信先 IP アドレスが書き換えられ、BWG の IP アドレスが選択されます。BWG でバーチャル IP によるループバックが設定されることはありません。

いずれのモードでも、選択された BWG は Pre-Attachment Response を送信します。

ロード バランシングの設定

ここでは、サーバ ロード バランシングに関する詳細設定の一覧を紹介します。これらの詳細設定は、特に明記されていない限り directed モード用です。

ロード バランシング設定作業のリスト

ここでは、ロード バランシングの設定に必要な作業の一覧を紹介します。必須作業とオプション作業が示されています。

1. Cisco IOS SLB で、次の作業を行います。
   a. サーバ ファームと実サーバの設定（必須）
   b. 仮想サーバの設定（必須）
   c. DFP サポートの設定（任意、ただし推奨）
2. Cisco 実 BWG で、次の作業を行います。
   a. SLB のループバック インターフェイスの設定（dispatched モードの場合は必須）
   b. BWG の DFP サポートの設定（任意、ただし推奨）

Cisco IOS SLB のロード バランシング設定

ここでは、サーバ ファームと実サーバの設定方法について説明します。Cisco IOS SLB サーバ ファームを設定するには、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実行します。

	コマンド	目的
ステップ 1	`Router-SLB(config)# ip slb serverfarm serverfarm-name Router(config-slb-sfarm)#`	Cisco IOS SLB 設定にサーバ ファーム定義を追加し、サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 2	`Router-SLB(config-slb-sfarm)# nat server`	サーバ ファームで NAT サーバ アドレス変換モードを設定します。
ステップ 3	`Router-SLB(config-slb-sfarm)# real ip-address [port]`	BWG のバーチャル テンプレート インターフェイスの IP アドレスを使用して、実 BWG をサーバ ファームのメンバとして識別し、実サーバ コンフィギュレーション モードを開始します。
ステップ 4	`Router-SLB(config-slb-real)# weight weighting-value`	（任意）サーバ ファーム内の他のサーバに対する実サーバの作業負荷を指定します。 （注）　DFP を使用する場合、**weight（サーバ ファーム）**コマンドで定義した静的重み付けは DFP が計算した重み付けにより上書きされます。DFP がネットワークから削除されている場合、Cisco IOS SLB は静的重み付けに戻ります。
ステップ 5	`Router-SLB(config-slb-real)# in service`	実サーバを Cisco IOS SLB で使用できるようにします。

設定例

```
ip slb serverfarm ASNGW-SR-SF
       nat server
 probe PINGPROBE
         !
 real 11.11.11.50
   weight 0
           inservice
         !
         real 11.11.11.70
           weight 0
                inservice
```

実 BWG の設定

BWG のロード バランシング設定

BWG でロード バランシングを設定するには、次の各項で所定の作業を行います。

- 「SLB のループバック インターフェイスの設定」
- 「BWG を DHP エージェントとして設定」（任意、ただし推奨）

SLB のループバック インターフェイスの設定

ロード バランシングをイネーブルにするには、ループバック インターフェイスにファームの 各 BWG の Cisco IOS SLB の仮想サーバと同じ IP アドレスを設定する必要がります。

ループバック インターフェイスを作成するには、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実行します。

	コマンド	説明
ステップ 1	`Router(config)# interface loopback number`	ループバック インターフェイスを作成します。ループバック インターフェイスは、常にアップ状態にある仮想インターフェイスです。
ステップ 2	`Router(config-if)# ip address ip-address mask`	IP アドレスをループバック インターフェイスに割り当てます。

BWG を DHP エージェントとして設定

DFP マネージャ（ここでは Cisco IOS SLB）が DFP エージェントへの接続に使用するポート番号を定義するには、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順番に入力します。

	コマンド	説明
ステップ 1	`Router-ASNGW(config)# ip dfp agent agw`	DFP エージェント サブシステムを指定し、DFP エージェント コンフィギュレーション モードを開始します。

ステップ 2	`Router- ASNGW(config-dfp)# port` *port-number*	DFP マネージャが DFP エージェントへの接続に使用するポート番号を定義します。
ステップ 3	`Router- ASNGW(config-dfp)# inservice`	DFP マネージャとの通信に使用する DFP エージェントをイネーブルにします。次の両方の条件が満たされるまで、DFP エージェントは非アクティブとなります。 • DFP エージェントが **inservice**（DFP エージェント）コマンドでイネーブルにされている。 • クライアント サブシステムにより DFP エージェントが変更されている。

設定例

```
ip dfp agent agw
    port 5555
    inservice
```

BWG でロード バランシングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# virtual` *x.y.z.m* `udp` *port* *no* `service asnr6`	BWG でロード バランシングをイネーブルにします。仮想サーバ コンフィギュレーション コマンドが拡張され、ASN をサポートします。
ステップ 2	`Router# idle asnr6 request` *timer value in seconds*	BWG のアイドル タイマー要求を設定します。

BWG の設定例

次の設定例は SAMI プラットフォームにしかあてはまりません。

スーパーバイザ カードの SLB 関連設定

```
7606-R6-sup720#show running-configuration | section slb
ip dfp agent slb
 port 5555
ip slb probe PINGPROBE ping
 interval 3
 faildetect 3
ip slb serverfarm ASNGW-SR-SF
 nat server
 probe PINGPROBE
 !
 real 11.11.11.50
  weight 0
  inservice
 !
 real 11.11.11.70
  weight 0
  inservice
ip slb vserver V-ASNGW-SR
 virtual 50.70.80.100 udp 2231 service asn r6
 serverfarm ASNGW-SR-SF
 idle asn r6 request 90
 inservice
ip slb dfp
 agent 11.11.11.50 5555 10 0 5
 agent 11.11.11.70 7777 10 0 5
7606-R6-sup720#
```

上記のスーパーバイザ カード設定に対応する、実 BWG の設定例です。

```
bwg-real-s4p5# show running-configuration | section dfp
ip dfp agent agw
 port 5555
 inservice
bwg-real-s4p5#

asngw-real-s4p7#sh runn | section dfp
ip dfp agent agw
 port 7777
 inservice
bwg-real-s4p7#
```

設定の確認

BWG でロード バランシングがイネーブルであることを確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **show ip slb session asnr6 [detail]**	ロード バランシング R6 セッションに関連する統計情報を表示します。
ステップ 2	Router# **show ip slb vserver detail**	vserver の統計情報の詳細を表示します。

設定例

BWG での SLB の **show** コマンドの設定例を次に示します。

```
7606-R6-sup720#show ip slb sessions asn r6

vserver         MSID             Base Station     real             state
---------------------------------------------------------------------------
7606-R6-sup720#show ip slb sessions asn r6

vserver         MSID             Base Station     real             state
---------------------------------------------------------------------------
V-ASNGW-SR      0000AAAAC38ECCCC 50.35.50.1       11.11.11.50      ASNR6_ESTAB
V-ASNGW-SR      0000AAAAC392CCCC 50.35.50.1       11.11.11.50      ASNR6_ESTAB
V-ASNGW-SR      0000AAAAC396CCCC 50.35.50.1       11.11.11.50      ASNR6_ESTAB
V-ASNGW-SR      0000AAAAC39ACCCC 50.35.50.1       11.11.11.50      ASNR6_ESTAB
V-ASNGW-SR      0000AAAAC39ECCCC 50.35.50.1       11.11.11.50      ASNR6_ESTAB
< S N I P P E D >

7606-R6-sup720#show ip slb vserver detail

V-ASNGW-SR, state = OPERATIONAL, v_index = 7, interface(s) = <any>
  virtual = 50.70.80.100/32:2231, UDP, service = ASNR6, advertise = TRUE
  server farm = ASNGW-SR-SF, delay = 10, idle = 3600
  asnr6: request idle = 90, Parse error pkt drops= 56,
         Number of reject responses = 0
  sticky: <none>
  sticky: group id = 0
  synguard counter = 0, synguard period = 0
  conns = 101, total conns = 509069, syns = 0,  syn drops = 0
  standby group = None
7606-R6-sup720#show ip slb reals

real                  farm name        weight  state          conns
-------------------------------------------------------------------
11.11.11.50           ASNGW-SR-SF      92      OPERATIONAL    83
```

```
11.11.11.70           ASNGW-SR-SF      92      OPERATIONAL    18
7606-R6-sup720#show ip slb serv
7606-R6-sup720#show ip slb serverfarms

server farm      predictor           nat   reals   bind id  interface(s)
-------------------------------------------------------------------------------
ASNGW-SR-SF      ROUNDROBIN          S     2       0        <any>
7606-R6-sup720#show ip slb sessions asn r6 de
7606-R6-sup720#show ip slb sessions asn r6 detail

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
   state = ASNR6_ESTAB, real = 11.11.11.50
   Key = 0000AAAAC38ECCCC, retry = 1

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
   state = ASNR6_ESTAB, real = 11.11.11.50
   Key = 0000AAAAC392CCCC, retry = 1

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
   state = ASNR6_ESTAB, real = 11.11.11.50
   Key = 0000AAAAC396CCCC, retry = 1

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
   state = ASNR6_ESTAB, real = 11.11.11.50
   Key = 0000AAAAC39ACCCC, retry = 1

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
   state = ASNR6_ESTAB, real = 11.11.11.50
   Key = 0000AAAAC39ECCCC, retry = 1

V-ASNGW-SR, client = 50.35.50.1:2231, virtual = 50.70.80.100:2231
   state = ASNR6_ESTAB, real = 11.11.11.50

< S N I P P E D >
7606-R6-sup720#
```

仮想サーバの設定

Cisco IOS SLB 仮想サーバを設定するには、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実行します。

	コマンド	目的
ステップ 1	`Router-SLB(config)# ip slb vserver virtual_server-name`	仮想サーバを指定し、仮想サーバ コンフィギュレーション モードを開始します。

ステップ 2	`Router-SLB(config-slb-vserver)# virtual ip-addr [netmask [group]] {esp | gre | protocol}`
	
	または
	
	`Router(config-slb-vserver)# virtual ip-addr [netmask [group]] {tcp | udp} [port | any] [service service]`
		仮想サーバの IP アドレス、接続の種類、オプションの TCP または UDP ポート番号、Internet Key Exchange（IKE）、Internet Security Association and Key Management Protocol（ISAKMP）、Wireless Session Protocol （WSP）の各設定、サービス カップリング

ステップ 3	`Router-SLB(config-slb-vserver)# serverfarm primary-farm [backup backup-farm [sticky]] [map map-id priority priority]`	実サーバ ファームと仮想サーバを関連付けます。 • **backup :**（任意）バックアップ サーバ ファームを設定します。 • **backup** *backup-farm* [**sticky**]：（任意）バックアップ サーバ ファームを設定し、オプションでバックアップ サーバ ファームでのスティッキ接続の使用を指定します。 • **map** *map-id* **priority** *priority*：（任意）IOS SLB プロトコル マップをサーバ ファームと関連付けて、そのマップのプライオリティを指定します。マップはプライオリティに基づいて検索されます。値が小さいほどプライオリティは高くなります。 **（注）** **map** キーワード オプションを設定すると **servermap** コマンドで複数のインスタンスを使用できます。デフォルトのサーバ ファーム（**map** キーワード オプションなし）では 1 つのインスタンスしか使用できません。 **（注）** マップ設定を変更するには、仮想サーバが非稼動状態である必要があります。 **（注）** 各マップで、プライマリおよびバックアップ サーバ ファームの NAT モードが一致している必要があります。
ステップ 4	`Router-SLB(config-slb-vserver)# idle [request] duration`	（任意）パケット アクティビティがない場合に Cisco IOS SLB が接続コンテキストを維持する最小時間を指定します。
ステップ 5	`Router-SLB(config-slb-vserver)# inservice`	仮想サーバを Cisco IOS SLB で使用できるようにします。

設定例

```
Router-SLB(config)# ip slb vserver V-ASNGW-SR
Router-SLB(config-slb-vserver)# virtual 50.70.80.100 udp 2231 service asn r6
Router-SLB(config-slb-vserver)#serverfarm ASNGW-SR-SF
Router-SLB(config-slb-vserver)# idle asn r6 request 90
Router-SLB(config-slb-vserver)#inservice
```

DFP サポートの設定

Cisco IOS SLB は DFP マネージャ、他の DFP マネージャ（Distributed Director など）の DFP エージェント、または同時にその両方として設定できます。ネットワーク設定によって、同一のデバイスまたは異なるデバイスで、コマンド入力により Cisco IOS SLB を DFP マネージャとして設定し、さらにコマンド入力により Cisco IOS SLB を DFP エージェントとして設定することができます。

Cisco IOS SLB を DFP マネージャとして設定し、Cisco IOS SLB が接続できる DFP エージェントを指定するには、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	説明
ステップ 1	`Router-SLB(config)# ip slb dfp [password [0|7] password [timeout]]`	DFP を設定し、オプションのパスワードを入力して、DFP コンフィギュレーション モードを開始します。
ステップ 2	`Router-SLB(config-slb-dfp)# agent ip_address port-number [timeout [retry_count [retry_interval]]]`	Cisco IOS SLB が接続できる DFP エージェントを指定します。

設定例

```
Router-SLB(config) # ip slb dfp
Router-SLB(config-slb-dfp)# agent 11.11.11.50 5555 10 0 5
Router-SLB(config-slb-dfp)# agent 11.11.11.70 7777 10 0 5
```

SLB スティッキ性のサポート

BWG 用の SLB では、R4 または R6 コントロール プレーン メッセージのロード バランシングができます。リリース 1.0 以降では、Pre-Attachment メッセージの基本的なロード バランシングのみができます。

BWG リリース 2.0 では次の機能を使用できます。

- BWS 向けのすべての種類の Wimax メッセージ（スティッキ エントリの有無を問わず、R4 参照ポイントと R6 参照ポイントの両方とも対象）。
- 使用可能なスティッキ エントリがない場合、Wimax ポートへのすべての R6/R4 メッセージは現在の DFP（または重み付けアルゴリズム）に基づいて、特定の実 BWG にロード バランシングされます。
- スティッキ MSID がすでに存在する場合は、BWG SLB はすべての Wimax コントロール プレーン メッセージをそれぞれ該当する実 BWG に転送します。

スティッキのアップデート

BWG は SLB にアップデート通知を送信します。認証が完了すると、BWG には MS のユーザ名（NAI）が設定されます。ISF（最初のフロー）が作成された直後に、BWG はスティッキ アップデートを SLB サーバに送信します。この中には NAI 値が含まれています。

スティッキ性の削除

次の 2 通りの状況で、SLB はスティッキ性を削除します。

- 特定の加入者セッションが削除されたことを示す信号を BGW が SLB に送信すると、スティッキ エントリが削除されます。
- 実 BGW で障害が発生した場合、その実 BWG に対応するすべてのスティッキ エントリが削除されます。

SLB のステートフル冗長性

信頼性を高めるため、BWG SLB ではプライマリ スーパーバイザとスタンバイ スーパーバイザの間でステートフル スイッチオーバーを行うことができます。

BWG と SLB の間のメッセージ

スティッキ アップデート通知

このメッセージは、BWG が SLB にスティッキの NAI アップデートを通知する場合に使用します。

表 2-14　スティッキ アップデート通知

SRC IP	バーチャル テンプレート IP（実 IP）	
DST IP	ASNLB のバーチャル IP	
UDP HDR	SRC_PORT	XXXX (?)
	DST_PORT	XXXX(?)
MSG HDR	MSG_TYPE	1
	MS ID（6 バイト）	（他の GW の場合は最大 20 バイトの場合もあり）
TLV	TYPE	1
	LENGTH	255（最大）
	VALUE	NAI（abc@cisco.com）

スティッキ削除通知

このメッセージは、セッションの最後の PDP が削除された場合に送信されます。これにより、SLB は該当するスティッキ エントリを削除できます。

表 2-15　スティッキ削除通知

SRC IP	バーチャル テンプレート IP（実 IP）	
DST IP	ASNLB のバーチャル IP	
UDP HDR	SRC_PORT	XXXX (?)
	DST_PORT	XXXX
MSG HDR	MSG_TYPE	2
	MSID（6 バイト）	

SLB サポートの設定

BWG が スティッキ性により SLB を実行できるようにするには、次の作業を行います。

	コマンド	説明
ステップ 1	`router(config)#  wimax agw slb notify {update| delete | …}`	BWG が CAC 障害などの場合に SLB に通知を送信するよう設定します。
ステップ 2	`router(config)#wimax agw slb port` *port* `vserver` *vserver-ip-addr* `[next-hop ip` *ip_addr* `vrf` *vrf_name*`]`	これらの通知の送信先となる SLB 仮想サーバを設定します。セッションの削除やアップデートの通知にはこのコマンドが必要です。 **next-hop** *ip address* と **vrf** *name* はいずれもオプションです。**next-hop** *ip address* が指定されていない場合、仮想サーバに到達するためのスタティック ルートを入力する必要があります。指定可能なポート範囲は 49152 ～ 65535 です。

合法的傍受

Lawful Intercept（LI; 合法的傍受）により、シスコは CALEA（Communications Assistance for Law Enforcement Act）などの世界各地の LI 要件を満たします。

パケット照合は特定の対象の Mobile Subscriber Identity（MSID）に基づいて行われます。

BWG の合法的傍受設定

SNMP ホストとユーザの設定

MIB の変数の設定や表示を行うには、まず認証済みホストの認証済みユーザになる必要があります。合法的傍受を実行するには、BWG で次のコマンドを設定します。

1. 所定の MIB にアクセスできるビューを作成します。

	コマンド	説明

ステップ 1	`router#snmp-server view` *view name* `ciscoTap2MIB included`
	
	`snmp-server view` *view name* `ciscoMobilityTapMIB included`
		BWG が MIB の変数を設定または表示できるようにします。

2. このビューにアクセスできるグループを作成します。

	コマンド	説明
ステップ 1	`router#snmp-server group` *group name*`> v3 priv read` *view name* `write` *view name* `notify` *view name*	BWG がこのビューにアクセスできるグループを作成できます。

3. このグループのメンバであるユーザを作成します。この新しいグループには読み取りおよび書き込み権限があるユーザを作成する必要があります。

	コマンド	説明
ステップ 1	router#snmp-server user *user name group name* v3 auth *sha/md5 auth password* priv *3des/aes/des priv password*	この新しいグループに読み取りおよび書き込み権限があるユーザを作成します。

4. このユーザが接続元として使用するホストを作成します。このユーザが BWG への接続のために使用するホストを指定する必要があります。

	コマンド	説明
ステップ 1	router#snmp-server host *IP address* version 3 priv *user name*	このユーザが BWG への接続のために使用するホストを指定します。

5. テスト用のエンジン ID を設定します。実稼動環境は必要ありません。

	コマンド	説明
ステップ 1	router#snmp-server engineID local *engine ID*	エンジン ID を指定します。

BWG LI の設定手順

BWG 合法的傍受の設定手順を以下に示します。

1. メディエーション デバイスの設定
2. 汎用ストリームの設定
3. 個別ストリームの設定
4. 汎用ストリームのイネーブル化

メディエーション デバイスの設定

認証済みホストから、次の CISCO-TAP2-MIB の変数を設定します。

表 2-16　関連するメディエーション デバイス変数

OID	変数名	説明
.1.3.6.1.4.1.9.9.399.1.1.2.1.2.x	DestAddressType	MD のアドレスの種類（IPv4 または IPv6）
.1.3.6.1.4.1.9.9.399.1.1.2.1.3.x	DestAddress	MD の IP アドレス（16 進表記）
.1.3.6.1.4.1.9.9.399.1.1.2.1.4.x	DestPort	データの送信先となる MD のポート
.1.3.6.1.4.1.9.9.399.1.1.2.1.5.x	SrcInterface	傍受したデータの送信に使用する傍受デバイスのインターフェイス
.1.3.6.1.4.1.9.9.399.1.1.2.1.10.x	TimeOut	現在の行と関連するすべてのストリーム テーブルの行が自動削除され、傍受機能が停止するまでの時間。将来の日付に設定する**必要があります**。この値は 16 進数で入力する必要があります（たとえば、07D8 07 0F 0A 3B 0A 00 は 2008 年 07 月 16 日 10 時 59 分 10 秒 00 を表します）。
.1.3.6.1.4.1.9.9.399.1.1.2.1.11.x	Transport	傍受したデータを MD に転送するためのプロトコル

表 2-16　関連するメディエーション デバイス変数 （続き）

.1.3.6.1.4.1.9.9.399.1.1.2.1.12.x	NotificationEnable	この MIB が現在のテーブル エントリに関する通知を生成するかどうかを示すブール値
.1.3.6.1.4.1.9.9.399.1.1.2.1.13.x	Status	行のステータス。主に特定のエントリの作成、破棄、アクティブ化に使用します。

この他にも使用できる転送オプションがあります。これらのオプションでは、追加のフィールドの設定が必要になる場合があります。

汎用ストリームの設定

認証済みホストから、次の CISCO-TAP2-MIB の変数を設定します。

表 2-17　関連する汎用ストリーム変数

OID	変数名	説明
.1.3.6.1.4.1.9.9.399.1.2.1.1.2.x.y	Type	汎用ストリームに関連付けるタップの種類を指定します。
.1.3.6.1.4.1.9.9.399.1.2.1.1.3.x.y	InterceptEnable	true に設定すると、個別ストリームがこの汎用ストリームに関連付けられた後でタップがアクティブになります。
.1.3.6.1.4.1.9.9.399.1.2.1.1.6.x.y	Status	行のステータス。主に特定のエントリの作成、破棄、アクティブ化に使用します。

ここでは、Status 変数を 5（作成および待機）に設定します。その後、Type 変数を 4（モビリティ傍受ストリーム）に設定します。最後に、個別ストリームをタップに関連付けるまで InterceptEnable 変数を 2（false）に設定します。

個別モビリティ ストリームの設定

認証済みホストから、次の CISCO-MOBILITY-TAP-MIB の変数を設定します。

表 2-18　関連するモビリティ ストリーム変数

OID	変数名	説明
.1.3.6.1.4.1.9.9.672.1.1.2.1.1	CalledSubscriberIDType	CalledSubscriberID フィールドに記録されている ID の種類。デフォルト値は UNKNOWN です。この BWG のリリースでは UNKNOWN のみを使用できます。
.1.3.6.1.4.1.9.9.672.1.1.2.1.2	CalledSubscriberID	コンタクト先の ID。この BWG のリリースでは使用できません。
.1.3.6.1.4.1.9.9.672.1.1.2.1.3	SubscriberIDType	SubscriberID に記録されている ID の種類。デフォルト値は UNKNOWN ですが、この BWG のリリースでは IMSI しか使用できません。
.1.3.6.1.4.1.9.9.672.1.1.2.1.4	SubscriberID	タップする加入者の ID。
.1.3.6.1.4.1.9.9.672.1.1.2.1.5	StorageType	ユーザがこの行のエントリを揮発性メモリと不揮発性メモリのどちらに保存するかを表します。BWG では VOLATILE オプションのみを使用できます。
.1.3.6.1.4.1.9.9.672.1.1.2.1.6	Status	行のステータス。主に特定のエントリの作成、破棄、アクティブ化に使用します。

汎用ストリームのイネーブル化

汎用ストリームの Status 変数を 1 に設定し、行をアクティブにします。最後に、InterceptEnable を true に設定しタップをアクティブにします。

傍受のプロビジョニング

傍受は SNMPv3 によりプロビジョニングされます。プロビジョニングは 3 つの段階で発生します。まず、個別の傍受の設定では、CISCO-TAP2-MIB で説明されている所定の変数の設定により、有効なメディエーション デバイス（MD）を設定する必要があります。MD の設定後には、汎用ストリームの設定が必要です。これについても CISCO-TAP2-MIB で説明しています。最後に、汎用ストリームと関連付ける個別ストリームを選択する必要があります。

BWG の場合、CISCO-MOBILITY-TAP-MIB で定義されたモビリティ ストリームが個別ストリームとなります。現在、BWG ではモビリティ ストリームのモビリティ加入者 ID に基づくタッピングのみを使用できます。このため、モビリティ ストリーム タップを設定する場合は、SubscriberID フィールドを傍受対象のトラフィックに該当する MSID に設定します。その後、SubscriberIDType フィールドを「MSID」に設定します。

パケットの傍受

概念上、BWG における合法的傍受の要件はパケットのレプリケーションと類似しています。加入者またはホストが特定されると、この加入者またはホストに向けたパケットはカプセル化が解除され、IP パケットがレプリケーションされます。その後、元のパケットは本来の宛先に送信されます。レプリケーションおよびカプセル化されたパケットはメディエーション デバイスに送信されます。BWG はパケットの種類を考慮せず、いずれかの方向に受信したパケットをレプリケーションし、レプリケーションされたパケットをメディエーション デバイスに送信します。これにより、BWG はデータ パケットだけでなく音声もレプリケーションできるようになります。

WiMAX NWG ではレプリケーションされたパケットをカプセル化する方法は定義されません。CISCO-TAP2-MIB では、MD が PacketCable UDP, Nack 弾性のある RTP、ヘッドオブライン ブロッキングがある TCP、ヘッドオブライン ブロッキングがある SCTP を使用して、レプリケーションされたパケットをカプセル化および転送できるよう設定できます。現在実装されている BWG は UDP（PacketCableTM）をカプセル化スキームとして使用しています。

現在合法的傍受で使用できない SNMP オプション

現在、BWG では CISCO-TAP2-MIB の Debug User オプションを使用できません。具体的には、CISCO-TAP2-MIB の次のオブジェクトは現在使用できません。

- cTap2DebugUserTable
- cTap2DebugUserEntry
- CTap2DebugUserEntry
- cTap2DebugUserName
- cTap2DebugUserTimeout
- cTap2DebugUserStorageType
- cTap2DebugUserStatus

BWG の設定

ここでは、BWG を正常に機能させるためのその他の各種の設定について説明します。ここでは、次の内容について説明します。

- 「BWG での SNMP 設定」
- 「MIB のサポート」

BWG での SNMP 設定

ここでは、BWG で Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を設定する方法について説明します。ここでは次の設定作業について説明します。

- 「ルータの SNMP アクセスの設定」
- 「SNMP サーバ ホストの設定」
- 「SNMP-Server Trap-Source の設定」
- 「SNMP トラップの設定」

ルータの SNMP アクセスの設定

コミュニティ アクセス ストリングを設定して簡易ネットワーク管理プロトコル（SNMP）にアクセスできるようにするには、次の作業を行います。

	コマンド	目的
ステップ 1	router(config)**# snmp-server community string [view** *view-name***] [ro | rw] [ipv6** *nacl***] [**_access-list-number_**]**	コミュニティ アクセス ストリングを設定して、簡易ネットワーク管理プロトコル（SNMP）にアクセスできるようにします。コマンドで **no** 形式を使用すると、指定したコミュニティ ストリングを削除します。
	string	1 ～ 32 文字の英数字で構成され、パスワードのように機能して SNMP へのアクセスを許可するためのコミュニティ ストリング。コミュニティ ストリングにスペースを使用することはできません。 **（注）** 「@」はコンテキスト情報の区切り記号として使用します。このコマンドを設定する場合、SNMP コミュニティ ストリングの一部として「@」記号を使用しないでください。
	view	（任意）定義済みのビューを指定します。このビューは SNMP コミュニティで使用できるオブジェクトを定義します。
	view-name	（任意）定義済みのビューの名前。
	ro	（任意）読み取り専用アクセス権を指定します。MIB オブジェクトの取得は、認証済みの管理ステーションだけが実行できます。
	rw	（任意）読み取り / 書き込みアクセス権を指定します。MIB オブジェクトの取得と変更は、認証済みの管理ステーションだけが実行できます。
	ipv6	（任意）IPv6 ネームド アクセス リストを指定します。
	nacl	（任意）IPv6 ネームド アクセス リスト。 （任意）IP アドレスの標準アクセス リストを指定する 1 ～ 99 の整数、または SNMP エージェントへのアクセスを許可されている IP アドレスの標準アクセス リストの名前を示す文字列（64 文字以内）。
	access-list-number	または、コミュニティ ストリングを使用した SNMP エージェントへのアクセスが許可されている標準アクセス リストの番号の拡張範囲にある IP アドレスのリストを指定する、1300 ～ 1999 の整数。

SNMP サーバ ホストの設定

簡易ネットワーク管理プロトコルによる通知の受信者を指定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`router(config)# snmp-server host host-addr [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port] [notification-type]`	簡易ネットワーク管理プロトコルによる通知の受信者を指定します。このコマンドの **no** 形式を使用すると、指定したホストを削除します。

このコマンドは、デフォルトでディセーブルになっています。通知は送信されません。キーワードを指定せずにこのコマンドを入力すると、デフォルトではホストにすべての種類のトラップが送信されます。このホストに応答要求は送信されません。

version キーワードが指定されていない場合、デフォルトはバージョン 1 です。**no snmp-server host** コマンドでキーワードが指定されていない場合、ホストへのトラップはディセーブルになりますが、応答要求はディセーブルにはなりません。応答要求をディセーブルにするには、**no snmp-server host informs** コマンドを使用します。

host-addr	ホスト（ターゲット受信者）の名前またはインターネット アドレス。
traps	（任意）このホストに SNMP トラップを送信します。これがデフォルトです。
informs	（任意）このホストに SNMP 応答要求を送信します。
version	（任意）トラップの送信に使用する簡易ネットワーク管理プロトコル（SNMP）のバージョン。バージョン 3 では **priv** キーワードでパケットの暗号化ができるため、このバージョンが最もセキュリティの高いモデルです。**version** キーワードを使用する場合、次のいずれかを指定する必要があります。 **1**：SNMPv1。このオプションは応答要求では使用できません。 **2c**：SNMPv2C **3**：SNMPv3 バージョン 3 キーワードのあとには次の 3 つのオプションのキーワードを使用できます。 • **auth**（任意）：MD5 および Secure Hash Algorithm（SHA）パケット認証をイネーブルにします。 • **noauth**（デフォルト）：noAuthNoPriv セキュリティ レベル。[auth | noauth | priv] キーワードの選択が指定されていない場合、これがデフォルトとなります。 • **priv**（任意）：Data Encryption Standard（DES; データ暗号規格）パケット認証（プライバシとも呼ばれています）をイネーブルにします。
community-string	通知の送信時に使用する、パスワードに類似したコミュニティ ストリング。このストリングは **snmp-server host** コマンドでも設定できますが、**snmp-server host** コマンドの前に **snmp-server community** コマンドを使用してこのストリングを定義することを推奨します。
udp-port *port*	使用するホストの UDP ポート。デフォルト値は 162 です。

notification-type	（任意）ホストに送信する通知の種類。どの種類も指定されていない場合、すべての通知が送信されます。通知の種類には、次のキーワードのうち 1 つ以上を指定できます。 • **bgp**：Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）状態変化通知を送信します。 • **config**：設定通知を送信します。 • **dspu**：Downstream Physical Unit（DSPU; 下流物理ユニット）通知を送信します。 • **entity**：エンティティ MIB 変更通知を送信します。 • **envmon**：環境しきい値を超過した時点で、シスコ独自の環境モニタ通知を送信します。 • **frame-relay**：フレーム リレー通知を送信します。 • **hsrp**：Hot Standby Routing Protocol（HSRP）通知を送信します。 • isdn：ISDN 通知を送信します。 • llc2：Logical Link Control, type 2（LLC2; 論理リンク制御、タイプ 2）通知を送信します。 • **repeater**：標準リピータ（ハブ）通知を送信します。 • rsrb：Remote Source-Route Bridging（RSRB; リモート ソースルート ブリッジング）通知を送信します。 • **rsvp**：Resource Reservation Protocol（RSVP; リソース予約プロトコル）通知を送信します。 • **rtr**：SA エージェント（RTR）通知を送信します。 • **sdlc**：Synchronous Data Link Control（SDLC）通知を送信します。 • sdllc：SDLLC 通知を送信します。 • **snmp**：簡易ネットワーク管理プロトコル（SNMP）を RFC 1157 の規定に従い送信します。 • **stun**：Serial Tunnel（STUN; シリアル トンネル）通知を送信します。 • **syslog**：エラー メッセージ通知（Cisco Syslog MIB）を送信します。送信するメッセージのレベルは **logging history level** コマンドで指定します。 • **tty**：TCP 接続が閉じた時点でシスコ独自の通知を送信します。 • **x25**：X.25 イベント通知を送信します。

SNMP-Server Trap-Source の設定

簡易ネットワーク管理プロトコル トラップの送信元となるインターフェイス（およびこれに対応する IP アドレス）を指定するには、次の作業を行います。

	コマンド	目的
ステップ 1	router(config)# **snmp-server trap-source** *interface* *interface*	簡易ネットワーク管理プロトコル トラップの送信元となるインターフェイス（およびこれに対応する IP アドレス）を指定します。コマンドの no 形式を使用すると、送信元の指定が削除されます。デフォルトの設定では、インターフェイスは指定されていません。 SNMP トラップの送信元となるインターフェイス。この引数のプラットフォーム特有の構文には、インターフェイスの種類と番号が含まれています。

SNMP トラップの設定

ルータが簡易ネットワーク管理プロトコル トラップまたは応答要求（SNMP 通知）を送信できるようにするには、次の作業を行います。

	コマンド	目的
ステップ 1	router(config)# **snmp-server enable traps** [*notification-type*] [*notification-option*]	ルータが簡易ネットワーク管理プロトコル トラップまたは応答要求（SNMP 通知）を送信できるようにします。このコマンドの **no** 形式を使用すると、SNMP 通知がディセーブルになります。 このコマンドは、デフォルトでディセーブルになっています。大部分の種類の通知はディセーブルになります。ただし、一部の種類の通知はこのコマンドでは制御できません。 このコマンドで *notification-type* キーワードを使用しない場合、デフォルトではこのコマンドで制御できるすべての種類の通知がイネーブルになります（ただし、ATM PVC 通知は atm pvc キーワードを使用しない限りイネーブルになりません）。

notification- type	（任意）イネーブルにする通知の種類。どの種類も指定されていない場合、デバイスで使用可能なすべての通知が送信されます。通知の種類には、次のいずれかのキーワードを指定できます。 • **atm pvc**：ATM Permanent Virtual Circuit（PVC; 相手先固定接続）通知をイネーブルにします。**atm pvc** キーワードが使用されている場合、追加の *notifcation-option* 値を指定できます（以下を参照）。ATM PVC 障害通知は CISCO-IETF-ATM2-PVCTRAP-MIB で「enterprise 1.3.6.1.4.1.9.10.29.2.1; 1 atmIntfPvcFailuresTrap」と定義されています。ATM PVC 障害通知は ATM インターフェイスの PVC が障害を起こした場合、または UP 動作状態でなくなった場合に送信されます。interval キーワード（MIB で atmIntfPvcNotificationInterval として保存されています）で指定されている期間に、ハードウェア インターフェイスごとに 1 つのトラップが生成されます。同じインターフェイスで他の PVC がこの期間内にダウン状態になると、トラップが生成され、fail-interval で指定した時間が経過するまで保持されます。この期間が経過し、PVC がまだダウン状態の場合、トラップが送信されます。PVC がダウン状態からアップ状態に戻った場合は、通知は生成されません。PVC の復旧を検出する必要がある場合は、SNMP 管理アプリケーションを使用して定期的にルータのポーリングをする必要があります。 • **bgp**：ボーダー ゲートウェイ プロトコル1（BGP）状態変化通知をイネーブルにします。 • **config**：設定通知をイネーブルにします。 • **entity**：エンティティ MIB 変更通知をイネーブルにします。 • envmon：環境しきい値を超過した時点で、シスコ独自の環境モニタ通知をイネーブルにします。**envmon** キーワードを指定している場合、*notification-option* 値を指定できます。 • **frame-relay**：フレーム リレー通知をイネーブルにします。 • **hsrp**：Hot Standby Routing Protocol（HSRP）通知をイネーブルにします。 • isdn：ISDN 通知をイネーブルにします。**isdn** キーワードを指定している場合、*notification-option* 値を指定できます。 • repeater：イーサネット ハブ リピータ通知をイネーブルにします。**repeater** キーワードが指定されている場合、*notification-option* 値を指定できます。 • **rsvp**：リソース予約プロトコル（RSVP）通知をイネーブルにします。 • **rtr**：SA エージェント/Response Time Reporter（RTR）通知をイネーブルにします。

notification- type	• **snmp [authentication]**：RFC 1157 SNMP 通知をイネーブルにします。**authentication** キーワードを使用しても、**authentication** キーワードを使用しない場合と効果は同じです。このコマンドの **snmp-server enable traps snmp** 形式と **snmp-server enable traps snmp authentication** 形式のいずれでも、次の SNMP トラップをグローバルにイネーブルにできます（no 形式を使用した場合はディセーブルになります）。 – authentication Failure – linkUp – linkDown – coldstart （この動作は Cisco IOS リリース 12.1(3)T および 12.0(20)S で修正されています） • **syslog**：エラー メッセージ通知（Cisco Syslog MIB）をイネーブルにします。送信するメッセージのレベルは **logging history level** コマンドで指定します。
notification- option	（任意） • **atm pvc [interval** ***seconds***] [**fail-interval** ***seconds***]：オプションの **interval** キーワードと *seconds* 引数を組み合わせると、連続するトラップの最小間隔を指定できます。値の範囲は 1 ～ 3600 です。この通知間隔の設定により、PVC トラップの生成が抑制され、トラップの過剰発生が防止されます。この間隔が経過するまでトラップは送信されません。デフォルトの間隔は、30 秒です。 オプションの fail-interval キーワードと seconds 引数を組み合わせると、障害タイムスタンプを保存する最小間隔を指定できます。値の範囲は 0 ～ 3600 です。fail-interval のデフォルト値は、0 秒です。 • **envmon** [**voltage**	**shutdown**	**supply**	**fan**	**temperature**]：**envmon** キーワードを使用すると、特定の種類の環境通知をイネーブルにしたり、環境モニタ システムからのすべての種類の通知を許可することができます。どのオプションも指定されていない場合、すべての環境通知がイネーブルになります。**voltage**、**shutdown**、**supply**、**fan**、**temperature** のうち 1 つ以上のキーワードを指定できます。 • **isdn** [**call-information**	**isdn u-interface**]：isdn キーワードが使用されている場合、call-information キーワードを指定すると ISDN MIB サブシステムの SNMP ISDN コール情報通知をイネーブルにできます。また、**isdnu-interface** キーワードを指定すると ISDN U インターフェイス MIB サブシステムの SNMP ISDN U インターフェイスをイネーブルにできます。 • **repeater** [**health**	**reset**]：**repeater** キーワードを使用すると、リピータ オプションを指定できます。どのオプションも指定されていない場合、すべてのリピータ通知がイネーブルになります。通知の種類には次のいずれかのキーワードを指定できます。 • **health**：IETF リピータ ハブ MIB（RFC 1516）ヘルス通知をイネーブルにします。 • **reset**：IETF リピータ ハブ MIB（RFC 1516）リセット通知をイネーブルにします。

設定例

次の例では、「public」というコミュニティ ストリングを使用して、ルータがすべてのトラップを「myhost.cisco.com」という名前のホストに送信できるようにしています。

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

次の例では、「public」というコミュニティ ストリングを使用して、ルータがフレーム リレーおよび環境モニタ トラップを「myhost.cisco.com」という名前のホストに送信できるようにしています。

```
snmp-server enable traps frame-relay
snmp-server enable traps envmon temperature
snmp-server host myhost.cisco.com public
```

次の例では、どのホストにもトラップを送信しません。BGP トラップがすべてのホストに対してイネーブルになっていますが、ホストへの送信がイネーブルになっているのは ISDN トラップのみです（この例ではイネーブルになっていません）。

```
snmp-server enable traps bgp
snmp-server host bob public isdn

router(config)# [no] logging snmp-authfail
```

（注）　**logging snmp-authfail** コマンドを使用すると、すべての SNMP 認証失敗メッセージのログがイネーブルになります。このコマンドの **no** 形式を使用すると、認証失敗メッセージのログがディセーブルになります。

（注）　ルータの SNMP 管理ツールで PPP セッションをモニタしていない場合、no virtual-template snmp コマンドを使用すると、仮想アクセス サブインターフェイスがルータの SNMP 機能で登録されてメモリを使用することがないようにできます。次に例を示します。
router(config)# [**no**] **virtual-template snmp**

BWG での SNMP 設定の例

ロギング

```
=========

!
logging snmp-authfail
logging queue-limit 100
logging buffered 1000000
enable password lab
!
```

仮想テンプレート

```
=============

!
no virtual-template snmp
!
```

SNMP トラップ

==========

```
snmp-server community private RW
snmp-server trap-source GigabitEthernet0/2
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps ds1
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps cnpd
snmp-server enable traps pw vc
snmp-server enable traps syslog
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ds3
snmp-server enable traps atm subif
snmp-server enable traps channel
snmp-server enable traps ima
snmp-server enable traps srp
snmp-server enable traps flash insertion removal
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps cpu threshold
snmp-server enable traps config-copy
snmp-server enable traps envmon
snmp-server enable traps aaa_server
snmp-server enable traps agw
snmp-server enable traps bgp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface-old
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps ipmulticast
snmp-server enable traps mvpn
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps ipsla
snmp-server enable traps stun
snmp-server enable traps dlsw
snmp-server enable traps bstun
snmp-server enable traps pppoe
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps ipmobile
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps event-manager
```

```
snmp-server enable traps alarms informational
snmp-server host 171.71.129.34 public
```

MIB のサポート

BWG では、ユーザとネットワークが SNMP コマンドを使用してリモートで BWG をモニタできるようにするためのオブジェクトを参照できる Management Information Base（MIB;管理情報ベース）を使用できます。BWG では次の独立した 2 つの MIB を使用できます。

1 つは、グローバル システム情報とパラメータ、ベース ステーション情報、加入者、フロー、トラフィックおよびトラップ通知情報が保存されているものです。

もう 1 つは、ベース ステーションと BWG の間で使用される R6 シグナリング プロトコル情報に関する情報が保存されているものです。これには、全体のゲートウェイ R6 情報と、ベース ステーションごとの情報が含まれます。

フェールオーバー時には BWG MIB 変数は同期されません。スタンバイ側からは同期された状態データを使用して各種の MIB 変数を再作成できます。NMS はこのような状況に対処しようと試み、またその結果発生する MIB データの矛盾を解決しようとします。既存の RF/CF MIB も使用できます。

MIB サポートの確認

各種の MIB パラメータを表示するには、次の作業を行います。

	コマンド	目的
ステップ 1	`router# show wimax agw`	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。
ステップ 2	`router# show wimax agw stat internal`	BWG 内部統計情報を表示します。
ステップ 3	`router# show wimax agw stat dhcp`	BWG DHCP 統計情報を表示します。
ステップ 4	`router# show wimax agw stat`	BWG 統計情報を表示します。
ステップ 5	`router# show wimax agw user-group`	BWG ユーザ グループ統計情報を表示します。
ステップ 6	`router# show wimax agw path`	BWG パス統計情報を表示します。

設定例

show wimax agw コマンドの出力例を次に示します。

```
router# show wimax agw
Access network gateway version 0.1, service is enabled

 AGW listening on UDP control port 2231
 Maximum Number of base station 500 allowed
 Maximum Number of subscriber 20000 allowed
  Number of signalling paths created 0
  Number of brearer paths created 0
  Number of subscribers connected 0
  Number of sessions created 0
  Number of flows created 0
  Traffic Sent 0 packets, 0 bytes
  Traffic Rcvd 0 packets, 0 bytes
  Number of framed routes
  Number of subscribers using the framed routes
  Current number of user auto-provisioned sessions
```

```
  The traffic is split for IP CS and ETH CS.
```

show wimax agw user-group コマンドの出力例を次に示します。

```
router# show wimax agw user-group
AGW User-Group-List
There are 3 user-groups configured in list wimax

User group domain name any
 User-Group overwritten Counter 0
 Service mode operational
 Sessions 0 associated
 IP-GRE Traffic Sent 0 packets, 0 bytes
 IP-GRE Traffic Received 0 packets, 0 bytes
 Eth-GRE Traffic Sent 0 packets, 0 bytes
 Eth-GRE Traffic Received 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes
 Traffic Received redirected 0 packets, 0 bytes


User group domain name cisco
 Service mode operational
 Sessions 0 associated
 Traffic Sent 0 packets, 0 bytes
 Traffic Received 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes


User group domain name unauthenticated
 Service mode operational
 Sessions 0 associated
 Traffic Sent 0 packets, 0 bytes
 Traffic Received 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes

router#show wimax agw user-group brief ?

Name            Sessions  Pkts-Tx   Bytes-Tx  Pkts-Rx   Bytes-Rx  VRF
any             0         0         0         0         0
cisco           0         0         0         0         0
unauthenticated 0         0         0         0         0

router#show wimax agw user-group any ?
  brief  Brief output
  |      Output modifiers
  <cr>

router#show wimax agw user-group any

User group domain name any
--------------------------------------
 Service mode operational
 Sessions 0 associated
 Traffic Sent 0 packets, 0 bytes
 Traffic Recevied 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes


router#show wimax agw user-group any brief
Name            Sessions  Pkts-Tx   Bytes-Tx  Pkts-Rx   Bytes-Rx  VRF
any             0         0         0         0         0

router#show wimax agw user-group name ?
```

```
  WORD  Enter User-group Name

router#show wimax agw user-group name cisco ?
  brief  Brief output
  |      Output modifiers
  <cr>

router#show wimax agw user-group name cisco

User group domain name cisco
-------------------------------------
 Service mode operational
 Sessions 0 associated
 Traffic Sent 0 packets, 0 bytes
 Traffic Recevied 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes


router#show wimax agw user-group name cisco brief ?
  |  Output modifiers
  <cr>

router#show wimax agw user-group name cisco brief
Name            Sessions  Pkts-Tx   Bytes-Tx  Pkts-Rx   Bytes-Rx  VRF
cisco 0         0         0         0         0


router#show wimax agw user-group unauthenticated ?
  brief  Brief output
  |      Output modifiers
  <cr>

router#show wimax agw user-group unauthenticated

User group domain name unauthenticated
-------------------------------------
 Service mode operational
 Sessions 0 associated
 Traffic Sent 0 packets, 0 bytes
 Traffic Recevied 0 packets, 0 bytes
 Ingress Address filtering 0 packets, 0 bytes

asn#sh wimax agw user-group unauthenticated b
asn#sh wimax agw user-group unauthenticated brief ?
  |  Output modifiers
  <cr>

router#show wimax agw user-group unauthenticated brief
Name            Sessions  Pkts-Tx   Bytes-Tx  Pkts-Rx   Bytes-Rx  VRF
unauthenticated    0         0         0         0           0
```

show wimax agw statistics コマンドの出力例を次に示します。

```
router# show wimax agw statistics
AGW Statistics
Message function type Undefined(0/0x0)

Message function type Data Path(3/0x3)
  Message type Deregistration Request(4/0x4)
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Deregistration Response(5/0x5)
```

```
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Deregistration Ack(6/0x6)
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Registration Request(12/0xC)
   Number of messages sent 0
   Number of messages received 0
   Number of messages resent 0
  Message type Registration Response(13/0xD)
   Number of messages sent 0
   Number of messages received 0
…
```

show wimax agw statistics dhcp-relay コマンドの出力例を次に示します。

```
router# show wimax agw statistics dhcp-relay
AGW DHCP Statistics
   Tx to DHCP server Discover 0, Request 0
   Tx to DHCP server Release 0, Decline 0
   Tx to DHCP server Inform 0
   Rx from DHCP server Offer 0, Ack 0
   Rx from DHCP server Nak 0, Unknown 0
```

この出力では、BWG 経由でリレーされる DHCP メッセージの統計情報が表示されます。BWG がいずれかの DHCP を開始した場合、これらのカウンタの値は増加しません。

show wimax agw statistics internal コマンドの出力例を次に示します。

```
Router# show wimax agw statistics internal
Last clearing of "show wimax agw statistics internal" counters 3d23h
 Signalling plane related statistics
  Signal packets processed messages 483
  Signal packets has pending messages 0
  Signal packets requeued messages 0
  Signal packets dropped too many pending messages 0
  Signal packets dropped service disabled 0
  Signal packets dropped service not ready 0
  Signal packets dropped no encapsulation interface 0
  Signal packets dropped CAC denied request 0
  Signal packets disposed by agw 0
 Data plane related statistics
  Data packets not ours encapsulation 0
  Data packets not ours encapsulation address 0
  Data packets not ours service disabled 0
  Data packets not ours invalid protocol type 0
  Data packets dropped invalid ip len 0
  Data packets dropped absent key data 0
  Data packets dropped flow not found 21
  Data packets dropped flow path not found 0
  Data packets dropped flow path invalid src address 0
  Data packets dropped session not found 0
  Data packets dropped subscriber not found 0
  Data packets dropped checksum error 0
  Data packets dropped ingress filtering 0
  Data packets dropped sequence number mismatch 0
  Data packets dropped invalid redirect address 0
  Data packets dropped throttling of punts from cef to process 0
  Data packets dropped gateway learning from upstream data packets 0
  Data packets dropped non-ARP and non-DHCP L2 multicast/broadcast data packets 0
  Data packets punted fragmented 0
  Data packets punted from cef path to process path 0
```

```
Other related statistics
 Number of N/w behind MS in usrgrp enabled 0
 Total subscriber created  41
 Total subscriber deleted 45
 Total session created  41
 Total session deleted 45
 Total flow created  4
 Total flow deleted 7
 Total host created  0
 Total host deleted 0
 Total signalling path created  3
 Total signalling path deleted 3
 Total data path created  2
 Total data path deleted 2
 Number of hosts rejected 0
 Number of packets dropped due to Static IP Host not allowed 0
 Number of static hosts aged out 0
 Total sessions rejected due to unapproved BS 0
Configuration related statistics
 Service flow profile not found 0
 QoS profile not found 0
 Classifier profile not found 0
 Sla profile not found 0
Handoff related statistics
 Total handoffs succeeded 0
 Total handoff failed 0
 Total cmac key update succeeded 0
 Total cmac key update failed 0
 Total security key exchange succeeded 0
 Total security key exchange failed 0
Miscellaneous statistics
 Maximum Subscriber exceeded 0
 Maximum BS exceeded 0
```

BWG リリース 1.1 での MIB 機能拡張

BWG 管理情報ベース（MIB）はアップデートされ、送信および受信したパケット数とバイト数のイーサネット CS 関連カウンタが追加されています。BWG リリース 1.1 では次の MIB オブジェクトがアップデートされています。

- 新しい EthCS 関連の送受信済みパケット数/バイト数の変数が含まれています。
- 変更された送受信済みパケット数/バイト数の説明が含まれています。

  たとえば、「受信したデータ の合計パケット数」は「受信した IP データ の合計パケット数」に変更されています。

ASN GW グローバル統計情報

- 受信した IP データ の合計パケット数
- 送信した IP データ の合計パケット数
- 受信した IP データ の合計バイト数
- 送信した IP データ の合計バイト数
- 受信したイーサネット CS データ の合計パケット数
- 送信したイーサネット CS データ の合計パケット数
- 受信したイーサネット CS データ の合計バイト数

- 送信したイーサネット CS データ の合計バイト数
- 拒否されたホストの合計数
- 期限切れになったスタティック ホストの合計数

MIB には ARP に関する統計情報（受信した ARP 要求の合計数、送信した ARP 応答の合計数、ドロップされた ARP パケットの合計数）、拒否されたホストに関する統計情報、期限切れのスタティック ホストに関する統計情報の新しいオブジェクトも含まれています。

GRE キー入力

各サービス フローの方向ごとに GRE キーが割り当てられています。GRE キーは、データ パス ベアラの作成に使用する RR-Request を使用して交換されます。BWG に対応する GRE キーは BWG により割り当てられ、サービス フローの作成時に RR-Request を使用して BS に送信されます。同様に、BS に対応する GRE キーの値は BS により割り当てられ、RR-Response メッセージを使用して BWG に送信されます。

BS 間モビリティ中に、新しいキーがベース ステーションにより割り当てられます。BWG は同じ GRE キーを保持します。

BWG は、リリースと同時に値が割り当てられないように GRE キーを割り当てます。

VRF のサポート

ユーザ グループには Virtual Route Forwarding（VRF; 仮想経路転送）のサポートを設定できます。これにより、内部 VRF エンティティを作成して特定のユーザ グループとの間で送受信されるすべてのトラフィックを接続することができます。

QoS サポート

QoS のサポートは、エアーリンク QoS とネットワーク上のマッピングの両方を意味します。所定のサービス フローの作成のため、ASNGW がベース ステーションに QoS パラメータを送信します。

- 特定のホストには追加の QoS パラメータを設定できます。
- ホスト IP アドレスに対応する新しい R6 ベアラ（サービス フロー）を作成できます。このサービス フローは複数のホストで使用できます。
- 新しい R6 サービス フローへのホストのマッピングが作成され、RR-Request により BS/MS に送信されます。

サービス フローごとの DSCP マーキング

各サービス フローは Diffserv Code Point（DSCP;DiffServ コード ポイント）に対して一意にマッピングされます。この DSCP 値は外部 IP ヘッダーのマーキングのため、ダウンストリーム パケットでは BWG、アップストリーム パケットでは BS により使用されます。

アップストリームおよびダウンストリーム パケットの内部 IP ヘッダーは、サービス フローのマッピングに従って、BWG により設定されます。ただし、CLI により明示的にディセーブルにされている場合を除きます。

ACL

ACL はサポートされており、ユーザ グループごとに設定できます。同じユーザ グループに接続するすべてのユーザに対して適用されます。

送信元 IP アドレスの検証

すべてのアップリンク パケットについて、対応する MS またはサービス フローに対して割り当てられた IP アドレスが検証されます。ミスマッチが検出されると、そのパケットは破棄されます。

この機能を設定するには、ゲートウェイ ユーザ グループ サブモードで **security subscriber address-filtering ingress** コマンドを使用します。

コントロールとデータで異なる BS のエンド ポイントのサポート

BS にはコントロールとデータ プレーンで異なるエンド ポイント IP アドレスが存在する場合があります。データ パス エンド ポイント ID TLV（フローの BS のパス登録応答メッセージで送信）の可用性によっては、BWG は GRE パスを作成し、使用可能な TLV から IPv4 を取得できます。

指定した TLV が存在しない場合、コントロール プレーンのエンド ポイントのアドレスがリモート データのエンド ポイントとして使用され、GRE パスが作成されます。

ベアラ アカウンティング

すべてのサービス フローで、ベアラのボリューム カウントが維持されています。これには、入力および出力パケットとオクテット カウントが含まれています。

制約事項

Cisco BWG リリース 1.0 以降では次の制約事項が適用されます。

- CPU 使用率の上昇による問題を回避するため、次の設定が推奨されます。
  - 起動時の CPU 使用率を抑えるには、**no logging console** グローバル コンフィギュレーション コマンドを設定し、コンソール端末へのロギングをディセーブルにします。
  - HSRP インターフェイスが同位 hello パケットを処理できる状態になるまでアクティブ状態を宣言しないようにするには、HRSP インターフェイスで **standby delay minimum 100 reload 100 interface** コンフィギュレーション コマンドを使用して、HSRP グループを初期化する前に遅延時間を設定します。
  - PPP PDP 処理（作成と削除）が高頻度である期間が長いなど、その他の理由で CPU 使用率が高くなる問題を最小限に抑えるには、**no logging event link-status** インターフェイス コンフィギュレーション コマンドを使用して、BWG のすべてのバーチャル テンプレート インターフェイスでのインターフェイス データ リンク ステータスの変更通知をディセーブルにします。

```
!
interface Virtual-Template1
description ASNGW-VT
ip unnumbered Loopback0
encapsulation agw
no logging event link-status
access-point-list wimax
end
```

ヒットレス ソフトウェア アップグレード

BWG リリース 2.0 では、新しい SR アトリビュートが導入されています。スタンバイ側がアップグレードした後、スタンバイ側では新しい BWG 2.0 SR アトリビュートを受信しません（アクティブ BWG は引き続き BWG 1.1/1.2 で稼動します）。元の BWG（アクティブ）から同期されないこれらの新しい BWG 2.0 SR アトリビュートについては、スタンバイ BWG に対して適切なデフォルト値を設定する必要があります。

次の条件を前提とした場合、この後に説明する手順を実行するとソフトウェアのアップグレードを正常に実行できます。

アクティブ BWG とスタンバイ BWG は BWG 1.2 (N-1) ソフトウェア イメージで稼動しています。説明を簡単にするために、元のアクティブ BWG をノード A、元のスタンバイ BWG をノード B とします。

アップグレード手順

- ノード A とノード B で startup-config を起動し、BWG 2.0 に適合させます。CLI は引き続き BWG 2.0 以前の製品に適合しているため、この手順が必要になるのは最初に何らかの BWG 2.0 の機能が必要である場合のみです。この手順が必要な場合は、**tftp-copy** により既存の startup-config ファイルを外部 TFTP デバイスにコピーし、手動で編集してから tftp-copy により再度 BWG にコピーします。
- スタンバイ側（ノード B）の BWG 1.2 を BWG 2.0 イメージにアップグレードします。スタンバイ側の BWG 2.0 は引き続きスタンバイ BWG として機能します。バルク同期が完了するまで待ちます。既存のすべてのセッションに BWG 2.0 用の該当機能があるわけではないことに注意してください。
- ノード A を BWG 2.0 イメージにアップグレードし、ノード A でスイッチオーバーを実行します。この時点で、ノード B（BWG 2.0 イメージ）がアクティブになります。
- バルク同期が完了するまで待ちます。バルク同期が完了すると、ノード A がスタンバイ状態になります。

制約事項

次の制約事項は、ヒットレス ソフトウェア機能に適用されます。

- BWG 2.0 の下位互換性は N-1 リリースに対してのみ維持されます。
- BWG 2.0 から N-1 リリースへのダウングレードはできません。

ユーザ グループごとに 2 台の DHCP サーバをサポート

BWG が DHCP リレーとして機能している場合、DHCP パケットを 2 台の DHCP サーバにリレーできます。DHCP 検出パケットと DHCP 要求パケットは両方の DHCP サーバに送信されます。

2 台の DHCP サーバを設定するには、ユーザ グループ設定に次のコマンドを追加します。

#dhcp server primary A.B.C.D backup E.F.G.H

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	`router(config)# wimax agw pmip profile verizon`
	`proxy-mn`
	`host-config-ext-request // RFC 4332`
		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	`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`
		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、BGW-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 BGW-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 が最小のパケット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	`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`
		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# show wimax agw`	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。 • 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# show wimax agw subscriber`	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。 • PMIP を使用する加入者の機能 • 次の MIP 情報： – 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 – 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`	上記の情報以外に、次の情報がこの CLI に追加されました。 • 次の MIP 情報： – 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`	次の情報が追加されました。 • 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`	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。
ステップ 6	`router# show wimax agw statistics dhcp-proxy`	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。
ステップ 7	`router# show wimax agw fsm dhcp-proxy`	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。

ステップ 8	`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`
		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。

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 スティッキ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
    encap 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 VirtualTemplate1
  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
!
```