

P-GW StarOS リリース 21.28 アドミニストレーション ガイド

最終更新：2025 年 8 月 25 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned 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. (1721R)

© 2022-2024 Cisco Systems, Inc. All rights reserved.



このマニュアルについて

（注） コントロールプレーンとユーザープレーンの分離（CUPS）は、StarOS ベースの製品の 3G、4G、および 5G のネットワークでの展開方法におけるアーキテクチャ上の著しい変更を表します。別段の指定がない限り、このドキュメントで言及されている設定（コマンド、統計、属性、MIB オブジェクト、アラーム、ログ、サービスを含むがこれらに限定されない）が、レガシー製品または CUPS 以外の製品との機能的な同等性を意味するものではありません。CUPS 製品または機能への言及は、情報提供のみを目的としています。この製品と CUPS 製品間のパリティに関するご質問については、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

（注） HA、HSGW、PDSN、および SecGW 製品はサポートが終了しており、このリリースではサポートされていません。これらの製品への参照（特定または暗黙的）において、本書に記載されている CLI コマンドやパラメータなどのコンポーネントまたは機能は偶然の一致によるものであり、サポートされていません。これらの製品のサポート終了に関する詳細については、https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5000-series/eos-eol-notice-c51-740422.html [英語] を参照してください。

この序文では、『*P-GW Administration Guide*』、その構成、および表記法について説明します。

Packet Data Network Gateway は、Cisco® ASR 5500 および仮想化プラットフォームで実行される StarOS アプリケーションです。

- 使用する表記法 （iv ページ）
- サポートされているマニュアルおよび関連情報 （vi ページ）
- カスタマー サポートへの問い合わせ （vii ページ）

使用する表記法

次の表に、このマニュアル全体で使用される表記法を示します。

通知タイプ	説明
情報メモ	重要な機能または手順に関する情報を提供します。
注意	プログラム、デバイス、またはシステムに損傷を与えるおそれがあることを注意喚起します。
警告	人身傷害または死亡事故のおそれがあることを警告します。また、電気的障害のおそれがあることを警告する場合もあります。

書体の表記法	説明
スクリーンディスプレイとして表されるテキスト	この書体は、端末画面に表示されるディスプレイを表します。次に例を示します。 ログイン：
commands として表現されるテキスト	この書体は、入力したコマンドを表します。次に例を示します。 **show ip access-list** このマニュアルでは、コマンドの完全表記に常に小文字を使用しています。コマンドには、大文字と小文字の区別はありません。
command *variable*として表されるテキスト	この書体は、コマンドの一部である変数を表します。次に例を示します。 **show card** *slot_number* *slot_number* は、目的のシャーシのスロット番号を表す変数です。

書体の表記法	説明
メニュー名またはサブメニュー名として表されるテキスト	この書体は、ソフトウェアアプリケーション内でアクセスするメニューとサブメニューを表します。次に例を示します。 [File] メニュー、[New] の順にクリックてください。

コマンドシンタックスの表記法	説明
{ keyword または変数 **}**	必須キーワードオプションと変数は、コマンドシンタックスの一部として入力する必要があるコンポーネントです。 必須キーワードオプションと変数は、波カッコ { } で囲まれています。次に例を示します。 **sctp-max-data-chunks { limit** *max_chunks* **| mtu-limit }** キーワードまたは変数が、波カッコまたは角カッコで囲まれていない場合、これは必須です。次に例を示します。 **snmp trap link-status**
[keyword または変数 **]**	オプションのキーワードや変数、またはユーザーが使用するかどうかを選択できるキーワードや変数は、角カッコで囲まれています。
|	コマンドによっては、複数のオプションをサポートしています。これらは、各オプションを縦棒で区切って、波カッコまたは角カッコ内に記述されます。 これらのオプションは、必須キーワードやオプションキーワードまたは変数と組み合わせて使用できます。次に例を示します。 **action activate-flow-detection { intitiation | termination }** または **ip address [count** *number_of_packets* **| size** *number_of_bytes* **]**

サポートされているマニュアルおよび関連情報

関連する共通マニュアル

この製品の最新情報は、各製品リリースに付属している製品のリリースノートで確認できます。

次の共通マニュアルが用意されています。

- *AAA Interface Administration Guide and Reference*
- *Command Line Interface Reference*
- *GTPP Interface Administration Guide and Reference*
- 設置ガイド（プラットフォームによって異なる）
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- システム アドミニストレーション ガイド（プラットフォームによって異なる）
- *Thresholding Configuration Guide*

関連マニュアル

以下の製品マニュアルも入手できます。これらの製品は P-GW と連携して動作します。

- *ADC Administration Guide*
- *ECS Administration Guide*
- *GGSN Administration Guide*
- *IPSec Reference*
- 『*eDRX Support on the MME*』機能の章を
- 「*Logging Support*」の章を参照してください。
- 『*NAT Administration Guide*』の
- *SAEGW Administration Guide*
- *S-GW Administration Guide*

マニュアルの入手方法

最新のシスコのマニュアルは、次の Web サイトで入手できます。

http://www.cisco.com/cisco/web/psa/default.html

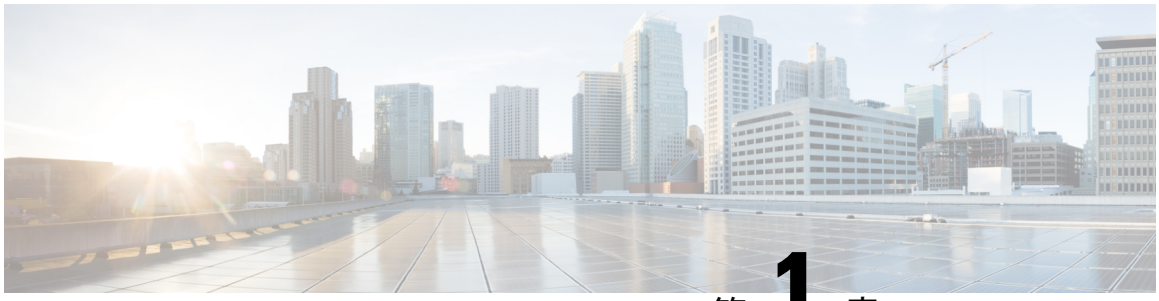
P-GW のマニュアルにアクセスするには、次のパスを選択します。

[Products] > [Wireless] > [Mobile Internet] > [Network Functions] > [Cisco PGW Packet Data Network Gateway]

カスタマー サポートへの問い合わせ

カスタマーサポートに連絡するには、この項の情報を使用してください。

最新の製品マニュアルについては、http://www.cisco.com のサポートエリアを参照するか、サービスリクエストを送信してください。このサイトにアクセスするには、有効なユーザー名とパスワードが必要です。詳細については、シスコの販売担当者またはサービス担当者にお問い合わせください。



第 1 章

PDN ゲートウェイの概要

Cisco® Packet Data Network（PDN）ゲートウェイ（P-GW）は、Evolved Packet Core（EPC）と呼ばれる 4G モバイルコアネットワークの重要なネットワーク機能です。P-GW は、3GPP2 Long Term Evolution-System Architecture Evolution（LTE-SAE）ネットワークと、インターネット、SIP ベースの IP Multimedia Subsystem（IMS）ネットワーク、および Evolved High Rate Packet Data（eHRPD）ワイヤレス データ ネットワークなどの他のパケットデータネットワーク間のインターフェイスとして機能します。

この概要には、次のような P-GW に関する一般的な情報が記載されています。

- 製品の説明 （1 ページ）
- ネットワーク展開 （4 ページ）
- 基本ソフトウェアの特長と機能 （19 ページ）
- 特徴と機能 - インラインサービスのサポート （79 ページ）
- オプションの拡張機能ソフトウェアの特長と機能 （86 ページ）
- PDN ゲートウェイの機能 （115 ページ）
- サポートされる標準 （126 ページ）

製品の説明

P-GW は、PDN への SGi インターフェイスを終端するノードです。UE が複数の PDN にアクセスしている場合、その UE に対して複数の P-GW が存在する可能性があります。P-GW は、UE のトラフィックが出入りするポイントになることによって、外部パケット データ ネットワークに UE への接続を提供します。UE は複数の PDN にアクセスするために複数の P-GW との同時接続を持つ場合があります。P-GW は、ポリシーの適用、各ユーザーへのパケットフィルタリング、課金サポート、合法的傍受、およびパケットスクリーニングを実行します。

図 *1*: 基本的な ***E-UTRAN/EPC*** ネットワークにおける ***P-GW***

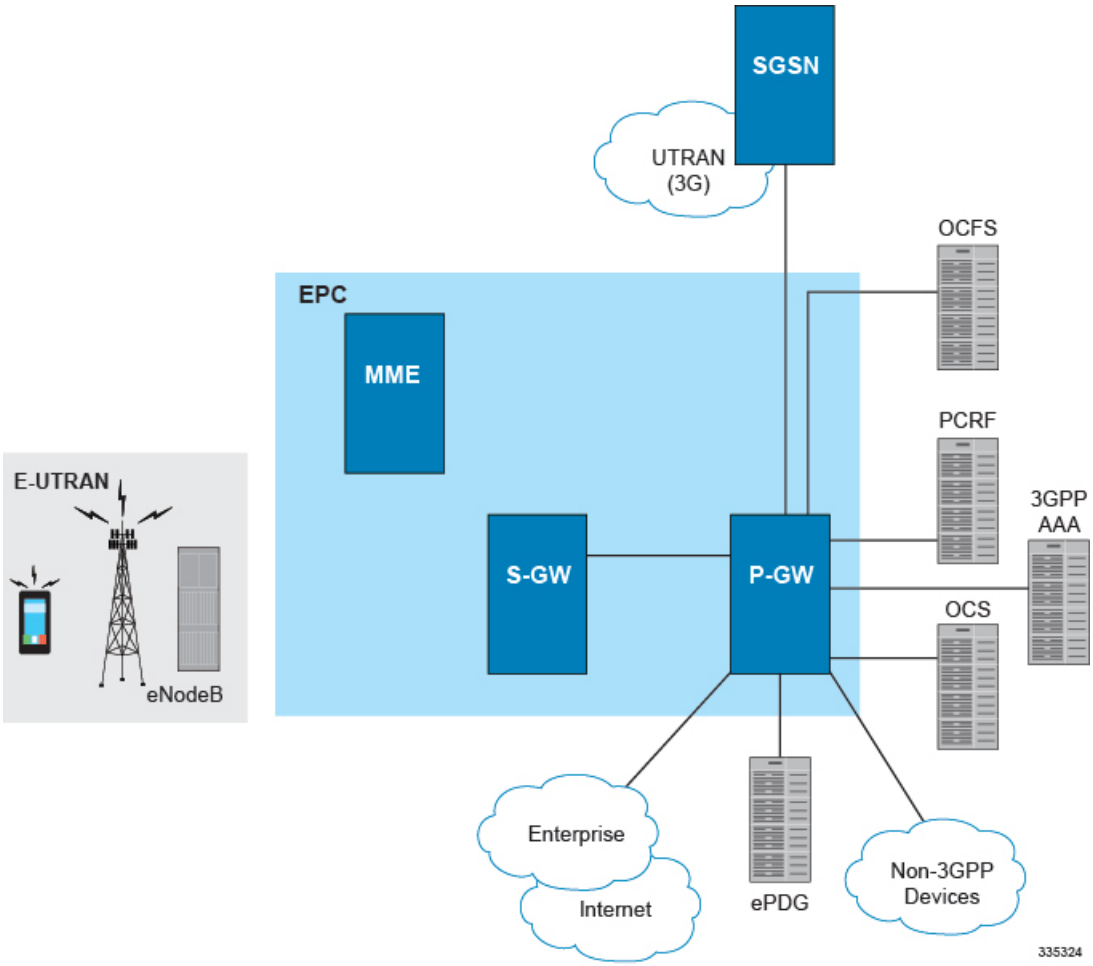
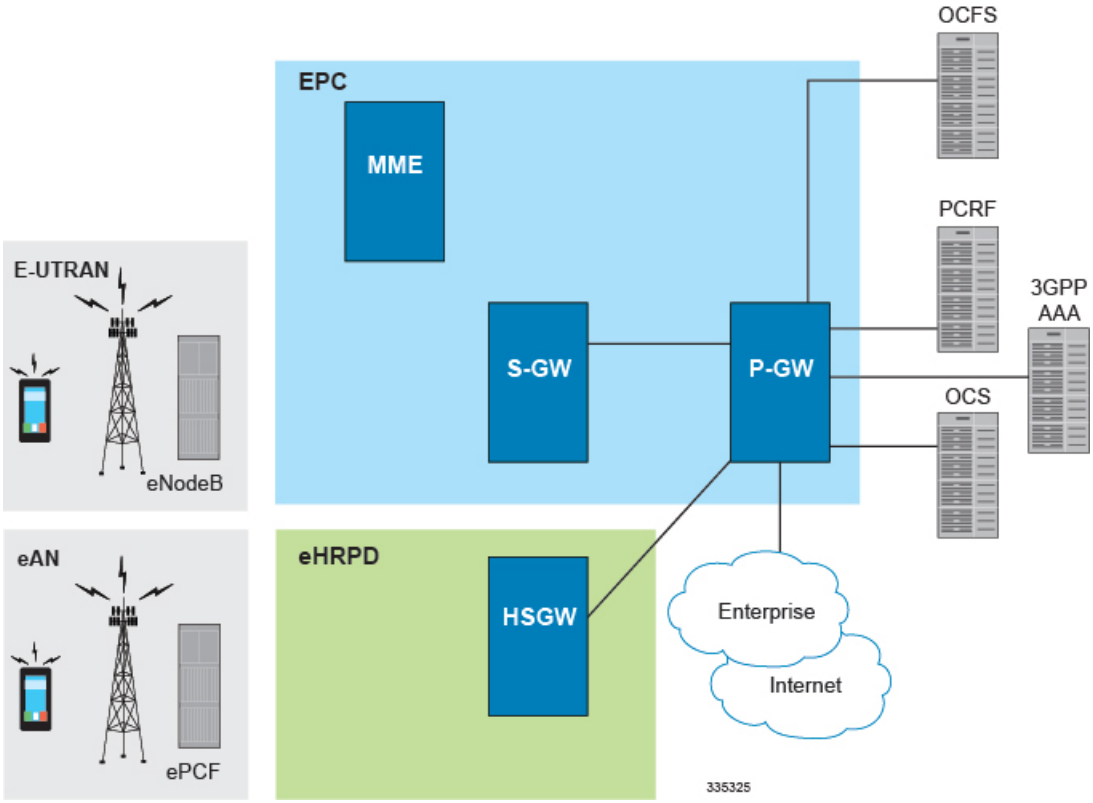


図 *2 :* 基本的な *E-UTRAN/EPC* および *eHRPD* ネットワークにおける *P-GW*



P-GW のもう一つの主な役割は、3GPP と非 3GPP 技術との間のモビリティアンカーとして機能することです。後者には、WiMAX や 3GPP2（CDMA 1X、EvDO）などがあります。

P-GW の機能は次のとおりです。

- 3GPP アクセスシステムと非 3GPP アクセスシステム間のモビリティに使用されるモビリティアンカー。これは、SAE アンカー機能と呼ばれることもあります。
- ポリシーの適用（ゲート処理およびレートの適用）
- ユーザー単位のパケットフィルタリング（ディープ パケット インスペクション）
- 課金サポート
- 合法的傍受
- UE IP アドレス割り当て
- パケットスクリーニング
- ダウンリンクでのトランスポート レベル パケット マーキング
- 集約最大ビットレート（AMBR）に基づくダウンリンクレートの適用

非 3GPP アクセス（eHRPD）をサポートする場合に追加される P-GW 機能は次のとおりです。

- PMIP ベースの S5 または S8 が使用されている場合、P-GW には draft-ietf-netlmm-proxymip6 に従ったローカルモビリティアンカー（LMA）の機能が追加されます。
- S2c が使用されている場合、P-GW には draft-ietf-mip6-nemo-v4traversal に記載されている DSMIPv6 ホームエージェントの機能が追加されます。

認定プラットフォーム

P-GW は、Cisco ASR 5500 および仮想化プラットフォームで実行される StarOS アプリケーションです。プラットフォームの詳細については、該当する『*System Administration Guide*』[英語]を参照するか、シスコのアカウント担当者にお問い合わせください。

ライセンス

P-GW は、シスコのライセンス製品です。別のセッションおよび機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

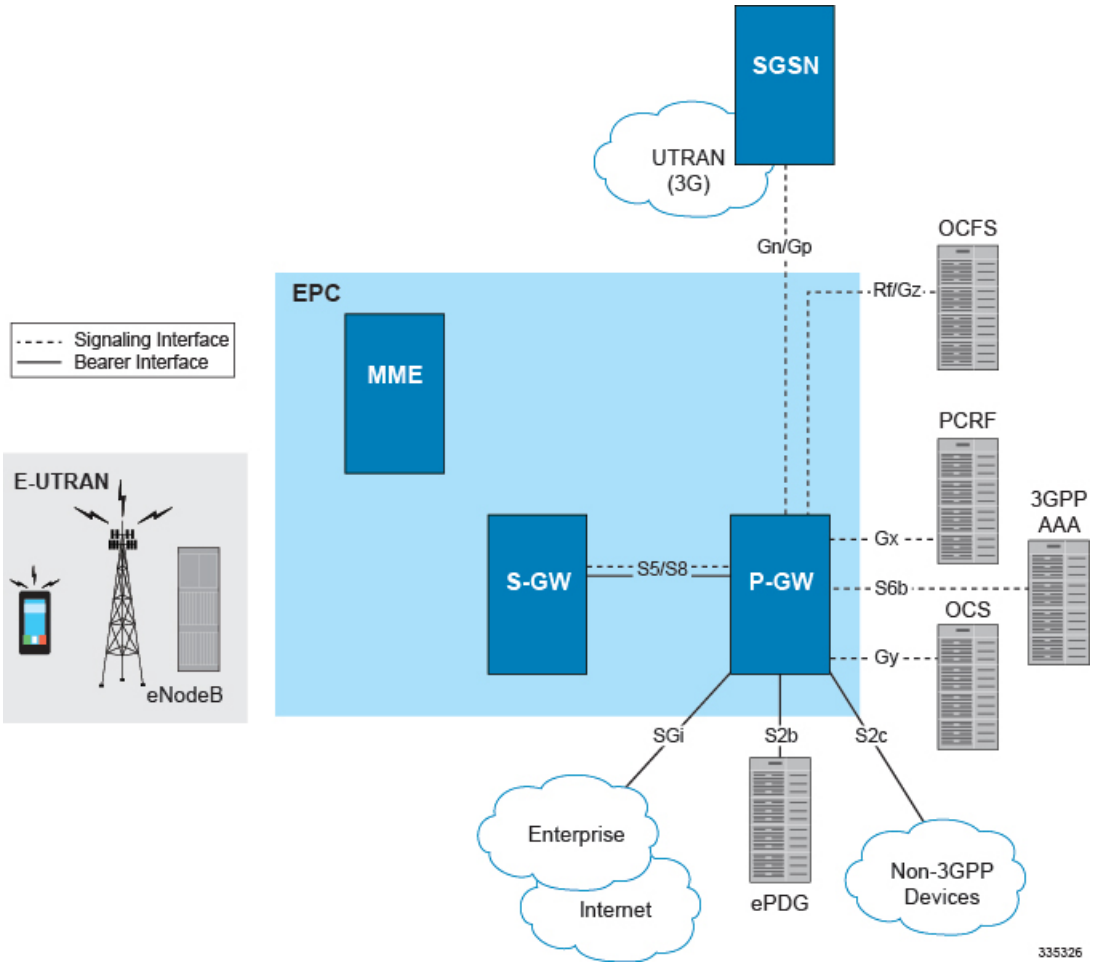
ネットワーク展開

ここでは、サポートされているインターフェイスと PDN ゲートウェイの展開シナリオについて説明します。

E-UTRAN/EPC ネットワークの PDN ゲートウェイ

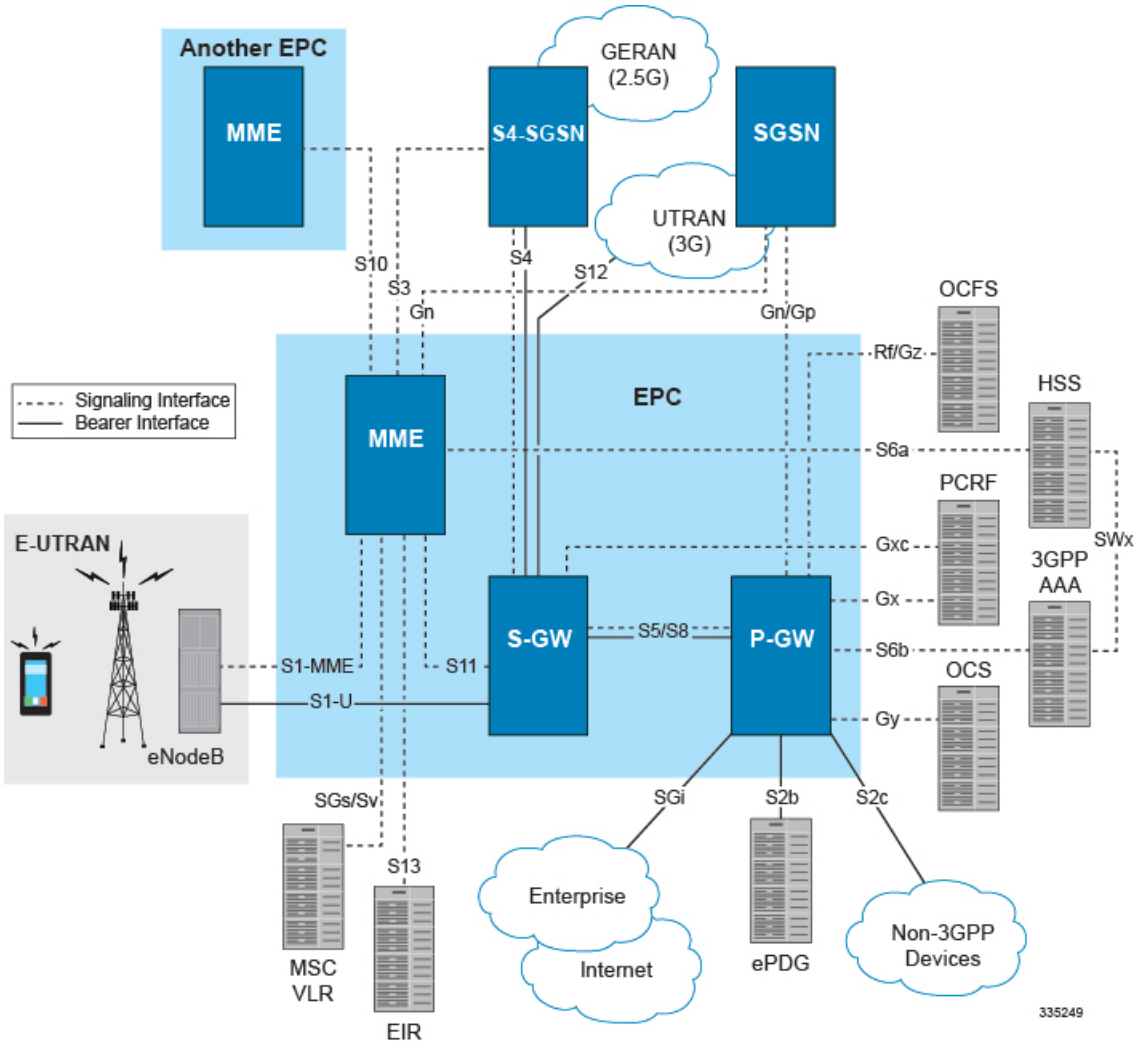
次の図は、P-GW でサポートされる特定のネットワークインターフェイスを示しています。各インターフェイスの詳細については、サポートされる論理ネットワークインターフェイス（参照ポイント）（14 ページ）を参照してください。

図 *3 : E-UTRAN/EPC* ネットワークでサポートされる *P-GW* インターフェイス



次の図は、P-GW のネットワーク展開の例を示しています。これには、他の 3GPP Evolved-UTRAN/Evolved Packet Core ネットワークデバイスとのすべてのインターフェイス接続が含まれています。

図 *4 : E-UTRAN/EPC* ネットワークにおける *P-GW*



サポートされる論理ネットワーク インターフェイス（参照ポイント）

P-GW は、E-UTRAN/EPC ネットワークのサポートにおいて次の論理ネットワーク インターフェイスを提供します。

S2b インターフェイス

非信頼非 3GPP ePDG（進化型パケットデータゲートウェイ）と P-GW の間で定義された S2b インターフェイス参照ポイントは、EPC へのアクセスを可能にするために PMIPv6（プロキシモバイル IP バージョン 6）を使用します。GTPv2-C は、S2b で使用されるシグナリングプロトコルです。S2b インターフェイスは、3GPP TS 29.274 に基づいています。

S2b インターフェイスは、PMIPv6 プロトコルを実行して、P-GW との WLAN UE セッションを確立します。また、WLAN UE によって実行される P-CSCF 検出の一環として、PBU（プロ

キシMIPバインディング更新）およびPBA（プロキシMIPバインディング確認応答）メッセージの P-CSCF 属性と DNS 属性の転送もサポートします。

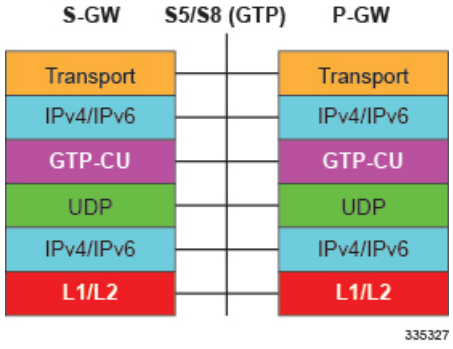
P-CSCFアドレス情報が欠落している場合、S4-SGSN から LTE（およびその逆）へのハンドオフ時にP-CSCF検出が開始されます。P-CSCFアドレス情報がすでに利用可能な場合は、S4-SGSN から LTE（およびその逆）へのハンドオフ時に、P-CSCF 検出を改めて明示的にトリガーする必要はありません。

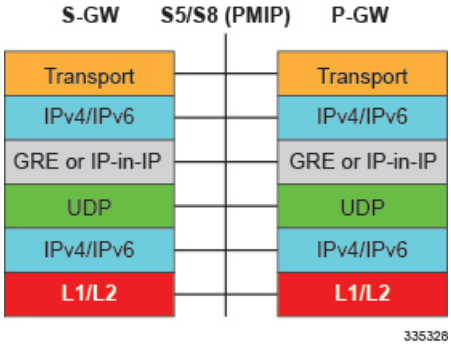
S5/S8 インターフェイス

この参照ポイントは、3GPP TS 23.401 および TS 23.402 で定義されている、S-GW と P-GW の間のトンネリングと管理を提供します。S8 インターフェイスは、ローミングシナリオ中に使用される S-GW と P-GW の間の PLMN 間参照ポイントです。S5 インターフェイスは、同じ管理ドメイン内（非ローミング）にある S-GW と P-GW の間で使用されます。これは、UE モビリティによるS-GWの再配置に使用され、また、S-GWが必要なPDN接続のために非コロケーション P-GW に接続する必要がある場合に使用されます。

サポートされるプロトコル

- トランスポート層：UDP、TCP
- トンネリング：
  - GTP：GTPv2-C（シグナリングチャネル）、GTPv1-U（ベアラーチャネル）
  - PMIPv6：GRE または IP-in-IP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット





S6b インターフェイス

この参照ポイント（PGW および 3GPP AAA のサーバーやプロキシ間）は、モビリティ関連認証に使用されます。また、ダイナミック PCC がサポートされていない場合に、モビリティに関連するパラメータの取得と要求を行ったり、UE の静的 QoS プロファイル（非 3GPP アクセス用）を取得したりするために使用されることもあります。

リリース 12.2 以降、S6b インターフェイスは、UE が割り当てた IPv6 アドレス（IPv6 プレフィックスと IPv6 インターフェイス ID）を AAA サーバーに渡すように拡張されています。S6b インターフェイスは、Framed-IPv6-Pool、Framed IP Pool、およびサービスパーティ IP アドレス AVP ベースの IP 割り当てもサポートしています。このサポートにより、AAA サーバーから受信したプール名と APN 名に基づいて、IP アドレスを割り当てるために設定から特定の IP プールの選択が行われます。

P-GW または GGSN の S6b インターフェイスを手動で無効にして、過負荷状態時に 3GPP AAA へのすべてのメッセージトラフィックを停止できます。インターフェイスが無効になっている場合、システムはローカルに設定された APN 固有の次のパラメータを使用します。Framed-Pool、Framed-IPv6-Pool、Idle-Timeout、Charging-Gateway-Function-Host、Server-Name（P-CSCF FQDN）。この手動による方法は、HSS/3GPP AAA が過負荷状態にあるときに、アプリケーションを回復させてサブスクライバへの影響を軽減できるようにするために使用されます。

リリース 12.3 以降では、S6b インターフェイスへの承認認証要求（AAR）を介した IPv6 アドレスレポートがデフォルト機能ではなくなりました。これは、CLI を使用して設定できるようになりました。

S6b インターフェイスのサポートのもう 1 つの強化点は、S6b インターフェイスで一意に定義された Diameter エラーコードを受信した場合に、GGSN および P-GW で自動トリガーを作成し、ローカルに設定された APN プロファイルを使用する新しい S6b 再試行および続行機能です。承認認証要求（AA-R）でのみ使用されます。この手順は、プロトコル、一時的、または永続的なエラーコードがプライマリとセカンダリの両方の AAA から GGSN または P-GW に返される場合に使用されます。再試行および続行機能においては、P-GW は APN に設定されているかどうかを DNS サーバーに問い合わせる必要があります。S6b の障害処理によってデータコールが続行されます。この動作は、aaa-custom15 Diameter ディクショナリにのみ適用されます。

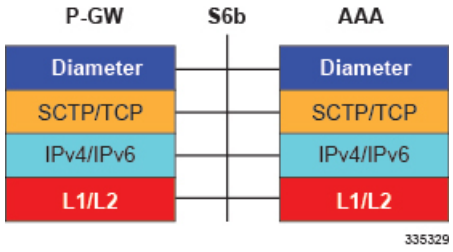
StarOS リリース 17 以降では、P-GW は、AAA サーバーから S6b インターフェイスを介して AVP「Restoration-Priority-Indicator」の受信をサポートしており、VoLTE が有効な IMS PDN 接

続と非 VoLTE が有効な IMS PDN 接続とを区別します。また、AVP 値に基づいて KPI が提供されます。

重要 AAA の長期的な停止が発生した場合は、CLI を使用して S6b インターフェイスを無効にできます。

サポートされているプロトコル

- トランスポート層：TCP、SCTP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット



SGi インターフェイス

この参照ポイントは、P-GW とパケットデータネットワーク（3GPP TS 23.401）間の接続を提供します。このインターフェイスは、外部のパブリックまたはプライベート PDN や内部の IMS サービス プロビジョニング ネットワークを含むさまざまなネットワークタイプへのアクセスを提供できます。

サポートされているプロトコル

- トランスポート層：TCP、UDP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット

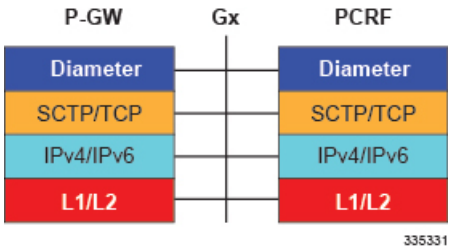


Gx インターフェイス

このシグナリングインターフェイスでは、P-GW のポリシーおよび課金適用機能（PCRF）と、ポリシーおよび課金ルール機能（PCRF）サーバー（3GPP TS 23.401）との間のポリシー制御および課金ルール情報（QoS）の転送がサポートされています。

サポートされているプロトコル

- トランスポート層：TCP、SCTP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット



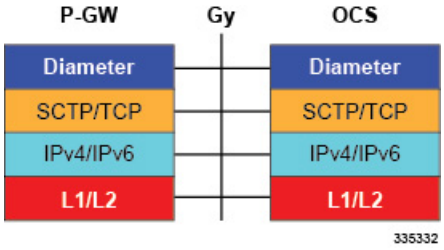
Gx インターフェイスの設定の詳細については、「ダイナミックポリシー課金制御（Gx 参照インターフェイス） （34 ページ）」を参照してください。

Gy インターフェイス

Gy 参照インターフェイスは、3GPP リリース 8 およびリリース 9 仕様に従って、P-GW でオンラインカウンティング機能を有効にします。

サポートされているプロトコル

- トランスポート層：TCP、SCTP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット



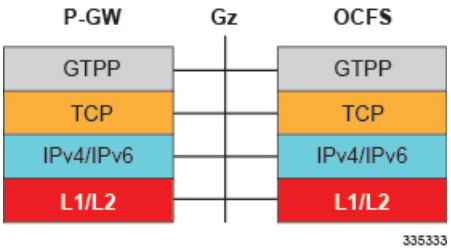
Gy インターフェイスおよびオンラインアカウンティングの詳細については、「Gy インターフェイスのサポート （41 ページ）」を参照してください。

Gz インターフェイス

Gz参照インターフェイスは、P-GWのオフラインアカウンティング機能を有効にします。P-GWは、無線ネットワーク使用量に関連する各モバイルサブスクライバUEの課金情報を収集します。

サポートされているプロトコル

- トランスポート層：TCP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット

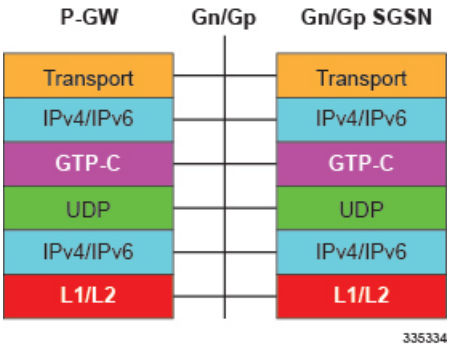


Gn/Gp インターフェイス

この参照ポイントは、EPS と 3GPP 2G および/または 3G ネットワーク間のハンドオーバー時に、P-GW と SGSN 間のトンネリングと管理を提供します（3GPP TS 29.060）。Gn/Gp インターフェイスの詳細については、Gn/Gp ハンドオフのサポート （43 ページ）を参照してください。

サポートされるプロトコル

- トランスポート層：UDP、TCP
- トンネリング：GTP：GTP-C（シグナリングチャネル）
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット

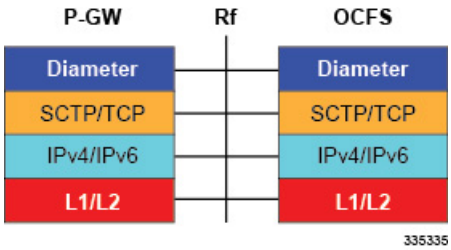


Rf インターフェイス

Rf インターフェイスは、3GPP リリース 8 およびリリース 9 仕様に従って、P-GW でオフラインアカウンティング機能を有効にします。P-GW は、無線ネットワーク使用量に関連する各モバイルサブスクライバ UE の課金情報を収集します。

サポートされているプロトコル

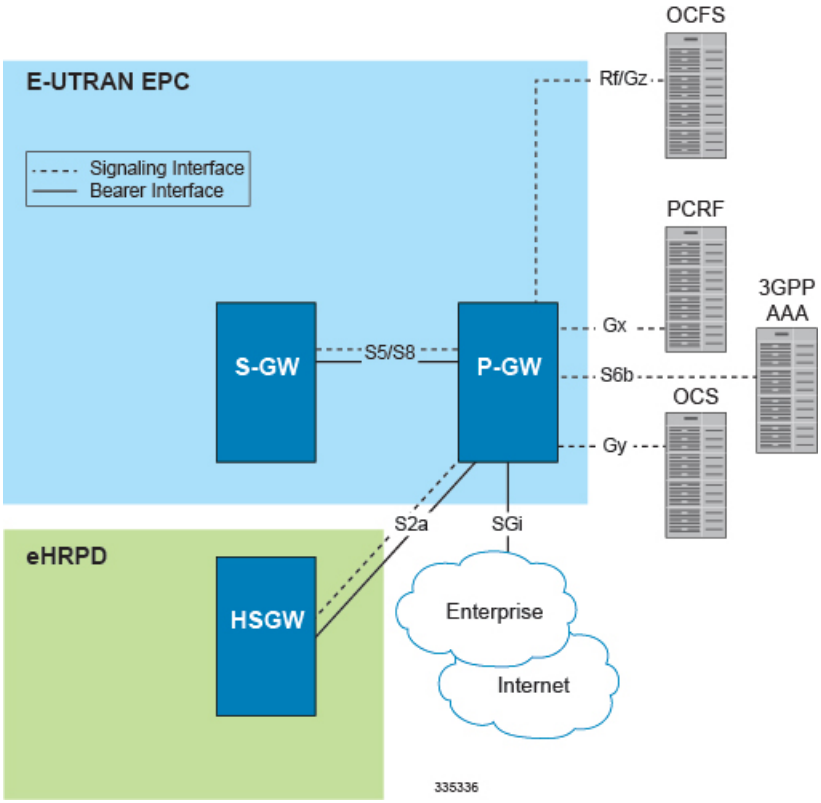
- トランスポート層：TCP、SCTP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット



eHRPD から E-UTRAN/EPC への接続をサポートする PDN ゲートウェイ

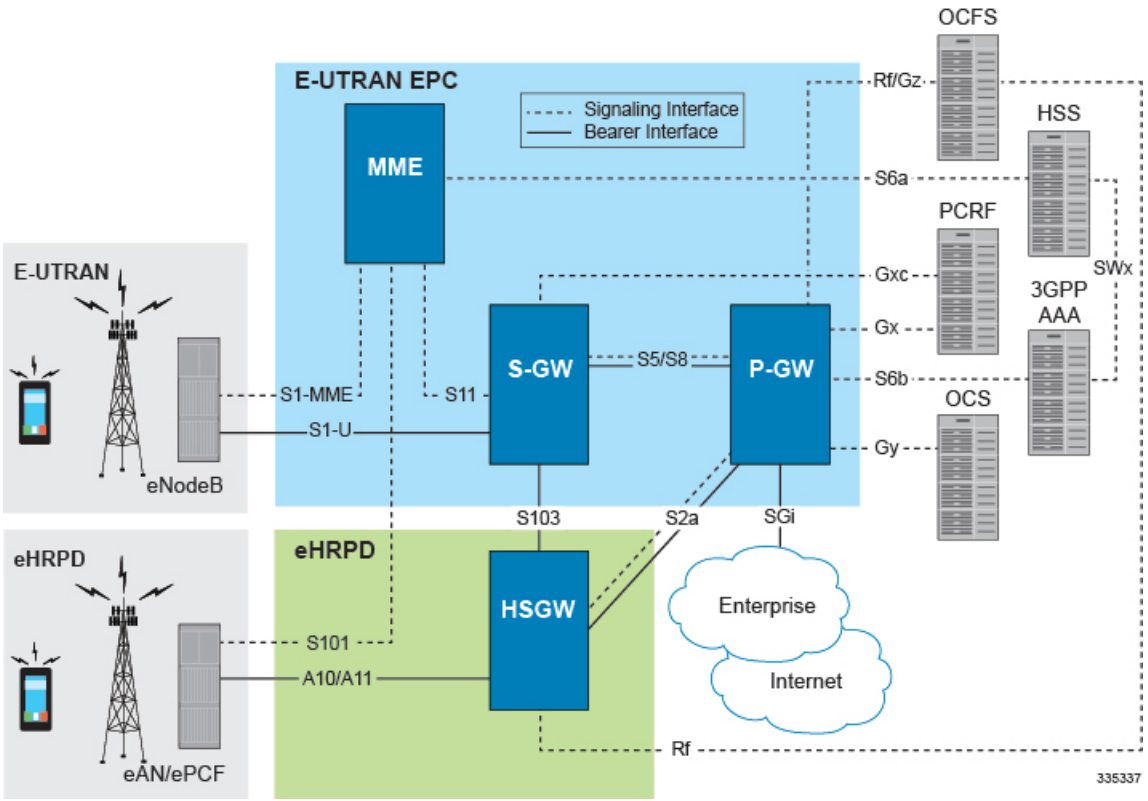
次の図は、eHRPD ネットワーク内の P-GW でサポートされる特定のネットワーク インターフェイスを示しています。各インターフェイスの詳細については、サポートされる論理ネットワーク インターフェイス（参照ポイント） （6 ページ）を参照してください。

図 *5 : eHRPD* から *E-UTRAN/EPC* への接続をサポートする *P-GW* インターフェイス



次の図は、eHRPD ネットワーク内の P-GW のネットワーク展開の例を示しています。これには、他の 3GPP Evolved-UTRAN/Evolved Packet Core ネットワークデバイスとのすべてのインターフェイス接続が含まれています。

図 *6 : eHRPD* ネットワークをサポートする *E-UTRAN/EPC* ネットワーク内の *P-GW*



サポートされる論理ネットワーク インターフェイス（参照ポイント）

P-GW は、eHRPD から E-UTRAN/EPC への接続のサポートにおいて次の論理ネットワークインターフェイスを提供します。

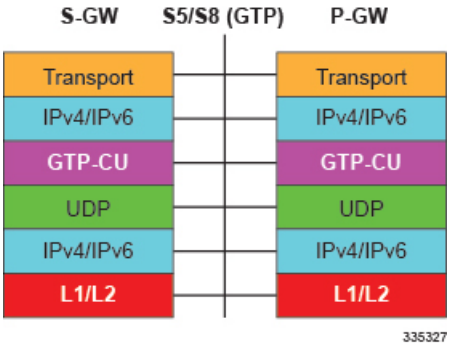
S5/S8 インターフェイス

この参照ポイントは、3GPP TS 23.401 で定義されている、S-GW と P-GW の間のトンネリングと管理を提供します。S8 インターフェイスは、ローミングシナリオ中に使用される S-GW と P-GW の間の PLMN 間参照ポイントです。S5 インターフェイスは、同じ管理ドメイン内（非ローミング）にある S-GW と P-GW の間で使用されます。これは、UE モビリティによる S-GW の再配置に使用され、また、S-GW が必要な PDN 接続のために非コロケーション P-GW に接続する必要がある場合に使用されます。

サポートされているプロトコル

- トランスポート層：UDP、TCP
- トンネリング：
  - GTP：IPv4 または IPv6 GTP-C（シグナリングチャンネル）および GTP-U（ベアラーチャンネル）
  - PMIPv6：IPv6 GRE または IP-in-IP

- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット

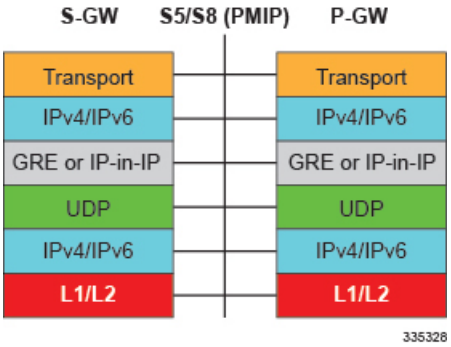


S2a インターフェイス

この参照ポイントは、信頼できる非 3GPP アクセスポイント（HSGW）と PDN ゲートウェイ間のシグナリングとモビリティのサポートを提供することで、ベアラーインターフェイスをサポートします。これはプロキシモバイル IP に基づいていますが、PMIP をサポートしない信頼できる非 3GPP IP アクセスポイントへの接続を可能にするクライアントモバイル IPv4 FA モードもサポートしています。

サポートされているプロトコル

- トランスポート層：UDP、TCP
- トンネリング：GRE IPv6
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット



S6b インターフェイス

この参照ポイント（P-GW および 3GPP AAA のサーバーやプロキシ間）は、モビリティ関連認証に使用されます。また、ダイナミック PCC がサポートされていない場合に、モビリティに関連するパラメータの取得と要求を行ったり、UE の静的 QoS プロファイル（非 3GPP アクセス用）を取得したりするために使用されることもあります。

リリース 12.2 以降、S6b インターフェイスは、UE が割り当てた IPv6 アドレス（IPv6 プレフィックスと IPv6 インターフェイス ID）を AAA サーバーに渡すように拡張されています。S6b インターフェイスは、Framed-IPv6-Pool、Framed IP Pool、およびサービスパーティ IP アドレス AVP ベースの IP 割り当てもサポートしています。このサポートにより、AAA サーバーから受信したプール名と APN 名に基づいて、IP アドレスを割り当てるために設定から特定の IP プールの選択が行われます。

P-GW または GGSN の S6b インターフェイスを手動で無効にして、過負荷状態時に 3GPP AAA へのすべてのメッセージトラフィックを停止できます。インターフェイスが無効になっている場合、システムはローカルに設定された APN 固有の次のパラメータを使用します。Framed-Pool、Framed-IPv6-Pool、Idle-Timeout、Charging-Gateway-Function-Host、Server-Name（P-CSCF FQDN）。この手動による方法は、HSS/3GPP AAA が過負荷状態にあるときに、アプリケーションを回復させてサブスクライバへの影響を軽減できるようにするために使用されます。

リリース 12.3 以降では、S6b インターフェイスへの承認認証要求（AAR）を介した IPv6 アドレスレポートがデフォルト機能ではなくなりました。これは、CLI を使用して設定できるようになりました。

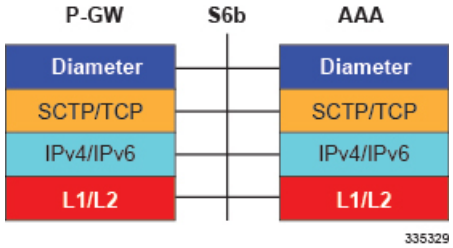
S6b インターフェイスのサポートのもう 1 つの強化点は、S6b インターフェイスで一意に定義された Diameter エラーコードを受信した場合に、GGSN および P-GW で自動トリガーを作成し、ローカルに設定された APN プロファイルを使用する新しい S6b 再試行および続行機能です。承認認証要求（AA-R）でのみ使用されます。この手順は、プロトコル、一時的、または永続的なエラーコードがプライマリとセカンダリの両方の AAA から GGSN または P-GW に返される場合に使用されます。再試行および続行機能においては、P-GW は APN に設定されているかどうかを DNS サーバーに問い合わせる必要があります。S6b の障害処理によってデータコールが続行されます。この動作は、aaa-custom15 Diameter ディクショナリにのみ適用されます。



重要 AAA の長期的な停止が発生した場合は、CLI を使用して S6b インターフェイスを無効にできます。

サポートされているプロトコル

- トランスポート層：TCP、SCTP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット

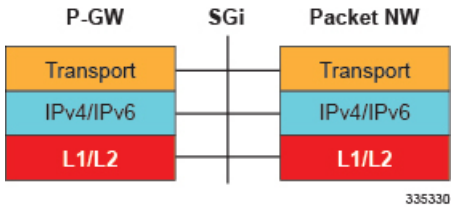


SGi インターフェイス

この参照ポイントは、P-GW とパケットデータネットワーク間の接続を提供します。このインターフェイスは、外部のパブリックまたはプライベート PDN や内部の IMS サービス プロビジョニング ネットワークを含むさまざまなネットワークタイプへのアクセスを提供できます。

サポートされているプロトコル

- トランスポート層：TCP、UDP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット

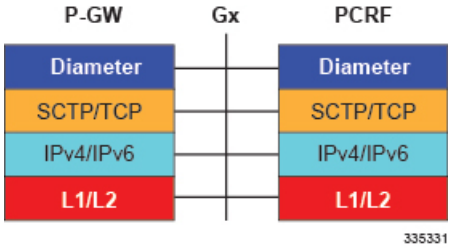


Gx インターフェイス

このシグナリングインターフェイスでは、P-GW のポリシーおよび課金適用機能（PCRF）と、ポリシーおよび課金ルール機能（PCRF）サーバー（3GPP TS 23.401）との間のポリシー制御および課金ルール情報（QoS）の転送がサポートされています。

サポートされているプロトコル

- トランスポート層：TCP、SCTP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット



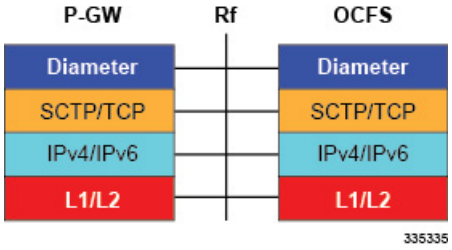
Gx インターフェイスの設定の詳細については、「ダイナミックポリシー課金制御（Gx 参照インターフェイス） （34 ページ）」を参照してください。

Rf インターフェイス

Rf 参照インターフェイスは、3GPP リリース 8 およびリリース 9 仕様に従って、P-GW でオフラインアカウンティング機能を有効にします。P-GW は、無線ネットワーク使用量に関連する各モバイルサブスクライバ UE の課金情報を収集します。

サポートされているプロトコル

- トランス層：TCP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット



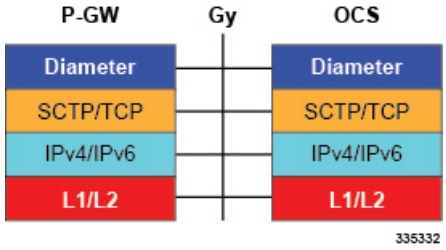
CCO アカウントの作成の詳細については、基本ソフトウェアの特長と機能 （19 ページ）を参照してください。

Gy インターフェイス

Gy 参照インターフェイスは、3GPP リリース 8 およびリリース 9 仕様に従って、P-GW でオンラインカウンティング機能を有効にします。

サポートされているプロトコル

- トランスポート層：TCP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット



Gy インターフェイスおよびオンラインアカウンティングの詳細については、「Gy インターフェイスのサポート （41 ページ）」を参照してください。

基本ソフトウェアの特長と機能

ここでは、P-GW サービスの基本ソフトウェアでデフォルトでサポートされる機能について説明します。この機能を実装するために追加のライセンスは必要ありません。

重要 P-GW 向けの基本的なサービスと機能をシステムで設定するには、本ガイドに記載されている設定例を参照してください。

Gx を介した 3GPP R9 通信量課金

この 3GPP R9 拡張機能は、Gx を介した累積使用量追跡とも呼ばれ、P-GW と PCRF 間の使用量クォータに基づいて、TS 29.212 で定義されている通信量と課金の制御機能のサブセットを提供します。クォータは、デフォルトのベアラーまたは PDN 接続の任意の専用ベアラーに割り当てることができます。

この機能により、Gx を介した通信量レポートが可能になります。これにより、IP-CAN セッションまたはサービスデータフローベースでのネットワークリソースの累積使用量の監視とレポートが提供されます。PCRF は、PCEF に必要な情報を提供することにより、セッションレベルまたはフローレベルでの使用量モニタリングに登録します。PCEF は、条件が満たされると、PCRF に使用量をレポートします。リアルタイムの合計ネットワーク使用量に基づいて、PCRF は動的なポリシー決定を行うための情報を入手します。

使用量監視が有効になっている場合、PCEF は IP-CAN セッションまたは該当するサービスデータフローの使用量を監視し、次のいずれかの条件に基づいて累積使用量を PCRF に報告できます。

- 通信量しきい値に達したとき
- 特定の使用量監視キーについての使用量監視が有効になっているすべての PCC ルールが削除または非アクティブ化されたとき
- 使用量モニタリングが PCRF によって明示的に無効化されたとき
- IP CAN セッションが終了したとき、または

- PCRF から要求されたとき

累積通信量レポートは、PCRF の要求に応じて、合計通信量、アップリンク通信量、またはダウンリンク通信量で測定できます。報告された使用量を PCEF から受信すると、PCRF は、該当する IP-CAN セッション、使用量モニタリングキー、または該当する場合はその両方に対して、許容される合計使用量から使用量レポートの値を差し引きます。

3GPP リリース 12 での原因コード IE のサポート

E-RAB またはデータセッションがドロップされたとき、通信事業者は場合により、詳細な RAN および/または NAS リリース原因コード情報と、アクセスネットワークからの ULI 情報を取得して、P-GW および S-GW CDR に追加する必要があります。これらの情報は、コールパフォーマンス分析、ユーザー QoE 分析、適切な請求調整に必要となります。通信事業者は、IMS セッションの P-CSCF で前記情報の取得が必要になる場合もあります。

S1 経由の E-RAB リリースコマンドおよび E-RAB リリース通知メッセージでは、「Per E-RAB Cause」を受信していました。ただし、RAN および NAS の原因は P-GW および S-GW に転送されず、P-GW によって PCRF に通知されてはいませんでした。

AS および/または NAS の原因を示す「RAN/NAS リリース原因」情報要素（IE）がセッション削除要求およびベアラー削除コマンドに追加されました。MME によって提供される「RAN/NAS リリース原因」は、S-GW によって P-GW に透過的に送信されます（P-GW へのシグナリングがある場合）。これにより、PCRF へとさらに伝達されます。

後方互換性のために、S-GW は引き続き、S4/S11 メッセージ内の CC IE から原因コードを受信します。また、一部のお客様のプライベート拡張機能からの原因コードも引き続き受信します。

AAA サーバグループ

企業または MVNO のお客様向けに VPN サービスのプロビジョニングを可能にする付加価値機能です。法人のお客様が、それぞれ固有の設定可能なパラメータとカスタムディクショナリを使用して、独自の AAA サーバーを維持できます。

この機能は最大 800 の AAA サーバーグループと 800 の NAS IP アドレスを単一のコンテキスト内またはシャーシ全体でプロビジョニングできるようサポートします。1 つのサーバーグループには合計 128 台のサーバーを割り当てることができます。シャーシあたり最大 1,600 のアカウンティングサーバー、認証サーバー、仲介サーバーがサポートされます。



重要 AAA アプリケーションは間接的に接続されたホストをサポートしないため、直接的に接続されたホストのみを設定します。

ANSI T1.276 準拠

ANSI T1.276は、ネットワーク要素（NE）のセキュリティ対策を規定しています。特に、パスワードの強度、保管、およびメンテナンスのセキュリティ対策に関するガイドラインを規定しています。

ANSI T1.276 は、パスワードセキュリティに関するいくつかの対策を規定しています。これらの対策には次のものが含まれます。

- パスワード強度のガイドライン
- ネットワーク要素のパスワード保管のガイドライン
- パスワードメンテナンス（定期的な強制パスワード変更など）

これらの対策は、ASR 5500 と要素管理システムに適用できます（両方ともパスワード認証を必要とするため）。これらのガイドラインのサブセットが各プラットフォームに適用可能である場合、それらが実装されます。どちらの製品にも適用されないガイドラインの既知のサブセットがあります（証明書認証など）。さらに、プラットフォームは、外部要素に依存するさまざまな認証方法（RADIUS や SSH など）をサポートしています。そのような場合の ANSI T1.276 準拠は、外部要素の領域になります。ANSI T1.276 ガイドラインは、ローカルで設定された通信事業者についてのみ導入されます。

APN のサポート

P-GW のアクセスポイント名（APN）のサポートにはいくつかの利点があります。

- APN に対する広範なパラメータ設定の柔軟性。
- APN内での個々のサブスクライバまたはサブスクライバセットのサブスクライバ階層の作成。
- 単一の APN 内におけるサービスの差別化を可能にする仮想 APN。

StarOS v12.x 以前では、最大 1024 の APN を P-GW で設定できます。StarOS v14.0 以降では、最大 2048 の APN を P-GW で設定できます。APN は、任意のタイプの PDP コンテキスト（つまり、PPP、IPv4、IPv6、または IPv4 と IPv6 の両方）に設定できます。APN ごとに多数のパラメータを個別に設定できます。

ここでは、設定可能な主なパラメータをいくつか示します。

- **アカウンティング**：RADIUS、GTPP、またはなし。使用するサーバーグループ。課金特性：中間サーバーとのインターフェイス。
- **認証**：CHAP や PAP などのプロトコル、または、なし。デフォルトのユーザー名とパスワード。使用するサーバーグループ。PDP コンテキストの数を制限します。
- **拡張課金**：使用するルールベースの名前。拡張された課金設定を保持します（例：EG-CDR のバリエーション、課金ルール、プリペイド/後払いオプションなど）。

- **IP**：IP アドレス割り当ての方法（例：P-GW、モバイル IP、DHCP などによるローカル割り当て）。IP アドレス範囲（APN 間での重複あり、またはなし）。
- **トンネリング**：PPP は L2TP でトンネリングできます。IPv4 は GRE、IP-in-IP、または L2TP でトンネリングできます。複数トンネル間でのロードバランシング。IPv6 は IPv4 でトンネリングされます。その他のトンネリング技術、たとえば IPsec や VLAN タグが APN によって選択される場合がありますが、APN とは別に P-GW で設定されます。
- **QoS**：IPv4 ヘッダー ToS の処理。さまざまな 3GPP トラフィッククラスのトラフィックレート制限。特定のハンドセットの参加解除を回避するための R98 QoS 属性のマッピング。ダイナミック QoS 再ネゴシエーション（別途説明あり）。

APN が P-GW によって決定された後、サブスクライバは AAA サーバーで認証/承認されます。P-GW により、AAA サーバーは、APN 設定の一部またはすべてをオーバーライドする VSA（ベンダー固有属性）を返すことができます。そのため、さまざまなサブスクライバ階層のプロファイルを AAA サーバーで設定し、サブスクライバの認証/承認中に P-GW に渡すことができます。



重要 APN 設定の詳細については、このガイドの「*PDN* ゲートウェイの設定」の章を参照してください。

Gy でのポジティブ想定に基づくクォータ追跡

現在の実装では、PCEF は、Diameter ベースの Gy インターフェイスを使用して OCS と対話し、各サブスクライバのデータセッション用のクォータを取得します。PCEF は、設定された量のクォータが使用された後、または設定された量の時間が経過した後に、OCS を再試行できるようになりました。クォータ値は DCCA サービス設定の一部になり、この DCCA サービスを使用するすべてのサブスクライバに適用されます。一時クォータはボリューム（MB）や時間（分）で指定され、両方のクォータ追跡メカニズムを個別にまたは同時に適用できます。

障害処理シナリオで使用するために設定された暫定合計クォータまたは時間をユーザーが消費すると、PCEF は OCS サーバーを再試行して、機能が復旧されたかどうかを判断します。サービスが復旧された場合、クォータの割り当てと追跡は、標準の使用状況レポート手順に従って続行されます。障害中に使用されたデータが OCS に報告されます。OCS サービスが復旧されていない場合、PCEF は、ユーザーに割り当てられた設定済みの量のクォータと時間を再割り当てする必要があります。OCS がオンラインに戻ると、PCEF は集積されたすべての使用済みデータを OCS に報告する必要があります。複数の再試行と暫定的な割り当てが発生した場合、PCEF はすべての割り当て期間中に使用されたクォータを報告します。

Gy インターフェイスを使用できない場合、P-GW は「ポジティブ想定」モードを開始します。各サブスクライバタイプに固有の処理が施されます。各機能アプリケーションには、Gx インターフェイスの PCRF からのコマンドレベルの AVP に基づいて、一意の一時クォータボリュームの量と期間が割り当てられます。さらに、PCRF によって Gx インターフェイスで送信されるコマンドレベルの AVP によって識別されるサブスクライバグループに対して、ポジティブ想定機能を無効にする設定が可能なオプションが追加されました。

egtpinmgr の非同期コア転送のサポート

egtpinmgr の再起動中の停止時間を最適化するため、egtpinmgr の非同期コア転送のサポートが追加されました。

これまでは、egtpinmgr が再起動すると、まずコアダンプファイルの作成および転送を完了させ、それからリカバリプロセスを開始していました。しかし、コアファイルの転送にはかなりの時間がかかります。egtpinmgr の再起動時の停止時間は、egtpinmgr のリカバリ時間とコアファイル転送時間とを合算した時間でした。

非同期コア転送がサポートされるようになったことで、リカバリプロセスに egtpinmgr が含まれるようになります。今後は、egtpinmgr プロセスがクラッシュすると、カーネルによるコアダンプファイルの転送とリソースの解放を待たずにリカバリが開始されます。その結果、egtpinmgr の再起動時の停止時間は、egtpinmgr のリカバリ時間のみに等しくなります。

この機能拡張により、egtpinmgr の再起動時の停止時間が短縮されます。停止時間は、egtpinmgr の回復に必要な時間のみとなり、コアファイルの作成と転送にかかる時間による影響を受けなくなります。

Gx、Gy、Gz、および LI インターフェイスでの SSID 情報の可用性

S2a インターフェイスでは、P-GW は、CREATE SESSION REQUEST メッセージの TWAN-IDENTIFIER 属性で Wi-Fi アクセスポイントのアイデンティティを受信します。この情報は、AP MAC アドレス、SSID、および CIVIC アドレスで構成されます（AP グループ名などの情報が含まれる場合もある）。

ロケーショントラッキングおよびロケーションベースのポリシーを目的として、上記の情報をポリシーサーバー（Gx）、クォータサーバー（Gy）、課金ゲートウェイ（Gz）、および LI サーバーに伝達する必要があります。この新しい機能によって P-GW が強化され、S2a インターフェイスで受信されるたびに、これらのすべてのインターフェイスに AP SSID、BSSID、およびシビックアドレスが伝播されます。

Gx インターフェイス

Gx インターフェイスでは、この情報は、CCR-I/CCR-U および CCR-T メッセージの TWAN IDENTIFIER 属性で PCRF に送信されます。これには標準 Gx ディクショナリ設定で十分です。

Gy インターフェイス

Gy インターフェイスでは、dcca_custom33 ディクショナリがこのインターフェイスに設定されている場合は常に、この情報が、CCR-I/CCR-U および CCR-T メッセージの、「Civic-Addr」という名前のシスコのベンダー固有属性でクォータサーバーに送信されます。

Gz インターフェイス

Gz インターフェイスでは、custom53 ディクショナリがこのインターフェイスに設定されている場合は常に、この情報が、CDR（課金データレコード）の TWANUserLocationInformation 属性で課金ゲートウェイに送信されます。

LI インターフェイス

LI インターフェイスでは、この情報は、IRI イベントの「twan_identifier」フィールドで LI サーバーに送信されます。これには特定のディクショナリの変更は必要ありません。



重要 PGW は、信頼できる WLAN ネットワークから（SaMOG を介して）s2a インターフェイスでこの SSID/BSSID/シビックアドレス情報を受信します。Cisco SaMOG が使用されている場合は、この情報を SaMOG から PGW に送信する機能を、設定によって制御できます（これについては、SaMOG の機能を参照）。この機能により、ベースライン AAAmgr メモリ使用率が 3 ～ 4% 増加します。

主要な KPI 統計のバックアップとリカバリ

主要な KPI 統計のバックアップとリカバリ機能が導入される前は、統計はバックアップされず、SessMgr タスクの再起動後に統計を回復できませんでした。この制限により、GGSN、P-GW、SAEGW、および S-GW ではタスクの再起動が発生するたびに統計が失われるため、KPI のモニタリングが問題でした。

KPI の計算では、2 つの時間間隔のカウンタ値間の差分を取得し、その時間間隔で特定の手順が正常に処理された割合を決定します。SessMgr がクラッシュしてから回復すると、GGSN、P-GW、SAEGW、および S-GW はカウンタ値を失い、ゼロにリセットされます。そのため、次の間隔で KPI を計算すると、その間隔については負の値になります。その結果、KPI 値を使用してプロットされたグラフが表示されなくなり、運用チームがネットワークパフォーマンスの一貫したビューを取得して、本当に問題があるかどうかを判断することが困難になります。

この機能により、SessMgr の再起動が発生した場合でも信頼性の高い KPI 計算を実行できます。



重要 主要な KPI 統計のバックアップとリカバリに関する詳細は、このガイドの「主要な *KPI* 統計のバックアップとリカバリ」の章を参照してください。

Gx および GTP ベースのインターフェイス全体でのビットレートマッピング

この機能により、より一貫性のある動作が実現され、ベアラーに正しい帯域幅が確実に割り当てられます。

さまざまなインターフェイスによって提供されるビットレートの細分性は、3GPP 仕様では調整されていませんでした。たとえば、PCRF は Gx でビット/秒を使用し、GTP はキロビット/秒を使用していました。bps から kbps への変換が原因で、丸め処理のために MBR/GBR 値の割り当てが正しくなくなる場合がありました。

この機能により、bps（Gx から受信）から kbps への変換が小数点以下の値になる場合、GTP インターフェイスで送信されるビットレート値が切り上げられます。ただし、ビットレート値（AMBR、MBR、GBR）の適用は同じであるままになります。アクセス側に送信される値（kbps 単位）がある場合、切り上げる必要があります。

この機能（ビットレートを kpbs で切り上げる）は、デフォルトで有効になっています。ただし、P-GW サービスでの CLI コマンド **[no] egtp bitrates-rounded-down-kbps** は、切り上げの動作を制御します。この CLI コマンドは、以前の切り捨ての動作を有効または無効にします。デフォルトでは、この CLI コマンドは、切り上げられたビットレート値を使用するように設定されています。CLI の設定に応じて、切り上げ（Ceil）ビットレート値または切り捨てビットレート値が GTP インターフェイスでアクセス側に送信されます。この CLI コマンド が有効になっている場合は、以前の動作になります。また、**show subscribers pgw-only full all** では、APN-AMBR が bps 単位で表示されます。以前は、 **show subscribers pgw-only full all** は、kpbs 単位で表示するために使用されていました。

CR（C4-132189）は、P-GW による GTP 変換のために TS 29.274 で定義されています。

バルク統計サポート

システムがバルク統計をサポートしているため、オペレータは自身にとって重要な統計を表示するだけでなく、その統計の表示形式を設定することもできます。これにより、外部のバックエンドプロセッサで解析できるように統計データをフォーマットすることが可能になるため、統計データの後処理が簡素化されます。

要素管理システム（EMS）とともに使用すると、データを解析、アーカイブ、グラフ化できます。

バルク統計（パフォーマンスデータ）を収集し、（レシーバーと呼ばれる）収集サーバーに送信するようにシステムを設定できます。バルク統計は、グループ内で収集される統計です。個々の統計はスキーマ別にグループ化されています。P-GW でサポートされるスキーマのリストを次に示します。

- **APN**：アクセスポイント名の統計を提供します
- **APN Expansion**：APN ごとおよび QCI ごとのレベルで、より詳細な GTP-C 統計を提供します
- **Card**：カードレベルの統計を提供します
- **Context**：コンテキストサービスの統計を提供します
- **Diameter-acct**：Diameter アカウンティングの統計を提供します
- **Diameter-auth**：Diameter 認証の統計を提供します
- **ECS**：Enhanced Charging Service の統計を提供します
- **eGTP-C**：Evolved GPRS トンネリングプロトコル - 制御メッセージの統計を提供します
- **FA**：FA サービスの統計を提供します

- **GTPC**：GPRS トンネリングプロトコル - 制御メッセージの統計を提供します
- **GTPP**：GPRS トンネリングプロトコル - プライムメッセージの統計を提供します
- **GTPU**：GPRS トンネリングプロトコル - ユーザーメッセージの統計を提供します
- **HA**： HA サービスの統計を提供します
- **IMSA**：IMS 承認サービスの統計を提供します
- **IP Pool**：IP プールの統計を提供します
- **LMA**：ローカル モビリティ アンカー サービスの統計を提供します
- **P-GW**：P-GW ノードレベルサービスの統計を提供します
- **P-GW eGTP-C S2a**：eGTP-C S2a インターフェイスの統計を提供します。
- **P-GW eGTP-C S2b**：eGTP-C S2b インターフェイスの統計を提供します。
- **P-GW eGTP-C S5/S8**：eGTP-C S5 および S8 インターフェイスの統計を提供します。
- **Port**：ポートレベルの統計を提供します
- **PPP**：ポイントツーポイント プロトコルの統計を提供します
- **RADIUS**：RADIUS サーバーごとの統計を提供します
- **System**：システムレベルの統計を提供します

システムは、最大4セット（プライマリ/セカンダリ）のレシーバーの設定をサポートします。各セットは、さまざまなスキーマから特定の統計セットを収集するように設定できます。統計は、システムから手動で取得することも、設定された間隔で送信することも可能です。バルク統計はレシーバにファイルで保存されます。

バルク統計データファイルの形式はユーザーが設定できます。ユーザーは、ファイル名、ファイルヘッダー、フッターの形式を指定して、日付、システムホスト名、システム稼働時間、統計を生成するシステムの IP アドレス（ヘッダーとフッターでのみ使用可能）、ファイルが生成された時刻などの情報を含めることができます。

EMS がレシーバとして使用されている場合、EMS では XML 解析、アーカイブ、グラフ化によって統計データをさらに処理できます。

EMS のバルク統計サーバーのコンポーネントは、収集された統計を解析し、その情報を PostgreSQL データベースに保存します。XML ファイルを生成して転送する必要がある場合は、この要素が XML 出力を生成し、さらなる処理のためにノースバウンド NMS か代替のバルク統計サーバーに送信できます。

さらに、収集された統計をアーカイブする必要がある場合は、バルク統計サーバーにより、サーバー上の代替ディレクトリにファイルを書き込むことができます。管理ユーザーが専用のディレクトリを設定することも、デフォルトディレクトリを使用することもできます。いずれの場合も、ディレクトリは、ローカルファイルシステム上、または EMS サーバーの NFS マウントファイルシステム上に配置できます。



重要 バルク統計の設定の詳細については、『システム アドミニストレーション ガイド』の「バルク統計の設定と維持」の章を参照してください。

輻輳制御

輻輳制御機能により、ポリシーとしきい値を設定して、高負荷状態に直面した場合のシステムの対応方法を指定できます。

輻輳制御は、システムに高い負荷がかかっている場合にパフォーマンスを低下させる可能性のある条件についてシステムをモニターします。通常、これらの条件は一時的なものであり（CPU使用率やメモリ使用率が高い場合など）、すぐに解決されます。ただし、こうした条件が特定の時間間隔で継続している場合や、いくつも発生した場合、システムがサブスクライバセッションにサービスを提供する能力に影響を与える可能性があります。輻輳制御は、このような条件を特定し、状況に対応するためのポリシーを呼び出すのに役に立ちます。

輻輳制御の動作は、次の設定に基づいています。

- **輻輳条件のしきい値**：しきい値は、輻輳制御が有効になっている条件を指定し、システムの状態（輻輳またはクリア）を定義するための制限を確立します。これらのしきい値は、システムに設定されている動作のしきい値と同様の方法で機能します（『Thresholding Configuration Guide』を参照）。主な違いは、輻輳のしきい値に達すると、サービス輻輳ポリシーと SNMP トラップ（starCongestion）が生成されることです。

  しきい値の許容度は、条件をクリアするために到達する必要がある、設定されたしきい値のパーセンテージを決定します。次に、SNMP トラップ（starCongestionClear）がトリガーされます。

  - **ポート使用率のしきい値**：ポート使用率のしきい値を設定した場合、システム内のすべてのポートの平均使用率が指定されたしきい値に達すると、輻輳制御が有効になります。

    - **ポート固有のしきい値**：ポート固有のしきい値を設定した場合、個々のポート固有のしきい値に到達すると、輻輳制御はシステム全体で有効になります。

  - **サービス輻輳ポリシー**：輻輳ポリシーは、サービスごとに設定できます。これらのポリシーは、輻輳状態のしきい値を超えたことをシステムが検出したときにサービスがどのように応答するかを指示します。



重要 輻輳制御の詳細については、『システム アドミニストレーション ガイド』の「軋轢制御」の章を参照してください。

デフォルトおよび専用 EPC ベアラー

コミットされた帯域幅リソース、ジッター、および遅延の要件に従って、さまざまなサービスやアプリケーションクラスの確定的なエンドツーエンド転送とスケジューリング処理を可能にすることで、Quality of User Experience（QoE）の向上に貢献するための基盤を提供します。その結果、各アプリケーションが、ユーザーが期待するサービス処理を受け取ります。

StarOS 9.0 リリース以降、Cisco EPC コアプラットフォームは、1 つ以上の EPS ベアラー（デフォルトと専用）をサポートします。EPS ベアラーは、GTP ベースの S5/S8 インターフェイスの場合は UE と P-GW の間で、PMIP ベースの S2a インターフェイスの場合は UE と HSGW（HRPD Serving Gateway ）の間で実行される 1 つ以上のサービスデータフロー（SDF）の論理的な集約です。GTP が S5/S8 プロトコルとして使用されるネットワークでは、EPS ベアラーは、P-GW にアンカーされた無線ベアラー、S1-U ベアラー、および S5/S8 ベアラーの組み合わせで構成されます。PMIPv6 が使用される場合、EPS ベアラーは、HSGW と P-GW 間の IP 接続を使用して、UE と HSGW の間で連結されます。



重要 P-GW は GTP ベースの S5/S8 および PMIPv6 S2a 機能をサポートしますが、PMIPv6 S5/S8 の商用サポートはありません。

EPS ベアラーは、GTP ベースの S5/S8 設計では UE と P-GW の間で、PMIPv6 S2a アプローチでは UE と HSGW の間で、共通の QoS 処理を受信するトラフィックフローを一意に識別します。サービスデータフロー間で異なる QoS スケジューリングの優先順位が必要な場合は、別々の EPS ベアラーに割り当てる必要があります。パケットフィルタは NAS 手順でシグナリングされ、PDN 接続ごとに一意のパケットフィルタ ID に関連付けられます。

1 つの EPS ベアラーは、UE が PDN に接続するときに確立され、PDN 接続のライフタイム全体にわたって確立されたままになり、その PDN への常時接続の IP 接続が UE に提供されます。このベアラーは、デフォルトベアラーと呼ばれます。PDN 接続は、モバイルアクセス端末と、IMS ネットワーク、ウォールド ガーデン アプリケーション クラウド、バックエンド企業ネットワークなどの外部パケットデータネットワーク（PDN）との間のトラフィックフロー集約を表します。同じ PDN に対して確立された追加の EPS ベアラーは、専用ベアラーと呼ばれます。EPS ベアラーのトラフィック フロー テンプレート（TFT）は、特定の EPS ベアラーに関連付けられたすべての 5 タプルパケットフィルタのセットです。EPC コア要素により、確立された EPS ベアラーごとに個別のベアラー ID が割り当てられます。ある時点で、UE は 1 つ以上の P-GW 上にある複数の PDN 接続を持つことができます。

DHCP Support

P-GW は、次の標準規格で定義されているように、Dynamic Host Control Protocol（DHCP）を使用した、サブスクライバ IP PDN コンテキストへのダイナミック IP アドレス割り当てをサポートします。

- RFC 2131、Dynamic Host Configuration Protocol
- RFC 2132、DHCP Options and BootP Vendor Extensions

IP アドレスを PDN コンテキストに割り当てる方法は、APN ごとに設定されます。各 APN テンプレートは、スタティックアドレスとダイナミックアドレスのどちらをサポートするかを決定します。サブスクライバ PDN コンテキストに動的に割り当てられる IP アドレスは、DHCP を使用して割り当てることができます。

P-GW は、UE に対して DHCP サーバーとして、外部 DHCP サーバーに対して DHCP クライアントとして機能します。P-GW の DHCP サーバー機能と DHCP クライアント機能は互いに完全に独立しています。一方は他方なしで存在できます。

DHCP は、IPv4 アドレスと IPv6 アドレスの両方をサポートします。

P-GW は DHCP リレーをサポートしていません。

遅延 IPv4 アドレス割り当て

初期アクセスシグナリング時に IP アドレスを取得するのとは別に、UE は、デフォルトベアラー確立後の DHCP を介した IP アドレスおよび関連設定の取得を選択することを PCO オプションを使用して示すことができます。これは遅延アドレス割り当てとも呼ばれます。

IPv4 アドレスは、ますます枯渇しつつあるリソースとなっています。LTE などの 4G ネットワークは常にオンになっているため、ECM-IDLE 状態の UE によって IPv4 アドレスなどの不足するリソースを独占することはできませんし、独占すべきでもありません。

PDN タイプ IPv4v6 では、デュアルスタックの導入が可能です。デフォルトでは、P-GW は IPv4v6 PDN タイプにのみ IPv6 アドレスを割り当てます。UE は、必要に応じて IPv4 アドレスの割り当てを遅延させ、割り当てられた IPv4 アドレスをグローバルプールに放出します。P-GW は、IPv4 アドレスをオンデマンドで提供するときに、任意の IPv4 アドレス方式（ローカルプールまたは外部 DHCP サーバー）を採用できます。

DHCP でのオプション 26 のサポート

P-GW は UE の IPv4 アドレスを取得している間、独立した DHCP サーバーやクライアントとして同時に機能します。UE に対しては DHCP サーバーとして機能し、外部 DHCP サーバーに対しては DHCP クライアントとして機能します。以前のリリースでは、P-GW を介した UE と外部 DHCP サーバー間で特定の DHCP オプションを交換できるようになりました。これには、IP-Addralloc プロキシモードで遅延アドレスの割り当てが設定された場合に、特定の外部 DHCP サーバーが提供するオプション（1、3、6、28、43）を IPv4 アドレスとともに UE にリレーするためのサポートが含まれています。

この機能により、DHCP サーバーから DHCP OFFER メッセージで受信するオプション 26 のサポートが追加されます。

P-GW では、UE と外部 DHCP サーバー間で交換される DHCP オプション 26 が保持されています。P-GW はこのオプションをリレーして、UE と外部 DHCP サーバー間の今後のメッセージ交換に対応します。P-GW の外部 DHCP サーバーコンポーネントは、外部 DHCP サーバーが提供する DHCP オプションを予約して保持するため、UE が DHCP リースを更新または再バインドしたときに、P-GW は保存されている値で応答できます。

この機能により、更新要求に関する動作が変更されます。以前は、ASR5500 が DHCP プロキシモードで設定され、DHCP サーバーが更新要求に応答しなかった場合、時間 T2（.85 * リー

ス時間）での再送信には、設定された両方の DHCP サーバーが含まれませんでした。RENEW 状態で一定回数の再試行後に、DHCP リースが期限切れになりました。

この機能で再送信回数が 2 に設定されているとすると、RENEW 状態で DHCP 要求メッセージに対して最大 2 回の再試行が実行されます。DHCP サーバーから応答が受信されず、REBIND 状態に変わった場合、DHCP 要求メッセージも 2 回再試行されます。

以前の動作：以前は、「再送信回数」の値が小さい場合（たとえば 2 以下）、DHCP 要求メッセージは REBIND 状態で再試行されませんでした。

新しい動作：DHCP 要求メッセージは、RENEW 状態と REBIND 状態の両方で設定されている回数だけ再試行されるようになりました。

DHCPv6 のサポート

IPv6 の Dynamic Host Configuration Protocol（DHCP）では、IPv6 ネットワークアドレスなどの設定パラメータを DHCP サーバーから IPv6 ノードに渡すことができます。これにより、再利用可能なネットワークアドレスの割り当て機能や追加機能が自動的に提供されます。

DHCPv6 サポートは、アドレス割り当てを提供するだけでなく、ネットワーク層の IP パラメータの要件も満たします。これらの標準的な使用モードとは別に、DHCPv6 のプレフィックス委任（DHCP-PD）も「UE 背後のネットワーク」シナリオのために 3GPP（Rel 10）で標準化されています。

P-GW は、IPv4 アドレスを管理するのと同様にして IPv6 プレフィックスのライフサイクルを管理します。したがって、セッションのライフタイム中でのこれらのプレフィックスの割り当て、更新、およびリリースは P-GW が行います。IPv6 プレフィックスは主に P-GW に接続された UE のセッションで使用され、委任されたプレフィックスは UE の背後にあるネットワークとデバイスで使用されます。IPv6 プレフィックスの場合、対応する設定に基づいて、ローカルプール、AAA（RADIUS/DIAMETER）サーバー、または外部 DHCPv6 サーバーのいずれかから P-GW が取得されます。委任 IPv6 プレフィックス割り当ての場合では、P-GW が設定に基づいて外部 DHCPv6 サーバーからこれを取得しました。

ユニキャスト アドレス サポート機能：要求された UE の IPv6 プレフィックス委任は、ローカルに割り当てられるか、P-GW、GGSN、SAEGW がこれらのノードの設定に基づいて外部 DHCPv6 サーバーから割り当てます。これらの DHCP メッセージは、宛先アドレスにマルチキャストアドレスを使用し、外部 DHCPv6 サーバーに送信されます。P-GW サーバーが多数存在するが、DHCP サーバーの数は少ないネットワークでは、マルチキャストアドレスの DHCPv6 メッセージはネットワーク全体を通過する必要があり、ネットワークの負荷が増加します。ユニキャストアドレス サポート機能により、通信事業者は、DHCP サービスで DHCPv6 サーバーの設定済みアドレスを使用して、ユニキャストアドレスのすべての DHCPv6 メッセージを外部サーバーに送信できます。この機能は CLI で制御されており、通信事業者は、DHCP サーバーに対するクライアントユニキャストの動作をサポートするように CLI を設定する必要があります。

P-GW の DHCPv6 サポートは、次の要件に対応しています。

- RFC 3315、Dynamic Host Configuration Protocol for IPv6 (Basic DHCPv6)
- RFC 3633、プレフィックス委任メカニズム



重要 DHCPv6 サービスの設定の詳細については、「*PDN* ゲートウェイの設定」の章の「*DHCPv6* 設定」セクションを参照してください。

ダイレクトトンネルサポート

プレリリース SGSN との Gn/Gp インターワーキングが有効になっている場合、P-GW 上の GGSN サービスはダイレクトトンネル機能をサポートします。

ダイレクトトンネルでは、ユーザープレーンからの SGSN トンネルの「スイッチング」遅延が排除されることで、ユーザーエクスペリエンスが向上します（Web ページの迅速な配信、会話型サービスのラウンドトリップ遅延の短縮など）。運用コストおよび資本コストの観点から見たダイレクトトンネルの他の利点は、ダイレクトトンネルでは、SGSN でのユーザープレーン処理の要件を排除することにより、ユーザープレーンリソースの使用が最適化されることです。

ダイレクト トンネル アーキテクチャにより、SGSN をバイパスして、RAN と GGSN の間で直接ユーザープレーントンネルを確立できます。SGSN は、引き続きコントロール プレーン シグナリングを処理し、通常は PDP コンテキストのアクティブ化でダイレクトトンネルの確立を決定します。ダイレクトトンネルは、PDP コンテキストのアクティブ化で SGSN によって実現されます。SGSN は、（GGSN への PDP コンテキスト更新要求を使用して）RNC と GGSN の間で直接ユーザープレーン（GTP-U）トンネルを確立します。

ダイレクトトンネル展開の主要な結果として、パケットコアの SGSN コンポーネントと GGSN コンポーネントの両方で、コントロールプレーンの負荷が大幅に増加します。そのため、展開された GGSN が、ダイレクトトンネル展開の一環として導入された追加のコントロールプレーンの負荷を処理できることを確認することがワイヤレスオペレータにとって最も重要です。Cisco GGSN および SGSN は、大規模なコントロール プレーン トランザクション機能を提供し、ダイレクトトンネルが展開された後、システム コントロール プレーンのキャパシティがキャパシティ制限要因にならないようにします。



重要 ダイレクトトンネルのサポートに関する詳細については、このガイドの「*4G*（*LTE*）ネットワークのダイレクトトンネル」の章を参照してください。

IPv4/IPv6 PDP コンテキストの DNS サポート

StarOS リリース 15.0 では、この機能により、PDN タイプ IPv4v6 用の機能が P-GW に追加されます。以前は、MS が IPv4 DNS アドレスを要求した場合、P-GW は IPv4 DNS アドレスを送信しませんでした。

MS は、PDP タイプ IPv4、IPv6、または IPv4v6 の PDP コンテキストアクティブ化プロシージャでプロトコル設定オプション IE を使用して（コンテナまたは IPCP プロトコル設定要求の一部として）、DNS サーバーの IPv4 または IPv6 アドレスを要求する場合があります。その場合、

P-GW は、PDP コンテキストアクティブ化応答メッセージで PCO IE 内の 1 つ以上の DNS サーバーの IP アドレスを返すことができます。DNS アドレスは、3GPP TS 24.008 で規定されているとおりに PCO にコード化されます。

PDP タイプ IPv4v6 の場合、MS が DNS サーバーの IPv4 アドレスを要求すると、IPv4 アドレスが返されませんでした。MS によって要求されたアドレスで応答するためのサポートが追加されました。

AAA サーバーは、Access-Accept 認証応答で DNS サーバーの IP アドレスを提供する場合もあります。このような場合、AAA が提供する DNS サーバーの IP は、APN で設定された IP よりも優先されます。

PCO 設定で DNS サーバーのアドレスが要求される場合は、次の優先順位に従います。

1. RADIUS サーバーから受信した DNS 値。
2. APN でローカルに設定した DNS 値。
3. **ip name-servers** CLI を使用してコンテキストレベルで設定した DNS 値。

ドメインベースフロー定義

このソリューションにより、DNS応答をスヌーピングすることで、地理的に適切で正確なサーバーの IP エントリを取得する際の柔軟性と精度が向上します。

現在のところ、ドメイン（m.google.com）に基づいてフィルタリングするように L7 ルールを設定できます。複数のサーバーがドメインにサービスを提供し、それぞれが独自の IP アドレスを持つ場合があります。HTTP ルールの代わりに IP ルールを使用すると、複数の IP ルールが作成されます。ドメインの「背後」にある各サーバーに対して 1 つの IP ルールが作成されるため、ドメインベースのフィルタのために IP アドレスのリストを維持するのに手間がかかる可能性があります。

このソリューションでは、ホスト名（ドメイン名）とホスト名（ドメイン名）の一部を指定するruledefを作成できます。ホスト名やドメイン名、またはそれらの一部の定義に応じて、P-GW は、UE に送信されたすべての DNS 応答をモニターし、ルールで指定されている q-name または a-name を持つ DNS 応答のみをスヌーピングして、DNS 応答から得られたすべての IP アドレスを特定します。DNSスヌーピングは、すべてのサブスクライバのライブトラフィックに対して実行されます。

DSCP マーキング

DSCP マーキングの精度の高い設定サポートが提供されます。

双方向トラフィッククラスの場合、P-GW は現在の優先順位に加えて、割り当てや保持の優先順位に基づいて、アップリンクおよびダウンリンク方向に対するゲートウェイごとのサービスや、APN ごとに設定可能な DSCP マーキングをサポートします。

次のマトリックスを使用すると、設定されたトラフィッククラスや割り当て/保持の優先順位に基づいて使用される Diffserv マーキングを決定できます。

表 *1* : デフォルトの *DSCP* 値マトリックス

割り当て優先順位	1	2	3
トラフィック処理の優先順位			
1	ef	ef	ef
2	af21	af21	af21
3	af21	af21	af21

さらに、P-GW では DSCP 値を使用した Diameter パケットおよび GTP-C/GTP-U エコーの設定が可能です。

RAT タイプベースの DSCP マーキング

通信事業者は、RAT タイプに基づいて、P-GW、SAE-GW、GGSN などのゲートウェイで DSCP マーキングを実行できます。これにより、通信事業者はさまざまな QoS サービスを設定し、RAT タイプ（EUTRAN、GERAN、UTRAN）に基づいてトラフィックを最適化できます。

RAT タイプベースの DSCP マーキングには次のものがあります。

- すべての QCI および ARP 値をサポートします。
- 標準および非標準 QCI をサポートします。
- 特定の RAT タイプが設定されていない場合、DSCP マーキング機能はすべての RAT タイプに適用されます。
- 仮想 APN に適用されます。
- RAT 間のハンドオフ時に、現在のハンドオフの RAT タイプに基づき DSCP マーキングが実行されます。
- RAT タイプごとの DSCP マーキングは、ユーザーデータトラフィックにのみ適用され、制御トラフィック（GTP-C パケット）には適用されません。

重要 既存の DSCP マーキングおよび IP-ToS 機能については、下位互換性が維持されています。

APN ごとの GTP-U

この機能により、APN ごとに異なる DSCP マーキングテーブルを柔軟に作成できるため、APN のニーズに応じて、各 APN のトラフィックを異なる方法でマーキングできます。

S-GW と P-GW は、S5 および S8 インターフェイスと Gn および Gp インターフェイスの QCI または THP テーブルに基づいて、GTP-U トンネルパケットの外部ヘッダーの設定可能な DSCP マーキングをサポートします。この機能により、APN ごとに DSCP マーキングテーブルを設定できます。

以前は、DSCP マーキングテーブルは P-GW サービスレベルで設定されていました。この要件の一環として、APN に qos-qci-mapping テーブルを関連付ける CLI が追加されました。



重要 有効なライセンスキーがインストールされていない場合、P-GW は非標準の QCI 値をサポートしません。

QCI 値 1 ～ 9 は、3GPP TS 23.203 で定義されている標準値です。P-GW はこれらの標準値をサポートします。

3GPP リリース 8 以降では、通信事業者固有/非標準の QCI がサポートされ、キャリアは QCI 128- 254 を定義できます。詳細については、非標準 QCI のサポート （103 ページ）を参照してください。

以前の設定との下位互換性を維持するために、DSCP マーキングテーブルが APN ではなく P-GW サービスに関連付けられている場合、P-GW サービス内のテーブルが使用されます。テーブルが P-GW サービスと APN の両方に関連付けられている場合は、APN 上のテーブルが優先されます。

動的 GTP エコータイマー

動的 GTP エコータイマーを使用すると、eGTP および GTP-U サービスで、ネットワーク輻輳時の GTP パスをより適切に管理できます。固定の間隔と再送信タイマーを使用するデフォルトのエコータイマーとは対照的に、動的エコータイマーは、完全な要求/応答手順が完了すると生成される、計算されたラウンドトリップタイマー（RTT）を追加します。輻輳期間中の追加サポートのために、計算に乗数を追加できます。



重要 詳細については、「*PDN* ゲートウェイの設定」の章の「*P-GW* でのオプション機能の設定」にある「*GTP* エコータイマーの設定」を参照してください。

ダイナミックポリシー課金制御（Gx 参照インターフェイス）

ダイナミックポリシーおよび課金制御は、IMS マルチメディア アプリケーションを実現するための主要な構成要素となります。静的にプロビジョニングされたアーキテクチャとは対照的に、ダイナミック ポリシー フレームワークは、すべてのアクセス側ネットワーク要素のグローバルな認識を、一元化されたサービス制御レイヤに提供します。一元化されたポリシー決定要素により、複数のアクセスゲートウェイにグローバルなポリシーをプロビジョニングするプロセスが簡素化されます。ダイナミックポリシーは、常時稼働の導入モデルで特に有用です。これは、使用パラダイムが短期からより長いオンラインセッションに移行する際に、消費されるデータ量が大量になる可能性があるためです。このような条件では、ダイナミックポリシー管理により動的な即時リソース割り当てが可能になり、ネットワークの容量とリソースをより効率的に保護できます。

ダイナミックポリシー制御とは、P-GWのポリシー課金適用機能（PCEF）とPCRF間で、サービスおよびアプリケーションフローを動的に許可および制御する機能を表します。ポリシー制御により、一元化された分割サービス制御アーキテクチャが可能になり、ベアラーリソースレイヤでサービスがプロビジョニングおよび割り当てられる方法を管理できます。

StarOS 9.0 リリースには、3GPP TS 29.212 および 29.230 の機能に準拠するための拡張機能が含まれています。Gx 参照インターフェイスは、Diameter トランスポートと IPv6 アドレッシングを使用します。サブスクライバは、Subscription-ID AVP 内の IMSI ベースの NAI を使用して、セッション確立時に PCRF へと識別されます。さらに、Equipment-Info AVP 内の IMEI は、ポリシーサーバーに対するサブスクライバアクセス端末の識別に使用されます。Gx参照インターフェイスは、以下の機能をサポートしています。

- パケットフローのベアラー確立の承認
- ダウンリンクおよびアップリンク IP CAN ベアラーの選択とポリシー適用のための PCC ルールでの、サービス データ フロー フィルタの動的な L3 および L4 転送
- ピアツーピアの検出などのインラインサービスをアクティブ化するためのトリガーとしてサポートされる、事前にプロビジョニングされた静的 L7 ルールベース名属性
- サービスデータフローの変更の承認
- パケットフローの承認の取り消し
- デフォルトまたは専用の EPS ベアラーにマッピングされたサービスデータフローの PCC ルールのプロビジョニング
- アクセス ネットワーク ゲートウェイまたは IP CAN の変更に基づき P-GW が開始するイベントトリガーのサポート
- デフォルト EPS ベアラーの APN-AMBR を設定または変更する機能の提供
- PCRF から PCEF 機能に送信される PCC ルールに QCI 値を含めることによる、QoS サービスの優先順位の作成または変更

Enhanced Charging Service（ECS）

Enhanced Charging Service は、サブスクライバのデータパケットを検査して詳細レコードを生成するための統合型インラインサービスを提供します。これにより、使用量やトラフィックパターンに基づく課金が可能になります。その他の特長には次のようなものがあります。

- コンテンツ分析サポート （38 ページ）
- コンテンツサービスのステアリング （39 ページ）
- 複数の詳細レコードタイプのサポート （39 ページ）
- Diameter クレジット制御アプリケーション （40 ページ）
- DCCA サーバーからの TCP 接続の受理 （41 ページ）
- Gy インターフェイスのサポート （41 ページ）

Enhanced Charging Service（ECS）は、システム内に統合されるインラインサービス機能です。ECS はモバイルキャリアの機能を強化し、バックエンド課金仲介システムとの統合機能を備え

たレイヤ 3 からレイヤ 7 のディープ パケット インスペクション（DPI）を使用して、サブスクライバに柔軟で差別化された詳細な課金情報を提供します。

ECS はアクティブ状態の仲介システムと連携して、リアルタイムの完全な前払いおよびアクティブな課金機能を提供します。このとき、アクティブな仲介システムがさまざまなアプリケーションの料金設定機能や請求機能を提供します。

さらに、ECS に組み込まれた広範なレコード生成機能は、ユーザーセッションを細部まで把握して後払い課金にも対応します。詳細については、複数の詳細レコードタイプのサポート（39 ページ）を参照してください。

主要コンポーネントは以下のとおりです。

- **サービスステアリング**：サブスクライバトラフィックを ECS サブシステムに転送します。サービスステアリングは、アクセス制御リスト（ACL）を介してサブスクライバトラフィック フローを選択して転送するために使用されます。これは、他のリダイレクトアプリケーションだけでなく、内部と外部サービスやサーバーにも使用されます。
- **プロトコルアナライザ**：パケット検査中に個々のプロトコルフィールドや状態を分析するソフトウェアスタック。次の 2 種類のパケットインスペクションを実行します。
  - **シャロー パケット インスペクション**：レイヤ 3（IP ヘッダー）およびレイヤ 4（UDP や TCP ヘッダーなど）情報の精査。
  - **ディープ パケット インスペクション**：レイヤ 7 および 7+ 情報の精査。ディープ パケット インスペクション機能により、以下が実行されます。
    - レベル 7 の URI（Uniform Resource Identifier）情報（HTTP、WTP、RTSP Uniform Resource Locator（URL）など）を検出します。
    - 終端プロキシの場合、真の宛先を識別します。シャローパケットインスペクションでは、終端プロキシの宛先 IP アドレスやポート番号のみが明らかになります。
    - MMS-over-WTP、WSP-over-UDP、IP-over-GPRS などの上位層プロトコルヘッダーのカプセル化を解除します。
    - トラフィックが、レイヤ 4 のポート番号が示すプロトコルに実際に準拠していることを確認します。
- **ルール定義**：プロトコルフィールドやプロトコル状態に基づいたユーザー定義の式により、特定のフィールド値が true の場合に実行するアクションを定義します。式にはオペランドのデータ型に基づいて、複数の演算子タイプ（文字列、=、> など）を含めることができます。各ルール定義は、それぞれのアナライザでサポートされている任意のフィールドや状態に適用する複数の式で構成されます。
- **ルールベース**：ルール定義と関連する請求ポリシーを集めたもの。ルールベースは、ルールが一致したときに実行されるアクションを決定します。複数のアクションを伴うルール定義を設定できます。

仲介と課金の方法

課金仲介システムと統合する際の柔軟性を最大限に高めるため、ECS は課金インターフェイスと承認インターフェイスを全範囲に渡ってサポートしています。

- **前払い**：前払い環境では、サブスクライバは使用前にサービスの料金を支払います。サブスクライバがサービスを使用している間、クレジットを使い果たすか、通話が終了するまで、サブスクライバのアカウントからクレジットが差し引かれます。前払いアカウンティングサーバーの役割は、ユーザーにアクセスを許可し、接続時間または使用量に対するクォータを付与する権限をネットワークノード（GGSN）に与えることです。クォータの使用状況の追跡はネットワークノードの役割です。これらの使用クォータが少なくなると、ネットワークノードは前払いサーバーにクォータを増やす要求を送信します。

  ユーザーが購入したクレジットに残高がある場合、サーバーはクォータを付与します。サブスクライバが利用できるクレジットがない場合は、通話が切断されます。ECS と DCCA はこの機能を管理するために、さまざまなサービスにクォータを設定する機能を提供します。

  ECS の前払いクォータは、DIAMETER クレジット制御アプリケーション（DCCA）を使用して実装されます。DCCA を使用することで、ネットワークアクセス、メッセージングサービス、ダウンロードサービスなどのさまざまなサービスにリアルタイムのクレジット制御機能を実装できます。

  DCCA はコストとクレジットをリアルタイムで制御するための一般的なソリューションであることに加えて、 次の機能を備えています。

  - **リアルタイム料金サービス情報**：DCCA はいつエンドサブスクライバのアカウント残高がなくなったか、あるいは期限切れになったかを確認できます。もしくは、追加の課金対象イベントを拒否できます。
  - **複数サービスのサポート**：DCCA は 1 つのサブスクライバセッション内での複数サービスの使用をサポートします。複数サービスのサポートには次が含まれます。 1）さまざまなコスト構造の対象となるサービスまたはサービスのグループを特定して処理する機能。2）単一のクレジット制御サブセッションで複数サービスのクレジットを個別に制御。

    詳細については、「Diameter クレジット制御アプリケーション （40 ページ）*Diameter* クレジット制御アプリケーション」を参照してください。

- **後払い**：後払い環境では、サブスクライバはサービスの使用後に支払います。AAA サーバーの役割は、ユーザーにアクセスを許可する権限をネットワークノード（GGSN）に与えることです。CDR システムは、事前に定義した使用量の測定間隔や時間ごとに課金情報の G-CDR/eG-CDR/EDRs/UDR またはカンマ区切り値（CSV）を生成します。



重要 Enhanced Charging Service 機能には、サービスライセンスが必要です。 ECS ライセンスは P-GW セッション使用ライセンスに含まれています。ECS の詳細については、『*ECS Administration Guide*』を参照してください。

コンテンツ分析サポート

Enhanced Charging Service では、OSI モデルの各種レイヤでさまざまなプロトコルのパケットのコンテンツ分析を実行できます。

ECS コンテンツアナライザは、OSI スタックのすべてのレイヤでさまざまなプロトコルの状態を検査して維持できます。ECS システムは、次のプロトコルをサポート、検査、分析します。

- IP
- TCP
- UDP
- DNS
- [FTP]
- TFTP
- SMTP
- POP3
- HTTP
- ICMP
- WAP：WTP および WSP
- Real-time Streaming：RTP および RTSP
- MMS
- SIP および SDP
- ファイル分析：HTTP や FTP などのファイル転送プロトコルからダウンロードされたファイルの特性（ファイルサイズ、転送されたチャンクなど）を調べます。

Enhanced Charging サブシステムのトラフィックアナライザは、設定されたルールに基づいて分析を実行します。トラフィック分析に使用されるルールは、パケットフローを分析して使用状況のレコードを形成します。使用状況レコードはコンテンツタイプごとに作成され、前払いサーバーまたは仲介/請求システムに転送されます。トラフィックアナライザは、IP パケットフローのシャロー パケット インスペクション（レイヤ 3 およびレイヤ 4）とディープ パケット インスペクション（レイヤ 4 より上位のレイヤ）を実行します。

トラフィックアナライザ機能は、IP パケットフローのシャローパケットインスペクション（レイヤ 3 およびレイヤ 4）とディープ パケット インスペクション（レイヤ 4 より上位のレイヤ）を実行できます。

すべてのレイヤ 3 パケット（およびバイト）を上位層のトリガー基準（たとえば、HTTP ヘッダーで検出された URL）と関連付けることができ、データパス用にポートを動的に開く FTP、RTSP、SIP などの複雑なプロトコルに対してステートフル パケット インスペクションも実行します。このようにして、ユーザープレーンのペイロードは「カテゴリ」に分類されます。

トラフィックアナライザはアプリケーションレベルでも機能し、サービスプラットフォームの干渉を受けることなくイベントベースの課金を実行します。



重要 この機能は、セッション使用ライセンスが必要な Enhanced Charging Service で使用できます。ECS の詳細については、『*ECS Administration Guide*』を参照してください。

コンテンツサービスのステアリング

コンテンツ サービス ステアリング（CSS）は、モバイルサブスクライバによって提供されるデータの内容に基づいて、選択的なサブスクライバトラフィックを ECS サブシステム（システム内部のインラインサービス）に転送します。

CSS は、アクセス制御リスト（ACL）を使用して、選択的サブスクライバ トラフィック フローをリダイレクトします。ACL は、システムに出入りするパケットのフローを制御します。ACL は、フィルタ基準に一致するパケットに対して実行されるアクションを制御する「ルール」（ACL ルール）またはフィルタで構成されます。

ACL はコンテキストごとに設定可能であり、接続先コンテキストのサブスクライバプロファイルまたは APN プロファイルを使用してサブスクライバに適用されます。



重要 CSS の詳細については、『*System Administration Guide*』の「*Content Service Steering*」の章 [英語] を参照してください。



重要 ACL の詳細については、『*System Administration Guide*』の「*IP Access Control Lists*」の章 [英語] を参照してください。

複数の詳細レコードタイプのサポート

標準ソリューションの要件を満たすと同時に、サービスの使用状況に関する柔軟で詳細な情報を提供するために、Enhanced Charging Service（ECS）は次のタイプの使用状況レコードを提供します。

- イベント詳細レコード（EDR）
- 使用量の詳細レコード (UDR)

ECS では、課金データファイルを生成できます。このデータファイルはシステムから定期的に取得でき、後処理のための課金仲介システムへの入力データとして使用できます。これらのファイルは標準形式で提供されるため、既存の請求/仲介システムへの影響を最小限に抑えると同時に、コンテンツに基づく請求に必要なすべての情報がこれらのレコードに含まれています。

ECS の GTPP アカウンティングにより、さまざまなタイプのデータトラフィックのカウンタを詳細レコードに収集できます。次のタイプの詳細レコードがサポートされています。

- **イベント詳細レコード（EDR）**：G-CDR によって提供される情報がコンテンツの課金を行うのに不十分な場合に、標準 G-CDR に代わる手段です。EDR はルールコマンドの明示的なアクション文に従って生成され、ユーザーが設定できます。EDR はカンマ区切り値（CSV）形式で生成され、またトラフィック分析ルールで定義されたように生成されたます。
- **ユーザー詳細レコード（UDR）**：特定のモバイルサブスクライバに関連するアカウンティング情報が含まれています。レポートされるフィールドはユーザーが設定でき、時間しきい値、ボリュームしきい値、ハンドオフ、およびコール終了のいずれかのトリガーで生成されます。UDR はカンマ区切り値（CSV）形式で生成され、またトラフィック分析ルールで定義されたように生成されたます。



重要 この機能は、セッション使用ライセンスが必要な Enhanced Charging Service で使用できます。ECS の詳細については、『*ECS Administration Guide*』を参照してください。

Diameter クレジット制御アプリケーション

次の**標準**に基づいて、リアルタイムでのコストとクレジットの制御を可能にするプリペイド請求メカニズムを提供します。

- RFC 3588、Diameter Base Protocol（2003 年 9 月）
- RFC 4006、Diameter Credit-Control Application（2005 年 8 月）

Diameter クレジット制御アプリケーション（DCCA）は、ネットワークアクセス、Session Initiation Protocol（SIP）サービス、メッセージングサービス、ダウンロードサービスなどのさまざまなエンドユーザーサービスにリアルタイムのクレジット制御を実装するために使用されます。

ECS と組み合わせて使用することで、DCCA インターフェイスでは、要求したサービスに対して課金される料金をユーザーに通知できるメカニズムが使用されます。さらに、ゲームや広告など、ユーザーアカウントからクレジットとデビットを利用できるサービスもあります。

DCCA は次の機能もサポートしています。

- **リアルタイム料金サービス情報**：エンドサブスクライバのアカウントの残高がなくなったとき、またはアカウントが期限切れになったときに確認する機能。または、追加の課金対象イベントを拒否する機能。
- **複数サービスのサポート**：1 つのサブスクライバセッション内での複数のサービスの使用がサポートされます。複数のサービスサポートには以下が含まれます。
  - 異なるコスト構造の対象となるサービスまたはサービスのグループを特定および処理する機能。

- 単一のクレジット制御サブセッションでの、複数のサービスの独立したクレジット制御。



重要 この機能は、セッション使用ライセンスが必要な Enhanced Charging Service で使用できます。ECS の詳細については、『*ECS Administration Guide*』を参照してください。

DCCA サーバーからの TCP 接続の受理

この機能により、ピアの Diameter クレジット制御アプリケーションサーバーが NGME への接続を開始できます。

また、Diameter サーバーが Diameter 着信要求を受信できない場合に、Diameter ピアノードは TCP ポート 3868 上の NGME に接続できます。



重要 StarOS 12.3 以前のリリースを使用している場合、Diameter 機能の詳細については、『*AAA and GTPP Interface Administration and Reference*』[英語] を参照してください。StarOS 14.0 以降のリリースを使用している場合は、『*AAA Interface Administration and Reference*』を参照してください。

Gy インターフェイスのサポート

Gy インターフェイスを使用すると、ワイヤレスオペレータは、リアルタイムコンテンツベースの課金のために標準化されたインターフェイスを導入でき、時間ベースの課金と使用量ベースの課金のレートを区別できます。

Gy インターフェイスはクォータメカニズムに基づいているため、Gy インターフェイスを使用することで、ワイヤレスオペレータは高額なプリペイドシステムのリソースを節約できます。

Gy インターフェイスでは、時間、使用量、およびイベントベースの課金モデルが可能であるため、オペレータは、サービス戦略に合わせた課金モデルを柔軟に導入できます。

Gy インターフェイスは、データサービスのリアルタイム コンテンツ ベースの課金のために、標準化された Diameter インターフェイスを実現します。これは 3GPP 標準規格に基づいており、クォータ割り当てに依存しています。

このインターフェイスは、ECS ディープ パケット インスペクション機能と連携するオンライン課金インターフェイスを実現します。Gy を使用すると、カスタマートラフィックをゲートウェイに送り、「オンライン」または「プリペイド」の形式で課金できます。時間ベースと使用量ベースの課金モデルがサポートされています。これらのすべてのモデルで、シャロー パケット インスペクションまたはディープ パケット インスペクションに基づいて、各種サービスに異なるレートを適用できます。

Gy は Diameter インターフェイスです。そのため、Diameter 基本プロトコル上に導入され、その機能を継承します。システムは、TLS またはプレーンテキスト TCP を使用して、直接接続

された、リレーされた、またはプロキシされたDCCAサーバーなど、該当する基本ネットワークとアプリケーション機能をサポートしています。

最も単純なインストールでは、システムは、Diameter TCP リンクを介して、システム自体と 1 台の「前払い」サーバーとの間で、Gy Diameter メッセージを交換します。インストールを堅牢化するには、複数のサーバーを使用します。これらのサーバーは、必要に応じて単一のクォータデータベースを共有またはミラーリングして、あるサーバーから別のサーバーへの Gy セッションのフェールオーバーに対応します。拡張性の高いインストールでは、プロキシまたは他のDiameterエージェントのレイヤを導入して、マルチパス メッセージルーティング、メッセージやセッションのリダイレクト機能などを提供できます。

シスコの導入は次の標準規格に基づいています。

- RFC 4006 汎用 DCCA（以下を含む）
  - CCR 初期、更新、および最終シグナリング
  - ASR および RAR 非同期 DCCA サーバーメッセージ
  - 時間、合計オクテット、およびサービス固有ユニットのクォータ管理
  - Multiple-Services-Credit-Control を使用した複数の独立クォータ
  - クォータとトラフィックの関連付けに関する料金設定グループ
  - CC-Failure-Handling 機能と CC-Session-Failover 機能
  - initial-Unit-Action での TERMINATE の動作
  - Tariff-Time-Change 機能
- 3GPP TS 32.299 オンラインモード「Gy」DCCA。これには以下が含まれます。
  - Final-Unit-Action REDIRECT の動作
  - Quota-Holding-Time：カテゴリごとにユーザートラフィックのアイドル時間を定義します。その後、使用状況が返され、新しいクォータは明示的に要求されません。
  - Quota-Thresholds：これらの AVP は、クォータが完全になくなる前に新しいクォータが要求される最低値のウォーターマークを定義します。ユーザートラフィックの中断を抑制することを目的としています。

    これらの AVP は、すべてのクォータフレーバー（「Time-Quota-Threshold」など）に対して存在します。
  - Trigger-Type：この AVP は、現在のセッションとそのクォータカテゴリの再認証を発生させるイベントのセットを定義します。

Framed-Route 属性のサポート

Framed-Route 属性は、このネットワーク アクセス サーバー（NAS）上のユーザーに対して設定するルーティング情報を提供します。Framed-Route 情報は、Access-Accept メッセージで RADIUS サーバーに返されます。

モバイルルータは、P-GW が RADIUS サーバーを使用して許可する PDN セッションをルータが作成できるようにします。RADIUS サーバーはこのルータを認証し、access-accept応答パケットに Framed-Route 属性を含めます。また、Framed-Route 属性は「モバイルルータ」用に P-GW にインストールされるサブネットルーティング情報も指定します。P-GW は、宛先アドレスが Framed-Route と一致するパケットを受信すると、関連付けられた PDN セッションを介してモバイルルータに転送されます。詳細については、「*APN* 上のモバイルステーション背後のルーティング」の章を参照してください。

Gn/Gp ハンドオフのサポート

この機能の統合されたサポートには、P-GW と GGSN の両方に有効なセッション使用ライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

LTE 展開では、3G/2G ネットワークと LTE ネットワーク間でのスムーズなハンドオーバーのサポートが必要です。Evolved Packet Core（EPC）は、さまざまなアクセステクノロジーに共通のパケットコアとして設計されています。P-GW は、ユーザー機器（UE）が異なるアクセステクノロジーに移行するときに、ハンドオーバーをサポートします。

シスコの P-GW は、4G アクセスと 3G/2G アクセス間のテクノロジー間モビリティハンドオーバーをサポートします。4G と 2G/3G SGSN の間のインターワーキングがサポートされており、このインターワーキングでは、Gn および Gp インターフェイスのみが提供され、S3、S4 または S5/S8 インターフェイスは提供されません。これらの Gn/Gp SGSN では、Evolved Packet System（EPS）のために導入された機能や、E-UTRAN との相互運用のために特に導入された機能は提供されません。これらのハンドオーバーは、GTP ベース S5/S8 でのみサポートされ、P-GW は、GTPv2 ベース S5/S8 と GTPv1 ベース Gn/Gp トンネル接続の間のハンドオフをサポートします。このシナリオでは、P-GW は EPC の IP アンカーとして機能します。

重要 GGSN と P-GW 間のセッションのシームレスなハンドオーバーをサポートするには、2 つの独立したサービスを同じノードに配置し、同じコンテキスト内で設定して、最適な相互運用性を実現する必要があります。

重要 Gn/GP ハンドオフの詳細については、「Gn/Gp インターフェイス （11 ページ）」を参照してください。

GTP-C パス障害の機能拡張とデバッグツールの改善

StarOS リリース 20.0 では、GTP-C パス障害機能を最適化し、GTP-C パス障害の問題に対するシステムのデバッグ機能を向上させるための機能拡張が追加されました。これらの機能拡張は、オペレータとエンジニアがシステムのさまざまな側面をデバッグし、ネットワーク内の GTP-C パス障害の根本原因を特定するのに役立ちます。これらの機能拡張は、S5、S8、S2b、および S2a インターフェイスを介したパス障害検出に影響を及ぼします。

この機能の一部として、次の拡張機能が追加されました。

- 誤ったメッセージや偽のメッセージが原因で低い値のリスタートカウンタを受信した場合、パス障害を検出しないようにノードを設定でき、コールの損失を防げます。エコー要求/応答メッセージや制御メッセージ要求/応答メッセージによるパス障害を無効にするオプションも使用できるため、パス障害の誤検出が発生した場合にコールの損失を防げます。
- ネットワーク内の問題の根本原因をより迅速に診断できるように、GTP-C パス障害の統計情報の精度が向上しました。
- ピアごとに最後の 5 つのパス障害に関するパス障害履歴を、ネットワーク内のパス障害のデバッグに使用できます。
- シームレスなパス障害処理が実装されているため、冗長性イベント中のコールの損失が回避されます。

誤ったパス障害検出を回避するためのサポート

誤ったパス障害検出を回避するノードの機能を促進するために、いくつかの機能強化が加えられました。

- ピアからのスプリアスメッセージや不正確なメッセージによるパス障害検出を回避するために、ソフトウェアの機能が強化されました。これらのメッセージにより、サービスの非アクティブ化とアクティブ化の数が原因でネットワークトラフィックの大規模なバーストが引き起こされ、ネットワーク輻輳が発生する可能性があります。この問題を解決するために、*eGTP-C* サービス コンフィギュレーション モードの **gtpc** コマンドが拡張されました。誤ったパス障害検出が GTP-C パス障害として検出されないようにするために、**max-remote-restart-counter-change** キーワードが追加されました。たとえば、**max-remote-restart-counter-change** が 10 に設定されており、現在のピアの再起動カウンタが 251 の場合は、新しい再起動カウンタが 252 ～ 255 または 0 ～ 5 の場合にのみ、eGTP はピアの再起動を検出します。同様に、保存された再起動カウンタが 1 の場合は、新しい再起動カウンタが 2 ～ 11 の場合にのみ、eGTP はピアの再起動を検出します。
- また、この機能強化の一環として、パス障害検出を有効または無効にするための新しいキーワードが *eGTP-C* サービス コンフィギュレーション モードの **path-failure detection-policy** コマンドに追加されました。
- EXEC モードの **show egtp-service all** コマンドが拡張され、ノードでエコー要求/エコー応答再起動カウンタの変更と制御メッセージ再起動カウンタの変更が有効か無効かが示されるようになりました。

GTP-C パス障害統計の改善

オペレータ/エンジニアが障害の原因をより迅速に特定できるように、GTP-C パス障害の品質を向上させるいくつかの改善が行われました。

- **show egtpc statistics path-failure-reasons** の出力が拡張され、demuxmgr および sessmgr での制御メッセージ再起動カウンタ変更の数とタイプが表示されるようになりました。このコマンドの出力が強化され、eGTP-C レイヤで無視された検出済みパス障害の数を追跡できるようになりました。
- **show egtpc peers path-failure-history** コマンドの出力が追加され、ピアごとに最後の 5 つのパス障害に関する詳細情報が提供されるようになりました。
- **show egtp-service all name** コマンドと **show configuration** コマンドの出力が拡張され、パス GTP-C パス障害検出ポリシーに固有の現在の設定が表示されるようになりました。

IMS 緊急ベアラーの処理

このサポートにより、UE は、緊急 PDN に接続して Enhanced 911（E911）コールを行いながら、必要なロケーション情報を公安アクセスポイント（PSAP）に提供することが可能になります。

E911 は、緊急事態が発生している人とそれを支援できる公共のリソースを結び付けるために設計された、電気通信ベースのシステムです。この機能は、LTE および IMS ネットワークを介した E911 ベースのコールをサポートしています。Voice over LTE のシナリオでは、サブスクライバは、PSAP への Voice over IP 接続を確立するために、「EPDN」（緊急 PDN）と呼ばれる専用のパケットデータネットワーク（PDN）にアタッチします。シグナリングがデフォルトの緊急ベアラーで発生するか、シグナリングと RTP メディアのフローが個別の専用緊急ベアラーを介して発生します。さらに、コールの確立を AAA および PCRF コンポーネントに依存する通常の PDN 接続とは異なり、EPDN 属性は P-GW でローカルに設定されるため、それらのシステムのいずれかが使用できないことで緊急コールが失敗する可能性がありません。

IMS 緊急セッションをサポートするために緊急ベアラーサービスが提供されます。緊急ベアラーサービスとは、緊急サービスをサポートするようにネットワークが設定されている場合に、サービスを提供しているネットワークによって提供される機能を指します。緊急ベアラーサービスは、通常どおりにアタッチされた UE のほかに、サービスが制限されている（現地のサービス規制、ポリシー、および制限に応じて）UE に提供されます。限定的なサービス状態での緊急サービスの受信には、サブスクリプションは不要です。

標準規格（3GPP TS 23.401 を参照）では、サポートされている次の 4 つの動作が特定されています。

- 有効な UE のみ
- 認証された UE のみ
- MSI は必須、認証はオプション
- すべての UE

緊急サービスを要求する際、UE には次の 2 つのオプションがあります。

- サービスが制限されている（ネットワークからのアタッチ拒否のため、または SIM が存在しないため）UE は、ATTACH を開始し、その ATTACH が緊急ベアラーサービスを受信するためのものであることを示します。アタッチに成功すると、ネットワークが UE に提供するサービスは、緊急ベアラサービスのコンテキストでのみ提供されます。
- セル上で通常通りにキャンプしている UE は、緊急サービスを必要とする場合、通常の ATTACH を開始します。通常のアタッチ済み UE は、緊急ベアラーサービスを要求する UE 要求 PDN 接続手順を開始しています。

IP アクセス コントロール リスト

IP アクセス制御リストを使用すると、さまざまな IP パケットパラメータに基づいて、システムに出入りするパケットのフローを制御するルールを設定できます。

IP アクセスリスト（一般にアクセス制御リスト（ACL）と呼ばれます）は、システムに出入りするパケットのフローを制御するために使用されます。これらはコンテキストごとに設定され、フィルタ基準に一致するパケットに対して実行されるアクションを制御する「ルール」（ACL ルール）またはフィルタで構成されます。設定が完了すると、ACL を次のいずれかに適用できます。

- 個別のインターフェイス
- コンテキストによって促進されるすべてのトラフィック（ポリシー ACL と呼ばれる）
- 個々のサブスクライバ
- 特定のコンテキストによって促進されるすべてのサブスクライバセッション



重要 IP アクセス制御リストの詳細については、『システムアドミニストレーションガイド』の「*IP アクセス制御リスト*」の章を参照してください。

IP アドレスホールドタイマー

このサブスクライバレベルの CLI は、アドレス隔離とも呼ばれ、以前に割り当てられた IP アドレスを IP アドレスプールから一時的にバッファリングして、新しいサブスクライバセッションにリサイクルされて再割り当てされるのを防ぎます。この機能は、モバイルデータセッションの一時的な喪失につながることがある、RAT 間ハンドオーバー時に特に役立ちます。

この機能により、リモートホストサーバーがモバイルデバイスに到達する必要があるロケーションベースのサービスでのより高品質なユーザーエクスペリエンスが可能になります。



重要 現在、P-GW は、IPv4 アドレスを使用したアドレスホールドタイマーのみをサポートしています。

IPv6 と IPv4 の機能

アドレス効率を向上させ、急速に枯渇に近づいている IPv4 アドレスの問題に対応するプレッシャーを軽減します。

P-GW は、次の IPv6 機能を提供します。

ネイティブ IPv6 および IPv6/IPv4 トランスポート

- P-GW の動的または静的アドレスプールからの IPv4、IPv6、またはデュアルスタック IPv4/v6 アドレス割り当ての任意の組み合わせのサポート。
- UDP および IPv4 ヘッダーでラップされたモビリティパケットのサポート。
- PMIPv6 S2a インターフェイスでのネイティブ IPv6/IPv4 トランスポートおよびサービスアドレスのサポート。このリリースの GTP S5/S8 接続のトランスポートは IPv4 ベースであることに注意してください。
- SGi 参照インターフェイスを介した、外部パケットデータネットワークへのアウトバウンドトラフィックの IPv6 トランスポートのサポート。
- サブスクライバセッションが P-GW に存在しない場合に、設定されたネクストホップアドレスに転送/リダイレクトされた SGi から受信するダウンリンク IPv4 データパケットのサポート。ネクストホップが ARP で解決できない場合、パケットはドロップされます。適切なインターフェイス統計が、転送されたパケット数とドロップされたパケット数で更新されます。



重要 ダウンリンク IPv4 データパケットの転送/リダイレクトをサポートするには、**unconnected-address next-system** *ip address* キーワードを有効にする必要があります。

アタッチされたエレメントへの IPv6 接続

IPv6 トランスポートとインターフェイスは、次のすべての接続でサポートされています。

- Diameter Gx ポリシー シグナリング インターフェイス
- Diameter Gy オンライン課金参照インターフェイス
- 外部 3GPP AAA サーバーへの S6b 認証インターフェイス
- Diameter Rf オフライン課金インターフェイス
- 合法的傍受（X1、X2 インターフェイス）

ルーティングおよびその他の機能

- OSPFv3
- MP-BGP v6 拡張機能
- IPv6 フロー（すべての Diameter QoS および課金インターフェイスと、インラインサービス（ECS など）でサポート）

RA メッセージでの IPv6 MTU オプションのサポート

RFC-4861 には、ルータアドバタイズメント（RA）メッセージで最大伝送ユニット（MTU）を送信するよう規定されています。P-GW は、IPv6 および IPv4v6 PDN タイプの RA で IPv6 MTU オプションを UE に送信することをサポートするようになりました。その結果、UE は、設定された MTU に基づいてアップリンクデータパケットを送信し、必要に応じて送信元でデータのフラグメンテーションを実行することが可能になりました。また、この機能により、ユーザーのネットワーク内の ICMPv6 *Packet Too Big Error* メッセージの数も減少します。

MTU サイズは、GGSN および P-GW のコマンドライン インターフェイス（CLI）を使用して設定できます。

サポートされる機能

RA メッセージ機能で IPv6 MTU オプションをサポートするために、P-GW/GGSN は、次の機能と動作をサポートしています。

- *APN* コンフィギュレーション モードで **ipv6 initial-router-advt option mtu value** コマンドを使用して、APN ごとにこの機能を有効または無効にすることができます。デフォルトでは、この機能は、すべての APN について有効になっています。
  - P-GW および SAEGW では、IPv6 初期ルータ アドバタイズメント オプションの MTU 値は、オクテット（整数*1280～2000*）で設定する必要があります。設定された値は、データトンネルの MTU ではなく、RA パケットで送信されます。



重要 この値は、RA パケットのアドバタイズメントにのみ使用され、ゲートウェイはこの値を強制する必要はありません。この CLI の「default」オプションと「no」オプションの動作は同じであるままになります。

  - P-GW および SAEGW では、セッションマネージャは、*APN* コンフィギュレーション モードで CLI コマンド **data-tunnel mtu** *1280-2000* を介して設定された MTU 値を送信します。
  - GGSN では、Framed-MTU 属性値ペア（AVP）で RADIUS から返される値が、*APN* コンフィギュレーション モードで **ppp mtu** *100-2000* CLI コマンドを介して設定された値よりも優先されます。

- GGSN では、RADIUS から返される MTU 値が最小 IPv6 MTU 未満の場合、1280 の最小 IPv6 MTU 値が RA メッセージの IPv6 MTU オプションフィールドで送信されます。
- GGSN では、**ppp mtu***100-2000* CLI コマンドが 1280 未満の MTU 値で設定されている場合、最小 IPv6 MTU 値は、RA メッセージの IPv6 MTU オプションフィールドで送信されます。
- RADIUS サーバーから MTU 値が取得されず、上記の両方の CLI コマンドが設定されていない場合、MTU にはデフォルト値の 1500 が使用されます。
- RA メッセージの MTU オプションは、GGSN/P-GW/SAEGW でサポートされています。
- この機能は、s2a/s2b/s5/s8 などのインターフェイスとは無関係に、P-GW でサポートされます。
- RA メッセージの MTU オプションは、IPv6 と IPv4v6 の両方の PDN タイプでサポートされています。
- RA メッセージの MTU オプションは、**monitor protocol** コマンドの出力で使用できます。
- ゲートウェイにより、コールの初期および定期 RA メッセージで同じ MTU 値が送信されます。
- PDN コールの RA の IPv6 MTU オプションを送信する動作は、セッションリカバリおよび ICSR スイッチオーバー後も維持されます。
- GGSN/P-GW/SAEGW での既存の MTU 関連データパスの動作は変更されません。

制約事項/制限

この機能には、次の制約事項/制限があることに注意してください。

- GGSN/P-GW/SAEGW では、RA の IPv6 MTU オプションで送信される MTU 値を計算するときに、GTP-U トンネルのオーバーヘッドが考慮されません。そのため、通信事業者は、トンネルのオーバーヘッドを考慮して **data-tunnel mtu** を設定する必要があります。『*3GPP TS 23.060*』の「*Annex-C*」の「*Link MTU Considerations*」を参照してください。
- GGSN/P-GW/SAEGW の既存 MTU 関連データパスの動作は変更されていません。
- Gn/Gp ハンドオーバーが発生し、その後にセッションリカバリが実行される場合、通信事業者は、「ステートレス IPv6 セッションが、ハンドオーバー後に現在の GGSN/P-GW サービスに設定された MTU 値でリカバリされる」という動作を確認できます。これは、この機能が設定されていない場合の既存の動作です。この機能を有効にすると、そのようなハンドオーバーが発生し、その後にセッションリカバリが実行される場合、回復された同じ MTU 値が定期的な RA メッセージで送信されます。
- この機能は、eHRPD ではサポートされていません。その結果、LTE から eHRPD へのハンドオーバー、または eHRPD から LTE へのハンドオーバーが発生するシナリオでは、新しいステートレス IPv6 セッションが、最新の APN 設定を使用して再作成されます。
- この機能が有効になっている場合、S6b インターフェイスを介してゲートウェイが受信する MTU 値はサポートされません。

LTE-Wi-Fiハンドオフのための IPv6 プレフィックスベース検索のサポート

特定顧客の一部の UE デバイスでは、Wi-Fi の RAT 間テスト中に、LTE から Wi-Fi へのハンドオフが失敗していました。これらの UE デバイスは、ステートレスアドレス自動設定を使用していました。この問題は、ハンドオフ中にセッション作成応答（CSResp）メッセージで変更された IPv6 アドレスを UE が送信している場合に、特定の UE デバイスでのみ確認できます。別のベンダーのデバイスでは、P-GW からのセッション作成応答（CSResp）中に最初に割り当てられた IPv6 アドレスを送信していたため、LTE から Wi-Fi へのハンドオフの問題は発生しませんでした。

P-GW が、完全な IPv6 128 ビットアドレス（プレフィックス＋インターフェイス ID）に基づいて既存の LTE セッションの IPv6 ルックアップを実行すると、そのハンドオーバーは、エラー EGTP_CONTEXT_NOT_FOUND で失敗します。

現在、P-GW は、LTE から Wi-Fi へのハンドオフ中に IPv6 プレフィックス（64 ビット）のみを使用して、既存の LTE セッションの IPv6 ルックアップを実行します。ステートレスアドレス自動設定により、通信事業者には、UE デバイスに対するこれらのコールでシームレスなハンドオーバーが見られるようになりました。P-GW は、UE が、PDN タイプ IPv6 および IPv4v6 のハンドオフ中のコール作成時に提供されるインターフェイス ID とは異なるインターフェイス ID を使用する場合、ハンドオフ要求を拒否しません。

重要 外部インターフェイスに変更はありません。この機能に含まれる唯一の変更点は、ハンドオフ時に 64 ビット IPv6 プレフィックスを使用して既存のセッションを検索する内部検索が実行されることです。

制約事項/制限

ステートレス自動設定が使用されるのは、UE が、P-GW によって提供されるものとは異なるインターフェイス ID を使用する場合です。その場合、UE は、後で別のロケーションに移動します。これにより、S-GW が変更される S1/X2 ハンドオーバーが発生します。その結果、S-GW は、同じ UE で、PDN について、P-GW によって維持されている IPv6 アドレス（つまり、初期アタッチ時に提供された IP アドレス）とは異なる IPv6 アドレスを持つ場合があります。これにより、P-GW と S-GW で CDR の servedPDPPDNAddress 要素に相違が生じる可能性があります。

この制限は、ベアラー変更変更/ベアラー変更応答などの 3GPP 変更手順における既存の制限（S1/X2 ハンドオーバー時に、P-GW および S-GW の間で、変更された UE IPv6 アドレスを交換できない）によるものです。

メディエーションデバイスは、ステートレス自動設定デバイスについて、CDR の IPv6 アドレスの 64 ビットプレフィックスを調べることが想定されています。

ローカルブレークアウト

この機能は、LTE事業者が、他のモバイル通信事業者とのローミング契約に基づいて訪問先のサブスクライバからのトラフィックを受け入れることにより、追加の収益を生み出すことを可能にする、標準ベースの手順を提供します。

ローカルブレークアウトは、LTEサービスプロバイダーネットワーク間のプロバイダー間ローミングで重要な役割を果たすポリシーベースの転送機能です。ローカルブレークアウトは、訪問先ネットワークとホームネットワーク間のローミングコールの処理に関するSLAによって決定されます。場合によっては、ホームネットワークにトラフィックをバックホールするための追加の転送コストを発生させるより、外部ネットワーク上のローミングコールを訪問先P-Wにローカルにブレークアウトする方が有益です。

2つのモバイル通信事業者がローミング契約を締結している場合、ローカルブレークアウトにより、訪問先ユーザーは、V-PLMNネットワークに接続し、訪問先ネットワーク内のローカルP-GWによってアンカーされることが可能になります。このローミングアーキテクチャは、ホームネットワークのHSSに依存しており、H-PLMNのH-PCRFとV-PLMNのV-PCRFの間にS9ポリシーシグナリングインターフェイスの概念も導入します。ユーザーが訪問先ネットワークのEUTRANセルとMME（モビリティマネージメントエンティティ）にアタッチすると、S6a NASシグナリングで要求されたAPN名がH-PLMNのHSSによって使用され、ローカルS-GW（サービングゲートウェイ）と訪問先EPCネットワークのP-GWが選択されます。

LTE ビデオコール

Voice over LTE（VoLTE）シナリオでは、P-GWはLTEビデオコール（LVC）をサポートします。この機能をサポートするために必要な追加の設定はありません。

P-GWは、ビデオコールのセットアップ時およびアクティブなビデオ通話中に定期的に、サブスクライバのデータ使用量クォータをチェックします。以下の機能が、データ使用量が制御される後払いサブスクライバに適用されます。

クォータチェック：コールセットアップ

コールセットアップ中にサブスクライバがデータ使用量クォータに達したとP-GWで判断されると、次の処理が行われます。

- コールの音声ベアラー部分はアクティブになりますが、コールのビデオベアラー部分はアクティブになりません。P-GWはPCRFに対して、クレジット制御要求の更新（CCR-U）をOCSから受信した「OUT_OF_CREDIT」イベントトリガーとFinal-Unit-Action（FUA）とともに送ります。PCRFはP-GWからサービスデータフロー（SDF）を削除し、ビデオベアラーチャネルのセットアップ失敗のP-CSCF通知を送信します。

クォータチェック：アクティブビデオコール中

回線がビデオコール中にデータ使用量を使い果たした場合：

- コールの音声ベアラー部分は保持され、コールのビデオベアラー部分は終了されます。P-GWはPCRFに対して、CCR-UをOCSから受信した「OUT_OF_CREDIT」イベントト

リガーと Final-Unit-Action（FUA）とともに送ります。PCRF は P-GW から SDF を削除し、ビデオベアラーチャネルのセットアップ失敗の P-CSCF 通知を送信します。

セッションマネージャでの高スループットセッションのマッピング

セッションマネージャがアップグレードされ、コアを共有せず、また CPU 負荷のボトルネックを発生させずに、複数の高スループットセッションを管理できるようになりました。

ゲートウェイ（S-GW、SAEGW、または P-GW）は、セッション作成要求の IE（FLAGS FOR USER PLANE FUNCTION（UPF）SELECTION INDICATION）にある DCNR フラグに基づいて、セッションを高スループットセッションに分類します。この DCNR フラグは、ゲートウェイによってチェックポイントとして扱われ、リカバリが行われます。

高スループットセッションは、他の高スループットセッションがないセッションマネージャに配置されます。すべてのセッションマネージャが高スループットセッションを処理している場合、これらのセッションはラウンドロビン方式を使用して割り当てられます。

（注）
- 高スループットではないセッションの場合のセッションマネージャの選択は、既存の設定と同じままです。
- 高スループットではないセッションは、同じセッションマネージャの高スループットセッションとともに配置されます。

制限事項

セッションマネージャでの高スループットセッションの管理には、次の制限があります。

- 次のシナリオでは、セッションマネージャに 2 つの高スループットセッションが配置される可能性があります。
  - 最初に eHRPD/2G/3G セッションから接続した。
  - IP アドレス（IPv4 と IPv6 の両方）が、同じセッションマネージャに配置された。
  - S-GW で、UE からの 2 番目のセッション作成要求（PDN）が、同じ UE の最初の PDN を持つセッションマネージャに直接到達した。
  - 折りたたまれたコールにおいて、UE からの 2 番目のセッション作成要求（PDN）が、同じ UE の最初の PDN を持つセッションマネージャに直接到達した。
  - DCNR 対応の UE からのマルチ PDN コール内。たとえば、VoLTE と、DCN 対応のインターネットは、同じセッションマネージャに配置されます。
- DCNR フラグは Wi-Fi の 3GPP では定義されていません。したがって、DCNR フラグがセットされている状態での Wi-Fi から LTE へのハンドオーバー中に、セッションをセッションマネージャに割り当てることはできません。

- この機能は、セッションマネージャでの高スループットセッションの分散を管理およびサポートしますが、サブスクライバでの高スループットを保証するものではありません。
- 場合によっては、ラウンドロビンメカニズムにより、他の高スループットセッションがすでに配置されているセッションマネージャに高スループットセッションが配置されることがあります。

ユーザー プレーン トラフィックの MPLS EXP マーキング

802.1p マーキングと同様に、MPLS EXP ビットマーキングは、P-GW の SGi インターフェイスで MPLS トンネリングを使用するエンタープライズ APN でサポートされています。LTE/EPC ネットワークで使用される QoS マーキング（EPS ベアラーごとの QCI）は、P-GW と L2/EPC スイッチや MPLS/PE ルータ間の 802.1p および MPLS EXP ビットマーキングにマッピングされます（これはP-GWからネットワークへのアップストリーム方向に適用されます）。QCI-QOS 設定テーブルの一部を、MPLS EXP マーキング関連の設定に使用できます。MPLS EXP マーキングは、そのパケットが属するベアラーの QCI に基づいて選択されます。



重要 有効なライセンスキーがインストールされていない場合、P-GW は非標準の QCI 値をサポートしません。

QCI 値 1 ～ 9 は、3GPP TS 23.203 で定義されている標準値です。P-GW はこれらの標準値をサポートします。

3GPP リリース 8 以降では、通信事業者固有/非標準の QCI がサポートされ、キャリアは QCI 128- 254 を定義できます。詳細については、非標準 QCI のサポート （103 ページ）を参照してください。

モバイル IP の登録失効

モバイル IP 登録失効機能には、次のようなメリットがあります。

- HSGW や P-GW でのモバイル IP リソースのタイムリーなリリース
- 正確なアカウンティング
- モバイルノードへのサービス変更のタイムリーな通知

登録失効は、同じモバイルノードにモバイル IP 機能を提供している P-GW または HSGW が、バインドの終了を他のモビリティエージェントに通知するための一般的なメカニズムです。モバイル IP の登録失効は、次のいずれかによって HSGW でトリガーできます。

- 何らかの理由でモバイルノードでセッションが終了した
- セッションの再ネゴシエーション
- コールの管理クリア

- セッション マネージャ ソフトウェアのタスク停止による HSGW セッションの喪失（回復できなかったセッション）

重要 登録失効機能は、プロキシモバイル IP でもサポートされています。ただし、プロキシ MIP コールの失効を開始できるのは P-GW のみです。

重要 MIP 登録失効サポートの詳細については、本のガイドの「モバイル *IP* の登録失効」の章を参照してください。

MTU サイズ PCO

表 *2:* 機能の履歴

機能名	リリース情報	説明
ローミングサブスクライバのダイナミックリンク MTU 設定	2025.02.0	この機能を使用すると、ローカルおよびローミングサブスクライバのさまざまな条件および要件を満たすさまざまなリンク MTU 設定が可能になり、リソースが最適化されて、きめ細かい制御が維持できます。 pc-options link-mtu 設定で新しい CLI オプションローミングを使用すると、さまざまなリンク MTU サイズを指定できます。 このような柔軟性により、データ伝送の効率とパフォーマンスが向上し、パケットセグメンテーションが減少して、ネットワーク全体の信頼性が向上します。 **変更された CLI**：**pco-options link-mtu** *bytes* **[roamer** *bytes* **]** **デフォルト値**：1500

通常、UE は IP 通信にハードコードされた MTU サイズを使用します。このハードコードされた値がサポートされているネットワーク値と同期していない場合、UE によって送信されるパケットに不要なフラグメントが発生する可能性があります。したがって、不要なフラグメントを回避するために、この機能は、UE でハードコードされた MTU の代わりにネットワークが提供する MTU サイズを使用できるようにします。

3GPP は、ネットワークが UE に IPv4 MTU サイズを提供できるように、リリース 10 仕様で新しい PCO オプションを定義しました。P-GW では、APN プロファイルで IPv4 リンク MTU サイズを設定するオプションがサポートされています。

初期接続または PDN 接続要求中に UE が PCO オプションで IPv4 リンク MTU サイズを要求した場合、P-GW は APN に基づいて事前設定された値を提供します。

APN で MTU サイズの設定が変更された場合、新しい MTU サイズは新規の PDN 接続と初期接続に対してのみ有効になります。P-GW は既存の PDN 接続は更新しません。

UE が IPv4 リンク MTU サイズを要求しない場合、P-GW には IPv4 リンク MTU サイズは含まれません。

UE がアウトバウンドローミング中の場合は、APN コンフィギュレーションモードで **pco-options** コマンドを使用して、リンク MTU サイズを柔軟に設定できます。詳細については、該当するリリースの『*Command Line Interface Reference, Modes A - B*』の「pco-options」の項を参照してください。

複数 PDN のサポート

IMS、インターネット、ウォールドガーデンサービス、オフデッキコンテンツサービスなど、さまざまなサービスに個別の接続を割り当てることができる APN ベースのユーザーエクスペリエンスを実現します。

S-GW の MAG 機能は、同じユーザーセッションに対して複数の PDN または APN 接続を維持できます。MAG は、P-GW の LMA 機能へのすべてのユーザーセッションに対し、シングルノードレベルのプロキシモバイル IPv6 トンネルを実行します。ユーザーが複数の PDN 接続を確立する場合、MAG は、同じ PMIPv6 セッションを介して 1 つ以上の P-GW LMA への複数の PDN 接続を確立します。次に、P-GW は、各 PDN 接続に個別の IP アドレス（ホーム ネットワーク プレフィックス）を割り当て、それぞれが 1 つまたは複数の EPC デフォルトおよび専用ベアラーを実行できます。さまざまな PDN 接続を要求するために、MAG には共通の MN-ID と個別のホーム ネットワーク プレフィックス、APN、および PMIPv6 バインディングアップデートのものに等しいハンドオーバー指示値が含まれます。

重要 最大 11 の複数 PDN 接続がサポートされます。

ノード機能 GTP エコー

この機能は、通信する 2 つの GTP ノードの機能を交換するのに役立ち、他方のノードでサポートされているかどうかに基づいて新しい機能を使用します。

この機能により、S-GW は、ピアエンティティと機能（MABR、PRN、NTSR）をエコーメッセージを介して交換できます。この機能により、両方のピアノードがいくつかの共通の機能をサポートしている場合、新しいメッセージを使用して相互に通信できます。

エコー要求/応答メッセージでの新しい「ノード機能」の IE サポートにより、各ノードは、サポート対象の機能（MABR、PRN、NTSR）を送信できます。この方法で、S-GWはピアノードでサポートされている機能を学習できます。S-GW でサポートされている機能は、いくつかの設定をサービスレベルで行うことで設定できます。

S-GW が P-GW 再起動通知などの新しいメッセージを使用する場合、S-GW は、ピアノードがこの新しい機能をサポートしているかどうかを確認する必要があります。ピアがサポートしていない場合、S-GW は古い動作にフォールバックする必要があります。

S-GW がピアノードから新しいメッセージを受信した場合に、S-GW がこの新しいメッセージをサポートしていなければ、S-GW はそのメッセージを無視する必要があります。S-GW が特定の機能をサポートしている場合は、仕様に従って新しいメッセージを処理する必要があります。

非最適化 e-HRPD からネイティブ LTE（E-UTRAN）へのモビリティハンドオーバー

この機能により、デュアルモード e-HRPD/e-UTRAN アクセス端末をサポートするシームレスなテクノロジー間ローミング機能が実現されます。

非最適化テクノロジー間モビリティ手順は、デュアル無線テクノロジー e-HRPD/E-UTRAN アクセス端末のハンドオーバーをサポートするためのモビリティアンカーポイントとしてのP-GWに基づいています。このタイプのコールハンドオーバーをサポートするために、P-GWは、GTP ベースの S5/S8（GTPv2-C/GTPv1-U）と PMIPv6 S2a トンネル接続間のハンドオフをサポートしています。また、共通アドレスプールから IPv4、IPv6、またはデュアルスタック IPv4/IPv6 PDN 接続をプロビジョニングし、テクノロジー間ハンドオーバー中に UE に割り当てられる IP アドレスを保持します。現在のリリースでは、ネイティブ LTE（GTP ベース）P-GW サービスアドレスは IPv4 ベースですが、e-HRPD（PMIP）アドレスは IPv6 サービスアドレスです。

UE が接続する各 APN の初期ネットワークアタッチ時に、HSS は、その APN の P-GW の FQDN を返します。MME は、DNS を使用して P-GW アドレスを解決します。PDN 接続が P-GW で確立されると、P-GW は、S6b 認証プロセスによって PDN が確立された時点で、P-GW の IP アドレスを使用して HSS を更新します。モバイルユーザーが e-HRPD ネットワークにローミングすると、HSS は、STa インターフェイスを介して P-GW 識別子で P-GW の IP アドレスを返し、そのコールは同じP-GWで終了します。また、P-GWは、ターゲットネットワークへのコールハンドオーバー後に、サービス提供アクセス接続でセッション終了を開始する役割も担います。

ハンドオーバー手順中に、すべての専用EPSベアラーを再確立する必要があります。ターゲット e-HRPD アクセスネットワークへの LTE ハンドオーバー時には、専用ベアラーが、モバイルアクセス端末によって開始されます。対照的に、e-HRPD から LTE アクセスネットワークへの反対方向のハンドオーバーでは、専用ベアラーは、PCRF サーバーとの Gx ポリシー相互作用を通じてネットワークによって開始されます。

最後に、テクノロジー間ハンドオーバーをサポートするために、P-GW は、さまざまな基準点に対して共通のインターフェイスと Diameter エンドポイントアドレスを使用します。

- S6b：非 3GPP 認証

- Gx：QoS ポリシーおよび課金
- Rf：オフライン課金

3 つのタイプのセッションはすべて、コールハンドオーバー中に維持されます。ベアラーバインドは、e-HRPD アクセス時に HSGW によって実行され、LTE アクセス時に P-GW によって実行されます。そのため、ベアラー バインド イベント レポート（BBERF）機能は、ハンドオーバー中に P-GW と HSGW の間を移行する必要があります。HSGW は、ベアラーバインドのために e-HRPD アクセス中に Gxa セッションを確立し、LTE アクセス中にセッションをリリースします。また、HSGW は、e-HRPD <-> LTE ハンドオーバー中に制限されたコンテキストを維持し、LTE RAN から e-HRPD ネットワークへのクイックハンドオーバーが発生した場合の遅延を減らします。



重要 ハンドオフインターフェイスの詳細については、「サポートされる論理ネットワーク インターフェイス（参照ポイント） （6 ページ）」を参照してください。

オンライン/オフライン課金

Cisco EPC プラットフォームは、外部 OCS や CGF/CDF サーバーとのオンラインおよびオフライン課金の連携動作をサポートします。

オンライン課金

Gy/Ro 参照インターフェイス

StarOS 9.0 オンラインプリペイド参照インターフェイスは、3GPP TS 23.203、TS 32.240、TS 32.251、TS 32.299 仕様と互換性があります。Gy/Ro 参照インターフェイスは、Diameter トランスポートと IPv6 アドレッシングを使用します。オンライン課金は、リソースの使用が発生するように、ネットワークリソース使用の課金情報をネットワークによって取得する必要があるプロセスです。この承認は、ネットワークからの要求に応じてオンライン課金システム（OCS）によって付与されます。P-GW は、課金特性プロファイルを使用して、オンライン課金をアクティブにするか非アクティブにするかを決定します。EPS ベアラーの確立、変更、または終了は通常、P-GW でオンライン課金 PCC ルールをアクティブにするための PCRF でのイベントトリガーとして使用されます。

ネットワークリソースの使用要求を受信すると、ネットワークは関連する課金情報を収集し、OCS への課金イベントをリアルタイムで生成します。次に、OCS は、範囲内で（データの量や期間などに基づいて）制限される可能性がある適切なリソース使用の承認を返します。OCS は料金設定グループにクォータを割り当て、サービスデータフローまたは IP CAN ベアラーを続行するか終了するかを P-GW に指示します。

次のオンライン課金モデルと機能がサポートされています。

- 時間ベースの課金
- 通信量ベースの課金

- 通信量および時間ベースの課金
- クォータが消費された場合の最終ユニット通知とサービスデータフローの終了またはリダイレクト
- 再承認がトリガーされ、マルチサービスクレジット制御（MSCC）インスタンスを使用して 1 つまたは複数の料金設定グループのクォータが再補充されます。
- イベントベースの課金
- 支払請求サイクルでの帯域幅レート制限：PDN GW とオンライン課金サーバー間の連携動作によって課金ポリシーが適用されます。課金エンフォースメントポイントは、サブスクライバセッションのアカウンティング情報を OCS に定期的に伝達し、課金ポリシーに設定されたしきい値を超えた分に対してアカウントから差し引かれます。サブスクライバにはそのティア（ゴールド、シルバー、ブロンズなど）の最大使用量を割り当てることができ、使用量は月、週、日、または 1 日以内のピーク時に渡ってトラッキングできます。サブスクライバが使用量上限を超過すると、帯域幅は特定の期間制限されるか、サービスのティアに応じてドロップされます。
- 公平な使用量制御

オフライン課金

Ga/Gz リファレンスインターフェイス

Cisco P-GW では、TS 32.251、TS 32.297、および 32.298 で定義されている 3GPP 準拠のオフライン課金がサポートされます。S-GW は、SGW-CDR を生成して PLMN リソースへのサブスクライバレベルのアクセスを記録しますが、P-GW は、PGW-CDR を作成して外部ネットワークへのユーザーアクセスを記録します。さらに、リリース前の SGSN との Gn/Gp インターワーキングが有効になっている場合、P-GW 上の GGSN サービスは、G-CDR を記録して、外部ネットワークへのユーザーアクセスを記録します。

サブスクライバレベルのアカウンティングを可能にするため、Cisco S-GW および P-GW は、統合された課金転送機能（CTF）と課金データ機能（CDF）をサポートしています。各ゲートウェイは、課金 ID を使用して、サブスクライバセッション内でデフォルトのベアラーと専用ベアラーを区別します。CDF と CGF 間の Ga/Gz リファレンスインターフェイスを使用して、GTPP プロトコルを介して課金レコードを転送します。標準規格ベースの実装では、CGF によって課金レコードが統合され、Bm リファレンスインターフェイス経由で FTP/S-FTP 接続によってバックエンドの課金仲介サーバーに転送されます。Cisco EPC ゲートウェイは、CDF サーバーと CGF サーバー間の FTP/S-FTP 課金レコードに対する機能も提供します。CDR レコードには、レコードタイプ、サービス対象 IMSI、課金 ID、APN 名、タイムスタンプ、コール持続時間、サービス対象 MSISDN、PLMN-ID などの情報が含まれます。ASR 5500 プラットフォームには、デュアル冗長 RAID ハードディスクのペアに搭載された永続的メモリでの一時的なファイルの保存と課金記録のバッファリングを可能にするためのローカルディレクトリが用意されています。各ドライブには 147GB のストレージが含まれており、最大 100GB のキャパシティが課金レコード保存専用となります。効率向上のために、GZIP などのプロトコルを使用してファイル圧縮を有効にすることもできます。オフライン課金を導入すると、隣接 CGF の組み込みハートビートモニタリングが使用可能になります。設定可能なポーリング間隔内に

Cisco P-GW がネイバー CGF から情報を受信しなかった場合、CGF が再度アクティブになってキャッシュされた課金レコードのブリングを開始できるようになるまで、課金レコードはローカルドライブ上で自動的にバッファリングされます。

P-GW は、隣接する OCS サーバーへの Gy 参照インターフェイスを介したフローベースのベアラー課金（FBC）を有効にするポリシー課金適用機能（PCEF）をサポートしています（上記の「オンライン課金」の説明を参照してください）。

Rf 参照インターフェイス

Cisco EPC プラットフォームは、P-GW の CTF 機能から外部 CDF/CGF サーバーへの課金ファイルの直接転送を可能にする Rf 参照インターフェイスもサポートしています。このインターフェイスは、Diameter アカウンティング要求（開始、停止、暫定、およびイベント）を使用して、課金レコードを CDF/CGF に転送します。各ゲートウェイは、トリガー条件に応じて、課金対象イベントを CDF/CGF に報告します。通常、EPS ベアラーがアクティブ化、変更、または削除されると、課金レコードが生成されます。EPC プラットフォームには、サブスクリプション ID（IMSI）、課金 ID（EPS ベアラー識別子）、および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個別のボリュームカウントなどの情報が含まれています。

egtpinmgr リカバリの最適化

ソフトウェアは、egtpinmgr タスクの再起動時にリカバリ停止期間を最適化するように機能拡張されました。この最適化は、egtpinmgr リカバリの内部アルゴリズムを最適化し、必要なデータ構造を最適化することによって実現されています。さらに、リカバリ時間は、IMSI のセッション数ではなく、一意の IMSI の数によってのみ決まるようになりました。

P-CSCF リカバリ

Wi-Fi 統合のための GTP ベース S2b インターフェイスの P-CSCF 検出をサポートする、仕様ベースのメカニズムをサポートします。これは Voice over Wi-Fi サービスに必要です。

P-GW は、AAA への初期登録時に受信した P-CSCF FQDN を保存できます。MME/S-GW から P-CSCF 復元フラグを受信すると、P-GW は、既存の P-CSCF FQDN を使用して新しい DNS クエリを実行し、PCO を使用して 3 つの P-CSCF IP アドレスの更新済みリストを提供します。

ピアの GTP ノードプロファイル設定サポート

通信事業者はピアのタイプやピアの IP アドレスに基づいて、GTP-C と合法的傍受用を柔軟に設定することができます。

ピアプロファイル機能により柔軟なプロファイルベースの設定が可能になるため、P-GW のピアノードのデフォルト値やアクションを使用して、カスタマイズ可能なパラメータの増え続ける要件に対応できます。この機能を使用すると、定義されたルールに基づいて MCC/MNC または IP アドレスごとに、GTP-C パラメータの設定や合法的傍受の無効化/有効化を実行できます。

ピアプロファイルとピアマップの新しいフレームワークが導入されました。ピアプロファイル設定では、GTP-C 固有の設定や合法的傍受の有効化/無効化の設定がキャプチャされます。GTP-C 設定の対象には、GTP-C 再送信（最大再試行回数と再送信タイムアウト）および GTP エコーの設定が含まれています。ピアマップ設定は、特定の基準に適用されるピアプロファイルと照合されます。ピアマップでは、ピアの MCC/MNC（PLMN-ID）やピアの IP アドレスなどの基準がサポートされます。さらに、ピアマップを P-GW サービスに関連付けることができます。

この機能の目的は、通信事業者が特定のピアのセットに適用可能なプロファイルを柔軟に設定できるようにすることです。たとえば、外部ピアにはホームピアと異なる再送信タイムアウトを設定できます。

PMIPv6 ハートビート

プロキシモバイル IPv6（PMIPv6）は、PMIPv6 モビリティ関連のシグナリングへのモバイルノードの参加を必要とせずにモビリティを提供する、ネットワークベースのモビリティ管理プロトコルです。コア機能エンティティであるモバイル アクセス ゲートウェイ（MAG）とローカルモビリティアンカー（LMA）は、モバイルノードのモビリティを管理するためにトンネルを動的に設定します。

MAG と LMA 間のハートビートメッセージによる経路管理メカニズムは、ピアの到達可能性を認識し、障害を検出し、ノード障害から回復した場合にピアに迅速に通知し、ピアが適切なアクションを実行できるようにするために重要です。

HSGW から P-GW への PMIP ハートビートは、RFC 5847 に従ってサポートされています。このハートビートを有効にし、ハートビートの変数を設定するには、LMA サービスモードまたは MAG サービスモードの **heartbeat** コマンドをそれぞれ参照してください。



重要 PMIPv6 ハートビートのサポートの詳細については、このガイドの「*PMIPv6* ハートビート」の章を参照してください。

Proxy Mobile IPv6（S2a）

サブスクライバがネイティブ EUTRAN と非ネイティブ e-HRPD アクセスネットワーク間をローミングするときに、単一の LTE-EPC コアネットワークがユーザーセッションのコールアンカーポイントを提供できるようにするモビリティ管理プロトコルを提供します。

S2a は、LTE-EPC コアネットワークと HSGW にアンカーされた evolved HRPD ネットワーク間の信頼された非 3GPP インターフェイスを表します。e-HRPD ネットワークでは、ネットワークベースのモビリティは、ホストが関与せずに IPv6 ノードのモビリティを提供します。Proxy Mobile IPv6 は、Mobile IPv6 シグナリングメッセージを拡張し、P-GW で HA 機能（現在は LMA と呼ばれる）を再利用します。このアプローチでは、モバイルノードが自身とホームエージェントとの間のシグナリングメッセージの交換に関与する必要はありません。ネットワーク内のプロキシ モビリティ エージェント（HSGW 上の MAG 機能など）はホームエージェントとの

シグナリングを実行し、ネットワークに接続されたモバイルノードに代わってモビリティ管理を行います。

S2a インターフェイスは、制御とデータの両方に IPv6 を使用します。PDN 接続の確立手順中に、P-GW は Proxy Mobile IPv6 シグナリングを介して IPv6 ホーム ネットワーク プレフィックス（HNP）を HSGW に割り当てます。HSGW はルーターアドバタイズメントで、または UE からのルータ要請リクエストに基づいて HNP を返します。PDN 接続の解放イベントは、UE、HSGW、または P-GW のいずれかによってトリガーできます。

Proxy Mobile IPv6 アプリケーションでは、HSGW（MAG 機能）と P-GW（LMA 機能）が単一の共有トンネルを維持し、個々のサブスクライバセッションを区別するために PMIP バインディング更新メッセージおよび確認応答メッセージに個別の GRE キーが割り当てられます。Proxy Mobile IP シグナリングに Protocol Configuration Options（PCO）が含まれている場合、シグナリングは P-CSCF または DNS サーバーアドレスの転送にも使用できます。

QoS ベアラーの管理

コミットされた帯域幅リソース、ジッター、および遅延の要件に従って、さまざまなサービスやアプリケーションクラスの確定的なエンドツーエンド転送とスケジューリング処理を可能にすることで、Quality of User Experience（QoE）の向上に貢献するための基盤を提供します。その結果、各アプリケーションが、ユーザーが期待するサービス処理を受け取ります。

EPS ベアラーは、GTP ベースの S5/S8 の場合は UE と P-GW の間で、PMIP ベースの S2a 接続の場合は UE と HSGW の間で実行される 1 つ以上のサービスデータフロー（SDF）の論理的な集約です。EPS ベアラーは、EPC/E-UTRAN でのベアラーレベルの QoS 制御の精度レベルです。Cisco P-GW は、インバウンドのサービスデータフロー（SDF）を EPS ベアラーにマッピングするために、ダウンリンク方向の 1 つ以上のトラフィック フロー テンプレート（TFT）を維持します。P-GW は、ダウンリンク TFT に基づいてトラフィックを S5/S8 ベアラーにマッピングします。Cisco PDN GW は、次のベアラーレベルの集約構造をすべて提供します。

QoS クラス識別子（QCI）：ベアラーレベルのパケット転送処理を制御する、通信事業者によるプロビジョニング値（スケジューリング重み、アドミッションしきい値、キュー管理しきい値、リンク層プロトコルの設定など）。Cisco EPC ゲートウェイは、QCI 値を S5/S8 接続の外側 GTP トンネルヘッダーの DiffServ コードポイントにマッピングする機能もサポートしています。さらに、このプラットフォームには、カプセル化されたペイロードから外側 GTP トンネルヘッダーに DSCP マーキングをコピーするための設定可能なパラメータも用意されています。

パケットをさまざまなトラフィッククラスにグループ化する際に使用される 802.1p ネットワークトラフィックの優先順位付けをサポートするために、P-GW では、通信事業者は QCI 値をアップリンクおよびダウンリンクパケットの 802.1p 優先度にマッピングできます。

重要 有効なライセンスキーがインストールされていない場合、P-GW は非標準の QCI 値をサポートしません。

QCI 値 1 ～ 9 は、3GPP TS 23.203 で定義されている標準値です。P-GW はこれらの標準値をサポートします。

3GPP リリース 8 以降では、通信事業者固有/非標準の QCI がサポートされ、キャリアは QCI 128- 254 を定義できます。詳細については、非標準 QCI のサポート （103 ページ）を参照してください。

保証ビットレート（GBR）：GBR ベアラーは専用の EPS ベアラーと関連付けられ、確定的な低遅延サービス処理を必要とする自動音声などのアプリケーションに固定ビットレートサービスを提供するために、保証された最小伝送レートを提供します。

最大ビットレート（MBR）：MBR 属性は、GBR ベアラーによって提供されることが期待されるビットレートを制限する設定可能なバーストレートを提供します（たとえば、過剰なトラフィックがレートシェーピング機能によって破棄される可能性があります）。MBR は、特定の専用 EPS ベアラーの GBR 以上である場合があります。

集約最大ビットレート（AMBR）：AMBR は、特定の PDN を宛先とするベアラーグループのトラフィックのビットレートを示します。集約最大ビットレートは通常、デフォルト EPS ベアラーを介してベストエフォート サービス データ フローのグループに割り当てられます。つまり、これらの EPS ベアラーのそれぞれが AMBR 全体を利用する可能性があります。たとえば、他の EPS ベアラーがトラフィックを伝送しない場合などです。AMBR は、AMBR を共有する EPS ベアラーによって提供されることが予想される集約ビットレートを制限します（たとえば、超過トラフィックがレートシェーピング機能によって破棄される場合があります）。AMBR は、同じ PDN 接続に属するすべての非 GBR ベアラーに適用されます。GBR ベアラーは AMBR の範囲外です。

ポリシング：Cisco P-GW は、さまざまなトラフィック調整機能と帯域幅管理機能を提供します。これらのツールを使用すると、サブスクライバごと、EPS ベアラーごと、または PDN/APN ごとに使用量制御を適用できます。APN ごとの AMBR キャパシティに帯域幅制御を適用することもできます。これらのアプリケーションは、シャロー L3/L4 分析または L7 でのハイタッチ ディープ パケット インスペクションを使用して、ユーザーセッションまたはユーザーセッション内のサービスデータフロー（SDF）の状態の検査および維持を可能にします。アウトオブプロファイルのフローまたはセッションの計測により、パケットが破棄されたり、ベストエフォート優先度に対する DSCP マーキングが削減されたりする可能性があります。

RADIUS サポート

次の標準規格に基づいて、サブスクライバの PDP コンテキストの承認、認証、およびアカウンティング（AAA）を実行するためのメカニズムを提供します。

- RFC-2618：RADIUS Authentication Client MIB, June 1999
- RFC-2620：RADIUS Accounting Client MIB, June 1999

- RFC-2865：Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866：RADIUS Accounting, June 2000
- RFC-2867：RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868：RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869：RADIUS Extensions, June 2000

Remote Authentication Dial-In User Service（RADIUS）プロトコルは、サブスクライバの PDP コンテキストに AAA 機能を提供するために使用されます（GTPP も使用できるため、RADIUS アカウンティングはオプションです）。

システムに設定されているコンテキスト内に、設定可能な AAA および RADIUS プロトコル固有のパラメータがあります。RADIUS プロトコル固有のパラメータは、RADIUS 認証サーバーと RADIUS アカウンティングサーバーの連携でさらに区別されます。

設定可能な RADIUS パラメータは次のとおりです。

- **Priority**：1 つのコンテキストで複数のサーバーを設定できるように、サーバーを使用する順序を指定します。
- **Routing Algorithm**：構成されたサーバー間で選択する方法を指定します。指定したアルゴリズムは、新しいセッション用に設定されている AAA サーバー間で AAA メッセージをどのように配信するかを決定します。セッションが確立され、AAA サーバーが選択されると、そのセッション以降のすべての AAA メッセージは同じサーバーに配信されます。

1 つのサーバーが到達不能になった場合、システムは設定されている他のサーバーとの通信を試みます。システムには、すべての RADIUS AAA サーバーが到達不能になった場合の動作を指定する設定可能なパラメータも用意されています。

システムは RADIUS サーバー構成グループをサポートすることで、柔軟性を向上させます。この機能により、通信事業者は PDP コンテキストを促進するために使用される APN に基づいて、サブスクライバの AAA サービスを区別できます。

一般に、システム上でコンテキストあたり 128 の AAA サーバー IP アドレス/ポートを設定でき、サーバー選択アルゴリズム（ラウンドロビン、最初のサーバー）に従ってこのリストからサーバーが選択されます。コンテキストごとにサーバーのリストを 1 つ用意する代わりに、この機能では複数のサーバーグループを設定できます。また、各サーバーグループは、サーバーのリストで構成されます。

この機能は次のように動作します。

- コンテキストレベルで設定されたすべての RADIUS 認証/アカウンティングサーバーは、「default」というサーバーグループの一部として扱われます。このデフォルトサーバーグループは、設定しなくてもレルム（ドメイン）を介してそのコンテキスト内のすべてのサブスクライバに使用可能です。
- この機能により、コンテキスト内に最大 399 個（「デフォルト」サーバーグループを除く）の「ユーザー定義」の RADIUS サーバーグループを作成できます。ユーザー定義の

RADIUS サーバーグループのいずれかを使用して、そのコンテキスト内の APN 設定を介してサブスクライバを割り当てることができます。

APN の設定では、使用する RADIUS サーバーグループだけでなく、アドレスを割り当てる IP アドレスプールを指定できるため、一部のインバンド RADIUS サーバー（通信事業者のネットワークではなく企業のネットワーク内にある RADIUS サーバー）の導入をサポートするメカニズムがシステムに実装されます。このとき、NAS-IP アドレスはサブスクライバプールの一部になります。これらのシナリオでは、P-GW は、RADIUS NAS-IP アドレスとして使用するために、サブスクライバプールの最初の IP アドレスの設定をサポートしています。

重要 StarOS 12.3 以前のリリースを使用している場合、RADIUS AAA 設定の詳細については、『*AAA and GTPP Interface Administration and Reference*』[英語] を参照してください。StarOS 14.0 以降のリリースを使用している場合は、『*AAA Interface Administration and Reference*』を参照してください。

プライベート拡張ベースの過課金機能の削除

StarOS リリース 21.0 より前では、Cisco P-GW および S-GW は、非 3GPP プライベート拡張情報要素（IE）と 3GPP インジケーション IE の両方を介して過課金保護データの送受信をサポートしていました。

ただし、過課金保護データを交換する 3GPP サポートが存在するため、通信事業者は過課金プライベート拡張（OCP）ベースのソリューションを使用していませんでした。また、P-GW によって送信される過課金保護データを伝送するプライベート拡張 IE が、他のベンダーの S-GW での問題につながることが一部の通信事業者によって報告されていました。

その結果、プライベート拡張ベースの過課金機能のサポートが Cisco P-GW および S-GW から削除されています。これには、他のベンダーの P-GW/S-GW で、過課金保護データを伝送するプライベート拡張 ID のデコードが原因により予期しないシナリオが発生するのを防ぐメリットがあります。

P-GW の以前の動作と新しい動作

次の表では、プライベート拡張 IE の過課金サポートの削除による、セッション作成要求（CSReq）とセッション作成応答（CSRsp）メッセージの P-GW での以前の動作と新しい動作について説明します。

表 *3:* 以前の動作と新しい動作：プライベート拡張 *IE* の過課金サポートの削除による *P-GW* での *CSReq* メッセージと *CSRsp* メッセージ

シナリオ番号	CSReq で S-GW から受信した OCP 機能の IE 伝送	以前の動作：CSReq で S-GW から受信した OCP 機能の IE 伝送	新しい動作：CSReq で S-GW から受信した OCP 機能の IE 伝送
1	インジケーション IE	インジケーション IE	変化なしインジケーション IE は CSRsp で送信されます。

シナリオ番号	CSReq で S-GW から受信した OCP 機能の IE 伝送	以前の動作：CSReq で S-GW から受信した OCP 機能の IE 伝送	新しい動作：CSReq で S-GW から受信した OCP 機能の IE 伝送
2	プライベート拡張 IE	プライベート拡張IE とインジケーション IE の両方。	S-GW から受信したプライベート拡張IEは無視されます。インジケーション IE は CSRsp で送信されます。
3	なし	プライベート拡張IE とインジケーション IE の両方。	インジケーション IE のみが CSRsp で送信されます。
4	プライベート拡張 IE とインジケーション IE の両方。	インジケーション IE	S-GW から受信したプライベート拡張IEは無視されます。インジケーション IE のみが CSRsp で送信されます。

次の表では、プライベート拡張IEの過課金サポートの削除による、ベアラー変更要求（MBReq）とベアラー変更応答（MBRsp）メッセージの以前の動作と新しい動作について説明します。

表 *4 :* 以前の動作と新しい動作：プライベート拡張 *IE* の過課金サポートの削除による *P-GW* での *MBRreq* メッセージと *MBRsp* メッセージ

シナリオ番号	MBReq で S-GW から受信した OCP 機能の IE 伝送	以前の動作：MBRsp で S-GW から受信した OCP 機能の IE 伝送	新しい動作：MBRsp で S-GW から受信した OCP 機能の IE 伝送
1	インジケーション IE	インジケーション IE	変化なしインジケーション IE は MBRsp メッセージで送信されます。
2	プライベート拡張 IE	プライベート拡張 IE	S-GW から受信したプライベート拡張IEは無視されます。インジケーション IE は MBRsp メッセージで送信されます。
3	なし	プライベート拡張 IE とインジケーション IE の両方。	インジケーション IE のみが MBRsp メッセージで送信されます。
4	プライベート拡張IE とインジケーション IE の両方。	インジケーション IE	S-GW から受信したプライベート拡張IEは無視されます。インジケーション IE のみが MBRsp メッセージで送信されます。

S-GW の以前の動作と新しい動作

次の表では、プライベート拡張 IE の過課金サポートの削除による、セッション作成応答（CSRsp）メッセージの S-GW での以前の動作と新しい動作について説明します。

表 *5:* 以前の動作と新しい動作：プライベート拡張 *IE* の過課金サポートの削除による *S-GW* での *CSRsp* メッセージ

シナリオ番号	以前の動作：**CSReq** で **P-GW** から受信した **OCP** 機能の **IE** 伝送	新しい動作：**CSReq** で **P-GW** から受信した **OCP** 機能の **IE** 伝送	以前の動作：**CSReq** で **MME** に送信された **OCP** 機能の **IE** 伝送	新しい動作：**CSReq** で **MME** に送信された **OCP** 機能の **IE** 伝送
12	インジケーション IE	変化なしインジケーション IE の一部として受信した OCP 機能が受け入れられます。	インジケーション IE	変化なしインジケーション IE は CSRsp で送信されます。
2	プライベート拡張 IE	プライベート拡張 IE の一部として受信した OCP 機能は無視されます。	gtpc private-extension overcharge-protection が egtpc サービスレベルで無効になっている場合：**プライベート拡張 IE**。 gtpc private-extension overcharge-protection が egtpc サービスレベルで有効になっている場合：**インジケーション IE**。	CLI コマンドが廃止されたため、プライベート拡張 IE は、不明なプライベート拡張 IE と同様に CSRsp 内の MME に転送されます。
3	プライベート拡張 IE とインジケーション IE の両方。	プライベート拡張 IE の一部として受信した OCP 機能は無視されます。インジケーション IE の一部として受信した OCP 機能のみが受け入れられます。	gtpc private-extension overcharge-protection が egtpc サービスレベルで無効になっている場合：**プライベート拡張 IE および インジケーション IE**。 gtpc private-extension overcharge-protection が egtpc サービスレベルで有効になっている場合：**インジケーション IE**。	CLI コマンドが廃止されたため、プライベート拡張 IE は、不明なプライベート拡張 IE と同様に CSRsp 内の MME に転送されます。
4	なし	変化なし	なし	変化なし

次の表では、プライベート拡張IEの過課金サポートの削除による、ベアラー変更応答（MBRsp）メッセージの S-GW での以前の動作と新しい動作について説明します。

表 *6 :* 以前の動作と新しい動作：プライベート拡張 *IE* の過課金サポートの削除による *S-GW* での *MBRsp* メッセージ

シナリオ番号	以前の動作：**MBRsp** で **P-GW** から受信した **OCP** 機能の **IE** 伝送	新しい動作：**MBRsp** で **P-GW** から受信した **OCP** 機能の **IE** 伝送	以前の動作：**MBRsp** で **MME** に送信された **OCP** 機能の **IE** 伝送	新しい動作：**MBRsp** で **MME** に送信された **OCP** 機能の **IE** 伝送
1	インジケーション IE	変化なしインジケーション IE の一部として受信した OCP 機能が受け入れられます。	インジケーション IE	変化なしインジケーション IE は MBRsp で送信されます。
2	プライベート拡張 IE	プライベート拡張 IE の一部として受信した OCP 機能は無視されます。	gtpc private-extension overcharge-protection が egtpc サービスレベルで無効になっている場合：**なし**。 gtpc private-extension overcharge-protection が egtpc サービスレベルで有効になっている場合：**インジケーション IE**。	CLI コマンドが廃止されたため、2 つの IE のいずれも MBRsp で OCP 機能の MME に送信されません。
3	プライベート拡張 IE とインジケーション IE の両方。	プライベート拡張 IE の一部として受信した OCP 機能は無視されます。インジケーション IE の一部として受信した OCP 機能のみが受け入れられます。	インジケーション IE	変化なしインジケーション IE は MBRsp で送信されます。
4	なし	なし	なし	変化なし

重要 現在のリリースでは、S-GW は一時停止/課金開始プロシージャのインジケーション IE のみを含む MBReq メッセージを送信します。プライベート拡張 IE は送信されません。

重要 S-GW が CSRsp/MBRsp メッセージで P-GW からプライベート拡張 IE のみを受信する場合、S-GW はプライベート拡張 IE を無視します。その結果、S-GW は、P-GW に対して過課金保護が無効になっていると想定します。したがって、このシナリオでは、S-GW で過課金の条件が満たされている場合でも、S-GW は P-GW に課金一時停止の MBReq メッセージを送信しません。

S-GW 復元サポート

S-GW 復元機能は、EPC ネットワークで発生した S-GW 障害に対応するのに役立ちます。影響を受けた PDN にサービスを提供する別の S-GW を選択することで、S-GW が原因の障害で影響を受けた PDN を復元できます。これにより、PDN のクリーンアップのためにシグナリングの不要なフラッディングが発生するのを回避できます。

GTP-C シグナリングのリカバリ IE 中にパス障害が検出された場合や S-GW の再起動が検出された場合、P-GW はセッションを維持します。P-GW はこのシナリオでドロップされたパケットが課金されないようにします。また、P-GW は S-GW 障害検出後に維持された PDN 接続で受信したベアラーの追加要求や変更要求を拒否します。これは、PDN が復元されるまで行われます。

MME によってセッションが復元され、P-GW が再起動された S-GW または別の S-GW からベアラー変更要求を受信すると、P-GW は受信したダウンリンクデータの転送を続行し、課金を開始します。

サブスクライバが S-GW 復元フェーズにある場合、すべての RAR（セッション終了を予測）は PCEF を拒否します。P-GW は、PCRF に対して CCR-U をトリガーできる内部更新をすべて拒否します。S-GW が復元時に変更された場合、P-GW は復元された PDN の AN-GW の変更を含む CCR-U をトリガーします。

MME/S4-SGSN は、同じ PLMN の P-GW が S-GW 復元機能をサポートしていることを認識するようにローカルで設定されます。この機能が P-GW で有効になっている場合、すべての S-GW/MME でサポートされます。

重要 MME/S4-SGSN によってトリガーされた S-GW 復元手順のみがサポートされます。

GTP-U パスの障害に基づく S-GW 復元の検出は、このリリースでは考慮されません。この機能を有効にするには、GTP-C パス障害検出を有効にする必要があります。

GTP-U パスの障害に基づく S-GW 復元の検出は、このリリースでは考慮されません。この機能を有効にするには、GTP-C パス障害検出を有効にする必要があります。

P-GW 再起動通知は、ピア P-GW に障害が発生し、再起動していないことを通知するために使用することもできます。この場合、P-GW 再起動通知には「P-GW not responding」という理由値が含まれます。PRN の送信中、S-GW はエコー応答に応じて、この新しい理由値を追加します。

重要　この機能の詳細については、本ガイドの「*S-GW* 復元サポート」の章を参照してください。

送信元 IP アドレスの検証

望ましくないスプーフィングや中間者攻撃の可能性を軽減することにより、接続されたサブスクライバ端末と PDN ゲートウェイ間の完全性を確保します。

P-GW には、PDN 単位で UE に IP アドレスを割り当てるためのローカル IPv4/IPv6 アドレスプールが存在します。P-GW は認識しているホストアドレスからのトラフィック受信を保証することで、プロビジョニングされたアドレスのバインディングを保護します。許可されていないホストからトラフィックを受信した場合に備えて、P-GW には許可されていないトラフィックをブロックする機能が組み込まれています。P-GW は IPv4 送信元アドレスを使用して、送信者と IPv6 送信元プレフィックス（IPv6 の場合）を確認します。

SRVCC PS から CS へのハンドオーバー指示のサポート

この機能は、音声ベアラーの削除時に PCC ルールが非アクティブ化された正確な理由を PCRF に通知するために役立ちます。この正確な理由は、その後に PCRF が適切に追加のアクションを実行するために役立ちます。

この機能により、SRVCC への完全な準拠（音声ベアラーがリリースされたときの PS から CS へのハンドオーバー指示のサポートを含む）が保証されます。SRVCC 機能のサポートは、StarOS リリース 12.2 で最初に追加されました。

LTE の SRVCC サービスは、IMS アンカー音声コールサービスにアクセスする単一の無線ユーザー機器（UE）が LTE ネットワークから回線交換ドメインに切り替わるときに、特定の時点で、その機器が、それらのアクセスネットワークのいずれかでのみ送受信できるようになる場面で登場します。これにより、UE が複数の無線アクセス技術（RAT）機能を備える必要がなくなります。

PS セッションをターゲットにハンドオーバーした後に、送信元 MME は、S-GW/P-GW に対する音声ベアラーを非アクティブ化し、ベアラー削除コマンドメッセージ（TS 29.274 v9.5.0）で Bearer Flags IE に VB（音声ベアラー）フラグを設定することにより、音声ベアラーを削除します。

IP-CAN ベアラーの終了が、PS から CS へのハンドオーバーによって発生する場合、PCEF は、PS_TO_CS_HANDOVER（TS 29.212 v10.2.0 および TS 23.203 v10.3.0）の値に設定された Rule-Failure-Code AVP を含めることによって、この IP-CAN ベアラーに関連する PCC ルールを報告することができます。

課金ルールインストール内の新しい AVP PS-to-CS-Session-Continuity（3GPP リリース 11 で追加）のサポート（PS から CS への連続性のためにベアラーが選択されているかどうかを示す）は、追加されていません。

サブスクライバレベルのトレース

コールのデバッグ、新しい機能のテスト、そしてLTE環境におけるアクセス端末向けに、3GPP標準規格に準拠したセッションレベルのトレース機能を提供します。

P-GW はシスコのプロトコルモニタリング機能を補完するものとして、3GPP 標準規格に準拠したセッションレベルのトレース機能をサポートしており、S5/S8、S2a、SGi、Gx などの監視対象インターフェイスで発生するすべてのコール制御イベントをモニターします。トレースを開始する方法は、以下に示すようにいくつか用意されています。

- CLI を直接設定して管理を開始
- S6a 参照インターフェイスを介した認証応答メッセージによるトレースのアクティブ化を通して、HSS で管理を開始
- サブスクライバのアクセス端末からのシグナリングを通してシグナリングベースでアクティブ化



重要 トレースがプロビジョニングされると、さまざまなシグナリングインターフェイスを介したアクセスクラウドを使用してプロビジョニングできるようになります。

セッションレベルのトレース機能では、トレースのアクティブ化の後にトリガーが実行されます。2 つのイベント間の時間は、合法的傍受と同様に扱われます。このとき、EPC ネットワーク要素はキャッチオンモニタリングを使用して、メモリ内でプロビジョニングされたサブスクライバのトレースアクティベーション命令をバッファリングします。アクティブコールのトレースファイルは、ASR 5500 プラットフォームのローカルデュアル冗長ハードドライブ上の不揮発性メモリを使用して XML ファイルとしてバッファリングされます。トレースの深さにより、トレース対象のデータの精度が定義されます。最大、最小、中を含む6つのレベルが定義され、ベンダー拡張機能に基づいて追加のレベルを設定できます。

アクティブなセッションと録音されたセッションに関するすべてのコール制御アクティビティは、FTP またはセキュア FTP（SFTP）接続を介して、標準ベースの XML 形式でオフラインのトレース収集エンティティ（TCE）に送信されます。

現在のリリースでは、IPv4インターフェイスを使用してTCEへの接続が提供されます。トレースのアクティブ化は、IMSI または IMEI をベースとしています。サブスクライバレベルのトレース要求がアクティブになると、S5/S8 シグナリングを介して伝達され、P-GW 上の同じサブスクライバコールに対応するトレースをプロビジョニングできます。トレース設定は、S-GW によって受信された設定済みのネットワーク要素タイプのリストでP-GWが指定されている場合にのみ伝達されます。トレース設定は、次のいずれかのメッセージタイプで指定または転送できます。

- S5/S8：セッション作成要求
- S5/S8：ベアラー変更要求
- S5/S8：トレースセッションのアクティブ化（TS 32.422 で定義された新しいメッセージ）

パフォーマンス目標：サブスクライバレベルのトレースは CPU に高い負荷がかかるアクティビティであるため、同時にモニターされる Cisco P-GW ごとのトレースセッションの最大数は 32 です。既存のサービスへの影響を最小限に抑えるために、実稼働ネットワークでの使用を制限する必要があります。

3GPP トレース機能は、StarOS リリース 15.0 で強化され、同時トレース数が 1000 に増えました。「プッシュ」モードが有効になっている場合、生成されたトレースファイルは (S)FTP を介して定期的に外部のトレース収集エンティティに転送されます。プッシュモードを使用しない場合、ファイルはローカルハードドライブに保存され、FTP または SFTP を使用して TCE によってプルされる必要があります。



重要 生成されるセッショントレースファイルの数は、使用可能なハードディスクのキャパシティによって制限されます。

サブスクライバをランダムに傍受するための 3GPP トレース

以前は、トレースを有効にするには、IMSI などのサブスクライバ識別子が必要でした。通信事業者はサブスクライバ ID を把握していなくてもトレースを有効にしたい場合があります。たとえば、通信事業者はコールの次の「n」数を監視したり、特定の IMSI 範囲内のサブスクライバを監視する必要がある場合があります。

3GPP トレース機能が StarOS リリース 15.0 で強化され、この機能を使用してランダムなサブスクライバを傍受できるようになりました。現在のセッショントレース機能は、シグナリングまたは管理ベースであり、特定のサブスクライバに非常に限られています。明示的にリンクされていない、GTP メッセージの IMSI によって識別されない、CLI を介して設定されていないランダムなサブスクライバをトレースすることが求められます。

ランダムなサブスクライバとは、IMSI 範囲内であり、特定のタイムインターバルでコンテキストがアクティブ化されているなどです。

セッショントレースは、特定の分析目的のために、限られた期間だけオンデマンドでアクティブ化されます。上限を設定すると、ランダムなサブスクライバトレース数を制限できます。ランダムセッショントレースは、シグナリングや管理ベースのセッショントレースよりも優先されます。

S-GW で 100 万の S1-U ピアをサポート

お客様のビジネス要件と実稼働予測に基づき StarOS のサポートが強化され、1 つの S-GW で 100 万の S1-U 接続に対応できるようになりました。

S1-U インターフェイスは、端末から受信したユーザーデータを eNodeB と S-GW の間で伝送するユーザー プレーン インターフェイスです。StarOS では、VPN コンテキストごとに S1-U ピアの数を 100 万まで拡張できるようになりました。

通信事業者は追加された新しい CLI コマンドを使用して、統計を収集する S1-U ピアの数を設定できます。StarOS のメモリ制限により、100 万ピア（128k）未満で設定する必要があります。

機能の仕組み

gtpumgr は次のガイドラインに従って、ピアを割り当てます。

- セッションインストールがセッションマネージャから実行されると、ピアが作成されます。統計情報がセッションマネージャで維持管理されている場合、gtpumgr は統計情報を含むピアレコードも作成します。
- ピアレコードはサービス単位で保持されます。
- ピアの数は、gtpumgr インスタンスレベルで維持されます。S1-U ピアの数の上限は gtpumgr インスタンスごとに 100 万です。
- 上限の 100 万ピアを超えると、ピアの作成に失敗します。これにより、gtpumgr ではコールのインストールに失敗し、監査がトリガーされると監査に失敗します。

機能の変更は、GGSN/S4-SGSN/SGW/PGW/SAEGW/ePDG/SaMOG/HNB-GW/HeNB-GW などの gtpu-service を使用する次のインターフェイス/サービスのすべてに影響します。

- General Packet Radio Service（GPRS）の Gn および Gp インターフェイス
- UMTS システムの Iu、Gn、および Gp インターフェイス
- Evolved Packet System（EPS）の S1-U、S2a、S2b、S4、S5、S8、および S12 インターフェイス。

リカバリ/ICSR の考慮事項

- セッションマネージャ/gtpumgr のリカバリ後、または ICSR スイッチオーバー後に、統計情報の収集用に設定された一連のピアが回復されます。
  - セッション数が 0 で統計情報がないピアは回復されません。
  - セッション数が 0 で統計情報があるピアは回復されます。
  - 拡張ヘッダーのサポートが無効になっているピアは回復されます。
- 以前のリリースからアップグレードする場合は、新しいリリースのシャーシ **gtpu peer statistics threshold** が以前のリリース以上であることを確認してください。これにより、GTPU ピアの統計情報がアップグレード時に保持されます。たとえば、リリース 19.0 から 20.2 にアップグレードする場合、19.0 のシステムに 17,000 の GTPU セッションがある場合は、20.2 のシャーシのしきい値も 17,000 に設定します。

設定/制限事項

- StarOS に接続される GTP-U エンティティの数が多いため、GTP-U パス管理機能を無効にすることを推奨します。
- 分散型のシステムであるため、統計情報の割り当てに関して設定するしきい値に厳しい上限はありません。統計情報を含む GTP-U ピアの合計数が、設定されたしきい値を若干超える可能性があります。

- 100 万個のピアすべてがポイントツーポイントでノードに接続されていないことを前提としています。ピアはルータを介して接続されます。
- StarOS がこの機能をサポートするために ARP のテーブルサイズが変更されることはありません。

TCP ウィンドウサイズ



重要 この機能は、このリリースでは完全には認定されていません。テスト目的でのみ使用できます。詳細については、シスコのアカウント担当者にお問い合わせください。

通信事業者は、すべてのダウンリンク TCP パケットの実効ウィンドウサイズを制限できます。この機能を有効にするために、新しい CLI コマンド **window-size** がルールベース コンフィギュレーション モードに追加されました。

P-GW は、実効ウィンドウサイズが設定されたウィンドウサイズよりも大きい場合、設定された値で TCP パケットを更新します。それ以外の場合、P-GW はパケットのウィンドウサイズを変更しません。

P-GW は（SYN フラグとともに送信される）ウィンドウ スケール オプションを制御できないため、新しく更新されたウィンドウサイズは設定されたウィンドウサイズと同じではない場合があります。したがって、更新されたウィンドウサイズは、ウィンドウスケールのオプションによって計算された値に最も近い値に丸められます。

非 SYN フローにはウィンドウスケールのオプションがないため、この機能は適用されません。

TCP ウィンドウサイズが有効になっている場合、ルールベースの変更と設定の変更は、新しく作成されたフローと既存のフローの両方に適用されます。これらのフローに対して TCP ウィンドウサイズ機能が有効になっていない場合、変更は適用されません。



（注） PGW は指定されたルールベースのすべてのダウンリンクパケットを更新するため、設定されたウィンドウサイズがパケット内の実効ウィンドウサイズよりも小さくなり、パフォーマンスに影響が及びます。

しきい値超過アラート（TCA）

システムでのしきい値設定は、エラーや停止を引き起こす可能性のある条件についてシステムをモニターするために使用されます。通常、これらの条件は一時的なものであり（高い CPU 使用率や、ネットワークでのパケットコリジョンなど）、すぐに解決されます。ただし、特定の時間間隔内にこれらのエラー状態が継続的に発生するか多数発生する場合は、より大きく、より重大な問題を示している可能性があります。しきい値設定の目的は、潜在的な重大状態の特定を容易にすることです。これにより、即時に対処して、システムのダウンタイムを最小限に抑えるか回避することが可能になります。

システムは、特定の主要リソース（CPU、メモリ、IP プールアドレスなど）に関するしきい値超過アラートをサポートしています。この機能により、通信事業者は、これらのリソースのしきい値を設定できます。それにより、リソースの枯渇が設定されたしきい値を超えると、SNMP トラップが送信されます。

システムでは、次のしきい値設定モデルがサポートされています。

- **アラート**：値がモニターされ、その値が、指定されたポーリング間隔内で、設定された上限しきい値に達するか、それを超えると、アラート状態が発生します。アラートが生成され、ポーリング間隔の最後に生成および/または送信されます。
- **アラーム**：値に関して、上限と下限の両方のしきい値が定義されます。その値が、指定されたポーリング間隔内で、設定された上限しきい値に達するか、それを超えると、アラーム状態が発生します。アラートが生成され、ポーリング間隔の最後に生成および/または送信されます。

しきい値設定では、次のいずれかのメカニズムを使用して状態が報告されます。

- **SNMP トラップ**：モニター対象の各値の状態（上限しきい値の超過やクリア）を示すSNMP トラップが作成されました。

  シャーシで、特定のトラップの生成を有効または無効にできます。重要な障害のみが表示されることを確認してください。SNMP トラップは、アラートモードとアラームモードの両方でサポートされています。

- **ログ**：システムは、アクティブログとイベントログを生成できる「threshold」と呼ばれるファシリティを提供します。他のシステムファシリティと同様に、ログが生成されます。モニター対象の値の状態に関するログメッセージは、WARNING のシビラティ（重大度）レベルで生成されます。

  ログは、アラートモデルとアラームモデルの両方でサポートされています。

- **アラームシステム**：指定されたポーリング間隔内に生成された上限しきい値アラームは、その条件が存在しなくなるか、条件クリアアラームが生成されるまで、「未処理」と見なされます。「未処理」アラームは、システムのアラームサブシステムに報告され、要素管理システムで表示できます。

  アラームシステムは、アラームモデルと組み合わせでのみ使用されます。



重要 しきい値超過アラートの設定の詳細については、『*Thresholding Configuration Guide*』を参照してください。

トランザクションレート KPI - 1 秒あたりのセッションイベント

重要業績評価指標（KPI）では、PDN セッションのアクティブ化および非アクティブ化における成功と失敗が区別されていませんでした。さらに、KPI は Voice-over-LTE（VoLTE）サービスに関する情報を提供しませんでした。

1 秒あたりのセッションイベント（SEPS）KPI は、上記の問題に対処するために実装されました。これらの KPI は、P-GW や ePDG のシグナリング負荷を測定します。さらに、VoLTE コールのセットアップと切断のイベントレートを測定するために、ネットワークにより開始されたセットアップまたはティアダウン KPI が追加されました。これらの測定値を合わせて使用すると、通信事業者が P-GW または ePDG ノードにおいてネットワークを測定および計画する際に役立ちます。

P-GW の場合、S5、S8、S2a、S2b の各インターフェイスで両方のタイプの KPI がサポートされます。また、P-GW では、関連付けられているすべての eHRPD と PMIP サービスで SEPS KPI がサポートされています。

具体的には、次の KPI が導入されました。

1 秒あたりのセッションイベント（SEPS）

1 秒あたりのセッションイベント KPI は、P-GW または ePDG のシグナリング負荷を測定するときに通信事業者を支援するために実装されています。これらの SEPS KPI には、以下が含まれます。

- 1 秒あたりの合計セッションイベント（セッションのセットアップと切断）。
- 1 秒あたりの成功したセッションイベント（セッションのセットアップと切断）。
- 1 秒あたりの失敗したセッションイベント（セッションのセットアップと切断）。

1 秒あたりのネットワークが開始したセットアップおよび切断イベント

ネットワークによって開始されたセットアップおよび切断イベント KPI が導入され、通信事業者が P-GW や ePDG で Voice over LTE（VoLTE）コールのセットアップと切断のレートを測定できるようになりました。ベアラー作成要求（CBReq）とベアラー削除要求（DBReq）の両方が最初に P-GW によって開始され、ホーム サブスクライバ サーバー（HSS）の結果として P-GW により開始された CBReq と DBReq、およびユーザー機器（UE）が開始したイベントは、これらの KPI でカウントされます。1 秒あたりのネットワークが開始したセットアップおよび切断イベント KPI には以下が含まれます。

- 1 秒あたりのネットワークが開始したセットアップおよび切断イベント（VoLTE ベアラーのセットアップおよび切断）。
- 1 秒あたりのネットワークが開始し成功したセットアップおよび切断イベント（VoLTE ベアラーのセットアップおよび切断）。
- 1 秒あたりのネットワークが開始し失敗したセットアップおよび切断イベント（VoLTE ベアラーのセットアップおよび切断）

操作

P-GW と ePDG には、1 秒あたりのセッションイベント KPI と 1 秒あたりのネットワークが開始したセットアップおよび切断イベント KPI の両方のトランザクションレート統計収集用に 8 つのバケットが含まれています。バケットは、設定可能な 1 ～ 20 分のバケット間隔に基づいています。設定された時間間隔中、バケット間隔全体の平均が計算されて保存されます。

最初の 8 バケットの間隔が経過して統計が収集された後、P-GW は 8 バケット間隔で順番に処理を続け、最終的に元の 8 バケット間隔をより新しいデータで上書きします。つまり、8 つのバケット間隔は、KPI が計算された最後の 8 バケット間隔の現行値を提供します。統計は最終的に新しい値で上書きされますが、すべての統計の合計は履歴統計に追加され、上書きされることはありません。

UE タイムゾーンのレポート

この機能により、スーパーオフピークの請求プランなど、特定のサービス料金について時間ベースの課金が可能になります

UE のタイムゾーンは、UE の場所（トラッキング領域やルーティング領域）に関連付けられています。UE タイムゾーン情報要素は、MME がトラッキングエリアリストに基づいて追跡する属性であり、S11 および、S5 または S8 シグナリングを介して P-GW に伝達されます。

タイムゾーンのレポートは、請求レコードに含めるか、外部 PCRF および OCS サーバーへの Gx または Gy シグナリングで伝達できます。

ユーザーロケーション変更レポートのサポート

ユーザー情報変更レポート機能は、GPRS 固有のイベントトリガーと GPRS 固有のクレジット再承認トリガーによって、PCRF を介して GGSN で有効になります。レポートの対象になるユーザー情報には、ロケーション変更レポート（ULI）と Closed Subscriber Group 情報変更レポート（UCI）が含まれます。

GGSN によって要求されたサブスクライバセッションのロケーション変更レポートについては、MS が GERAN、UTRAN、GAN の RAT タイプのいずれかにある場合、SGSN にはユーザロケーション情報（ULI）が含まれます。また、MS がセル、サービス、ルーティングエリアに存在するかに応じて、CGI、SAI、RAI もそれぞれ含まれます。SGSN には、他の RAT タイプのユーザーロケーション情報を必要に応じて含めることができます。

Closed Subscriber Group（CSG）は、CSG のメンバーとして PLMN の 1 つ以上の CSG セルにアクセスできるサブスクライバグループを識別します。CSG ID は PLMN の範囲内にある一意の識別子であり、CSG セルまたは CSG セルのグループに関連付けられた PLMN の CSG を識別します。GGSN によって要求されたサブスクライバセッションの CSG 情報変更レポートについては、MS が CSG セルまたはハイブリッドセル内にある場合、SGSN にはユーザー CSG 情報が含まれます。

リリース 20.0 以降では、PDN（ゼロ以外の TEID や IMSI + NSAPI）を識別するための有効な情報、および適切な ULI や UCI 情報とともに受信した MS 情報の変更通知を処理するための機能が追加されています。MS 情報変更メッセージと NRUPC が競合した場合、GGSN は最初に MS 情報変更要求を処理し、MS 情報変更応答を送信します。その後に、NRUPC が再試行されます。



重要 CSG レポートは、GGSN、P-GW、SAEGW ではまだサポートされていません。

制限事項

この機能には次の制限があります。

- PCRF からの UCI トリガーはサポートされていません。
- 次の場合、MS 情報変更のレポートアクションのトリガーは回復されません。
  - トリガーが変更された
  - MS レポートアクションが CPC/UPC/NRUPC にない
  - セッションマネージャ（SM）のリカバリが発生した
- MS 変更情報メッセージが UE レベルでレポートされた場合はサポートされません。

3GPP ULI レポートのサポート拡張

この機能拡張は、3GPP 標準規格に従って P-GW および GGSN の ULI 関連のギャップをカバーします。

機能変更

この機能拡張は、3GPP 標準規格に従って P-GW および GGSN の ULI 関連のギャップをカバーします。

S4SGSN は、S-GW を介して P-GW に ULI を報告します。P-GW は、以前に受信した ULI を使用して ULI の変更を決定します。変更が検出され、同じ変更が PCRF によってイベントトリガーとして要求されている場合、ULI が PCRF に報告されます。

SGSN は GGSN に ULI を報告します。GGSN は、以前に受信した ULI を使用して ULI の変更を決定します。変更が検出され、同じ変更が PCRF によってイベントトリガーとして要求されている場合、ULI が PCRF に報告されます。GGSN で ULI フィールドの一部として受信した RAI における変更の検出のサポートも追加されています。

次の表は、P-GW が S4 SGSN と通信する PCRF から受信したイベントトリガーに基づく変更レポートアクション（CRA）の値をまとめたものです。

PCRF からのイベントトリガー	**S4 SGSN に送信される CRA**
USER_LOCATION_CHANGE（13）	Start Reporting CGI/SAI and RAI（5）
RAI_CHANGE（12）	Start Reporting RAI（2）
USER_LOCATION_CHANGE + RAI_CHANGE	Start Reporting CGI/SAI and RAI（5）

次の表は、GGSN が SGSN と通信する PCRF から受信したイベントトリガーに基づく MS 情報変更レポートアクションの値をまとめたものです。

PCRF からのイベントトリガー	SGSN に対する MS 情報変更レポートアクション
USER_LOCATION_CHANGE（13）	Start Reporting CGI/SAI（1）
RAI_CHANGE（12）	Start Reporting RAI（2）
BOTH（12,13）	Start Reporting CGI/SAI（1）

P-GW/GGSN は、イベントトリガーを受信すると、他のイベント（APN/AMBR の更新や QoS の更新など）を待つことなく、すぐに CRA/MS 情報変更レポートアクションを報告します。

動作の変更

以前の変更レポートアクション：次の表は、アクセスノードが S4SGSN である場合の、PCRF から受信したイベントトリガーに関する変更レポートアクションの以前の動作と新しい動作を示しています。

PCRF からのイベントトリガー	S4SGSN に送信される CRA	S4SGSN に送信される CRA
ULI_CHANGE（13）	6 (START_REPORTING_TAI_ECGI)	5（START_REPORTING_CGI_RAI）
RAI_CHANGE（12）	CRA が送信されない	2（START_REPORTING_RAI）
BOTH（12,13）	6 (START_REPORTING_TAI_ECGI)	5（START_REPORTING_CGI_RAI）

MS 情報変更レポートアクションの動作：次の表は、アクセスノードが SGSN である場合の、PCRF から受信したイベントトリガーに関する MS 情報 CRA の以前の動作と新しい動作を示しています。

PCRF からのイベントトリガー	SGSN に送信される CRA	SGSN に送信される CRA
ULI_CHANGE（13）	1 (START_REPORTING_CGI/SAI)	1（START_REPORTING_CGI/SAI）
RAI_CHANGE（12）	CRA が送信されない	2（START_REPORTING_RAI）
BOTH（12,13）	1 (START_REPORTING_CGI/SAI)	1（START_REPORTING_CGI/SAI）

制限事項

1. GGSN では、ネットワーク要求更新済み PDP コンテキスト（NRUPC）応答で新しい ULI を受信しても、それが PCRF に報告されません。

2. GGSN では、専用ベアラーが削除されるか、コールがドロップされると、URI の変更は検出されません。

仮想 APN のサポート

仮想 APN は、単一の APN 内におけるサービスの差別化を可能にします。

仮想 APN 機能により、キャリアは単一の APN を使用して差別化されたサービスを設定できます。MME によって提供される APN は、複数の設定可能パラメータを用いて P-GW により評価されます。次に、P-GW は、指定された APN とそれらの設定可能パラメータに基づいて APN 設定を選択します。

APN設定は、P-GWにおけるセッションのすべての側面を決定します。ポリシーが異なる場合は、APN も異なります。ただし、基本的な APN の選択後、次のパラメータに基づいて内部で再選択される場合があります。

- サービス名
- サブスクライバタイプ
- IMSI の MCC-MNC
- ユーザー名のドメイン名部分（user@domain）
- S-GW アドレス



重要 詳細については、『*Command Line Interface Reference*』の「*Context Configuration Mode Commands*」に記載の **virtual-apn preference** コマンドを参照してください。

特徴と機能 - インラインサービスのサポート

ここでは、P-GW でサポートされているインラインサービスの特徴と機能について説明します。これらのサービスでは、機能を実装するための追加ライセンスが必要です。

コンテンツ フィルタリング

Cisco P-GW は、ネットワーク制御コンテンツフィルタリングとペアレント コントロール サービスの2つのバリエーションを提供しています。各アプローチでは、プラットフォームのネイティブの DPI 機能を利用して、HTTP URL または WAP/MMS URI 要求に基づきモバイルサブスクライバから関心を持たれているイベントを検出およびフィルタリングします。

- **統合コンテンツフィルタリング**：Cisco P-GW 上でのポリシー適用ポイントとカテゴリベースの評価データベースを備えたターンキーソリューション。サブスクライバセッションが確立されると、オフボード AAA や PCRF はサブスクライバ別のコンテンツフィルタリング情報を提供します。コンテンツ フィルタリング サービスは、DPI を使用して HTTP 要

求メッセージ内の URL や URI を抽出し、それらを静的評価データベースと比較してカテゴリの一致を判断します。プロビジョニングされたポリシーは、個々のサブスクライバがコンテンツを表示する権限があるかどうかを判断します。

- **コンテンツフィルタリング ICAP インターフェイス**：このソリューションは、アクティブコンテンツフィルタリング外部サーバーをすでに設置しているモバイル通信事業者に適しています。このサービスは継続的に ASR 5500 プラットフォームの DPI 機能を利用して、関心の高いイベントを抽出します。ただしこの場合、抽出された要求は、サブスクライバの識別情報とともに Integrated Content Adaptation Protocol（ICAP）を介して、カテゴリ評価データベースとコンテンツ決定機能を備えた外部 ACF サーバーに転送されます。

統合アダルトコンテンツフィルタ

未成年者に害を与える不快なコンテンツが意図せず表示されるのを防ぐ付加価値サービスを提供します。コンテンツフィルタリングは、ペアレントコントロールとコンテンツフィルタリングのためのネットワークベース ソリューションを通じて、モバイル通信事業者にデータ ARPU とサブスクライバの維持率を向上させる方法を提供します。この統合ソリューションにより、単一のポリシー決定および適用ポイントが実現され、外部 AAA/ポリシーマネージャサーバーとのシグナリング相互作用の回数が合理化されます。Enhanced Content Charging（ECS）などの他のサービスと併用すると、モバイルサブスクライバが、アクセスを許可されているサイトへの訪問についてのみ課金されることが保証されるため、課金レコードの請求情報の精度が向上します。

統合アダルトコンテンツフィルタは、P-GW サービスを実行する ASR 5500 でプロビジョニングされるサブスクライバ対応のインラインサービスです。統合コンテンツフィルタリングは、ローカル DPI エンジンを利用し、システム上のアクティブな P-GW セッションの数に合わせて拡張できる分散ソフトウェアアーキテクチャを活用します。

コンテンツ フィルタリング ポリシーの適用は、サブスクライバが特定のコンテンツを受信できるかどうかを決定するプロセスです。一般的なオプションは、コンテンツの評価と、そのコンテンツおよびサブスクライバに対して定義されたポリシーに基づく、コンテンツの許可、ブロック、または置換/リダイレクトです。ポリシー定義は、AAA サーバーからの認証応答か、Gx 参照インターフェイスを介した付加 PCRF からの Diameter ポリシーメッセージで転送されます。ポリシーは、ルールベースまたは APN/サブスクライバ設定を介してサブスクライバに適用されます。ポリシーにより、カテゴリに基づいてコンテンツ要求に対して実行されるアクションが決定されます。最大 1 つのポリシーをルールベースに関連付けることができます。

ICAP インターフェイス

未成年者に害を与える不快なコンテンツが意図せず表示されるのを防ぐ付加価値サービスを提供します。コンテンツフィルタリングは、ペアレントコントロールとコンテンツフィルタリングのためのネットワークベース ソリューションを通じて、モバイル通信事業者にデータ ARPU とサブスクライバの維持率を向上させる方法を提供します。コンテンツフィルタリング ICAP ソリューションは、ネットワーク内にアクティブ コンテンツ フィルタリング サーバーをすでに設置している通信事業者に適しています。

P-GW の Enhanced Charging Service（ECS）は、合理化された Internet Content Adaptation Protocol（ICAP）インターフェイスを提供し、ディープ パケット インスペクション（DPI）を活用して、外部アプリケーションサーバーが DPI 機能を実行したり、データフローに挿入したりせずに、サービスを提供できるようにします。外部のアクティブコンテンツフィルタリング（ACF）プラットフォームの使用を希望する通信事業者にとって、ICAP インターフェイスは魅力的な場合があります。サブスクライバが WAP（WAP1.x または WAP2.0）または Web セッションを開始すると、後続の GET/POST 要求がディープ パケット インスペクション機能によって検出されます。GET/POST 要求の URL は、ASR 5500 プラットフォームのローカル DPI エンジンによって抽出され、サブスクライバ識別情報とサブスクライバ要求とともに ICAP メッセージでアプリケーションサーバー（AS）に渡されます。AS は、カテゴリや、タイプ、アクセスレベル、コンテンツカテゴリなどの他の分類に基づいて URL をチェックし、GET/POST メッセージに応答することで、要求を許可、ブロック、またはリダイレクトする必要があるかどうかを決定します。ACF サーバーから受信した応答に応じて、P-GW は要求を変更なしで渡すか、またはメッセージを破棄して、適切なリダイレクトメッセージまたはブロックメッセージでサブスクライバに応答します。

ヘッダーの拡張機能：ヘッダーの挿入と暗号化

ヘッダーの拡張機能は、アプリケーションサーバーへの HTTP 要求にサブスクライバ固有の情報を含めて、サブスクライバインテリジェンスを収益化する、付加価値のある機能をモバイル通信事業者に提供します。

拡張ヘッダー（X-Header）フィールドは、特定の目的でプロトコルのヘッダーに追加できるフィールドです。拡張ヘッダーでは、プロトコルを変更せずに追加の entity-header フィールドを定義できますが、entity-header フィールドは受信者が認識できるフィールドとは想定されていません。認識されないヘッダーフィールドは、受信者によって無視されて、トランスペアレントプロキシによって転送される必要があります。

拡張ヘッダーは、HTTP/WSP の GET および POST 要求パケットでサポートできます。P-GW の Enhanced Charging Service（ECS）には、HTTP/WSP GET および POST 要求パケットに x-Header を挿入するための APN ベースの設定とルールが用意されます。ルールに関連付けられた課金アクションには、パケットに挿入される X-Header のリストが含まれます。サポートされているプロトコルは、HTTP、WAP 1.0 および WAP 2.0 の GET メッセージと POST メッセージです。



重要 ECS の詳細については、『*ECS Administration Guide*』[英語] を参照してください。

挿入された HTTP ヘッダー属性で渡されるデータは、エンドアプリケーション サーバー（アップセルサーバーとも呼ばれる）によって、サブスクライバおよびセッション情報を識別するために使用されます。このサーバーは、その特定のサブスクライバに合わせてカスタマイズされた情報を提供します。

Cisco P-GW は、HTTP ヘッダーに次の情報を含めることができます。

- ユーザーがカスタマイズ可能な任意のテキスト文字列

- サブスクライバの電話番号（クリアテキストの RADIUS calling-station-id）
- サブスクライバの IMSI
- サブスクライバの IP アドレス
- S-GW の IP アドレス（クリアテキスト）

X-Header の暗号化により X-Header の挿入機能が強化されます。サポートされるフィールド数が増えるのに加え、フィールド挿入前の暗号化も可能になります。

WSP ヘッダーに X-Header フィールドを挿入する際、次の制限が適用されます。

- X-Header フィールドは、StarOS v14.0 より前のフラグメント化された IP パケットには挿入されません。
- 連結要求の場合、X-Header フィールドは最初の GET 要求または POST 要求にのみ挿入されます（ルールが同じ要求で一致する場合）。連結要求の 2 番目以降の GET/POST 要求には X-Header フィールドは挿入されません。たとえば、パケットに ACK+GET がある場合、GET パケットに X-Header が挿入されます。ただし、GET1+GET2 がパケット内に存在し、ルールが GET2 で一致し、GET1 で一致しない場合、X-Header は引き続き GET2 に挿入されます。GET+POST の場合も、POST に X-Header は挿入されません。
- CO の場合、WTP パケットが誤った順序で受信された場合でも（適切に順序変更された後でも）X-Header フィールドは挿入されません。
- MMS へのルートが存在する場合、X-Header は挿入されません。
- ヘッダーがセグメント化されている場合、WSP POST パケットに X-Header は挿入されません。POST には、X-Header ヘッダーの追加後に変更が必要なヘッダー長フィールドが含まれているためです。セグメント化された WSP ヘッダーでは、ヘッダー長フィールドが 1 つのパケットに存在し、ヘッダーが別のパケットで完了することがあります。

ヘッダー機能拡張のためのハッシュ値のサポート

ハッシュ値文字列は、ヘッダー機能拡張の一部として実装されます。P-GW は、各サブスクライバの PCRF から受信したハッシュ値を保存するように拡張されています。保存されたハッシュ値は HTTP/WSP ヘッダーに挿入され、通信事業者がサブスクライバプロファイルを処理する際に使用できます。

一部のモバイル広告プラットフォームでは、サブスクライバの MSISDN 値に基づいてハッシュ文字列が生成されます。ハッシュ文字列がコンテンツプロバイダーに送信されると、コンテンツプロバイダーはサブスクライバのプロファイル情報を識別し、ユーザーのプロファイルに基づいてサブスクライバのブラウザに広告を挿入します。

PCRF からハッシュ値を受信するには、データ型がオクテット文字列の新しい AVP の **Hash-Value** を Gx インターフェイスに実装します。この AVP は、最大 80 文字をサポートします。最大長を超えると、P-GW はハッシュされた文字列を無視します。PCRF から受信したハッシュ値は、サブスクライバの HTTP ヘッダーの機能拡張が有効になっている場合にのみ、HTTP/WSP ヘッダーに挿入されます。

X-Header フィールドは、HTTP/WSP ヘッダーにハッシュ値を挿入するために使用されます。ハッシュ値は、X-Header フィールドの既存の暗号化メカニズムに基づいて暗号化できます。これらのハッシュ値（暗号化されているかどうかにかかわらず）は、課金アクションで設定した X-Header 形式に基づいて HTTP/WSP ヘッダーに挿入されます。

（注） ハッシュ値には、サブスクライバのセッション情報の一部としてチェックポイントが付けられます。PCRF からハッシュ値が受信されるとすぐにチェックポイントが付けられます。

IPNE サービスサポート

P-GW は、IP Network Enabler（IPNE）サービスをサポートしています。IPNE は、セッション情報とネットワーク情報を収集して MINE サーバーに配信する、Mobile and IP Network Enabler（MINE）クライアントコンポーネントです。MINE クラウドサービスは、ワイヤレス通信事業者とパートナーがセッションおよびネットワークの情報を共有および交換してインテリジェントなサービスを実現するための、一元化されたポータルを提供します。IPNE の詳細については、このガイドの「*IP Network Enabler*」の章を参照してください。

Network Address Translation（NAT）

NAT では、ルーティング不可能なプライベート IP アドレスが、NAT 用に指定されているパブリック IP アドレスのプールからのルーティング可能なパブリック IP アドレスに変換されます。この変換により、外部ネットワークとの通信に必要なパブリック IP アドレスの数を節約でき、内部ネットワークの IP アドレススキームが外部ホストからマスクされ、各送受信パケットがこの変換プロセスを通過するため、セキュリティが保証されます。

NAT は、着信と発信両方の IP データグラムを検査し、必要に応じて、発信データグラム用に設定された NAT アドレスマッピングを反映するように IP ヘッダーの送信元 IP アドレスとポート番号を変更することによって機能します。逆 NAT 変換は着信データグラムに適用されます。

NAT は、簡易 IP とモバイル IP のアドレス変換を実行するために使用できます。NAT は、フローの L3/L4 の特性（送信元 IP、送信元ポート、接続先 IP、接続先ポート、およびプロトコル）に基づいて、サブスクライバから発信されるさまざまなフロー（5 タプル接続）に選択的に適用したり、適用を拒否したりすることができます。

NAT は次のマッピングをサポートしています。

- 1 対 1
- 多対 1

重要 NAT の詳細については、『*NAT Administration Guide*』[英語] を参照してください。

NAT64 のサポート

この機能により、ネットワーク内での IPv6 アドレッシングスキームとの共存と、このスキームへの段階的な移行が促進されます。NAT64 を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

IPv4 パブリックアドレス空間が縮小し、より多くのルーティング可能アドレスの必要性が高まる中、サービスプロバイダーと企業は IPv6 ネットワークの構築と展開を今後も続行します。ただし、IPv4 が大規模に導入されているため、世界が一晩で IPv6 に変化するというのは現実的ではありません。IPv4 への投資を保護する必要性と、ネットワークの拡張と拡大の必要性という両方の要因により、IPv4 ネットワークと IPv6 ネットワークをかなりの期間にわたって共存させ、エンドユーザーのエクスペリエンスをシームレスに維持することが求められます。

推奨されるアプローチは、エンドホスト上のデュアルスタック（IPv4 と IPv6 の両方）、デュアル スタック ルーティング プロトコル、およびデュアルスタック対応アプリケーションを実行することです。上記がすべて実行可能な場合、エンドホストは IPv6 または IPv4（NAT を使用）を使用してネイティブに通信します。可能な限り通信を実現するために次に推奨される方法は、IPv4 または IPv6 を使用したトンネリングです。これらのオプションがすべて失敗した場合は、変換が推奨されます。

ステートフル NAT64 は、IPv6 パケットを IPv4 パケットに（またはその逆に）変換するためのメカニズムです。システムは、そのフレームワークが draft-ietf-be have-v6v4-framework-10 で説明されている IETF Behave WG ドラフトに基づいて、ステートフル NAT64 トランスレータをサポートしています。ステートフル NAT64 は、現在のシステム実装の既存の NAT ライセンスの一部として使用できます。NAT44 と NAT64 はシャーシ上で共存し、NAT 動作に必要なリソースを共有します。

ピアツーピアの検出

通信事業者はネットワーク内の P2P トラフィックを識別し、適切な制御機能を適用して、すべてのサブスクライバに帯域幅を公平に分配できます。

ピアツーピア（P2P）とは、2 つのわずかに異なるコンテキストで使用される用語です。機能レベルでは、クライアントサーバー方式とは対照的に、ピアリング方式で対話するプロトコルを意味します。ノードの機能の間に明確な区別はありません。どのノードもクライアント、サーバー、またはその両方として機能できます。プロトコルはこの 2 つを明確に区別しない場合があります。たとえば、ピアリング交換には、クライアントとサーバーの機能や情報の送受信が同時に含まれることがあります。

ピアツーピアプロトコルを検出するには、プロトコルを一意に識別する特性をリアルタイムで認識する必要があります。一般的なパケット分類では、特定のプロトコルを実行しているパケットストリームのヘッダーに入力された一意の情報のみを識別する必要があります。実際、多くのピアツーピアプロトコルは、単純なパケット ヘッダー インスペクションで検出できます。ただし、一部の P2P プロトコルは異なるため、従来の方法では検出できません。これは、意図的に検出を回避するために一部の P2P プロトコルに組み込まれています。これらのプロトコルの作成者は、意図的に仕様を公開しません。スモールクラスの P2P プロトコルはよりステ

ルス性が高く、検出がより困難になります。一部のプロトコルでは、固定マーカーのセットをプロトコル固有のものとして確実に識別できません。

通信事業者は、一部の P2P アプリケーション（Bittorrent、Skype、eDonkey など）の動作のためにP2P トラフィックについて注意を払う必要があります。ほとんどのP2P アプリケーションは、20% の P2P ユーザーが残りの 80% の非 P2P ユーザーと同等の量のトラフィックを生成できるように、ネットワーク帯域幅を占有できます。これにより、P2P ユーザーが帯域幅を過剰に使用するため、非P2P ユーザーが正当に使用するための十分なネットワーク帯域幅を取得できない状況が発生する可能性があります。通信事業者はネットワーク帯域幅やトラフィックを動的に管理する機能を配置し、すべてのユーザー間でネットワーク帯域幅を公平に分配する必要があります。これには、ネットワーク内のP2P トラフィックを識別し、適切な制御機能を適用することが含まれます（コンテンツベースのプレミアム課金、QoS の変更、その他の同様の処理など）。

シスコのP2P 検出テクノロジーでは、革新的で高精度なプロトコル動作検出技術が活用されています。

重要 ピアツーピア検出の詳細については、『*ADC Administration Guide*』を参照してください。

パーソナル ステートフル ファイアウォール

パーソナル ステートフル ファイアウォールは、サブスクライバトラフィックを検査し、個々のサブスクライバセッションに対する IP セッションベースのアクセス制御を実行するインラインサービス機能で、サブスクライバを悪意のあるセキュリティ攻撃から保護します。

パーソナル ステートフル ファイアウォールは、設定に基づくステートレスおよびステートフル インスペクションとフィルタリングをサポートします。

ステートレスインスペクションでは、ファイアウォールがパケットを検査して、パケットに含まれる 5 タプル（送信元および宛先 IP アドレスとポート、およびプロトコル情報）を判定します。この静的情報を設定可能なルールと比較して、パケットを許可するかドロップするかを決定します。ステートレスインスペクションでは、ファイアウォールは各パケットを個別に検査します。その前に通過したパケットを認識せず、特定のパケットが既存の接続の一部であるか、新しい接続を確立しようとしているか、または不正なパケットであるかは一切把握できません。

ステートフル インスペクションでは、ファイアウォールがアプリケーション レイヤ/レイヤ 7 までパケットを検査して、パケットのヘッダー情報とデータコンテンツを確認するだけでなく、接続の状態をモニターし追跡を継続します。ファイアウォールを経由するすべてのアクティブな接続について、状態情報（関連する IP アドレスとポート、接続を通過するパケットのシーケンス番号と確認応答番号、TCPパケットフラグなどを含む）が状態テーブルで維持されます。フィルタリングの決定は、ルールだけでなく、該当する接続での先行パケットによって確立された接続状態にも基づいています。この仕様により、さまざまな DoS、DDoS、およびその他のセキュリティ違反を防止することができます。接続が切断されるか、タイムアウトになると、状態テーブルのエントリは破棄されます。

Enhanced Charging Service（ECS）/Active Charging Service（ACS）インラインサービスは、パケット検査および課金を実行するための主な手段です。ECS の詳細については、『*ECS Administration Guide*』[英語] を参照してください。

重要 パーソナル ステートフル ファイアウォールの詳細については、『*PSF Administration Guide*』[英語] を参照してください。

オプションの拡張機能ソフトウェアの特長と機能

ここでは、P-GW サービスのオプションの拡張機能について説明します。

次の各機能を使用するには、追加のライセンスを購入して、P-GW サービスの機能を実装する必要があります。

重要 ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

ePDG および P-GW での 3GPP R13 緊急通話のサポート

ePDG と P-GW により、3GPP リリース 13 に従って、P-GW の信頼できない Wi-Fi を介した緊急通話の確立がサポートされます。IMS 緊急セッションをサポートするために緊急ベアラーサービスが提供されます。緊急ベアラーサービスとは、緊急サービスをサポートするようにネットワークが設定されている場合に、サービスを提供しているネットワークによって提供される機能を指します。緊急ベアラーサービスは、通常どおりにアタッチされた UE のほかに、現地の規制に応じてサービスが制限されている UE に提供されます。限定的なサービス状態での緊急サービスの受信には、サブスクリプションは不要です。

Diameter への認証承認要求（AAA）が、信頼できない Wi-Fi 緊急通話用の新しい Emergency-Indication AVP を伝送するようになりました。緊急サービス用の PDN 接続に関連する Diameter 要求が最も優先されます。地域/国の要件やネットワーク通信事業者のポリシーに応じて、これらの Diameter 要求は、3GPP AAA サーバーでトラフィックの削減を適用する必要がある場合に最後にスロットルされます。詳細については、「ePDG および P-GW での 3GPP R13 緊急コールのサポート」の項を参照してください。

AAA とプレフェックス委任 DHCP の関連付け

この機能を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

現在 DHCP サーバーでは、割り当てられた IPv6（/64）プレフィックスを特定のサブスクライバに関連付けるメカニズムが DHCPv6 に実装されていません。この機能は、PDN 接続の設定時に、AAA サーバーから割り当てられたデフォルトのプレフィックスを、外部 DHCPv6 サーバーから割り当てられた委任済みプレフィックスに関連付けます。

DHCP クライアントプロファイルのコンフィギュレーション モードには、委任済みプレフィックスの設定時に、P-GW から外部 DHCPv6 サーバーに DHCPv6 メッセージの USER_CLASS_OPTION を送信するためのオプションがあります。

APN バックオフタイマーのサポート

以前は、P-GW で遅延耐性または優先順位の低いデバイスからのシグナリングトラフィック（優先順位の低いマシン間トラフィックなど）が区別されませんでした。

UE は、NAS や接続要求メッセージを介して MME にデバイスプロファイルを示すことができました。MME は、S5 インターフェイスのシグナリング優先順位表示情報要素（IE）を介して、この情報を P-GW に渡すことができました。一部の UE は、P-GW への S5 インターフェイスでのシグナリング優先順位表示 IE の提供をサポートしていなかった可能性があります。その結果、P-GW はシグナリングタイプを区別できませんでした。現在のリリースでは、P-GW はこれらのシグナリングタイプを区別できます。

また、過負荷状態のとき、P-GW は LAP デバイスからの新しいセッションを許可し、Low Access Priority Indicator（LAPI）デバイスからのトラフィックを通常の UE と同じ優先順位で処理していました。現在の StarOS リリースでは、過負荷状態のときに、P-GW が LAPI として識別されたトラフィックをバックオフするように設定できます。APN 設定またはシグナリング優先順位表示 IE のいずれかに基づいて、この識別が行われます。

バックオフ タイマー アルゴリズムと R12 GTP-C 負荷/過負荷制御アルゴリズムが連携するようになりました。この機能のメリットは、優先順位の低いコールが拒否されることです。その結果、優先順位の高いコールの帯域幅を増やすことができます。

詳細については、本ガイドの「*APN* バックオフタイマーのサポート」の章を参照してください。

ARP 値別の GTP-C メッセージのバルク統計

「Long Term Evolution (LTE) Access Network Government Industry Requirements (GIR) for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority」に適合し、Voice over LTE（VoLTE）上の緊急通話をサポートするために、この機能にはいくつかのキーパフォーマンス インジケータ（KPI）が導入されています。この機能は、指定された間隔（分単位）に Enhanced Multimedia Priority Service（eMPS）セッションで受信された GTP-C メッセージの合計数の統計を収集するために使用されます。GTP-C メッセージのリストは、GIR のドキュメントに従って定義されます。この機能の一部として、次の処理が実行されます。

- S-GW は、NS/EP NGN-PS の使用に割り当てられた値のセットから選択された割り当ておよび保持プライオリティ（ARP）を含む、受信した GTP-C メッセージの総数のペグカウントを指定された間隔（分単位）で生成します。このペグカウントは、S-GW レベルで管理されます。

- P-GW は、NS/EP NGN-PS の使用に割り当てられた値のセットから選択された ARP を含む、受信した GTP-C メッセージの総数のペグカウントを指定された間隔（分単位）で生成します。このペグカウントは、特定の P-GW レベルで管理されます。
- GTP-C メッセージのペグカウントは、既存の GTP-C メッセージカウンタと同様にメッセージタイプ別に分類されます。バルク統計は、該当する S-GW および P-GW サービス、および S5、S8、S11、S4 インターフェイスによって分類されます。

eMPS セッション/メッセージのバルク統計が追加されました。

ピギーバックメッセージ

ピギーバックメッセージの場合、いずれかのメッセージが一致する ARP を含む場合、または最終的に非 eMPS セッションが eMPS セッションに変換される場合、両方のメッセージが eMPS メッセージとしてカウントされ、両方のメッセージに対応する統計が増分されます。

ベアラー変更要求が S-GW の S11 インターフェイスでベアラー作成応答と共にピギーバックされ、ベアラー作成応答が最終的に非 eMPS セッションから eMPS セッションに変換される場合、ベアラー変更応答の統計は増分されません。

バルク統計の収集とリセット

バルク統計は、eGTP-C スキーマと pgw-egtpc-s5s8 スキーマに追加されます。eGTP-C スキーマおよび pgw-egtpc-s5s8 スキーマのこれらの eMPS バルク統計は、次のバルク統計までの間のみ値を保持します。つまり、これらのバルク統計の値は、次のバルク統計までに交換された eMPS メッセージの数を示します。

詳細については、「*ARP* 値別の *GTP-C* メッセージのバルク統計」の項を参照してください。

共通ゲートウェイアクセスのサポート

共通ゲートウェイアクセスのサポートは、HA、P-GW、および GGSN の論理サービスをサポートする共通ゲートウェイに 3G および 4G アクセステクノロジーを組み合わせた統合ソリューションであり、利用可能なアクセステクノロジーに関係なく、同じユーザーエクスペリエンスを得ることができます。

現代のシナリオでは、オペレータは、複数のアクセスネットワーク（CDMA、eHRPD、LTE）に加えて、国際ローミングのための GSM/UMTS ソリューションを用意する必要があります。そのため、オペレータは、アクセステクノロジー（3G または 4G）に関係なく、同じ IP アドレッシング動作でサービスにアクセスし、共通の出力インターフェイスセットを使用できるようにするソリューションを必要としています。

このソリューションにより、静的なお客様は、接続のタイプ（CDMA、eHRPD/LTE、または GSM/UMTS）に関係なく、ワイヤレスデータに割り当てられた同じ IP アドレッシング空間でネットワークサービスにアクセスできます。静的 IP アドレッシングを使用するサブスクライバは、アクセステクノロジーに関係なく、同じ IP アドレスを取得できます。

ダイナミック RADIUS 拡張機能（認可変更）

ダイナミック RADIUS 拡張機能（CoA および PoD）を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

ダイナミック RADIUS 拡張機能のサポートにより、データトラフィックを動的にリダイレクトしたり、PDP コンテキストを切断したりする機能が提供され、通信事業者はサブスクライバの PDP コンテキストのより詳細な制御が可能になります。

この機能は、RFC 3576「Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)」（2003 年 7 月）標準に基づいています。

システムは、次のダイナミック RADIUS 拡張機能の設定と使用をサポートしています。

- **認可変更**：システムは、AAA サーバーからの CoA メッセージをサポートして、サブスクライバセッションに関連付けられているデータフィルタを変更します。AAA サーバーからの CoA 要求メッセージには、NAS とサブスクライバセッションを識別する属性と、サブスクライバセッションに適用するデータフィルタのデータフィルタ ID が含まれている必要があります。
- **切断メッセージ**：DM メッセージは、RADIUS サーバーからのシステム内のサブスクライバセッションを切断するために使用されます。DM 要求メッセージには、サブスクライバセッションを識別するために必要な属性が含まれている必要があります。

上記の拡張機能を使用して、プロビジョニングやアカウントのセットアップなどの機能を実行するために、サブスクライバの PDP コンテキストを代替アドレスに動的にリダイレクトできます。この機能は、セッションリダイレクト、またはホットラインと呼ばれます。

セッションリダイレクトは、既存または新しいサブスクライバセッションのトラフィックに ACL ルールを適用することにより、サブスクライバのトラフィックを外部サーバーにリダイレクトする手段を提供します。サブスクライバからの TCP/IP または UDP/IP パケットの宛先アドレスと宛先ポート（オプション）が書き換えられ、パケットが指定のリダイレクトアドレスに転送されます。

サブスクライバに戻るトラフィックでは、送信元アドレスとポートが元の値に書き換えられます。リダイレクト ACL は、RADIUS 認可変更（CoA）拡張機能によって動的に適用されます。



重要 ダイナミック RADIUS 拡張機能のサポートの詳細については、このガイドの「*CoA、RADIUS DM、セッションのリダイレクト（ホットライン）*」の章を参照してください。

VoLTE/緊急コールの拡張優先順位付け

National Security/Emergency Preparedness（NS/EP）Next Generation Network（NGN）Priority Services（NGN-PS）（旧称 NGN Government Emergency Telecommunications Service（GETS））とは、パブリックパケット交換サービスプロバイダーから利用可能なサービスに基づく一連の音声、動画、およびデータのサービスです。NS/EP NGN-PS は、サービスユーザーの NS/EP 通信に関

する優先処理を提供するものであり、サービスプロバイダーのネットワークで、輻輳を原因とする障害が発生したり、自然災害（洪水、地震、ハリケーンなど）による損傷が発生したり、人為的な災害（物理攻撃、サイバー攻撃、または他の形態のテロ攻撃など）が発生したりした場合に特に必要です。

eMPS セッションに属する制御メッセージ、または eMPS プロファイルに関連付けられている割り当ておよび保持プライオリティ（ARP）を含む制御メッセージの場合、DSCP マーキングは eMPS プロファイルで設定された DSCP 値に基づいています。

この機能拡張の一部として、Government Industry Requirements（GIR）NS/EP NGN で定義されている優先処理のために、P-GW および S-GW で特定の GTP-C メッセージをマーキングするためのサポートも追加されています。詳細については、「*VoLTE*/緊急コールの拡張優先順位付け」を参照してください。

PCO を使用した ePDG の選択

この機能の目的は、PGW が通信事業者の PCO で ePDG の IP アドレスを送信できるようにして、Wi-Fi ネットワークへの接続時に UE が地理的に最も近い ePDG に接続されるようにすることです。これにより、最も近い ePDG への IPSEC トンネルのセットアップが容易になり、VoWIFI やその他の機能の遅延が減少します。

ネットワーク内の PCO オプションをカスタマイズするために、新しい CLI が導入されました。

重要 これはライセンスで制御される機能です。ライセンスの詳細については、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

重要 ePDG PCO は、S5-S8 インターフェイスで受信される CS 要求に対してのみサポートされます。この機能は、GGSN コールには適用されません。

この機能の詳細については、本ガイドの「*PCO* を使用した *ePDG* の選択」の 章を参照してください。

GRE プロトコルインターフェイスのサポート

GRE インターフェイス トンネリングを使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

P-GW は、RFC 2784：Generic Routing Encapsulation（GRE）に従って、GRE 汎用トンネルインターフェイスをサポートします。GRE プロトコルにより、モバイルユーザーは、GRE トンネルを介して企業ネットワークに接続できます。

企業顧客は、GRE トンネルを使用して、1）APN に対応する AAA パケットを、GRE トンネルを介して企業 AAA サーバーに転送し、2）企業サブスクライバパケットを、GRE トンネルを介して企業ゲートウェイに転送することができます。

企業サーバーはプライベート IP アドレスを持つことができるため、異なる企業に属するアドレスが重複する可能性があります。各企業は、「VRF」と呼ばれる一意の仮想ルーティングドメイン内に存在する必要があります。同じローカルエンドとリモートエンドのセット間のトンネルを区別するために、GRE キーが区別要因として使用されます。

GRE トンネリングは、単一プロトコルバックボーン上でマルチプロトコルローカルネットワークを有効にし、非隣接ネットワークを接続して、WAN 間の仮想プライベートネットワークを有効にするための一般的な手法です。このメカニズムでは、別のプロトコル内の 1 つのプロトコルからのデータパケットをカプセル化し、外部ネットワークでデータパケットを変更せずに転送します。（IPsec などのように）暗号化が含まれていないため、GRE トンネリングでは、カプセル化されたプロトコルが保護されないことに注意してください。

GRE トンネリングは、次の 3 種類の主要コンポーネントから構成されます。

- パッセンジャプロトコル：カプセル化されるプロトコル。CLNS、IPv4、IPv6 などです。
- キャリアプロトコル：カプセル化を実行するプロトコル。GRE、IP-in-IP、L2TP、MPLS、IPSec などです。
- トランスポートプロトコル：カプセル化したプロトコルを伝送するために使用するプロトコル。主なトランスポート プロトコルは IP です。



重要 GRE プロトコルインターフェイスのサポートの詳細については、このガイドの「*GRE* プロトコルインターフェイス」の章を参照してください。

GTP ベース S2a インターフェイスのサポート

S2a インターフェイスは、SAEGW のスタンドアロン P-GW と P-GW を eHRPD の HSGW に接続します。

GTP ベース S2a インターフェイスのサポートは、P-GW および SAEGW で利用できます。WLAN が通信事業者によって信頼されていると見なされると、信頼できる WLAN アクセスネットワーク（TWAN）が、P-GW への S2a インターフェイスを介して、信頼できる非 3GPP アクセスとして EPC とインターフェイス接続されます。SAEGW サービスの Make と Break を使用して、Wi-Fi から LTE へのハンドオーバーのサポートが拡張されました。マルチ PDN ハンドオーバーも、この機能の一部としてサポートされています。

SAEGW に展開している通信事業者は、この機能を使用して信頼できる Wi-Fi ネットワーク機能を統合できるようになりました。

以下のような機能がサポートされています。

- 初回アタッチ

- Wi-Fi から LTE へのハンドオーバー
- LTE から WiFi へのハンドオーバー
- マルチ PDN ハンドオーバー

GTP ベース S2b インターフェイスのサポート

Wi-Fi 統合機能を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

このセクションでは、P-GW での GTP ベース S2b インターフェイスの導入について説明します。S2b インターフェイスでは、P-GW が ePDG に接続されます。UE は、ホームネットワークが同時接続をサポートしている場合にのみ、異なるアクセスネットワーク経由で異なる APN への同時接続を試みます。UE は、APN 単位のシステム間ルーティングポリシーでプロビジョニングされているか、このポリシーを受信済みの場合に、ネットワークが複数のアクセスでのこのような同時接続をサポートしていると判断します。したがって、UE は、複数のアクセスタイプによる個別の PDN 接続を確立できます。サポートされるアクセスタイプは 4G と Wi-Fi です。

S2b インターフェイスの導入では、次の要素がサポートされます。

- Wi-Fi アクセスを介して PDN に接続する UE
- UE の複数 PDN 接続
- 初回アタッチ
- LTE から Wi-Fi へのハンドオフ
- Wi-Fi から LTE へのハンドオフ



重要 Wi-Fi 統合機能の詳細については、このガイドの「*P-GW* および *SAEGW* での *GTP* ベース *S2b* インターフェイスのサポート」の章を参照してください。

Voice Over Wi-Fi のサポート

UE が Wi-Fi から LTE に移行すると、P-GW は、ベアラー削除要求を ePDG（Wi-Fi アクセス）に送信します。以前は、ハンドオフのセッション作成要求が P-GW で受信されると、すぐにベアラー削除要求が送信されていました。一部の使用例では（特定のハンドセットの場合）、この動作によりハンドセットと WAP 間の IPsec トンネルが切断されます。こうした状況では、ハンドオフに失敗していました。ハンドオフの失敗を回避するには、P-GW がまずセッション作成応答を送信し、UE のハンドオフが完了するまでベアラー削除要求を遅らせる必要があります。次に、UE がベアラー変更要求を生成してハンドオフの完了を通知します。ベアラー削除要求は、P-GW がベアラー変更要求を受信した後にのみ生成されます。これは、P-GW でベアラー変更要求が受信されるまで、両方のアクセスタイプ（Wi-Fi と LTE）がアクティブのままであることを示しています。UE が LTE から Wi-Fi に移行すると、セッション作成応答でハンドオフが完了します。

GTP スロットリング

GTP および Diameter インターフェイス スロットリングを使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

この機能は、P-GW と GGSN での着信および発信メッセージのレートを制御するのに役立ちます。これは、P-GW と GGSN が GTP 制御プランのメッセージによって過負荷にならないようにするのに役立ちます。さらに、P-GW と GGSN が、GTP コントロール プレーン メッセージでピア GTP-C ピアを過負荷にしないようにするのに役立ちます。

この機能を使用するには、Gn または Gp インターフェイスおよび S5 または S8 インターフェイスを介した GTP（v1 および v2）制御メッセージのシェーピングおよびポリシングが必要です。この機能は、P-GW および GGSN ノードとそれが通信する他の外部ノードの過負荷保護を行います。スロットリングは、セッションレベルの制御メッセージに対してのみ実行されます。パス管理メッセージはレート制限されません。

外部ノードの過負荷は、P-GW または GGSN が他のノードで処理できるレートよりも高いレートでシグナリング要求を生成するシナリオで発生する可能性があります。受信メッセージレートが、設定されたメッセージレートよりも高い場合、余分なメッセージが通知なしにドロップされます。また、実際のコールセットアップレートが、設定されたメッセージレートよりも低くなる可能性もあります。これは、低速なピアノードや SM の過負荷といった多くの理由により、セッションのセットアップが遅延している場合に発生する可能性があります。さらに、このスロットリングの一部として実行されるドロップはどこにも通知されないため、非エコーメッセージがパス障害であると設定されている場合、パス障害と見なされる可能性があります。

P-GW または GGSN 制御シグナリングにより外部ノードが過負荷にならないよう保護するために、フレームワークを使用して、外部インターフェイスへのアウトバウンド制御メッセージのシェーピングおよびポリシングを処理します。

レート制限機能のバイパス

レート制限のバイパス機能は、既存の GTP スロットリング機能を拡張したものです。

この機能拡張には追加ライセンスは必要ありません。GTP スロットリング機能（RLF ライセンス）および VoLTE 優先順付け処理機能の既存のライセンスが次のように適用および使用されています。

- **RLF ライセンス**：GTP スロットリング機能のライセンスが拡張され、message-type に基づいた RLF スロットリングバイパスに対応するようになりました。
- **VoLTE 有線順位付け処理機能ライセンス**：このライセンスは、緊急コール、プライオリティコール、および apn-name に基づいた RLF スロットリングバイパスに対応するように拡張されました。

GTP スロットリング機能は、P-GW の着信/発信メッセージのレート制御に役立ちます。これにより、P-GW から S-GW および MME へのメッセージフラッディングを防止できます。現在、次の発信メッセージは、RLF フレームワークを使用して P-GW によってスロットリングされます。

- ベアラー作成要求（CBR）
- ベアラー削除要求（DBR）
- ベアラー更新要求（UBR）
- NRUPC
- IPCA
- NRDPC

発信メッセージに対してスロットリングを有効にすると、すべての発信メッセージがスロットリングされます。ただし、セッション作成応答メッセージと共にピギーバックされるベアラー作成要求（CBR）メッセージは除外されます

この機能は、スロットリングされている一部のメッセージのバイパスを制御するように拡張されました。

既存の CLI コマンド **gtpc overload-protection egress rlf-template rlf-temp** に新しいコマンドオプション **throttling-override-policy** が追加されました。これにより、設定されたメッセージタイプ、または緊急コールまたはプライオリティコールのすべてのメッセージ、または設定された APN のコールのすべてのメッセージに対して、スロットリングを選択的にバイパスできます。新しい CLI コマンドモード **throttling-override-policy** も導入され、スロットリングのオーバーライドポリシーの汎用シンタックスが使用できるようになりました。

重要 これらのコマンドの詳細については、*CLI* のリファレンスガイドを参照してください。

通信事業者は、出力側での過負荷制御機能とともに、P-GW で過負荷保護/RLF スロットリングオーバーライド（RLFのバイパス）を設定できます。このシナリオでは、ピアの削減メトリックに基づく過負荷制御が優先され、メッセージは最初に過負荷制御機能に基づいてスロットリングされます。

メッセージが過負荷制御機能の処理後に RLF スロットリングに渡される場合、設定に従って、スロットリングのオーバーライド（RLF のバイパス）が後に適用されます。過負荷制御機能が設定されておらず、RLF スロットリングと RLF スロットリングのバイパスが設定されている場合、メッセージは RLF およびスロットリング オーバーライド（RLF のバイパス）機能に基づいてスロットリングされます。

重要 このコマンドの詳細については、R12 GTP-C 負荷および過負荷制御機能 （106 ページ）を参照してください。

HSS および PCRF ベースの P-CSCF 復元のサポート

P-CSCF 復元を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

この機能により、P-CSCF 復元のサポートが有効になります。P-CSCF の復元手順が標準化され、P-CSCF 障害後のコール終了により UE と通信できなくなる時間が最小限に抑えられました。3GPP 標準規格リリース 13 に準拠して、この機能には次の P-CSCF 復元メカニズムが含まれています。

- 信頼できるまたは信頼できない WLAN アクセス（S2a/S2b）のための HSS ベース P-CSCF 復元
- LTE（S5/S8）および信頼できるまたは信頼できない WLAN アクセス（S2a/S2b）のための PCRF ベース P-CSCF 復元



重要 この機能の詳細については、このガイドの「*HSS* および *PCRF* ベースの *P-CSCF* 復元のサポート」の章を参照してください。

シャーシ間セッションリカバリ

シャーシ間セッションリカバリを使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

ASR 5500 は、業界をリードするキャリアクラスの冗長性を実現します。システムは、すべてのシングルポイント障害（ハードウェアおよびソフトウェア）から保護され、複数の障害が同時に発生した場合、動作状態を回復しようとします。

システムは、いくつかのレベルのシステム冗長性を実現します。

- 通常の N+1 PSC/PSC2 ハードウェア冗長性では、致命的なパケット処理カードの障害が発生した場合、影響を受けるすべてのコールが可能な限りスタンバイパケット処理カードに移行されます。移行できないコールは適切なコール終了シグナリングによって正常に終了され、内部チェックポイントまでの正確な統計を使用してアカウンティングレコードが生成されます。
- セッションリカバリ機能が有効になっている場合、PSC/PSC2 の全面的な障害によって PSC スイッチオーバーが発生し、サポートされているコールタイプに対して確立されたすべてのセッションがセッション損失なしで回復されます。

シスコはこれら 2 つのスキームによる優れたシャーシ内冗長性を提供していますが、IP ルーティングの障害、ライン切断、電力損失、シャーシの物理的破壊など、シャーシ全体の停止を引き起こす可能性のある特定の致命的な障害をこの方法で保護することはできません。こうした状況では、MME シャーシ間セッションリカバリ機能がサイト間の地理的冗長性を提供します。この機能には、致命的な障害が発生してもサブスクライバのエクスペリエンスが向上するという利点がありますが、RAN などの他のシステムをサブスクライバの再アクティブ化ストームから保護することも可能にします。

シャーシ間セッションリカバリ機能は、サブスクライバのサービスを中断することなく継続的なコール処理を可能にします。回復は冗長シャーシを使用して達成されます。シャーシはプラ

イマリとバックアップとして設定されます。1 つはアクティブで、もう 1 つはリカバリモードになります。チェックポイントの期間タイマーは、アクティブシャーシから非アクティブシャーシにサブスクライバデータが送信されるタイミングの制御に使用されます。コールトラフィックを処理しているアクティブシャーシがサービス停止になると、非アクティブシャーシはアクティブ状態に移行し、サブスクライバセッションを中断せずにコールトラフィックの処理を続行します。シャーシは、冗長性リンクと呼ばれる適切な TCP ベースの接続を介して、どちらがアクティブであるかを判別します。このリンクは、プライマリシャーシとバックアップシャーシの間で Hello メッセージを交換するために使用されるもので、適切なシステム運用のために維持する必要があります。

- **シャーシ間の通信**

  シャーシ間セッションリカバリをサポートするように設定されたシャーシは、定期的に Hello メッセージを使用して通信します。これらのメッセージは、各シャーシによって、現在の状態をピアに通知するために送信されます。Hello メッセージには、設定や優先順位などのシャーシに関する情報が含まれています。dead 間隔は、シャーシのピアから受信される Hello メッセージの時間制限を設定するために使用されます。スタンバイシャーシが dead 間隔の間にアクティブシャーシから Hello メッセージを受信しない場合、スタンバイシャーシはアクティブ状態に移行します。冗長性リンクがサービス停止になる状況では、どのシャーシがセッションを処理するかを決定するために優先順位スキームが使用されます。次の優先順位スキームが使用されます。

  - ルータ ID
  - chassis priority
  - SPIO MAC アドレス

- **チェックポイントメッセージ**

  チェックポイントメッセージは、アクティブシャーシから非アクティブシャーシに送信されます。チェックポイントメッセージは、特定の間隔で送信され、そのシャーシがアクティブになった場合にスタンバイシャーシ上のセッションを再作成するために必要なすべての情報を含んでいます。セッションがチェックポイント期間を超えると、そのセッションでチェックポイントデータが収集されます。checkpoint パラメータは、セッションがチェックポイントメッセージに含められる前にアクティブでなければならない時間を決定します。

重要 シャーシ間セッションリカバリのサポートに関する詳細については、『*System Administration Guide*』の「*Interchassis Session Recovery*」の章 [英語] を参照してください。

IP セキュリティ（IPSec）暗号化

ネットワーク ドメイン セキュリティを使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

IPSec 暗号化により、すべての IP パケット交換 LTE-EPC ネットワークでドメインセキュリティが可能になり、機密性、整合性、認証、およびアンチリプレイ保護を提供できるようになります。これらの機能は、暗号技術によって守られます。

Cisco P-GW は、IPv4 アドレッシングを使用した IKEv1 および IPSec 暗号化をサポートしています。IPSec により、次の 2 つのユースケースを実現できます。

- P-GW が S-GW とは別の管理ドメインにある場合のローミングアプリケーションにおける S8 セッションと EPS ベアラーの暗号化
- 3GPP TS 33.210 に準拠した IPSec ESP セキュリティが、S1 コントロールプレーン、S1 ベアラープレーン、および S1 管理プレーンのトラフィックに提供されます。EPC コアネットワークの通信事業者がローミングパートナーのネットワークから無線容量をリースする場合、S1 リファレンス インターフェイス上のトラフィックを暗号化することが望ましいです。



重要 IPSec のサポートに関する詳細については、『*IPSec Reference*』[英語] を参照してください。

RADIUS サーバーおよびローカルプールからの IPv6 プレフィクスの委任

この機能により、RADIUS サーバーまたは GGSN/P-GW/SAEGW で設定されたローカルプールから DHCPv6 プレフィックス委任を取得するためのサポートが追加されます。RADIUS サーバーからのインターフェイス ID の割り当てもこの機能でサポートされています。

ユーザー機器（UE）または顧客宅内機器（CPE）がプレフィックス委任を要求します。次に、P-GW または GGSN は、RADIUS サーバーまたはローカルプールからこのプレフィックスを取得します。P-GW と GGSN は、RADIUS サーバーまたはローカルプールのいずれかから取得されたプレフィックスを UE クライアントまたは CPE にアドバタイズします。

この機能は、次の 3 つの機能に分かれています。

- RADIUS サーバーからの IPv6 プレフィックス委任
- ローカルプールからの IPv6 プレフィックス委任
- RADIUS サーバーからの IPv6 インターフェイス ID



重要 IPv6 プレフィックス委任の詳細については、「*RADIUS* サーバーおよびローカルプールからの *IPv6* プレフィクスの委任」を参照してください。

L2TP LAC サポート

L2TP LAC を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

レイヤ 2 トンネリング プロトコル アクセス コンセントレータ（LAC）として設定されたシステムでは、L2TP ネットワークサーバー（LNS）との通信が可能になり、オペレータとサブスクライバの社内ネットワークまたはホームネットワークとの間にセキュアな仮想プライベートネットワーク（VPN）トンネルを確立できます。

VPN ネットワークでの L2TP の使用は、企業が認証と IP アドレスの割り当てをより詳細に制御できるようにするために頻繁に使用されます。オペレータは最初のレベルの認証を実行できますが、ユーザー名とパスワードの交換には PPP を使用し、アドレスの要求には IPCP を使用する場合があります。P-GW と企業間の PPP ネゴシエーションをサポートするには、LAC サービスを実行している P-GW で L2TP トンネルをセットアップする必要があります。

L2TP は、サブスクライバの PPP 接続を L2TP セッションとしてトンネリングする前に、LAC と LNS の間に L2TP 制御トンネルを確立します。LAC サービスは、P-GW と同じアーキテクチャに基づいており、動的なリソースの割り当て、メッセージとデータの分散処理のメリットを利用できます。

また、LAC セッションを冗長に設定することで、ハードウェアまたはソフトウェアの問題の影響を軽減することもできます。トンネル状態は、プロセッサカード間で情報をコピーすることによって保持されます。



重要 この機能のサポートに関する詳細については、本ガイドの「*L2TP* アクセスコンセントレータ」の章を参照してください。

合法的傍受

P-GW の合法的傍受機能の使用ライセンスは、P-GW セッション使用ライセンスに含まれています。

シスコの合法的傍受機能は、P-GW でサポートされています。合法的傍受は、ライセンス対応の標準ベースの機能であり、法執行機関が疑わしい個人の潜在的な違法行為を監視するのを支援するメカニズムを、電気通信サービスプロバイダーに提供します。合法的傍受機能の詳細とマニュアルについては、シスコのアカウント担当者にお問い合わせください。

レイヤ 2 トラフィック管理（VLAN）

レイヤ 2 トラフィック管理を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

仮想 LAN（VLAN）は、コンテキストおよびサービスの設定と使用の柔軟性を高めます。

VLANはポートごとに「タグ」として設定され、より複雑な設定を実装することができます。VLAN タグを使用すると、1 つの物理ポートを複数の論理インターフェイスにバインドして、それぞれを異なるコンテキストに設定できます。したがって、VLAN タグが使用されている場合、各イーサネットポートに多くの論理ポートが含まれているように表示されることがあります。



重要 VLAN のサポートの詳細については、『*System Administration Guide*』の「*VLANs*」の章を参照してください。

ローカルポリシー意思決定エンジン

ローカルポリシー意思決定エンジンを使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

ローカルポリシーエンジンは、Gx と同様な QoS とポリシー制御を提供するイベント駆動型のルールエンジンであり、ユーザーまたはアプリケーションの権限付与を可能にします。名前が示すように、通信事業者が PCRF を使用しないことを選択した場合、または外部 PCRF への接続が中断されたシナリオの場合に、PCRF のサブセットを提供するように設計されています。ローカルポリシーは、QoS、データ使用量、サブスクリプションプロファイル、サーバー使用量など、セッションのさまざまな側面をローカルに定義されたポリシーに従って制御するために使用されます。P-GW システムでは、最大 1,024 のローカルポリシーをプロビジョニングできます。

ローカルポリシーは、特定のイベントが発生したり、関連する条件が満たされたりした場合にトリガーされます。たとえば、新しいコールが開始されたときに、コールに適用される QoS は、IMSI、電話番号、および APN に基づいて決定できます。

ローカルポリシー意思決定エンジンの使用例には次のようなものがあります。

- モバイルコアネットワークで PCRF が失われた場合のディザスタ リカバリ データ バックアップ ソリューション。
- 緊急音声コールの専用ベアラーの確立。
- LTE から非 3GPP へのドメイン間ハンドオーバーでネットワークによって開始されるベアラーの確立。



重要 ローカルポリシー意思決定エンジンの設定の詳細については、このガイドの「*PDN* ゲートウェイの設定」の章の「ローカル *QoS* ポリシーの設定」を参照してください。

制御されたパラメータを使用したベアラー変更応答

P-GW サービスでは、課金 ID、課金 FQDN または課金ゲートウェイアドレス、および MSISDN をベアラー変更応答に含めるための設定可能なパラメータが提供されます。S-GW の再配置や GnGp から LTE へのハンドオーバーといったシナリオとは無関係に、CLI が有効になっている場合には、すべてのベアラー変更応答メッセージでこれらのパラメータが送信されます。この機能はライセンス制御されておらず、CLI を使用して動作が制御されます。

この機能の詳細については、このガイドの「制御されたパラメータを使用したベアラー変更応答」の章を参照してください。

LDP を使用した MPLS 転送

MPLS を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

マルチ プロトコル ラベル スイッチング（MPLS）とは、利用可能なネットワークパスをより有効に利用することで、ネットワークのトラフィックのフローを高速化するために使用される操作スキームまたはメカニズムです。BGP や OSPF などのルーティングプロトコルと連携して動作するので、ルーティングプロトコルではありません。

MPLS は固定長のラベルを生成し、IP パケットのヘッダーに付加またはバインドして、データのフローおよび宛先を制御します。IP パケットへのラベルのバインドは、Label Distribution Protocol（LDP; ラベル配布プロトコル）によって行われます。転送等価クラス（FEC）内のすべてのパケットは、MPLS ノードとも呼ばれるラベルスイッチングルータ（LSR）によって転送されます。LSR はラベルスイッチングパス（LSP）の確立のために、LDP を使用して転送先ネイバーに信号を送り、ラベルを配布します。

多くの異なるアドレッシングモデルと要件を持つ企業 APN の増加に対応するために、MPLS は少なくとも次の 2 つの要件を満たすように展開されます。

- 企業 APN トラフィックは、セキュリティ上の理由から、他の APN とは分離されるように維持する必要があります。
- 異なる APN での IP アドレスの重複。

展開されると、MPLS バックボーンは、IP パケットにバインドされたラベルを使用して自動的にルートをネゴシエートします。LSR である Cisco P-GW は、接続されたプロバイダーエッジ（PE）からデフォルトルートを学習し、PE は P-GW によって提供されるルートをルーティングテーブルに入力します。

重要 MPLS のサポートの詳細については、このガイドの「マルチプロトコル ラベル スイッチング（*MPLS*）のサポート」の章を参照してください。

NEMO サービスのサポート

NEMO を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

P-GW は、ネットワークモビリティ（NEMO）サービスを有効または無効にするように設定できます。

有効にすると、システムには、P-GW プラットフォームにおけるモバイル IPv4 ネットワークモビリティ（NEMO-HA）の NEMO サポートが含まれ、エンタープライズ PDN に接続するモバイルルータ（MR）からのモバイル IPv4 ベースの NEMO 接続が終端されます。NEMO 機能により、MR の背後にいるユーザーと固定ネットワークサイト上のユーザーまたはリソース間で、アプリケーションに依存しない双方向の通信が可能になります。

同じ NEMO4G-HA サービスとそのバインドされたループバック IP アドレスが、 NEMO 接続をサポートします。NEMO 接続の基盤となる PDN 接続は、GTP S5（4G アクセス）または PMIPv6 S2a（eHRPD アクセス）を介して行われます。



重要 NEMO サポートの詳細については、このガイドの「 ネットワークモビリティ（*NEMO*）」の章を参照してください。

GGSN での NEMO サポート

GGSN で Dynamic Network Mobile Routing（NEMO）を使用するには、有効なライセンスキーをインストールする必要があります。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

NEMO サポートが P-GW と GGSN に追加され、3G（UMTS/GERAN）ネットワーク上でローミング中のサブスクライバに対して NEMO がサポートされるようになりました。

この機能は、GGSN で標準ベースの NEMO 機能をサポートします。これにより、通信事業者は迅速な導入とお客様に合わせた柔軟な帯域幅調整のメリットを活かして、エンタープライズ VPN サービスをサポートできます。

NEMO（NEtwork MObility）は、3G/4G ネットワークを介してエンタープライズのコアネットワークとリモートサイト間のワイヤレス接続を提供します。ワイヤレス接続は、プライマリリンクまたはバックアップリンクとして使用できます。リモートサイトのすべてのホストは、NAT を使用せずにコアネットワーク内のホストと直接通信できます。

エンタープライズ VPN サービスは、この機能の主要なユースケースの 1 つです。迅速な導入とお客様に合わせた柔軟な帯域幅調整は、このサービスのメリットの一部です。お客様には、銀行、金融機関、マルチサイト企業、地方自治他、公安局、輸送機関などが含まれます。

IMS のネットワーク提供ロケーション情報

NPLI を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

この機能により、P-GW は、3GPP-User-Location-Info AVP、User-Location-Info-Time AVP（使用可能な場合）、および/または 3GPP-MS-TimeZone AVP（PCRF によって要求される場合）内の PCRF に必要なアクセスネットワーク情報を提供できます。P-GW は、Event-Trigger AVP 内の ACCESS_NETWORK_INFO_REPORT イベントトリガーも提供します。

ベアラーの非クティブ化または UE 切断手順中に、P-GW は、3GPP-User-Location-Info AVP 内の PCRF へのアクセスネットワーク情報と、User-Location-Info-Time AVP 内のその位置で UE が最後に認識された日時に関する情報を提供します。PCRF が Required-Access-Info AVP の一部としてユーザー位置情報を要求しており、その情報が P-GW にない場合、P-GW は、3GPP-SGSN-MCC-MNC AVP 内のサービング PLMN 識別子を提供します。

以前は、P-GW は、値が変更された場合にのみ ULI/MS-TimeZone/PLMN-ID を ECS/IMSA/PCRF に通知していました。この機能により、値が変更されたかどうかに関係なく、P-GW は ECS によって送信されたルールで NetLoc 通知を受信し、これを ECS/IMSA/PCRF に送信します。P-GW は NetLoc を「1」と受信すると、MS-Timezone に通知します。P-GW は NetLoc を「0」と受信すると、ULI および ULI タイムスタンプを通知します。このケースで ULI が使用できない場合は、PLMN-ID が送信されます。更新の NetLoc 通知を受信した場合、P-GW は RetLoc Indication フラグを使用して、この情報を UBReq でアクセス側に示します。

これは VoLTE に必要であり、IMS ドメインの課金および LI 機能を支援します。この機能により、EPC コアはサブスクライバの ULI およびタイムゾーン情報を IMS コアネットワークに報告する効率的な方法をサポートできます。

古いセッションの新しいコールポリシー

古いセッションに対して新しいコールポリシーを使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

新しいコールポリシーが **reject release-existing-session** に設定され、セッション作成要求で受信した IMSI/IMEI の既存のセッションがある場合、それらは削除されます。これにより、新しいコール ポリシーでリリース拒否が設定されていてもノードでセッションがハングしません。GGSN/P-GW/SAEGW/S-GW が既存のコールをリリースすると、アカウンティング終了の送信、PCRF/OCS への CCR-T の送信、CDR の生成という適切なリリースプロセスに従います。

（注） **reject release-existing-session** CLI は、S-GW や P-GW サービス中に緊急 APN コールで接続されたサブスクライバをサポートしません。

非標準 QCI のサポート

非標準 QCI を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

通常、GGSN/P-GW/SAEGW/S-GW/ePDG では、1 ～ 9 の標準ベース QCI 値のみがサポートされます。3GPP リリース 8 以降では、通信事業者固有/非標準の QCI が P-GW/GGSN（スタンドアロン GGSN ではない）でサポートされ、キャリアは QCI 128-254 を定義して、キャリアがネットワーク内のエンドユーザーに提供するさまざまなサービス/アプリケーションを区別できます。



重要 非標準 QCI のサポートの詳細については、このガイドの「拡張 *QCI* のオプション」の章を参照してください。

Wi-Fi EPC の NetLoc

この機能により、IMS ネットワークは WLAN アクセスネットワークから UE の位置情報を取得できます。これにより、通信事業者のための位置関連の機能が向上します。この機能は、位置情報に基づいてサブスクライバに課金する場合にも有用です。

LTE NetLoc は以前のリリースからすでサポートされていることに注意してください。このリリースでは、NetLoc のサポートが WLAN アクセスに拡張されています。SM、IMSA、および ECS などのさまざまな内部モジュールに、必要なパラメータを渡すための基本的な実装はすでにサポートされています。詳細については、「*Wi-Fi EPC* の *NetLoc*」セクションを参照してください。

過課金保護のサポート

過充電保護を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

過課金保護は、UE がアイドルモードの間にドロップされたダウンリンクパケットのサブスクライバへの課金を回避するのに役立ちます。一部の国では、このような過課金を避けることが規制上の要件となっているため、そのような国の通信事業者には必須の機能となります。全体として、この機能は、サブスクライバがアイドルモードのときにサブスクライバが過課金にならないようにするのに役立ちます。

P-GW は UE の状態（アイドルまたは接続モード）を認識しません。ダウンリンクデータの課金は、UE がアイドルモードの場合でも、P-GW で適用されます。バッファオーバーフローまたはページングの遅延が原因で、UEがアイドルモードになっている場合、UEのダウンリンクデータが S-GW でドロップされることがあります。したがって、P-GW は、ドロップされたパケットの料金をサブスクライバに課金しますが、これは望ましくありません。この問題に対処するために、過課金保護機能を有効にすることで、S-GW は、S-GW でドロップされたパケッ

トおよびUEのアイドル状態からアクティブ状態への遷移に基づいて、課金を停止または再開するよう P-GW に通知します。

「課金停止」をシグナリングする基準が満たされると、S-GWは、ベアラー変更要求（MBReq）を P-GW に送信します。PDN に対して MBReq が送信され、S-GW でドロップされるパケットが指定されます。MBReq には、「課金停止」および「課金開始」通知を P-GW に送信するための新しいプライベート拡張 IE があります。

PDN の S-GW から課金停止を含む MBReq を受信すると、P-GW はダウンリンクパケットの課金を停止しますが、S-GW へのパケットの送信は続行します。

P-GW は、次のいずれかの条件が満たされると、「課金停止」要求を受信した後に、ダウンリンクパケットの送信を再開します。

- （以前に MBReq で「stopcharge」を送信していた）S-GW が、MBReq で「startcharge」を送信したとき。
- S-GW が変更された場合（これは、UE が新しい S-GW に再配置された可能性があることを示します）。



重要 過課金保護機能が P-GW サービスと APN の両方で設定されている場合、APN での設定が優先されます。

ページングポリシー差別化

この機能を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

S-GW/P-GW は、ユーザーデータグラム パケットと外部 IP パケット（GTP-U トンネル IP ヘッダー）の DSCP 値を変更するための設定制御を提供します。DSCP マーキングは、設定に応じてさまざまなレベルで実行されます。ただし、ページングポリシー差別化（PPD）機能が有効になっている場合、ユーザーデータグラム パケット DSCP（トンネル化 IP パケット）のマーキングは変更されません。

現在、標準規格では、外部 GTP-U ヘッダーの QCI から DSCP へのマーキングのみが規定されています。ユーザーデータグラム パケットの DSCP 値を変更する ECS、P-GW、および S-GW のすべての設定は非標準です。標準ベースの PPD 機能では、P-CSCF または同様の Gi エンティティによって、ユーザーデータグラム パケットの DSCP がマーキングされます。このユーザーデータグラム パケットの DSCP 値は、S-GW によって MME/S4-SGSN に DDN メッセージで送信されます。MME/S4-SGSN は、この DSCP 値を使用してページング優先順位を付けます。



重要 P-GW と S-GW は、デフォルトと専用の両方のベアラーに PPD 機能を適用する必要があります。仕様に従って、P-GW はユーザーデータグラム パケットを透過的に S-GW に渡します。つまり、PPD 機能が有効になっている場合、通信事業者はデフォルトベアラーと専用ベアラーに異なる動作を適用できません。



重要 ページングポリシー差別化の詳細については、このガイドの「ページングポリシー差別化」の章を参照してください。

QCI ごとのパケットドロップカウンタと QCI レベルカウンタの ARP 精度

QCI および ARP の可視性のサポート

StarOS リリース 20.2 では、ソフトウェアの機能が強化されており、Quality of Service Class Index（QCI）および Allocation and Retention Priority（ARP）ベースの QoS 統計の表示がサポートされています。

ARP は、ネットワークが輻輳した状況で優先順位の低いベアラーをドロップまたはダウングレードするための 3GPP メカニズムです。ネットワークは ARP を確認し、新しい専用ベアラーを無線ベースステーションを介して確立できるかどうかを判断します。QCI は通信事業者のプロビジョニング値であり、ベアラーレベルのパケット転送処理を制御します。

この機能が拡張されたため、通信御者は、同じ QCI 値で実行されている複数のサービスを識別する QoS 統計情報をモニターできるようになりました。さらに、Enhanced Charging Service（ECS）がパケットをドロップした具体的な理由を提供するためのパケットドロップカウンタが導入されました。パケットドロップカウンタは、ARP ごとに出力されます。これにより、通信事業者はサービスに影響を与える可能性のあるネットワーク問題の特定とトラブルシュートを行う際に使用できる追加情報を得ることができます。



重要 ARP 値については、Allocation/Retention Priority（ARP）情報要素（IE）の優先度レベル値のみが考慮されます。ARP IE のプリエンプション脆弱性（PVI）およびプリエンプション機能（PCI）フラグは考慮されません。

既存の **show apn statistics name** *apn-name* および **show apn statistics** *Exec Mode* CLI コマンドが強化されました。これらのコマンドの出力で、QCI/ARP ベースの QoS 統計情報が可視化されるようになりました。



重要 詳細については、このガイドの「拡張 *QCI* のオプション」の章を参照してください。

ライセンス

QCI レベルカウンタの ARP 精度はライセンス制御機能です。QCI ごとのパケットドロップカウンタ機能にはライセンスは必要ありません。ライセンスの詳細については、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

S2b インターフェイスでのピギーバックのサポート

この機能は、S2b インターフェイスを介した ePDG および P-GW での「セッション作成応答」メッセージと「ベアラー作成要求」メッセージのピギーバックをサポートしています。セッション作成要求で ePDG によってピギーバックフラグが設定されると、P-GW は、セッション作成応答とベアラー作成要求を一緒に ePDG に送信できるようになり、これらのメッセージの順序が変更される可能性が排除されます。

R12 GTP-C 負荷および過負荷制御機能

GTP-C の負荷制御機能はライセンス方式のオプション機能です。この機能により、GTP コントロールプレーンノードはピアの GTP コントロールプレーンノードに負荷情報を送信できます。受信側の GTP コントロールプレーンノードは、この情報を使用して GW と S-GW で既存の GW 選択プロシージャを強化します。負荷情報には、発信元の GTP コントロールプレーンノードのリソースの動作ステータスが反映されます。

GTP コントロールプレーンのシグナリングを使用するノードは、ピアノードで実行されるアクションを通じてノードの過負荷状態を軽減するために、過負荷制御情報の通信をサポートする場合があります。この機能は、GTPv2 コントロール プレーン プロトコルを介して S5 および S8 インターフェイスでサポートされます。

GTP-C ノードが公称容量を超えて動作している場合に、そのノードは過負荷状態になっていると見なされ、結果としてパフォーマンスが低下します（着信トラフィックや発信トラフィック処理への影響もあります）。過負荷制御情報には、発信元ノードがそのような状況に達した日時が示されます。この情報が GTP-C ノード間で送信されると、これらのノード間の GTP-C シグナリングトラフィック量を削減またはスロットリングするために使用できます。このように過負荷制御情報によって、受信ノードがアクションを決定するためのガイダンスが提供されるため、情報の送信側の負荷軽減につながります。

負荷制御と過負荷制御を簡単に説明すると、次のようになります。

- 負荷制御により、GTP-C エンティティ（S-GW/P-GW など）は負荷情報を GTP-C ピア（MME/SGSN、ePDG、TWAN など）に送信できます。これにより、同じ機能をサポートするエンティティ（S-GW クラスタなど）間で、有効な負荷に応じてセッション負荷を適宜分散させることができます。負荷情報には、GTP-C エンティティリソースの動作ステータスが反映されます。
- 過負荷制御により、過負荷状態または過負荷状態になりつつある GTP-C エンティティで着信シグナリングの負荷を軽減できます。トラフィックを正常に処理するために使用できるシグナリング容量に従って、送信トラフィックを減らすように GTP-C ピアに指示します。GTP-C エンティティがそのシグナリング容量を超えて動作すると過負荷状態になり、パフォーマンスが低下します（着信トラフィックや発信トラフィック処理への影響もあります）。

最大 64 の異なる負荷プロファイルおよび過負荷プロファイルを設定できます。



重要 R12負荷および過負荷制御機能を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

R12 負荷および過負荷係数の計算機能の拡張

キャパシティテストおよびお客様のご利用環境において、sessmgr カードの CPU 使用率が高い場合でも、R12の負荷および過負荷サポート機能が誤ったシャーシの負荷係数値を提供することが確認されました。根本原因は、sessmgr カードと demux カードの CPU 使用率の平均を取得して負荷係数が計算される際、demux カードの CPU 使用率が sessmgr カードの CPU 使用率を上回らないためです。そのため、sessmgr カードの CPU 使用率が高くても、システムは過負荷状態に移行しませんでした。

R12 負荷/過負荷制御プロファイル機能が強化され、CPU 負荷とメモリでは、同タイプのカードの大きいほうの値に基づいて負荷係数が計算されるようになりました。demux カードの CPU 使用率の値が sessmgr カードの CPU 使用率の値よりも高い場合、負荷係数の計算には demux カードの CPU 使用率の値が使用されます。

リソースマネージャに複数のポーリング間隔を設定するための新しいCLIコマンドが導入されました。これにより、demuxmgr はさまざまなシステム要件に基づいて負荷係数を計算できます。



重要 この機能の詳細については、本ガイドの「*P-GW*、*SAEGW* および *S-GW* での *GTP-C* 負荷および過負荷制御のサポート」の章を参照してください。

動作

ノードは、ノードレベルの負荷制御情報に必要なさまざまなパラメータ（ライセンスセッション使用率、システム CPU 使用率、システムメモリー使用率など）を定期的に取得します。取得後、ノードは、ユーザーが指定する重み係数に基づいて、またはデフォルトの重み係数を使用して、負荷制御情報それ自体を計算します。

ノードレベルの負荷制御情報は 30 秒ごとに計算されます。リソースマネージャは、システムレベルでシステム CPU 使用率とシステムメモリー使用率を計算します。

設定されているサービスごとに、負荷制御情報が異なる場合があります。これは、サービスライセンスごとにアクティブセッション数に重みを付けることで実現できます。たとえば、[（サービスごとのアクティブセッション数/サービスライセンスに許可された最大セッション数）* 100] とします。

ノードのリソースマネージャは、すべてのカードの CPU とメモリーの使用率を平均することにより、システムレベルでのシステム CPU 使用率とシステムメモリー使用率を計算します。この値は、個々のカードレベルで計算された値とは異なる場合があります。

S6b から MDN を取得する

現在の実装では、最初のアタッチの際に、P-GWは、モバイルディレクトリ番号（MDN）またはモバイルステーション国際サブスクライバディレクトリ番号（MSISDN）を S6b インターフェイスから選択します。その後、コールが P-GW から eHRPD/信頼 Wi-Fi/非信頼 WiFi などの他のサービスにハンドオフされるか、これらのサービスからP-GWへのハンドオフが実行されると、セッション作成（CS）要求から MDN/MSISDN が選択され、S6b で承認された MDN/MSISDN が失われます。その結果、異なる値の MDN/MSISDN が Rf レコードで送信されます。通常、オペレータは MDN を使用してサブスクライバに請求するため、収益の損失が発生します。

この機能では、最初のアタッチの際に、また P-GW と eHRPD/信頼 Wi-Fi/非信頼 Wi-Fi 間のハンドオフでも、S6bインターフェイスまたはCS要求からのMDN/MSISDN値が保持されます。MDN/MSISDN の値は、コールの有効期間中は変更されません。そのため、セッションのすべての Rf レコードには同じ MDN/MSISDN の値が含められます。

新しいキーワード retain-mdn が CLI コマンド authorize-with-hss に追加されました。この CLI コマンドキーワードを設定すると、MDN/MSISDN値が保持されます。このCLIコマンドキーワードが設定されていない場合、MDN/MSISDN 値は S6b インターフェイスから受信されません。この場合、CS 要求で受信した MDN/MSISDN の値が使用されます。

重要 この機能は、GnGp ハンドオフには適用されません。

この機能の詳細については、このガイドの「*S6b から MDN を取得する*」の章を参照してください。

セッションリカバリサポート

P-GW のセッションリカバリ機能の使用ライセンスは、P-GW セッション使用ライセンスに含まれています。

セッションリカバリ機能は、システム内のハードウェアまたはソフトウェアに障害が発生した場合に、サブスクライバセッション情報のシームレスなフェールオーバーと再構築を行い、完全に接続されたユーザーセッションが切断されるのを防ぎます。

電気通信業界では、すべての機器の障害の 90% 以上がソフトウェアに関連しています。堅牢なハードウェア フェールオーバーと冗長性保護により、システム上のカードレベルのハードウェア障害を迅速に修正できます。ただし、さまざまな理由でソフトウェアの障害が発生する可能性があり、多くのの場合、何の前触れもありません。StarOS リリース 9.0 では、P-GW セッションのステートフルシャーシ内セッションリカバリをサポートする機能が追加されています。

セッションリカバリが発生すると、システムは次のサブスクライバ情報を再構築します。

- 正しいコール動作を維持するために必要なデータと制御状態情報
- サブスクライバデータ統計は、アカウンティング情報を確実に保持するために必要です。

- コール期間、絶対時間などのさまざまなタイマー値を回復するためのベストエフォート型の試行

ソフトウェアパッチのアップグレードアクティビティには、セッションリカバリも役立ちます。ソフトウェアパッチのアップグレード中にセッションリカバリが有効になっている場合、アップグレードプロセス中にアクティブな PSC/PSC2 で既存のセッションを保持できます。



重要 セッションリカバリのサポートに関する詳細については、『*System Administration Guide*』の「*Session Recovery*」の章を参照してください。

スマートフォンテザリング検出のサポート

スマートフォンテザリング検出を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

P-GW では、インラインヒューリスティック検出メカニズムを使用して、モバイルデバイスからのトラフィックと、モバイルデバイスに接続されているテザリング中のデバイスを検出して、区別できるようになりました。

トラフィック ポリシング

サブスクライバ単位のトラフィックポリシングを使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

トラフィックポリシングにより、ネットワーク上の帯域幅の使用状況を管理し、サブスクライバへの帯域幅の許容範囲を制限できます。

トラフィックポリシングにより、3GPP/3GPP2 サービスの特定のトラフィッククラスの個々のサブスクライバや APN の帯域幅制限を設定して適用できます。

帯域幅の適用は、ダウンリンクとアップリンクの方向で個別に設定および適用されます。

トークンバケットアルゴリズム（trTCM の修正版）[RFC2698] を使用して、トラフィックポリシング機能が導入されます。使用されるアルゴリズムは、パケットのマーキング方法を決定する際に、次の基準を測定します。

- **認定データレート（CDR）**：サンプリング間隔中の、サブスクライバに対してパケットを送信/受信できる保証レート（ビット/秒）。
- **ピークデータレート（PDR）**：サンプリング間隔中の、サブスクライバに対してサブスクライバパケットを送信/受信できる最大レート（ビット/秒）。
- **バーストサイズ**：認定（CBS）およびピーク（PBS）レート条件の両方について、サンプリング間隔中にサブスクライバに対して送受信できる最大バイト数。これは、サブスクライバの「バケット」に格納できるトークンの最大数を表します。認定バーストサイズ

（CBS）は、各サブスクライバのピークバーストサイズ（PBS）に等しいことに注意してください。

システムは、超過または違反と判断されたパケットに対して、次のいずれかのアクションを実行するように設定できます。

- **ドロップ**：問題のあるパケットは破棄されます。
- **送信**：問題のあるパケットは渡されます。
- **IP プレシデンスを引き下げる**：パケットの ToS ビットは「0」に設定されるため、パケットが渡される前にベストエフォートにダウングレードされます。パケットの ToS ビットがすでに「0」に設定されている場合、このアクションは「送信」と同等になることに注意してください。



重要 トラフィックポリシングの詳細については、このガイドの「トラフィックのポリシングとシェーピング」の章を参照してください。

トラフィック シェーピング

トラフィックシェーピングは、トラフィックポリシングと同様のレート制限方法ですが、設定された制限を超えるパケットに対してバッファ機構を提供します。パケットが data-rate を超過すると、パケットはバッファ内のキューに入れられ、後で配信されます。

帯域幅の適用は、ダウンリンクとアップリンクの方向で個別に実行できます。サブスクライバデータに使用できるバッファスペースがなくなった場合、パケットをドロップするか、次にスケジュールされているトラフィックセッション用に保持するかを、システムで設定できます。

トラフィックは設定された APN-AMBR 値にシェーピングされます。これまでは、GBR 以外のベアラーで伝送されるデータは、設定された APN-AMBR レートでポリシングされていました。APN-AMBR ポリシングにより、設定された APN-AMBR と一致しないデータがドロップされました。APN-AMBR トラフィックシェーピングでは、設定された APN-AMBR レートと一致しない GBR 以外のデータがバッファされます。十分なメモリトークンが使用可能になると、データが送信されます。さらに、通信事業者は、バッファ制限に達したときに、通信事業者がデータをドロップまたは送信することを可能にするオプションを使用できます。



重要 トラフィックシェーピングの詳細については、このガイドの「トラフィックのポリシングとシェーピング」の章を参照してください。

UBR 抑制機能

ベアラー更新要求（UBR）抑制機能は、ライセンス制御機能です。詳細については、シスコのアカウント担当者またはサービス担当者にお問い合わせください。

ビットレートは Gx では bps 単位、GTP では kbps 単位で表されるため、P-GW は、Gx 要求を GTP 要求に変換するための丸め処理を行います。P-GW が最小限のビットレート変更（bps 単位）で PCRF から RAR を受信すると、ベアラーに同じ QoS（Kbps 単位）がすでに設定されている場合でも、UBR が送信されます。UBR 抑制機能により、P-GW は、ベアラーのパラメータのいずれにも更新がない UBR を抑制できます。

UBR 抑制を有効にするために、新しい CLI コマンド **suppress-ubr no-bitrate-change** が P-GW サービス設定に追加されました。この CLI が設定されると、P-GW は、丸め処理の後もビットレートが同じである場合、UBR を抑制します。

UBR に複数のベアラーコンテキストがある場合、丸め処理の後のビットレート変更が 1 kbps 未満になるベアラーコンテキストが抑制されます。UBR をトリガーする可能性のある他のパラメータ（QCI、ARP、TFT など）が変更される場合、丸め処理の後もビットレートに変更がないときは、UBR は抑制されません。UBR 抑制は、CCA-I、RAR、およびベアラー変更コマンドによってトリガーされる UBR に適用されます。

要約すると、UBR 抑制のライセンスが有効になっており、CLI コマンド **suppress-ubr no-bitrate-change** が設定されている場合、丸め処理の後も kbps 単位のビットレートが同じであり、UBR をトリガーする可能性のある他のすべてのパラメータ（QCI、ARP、TFT など）も変更されていないときは、UBR が抑制されます。

ユーザーロケーション情報レポート

ユーザーロケーション情報（ULI）レポートを使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

ULI レポートにより、P-GW から要求されたときに、eNodeB が UE のロケーションを MME に報告できます。

MME と eNodeB 間のロケーションレポートを開始および停止するには、次の手順を、S1-MME インターフェイスを介して使用します。

- **ロケーションレポート制御**：ロケーションレポート制御手順の目的は、UE の現在のロケーションを報告することを MME が eNodeB に要求できるようにすることです。この手順では、UE 関連シグナリングを使用します。
- **ロケーションレポート失敗表示**：ロケーションレポート失敗表示手順は、ロケーションレポート制御手順が失敗したことを MME に通知するために、eNodeB によって開始されます。この手順では、UE 関連シグナリングを使用します。
- **ロケーションレポート**：ロケーションレポート手順の目的は、UE の現在のロケーションを MME に提供することです。この手順では、UE 関連シグナリングを使用します。

UE のロケーションレポートの開始/停止トリガーは、S-GW によって S11 インターフェイスを介して MME に報告されます。この目的のために、変更レポートアクション（CRA）情報要素（IE）が使用されます。MME は、ユーザーロケーション情報（ULI）IE を使用して S-GW へのロケーションを更新します。

MME と S-GW 間で CRA および ULI 情報を転送するために、次の S11 メッセージが使用されます。

- **セッション作成要求**：E-UTRAN 初期アタッチおよび UE 要求 PDN 接続手順用の URI IE が含まれます。これには ECGI と TAI が含まれます。P-GW がロケーション情報変更レポートを要求し、MME がロケーション情報変更レポートをサポートしている場合、MME には TAU/X2 ハンドオーバー手順用の ULI IE が含まれます。S-GW は、MME から ULI を受信すると、S5/S8 交換に ULI IE を含めます。MME が変更レポートをサポートしている場合は、対応する表示フラグがセッション作成要求メッセージに設定されます。
- **セッション作成応答**：S-GW は、必要なレポートのタイプを示すために、セッション作成応答メッセージに CRA IE を入力できます。
- **ベアラー作成要求**：MME のサブスクライバに対してロケーション変更レポートメカニズムを開始または停止する場合、CRA IE が、適切なアクションフィールドとともに含まれます。
- **ベアラー変更要求**：P-GW がロケーション情報変更レポートを要求し、MME がロケーション情報変更レポートをサポートしている場合、MME には TAU/ハンドオーバー手順および UE 開始サービス要求手順用の ULI IE が含まれます。S-GW は、MME から ULI を受信すると、S5/S8 交換にこの IE を含めます。
- **ベアラー変更応答**：MME のサブスクライバに対してロケーション変更レポートメカニズムを開始または停止する場合、CRA IE が、適切なアクションフィールドとともに含まれます。
- **セッション削除要求**：P-GW がロケーション情報変更レポートを要求し、MME がロケーション情報変更レポートをサポートしている場合、MME にはデタッチ手順用の ULI IE が含まれます。S-GW は、MME から ULI を受信すると、S5/S8 交換にこの IE を含めます。
- **ベアラー更新要求**：MME のサブスクライバに対してロケーション変更レポートメカニズムを開始または停止する場合、CRA IE が、適切なアクションフィールドとともに含まれます。
- **変更通知要求**：UE に対して既存の手順が実行されていない場合は、S1-AP ロケーションレポートメッセージの受信時に変更通知要求が送信されます。既存の手順が実行されている場合、次のいずれかのメッセージにより ULI が報告されます。
  - セッション作成要求
  - ベアラー作成応答
  - ベアラー変更要求
  - ベアラー更新応答
  - ベアラー削除応答
  - セッション削除要求

  既存の変更通知要求が保留中の場合は、中止され、新しい要求が送信されます。



重要 ユーザーロケーション情報（ULI）レポートサポートの設定については、『*MME Administration Guide*』の「*Mobility Management Entity Configuration*」の章にある「*Configuring Optional Features on the MME*」の項を参照してください。

3GPP ULI レポートのサポート拡張

この機能拡張は、3GPP 標準規格に従って P-GW および GGSN の ULI 関連のギャップをカバーします。

機能変更

この機能拡張は、3GPP 標準規格に従って P-GW および GGSN の ULI 関連のギャップをカバーします。

S4SGSN は、S-GW を介して P-GW に ULI を報告します。P-GW は、以前に受信した ULI を使用して ULI の変更を決定します。変更が検出され、同じ変更が PCRF によってイベントトリガーとして要求されている場合、ULI が PCRF に報告されます。

SGSN は GGSN に ULI を報告します。GGSN は、以前に受信した ULI を使用して ULI の変更を決定します。変更が検出され、同じ変更が PCRF によってイベントトリガーとして要求されている場合、ULI が PCRF に報告されます。GGSN で ULI フィールドの一部として受信した RAI における変更の検出のサポートも追加されています。

次の表は、P-GW が S4 SGSN と通信する PCRF から受信したイベントトリガーに基づく変更レポートアクション（CRA）の値をまとめたものです。

PCRF からのイベントトリガー	**S4 SGSN に送信される CRA**
USER_LOCATION_CHANGE（13）	Start Reporting CGI/SAI and RAI（5）
RAI_CHANGE（12）	Start Reporting RAI（2）
USER_LOCATION_CHANGE + RAI_CHANGE	Start Reporting CGI/SAI and RAI（5）

次の表は、GGSN が SGSN と通信する PCRF から受信したイベントトリガーに基づく MS 情報変更レポートアクションの値をまとめたものです。

PCRF からのイベントトリガー	**SGSN に対する MS 情報変更レポートアクション**
USER_LOCATION_CHANGE（13）	Start Reporting CGI/SAI（1）
RAI_CHANGE（12）	Start Reporting RAI（2）
BOTH（12,13）	Start Reporting CGI/SAI（1）

P-GW/GGSN は、イベントトリガーを受信すると、他のイベント（APN/AMBR の更新や QoS の更新など）を待つことなく、すぐに CRA/MS 情報変更レポートアクションを報告します。

動作の変更

以前の変更レポートアクション：次の表は、アクセスノードが S4SGSN である場合の、PCRF から受信したイベントトリガーに関する変更レポートアクションの以前の動作と新しい動作を示しています。

PCRF からのイベントトリガー	S4SGSN に送信される CRA	S4SGSN に送信される CRA
ULI_CHANGE（13）	6（START_REPORTING_TAI_ECGI）	5（START_REPORTING_CGI_RAI）
RAI_CHANGE（12）	CRA が送信されない	2（START_REPORTING_RAI）
BOTH（12,13）	6（START_REPORTING_TAI_ECGI）	5（START_REPORTING_CGI_RAI）

MS 情報変更レポートアクションの動作：次の表は、アクセスノードが SGSN である場合の、PCRF から受信したイベントトリガーに関する MS 情報 CRA の以前の動作と新しい動作を示しています。

PCRF からのイベントトリガー	SGSN に送信される CRA	SGSN に送信される CRA
ULI_CHANGE（13）	1（START_REPORTING_CGI/SAI）	1（START_REPORTING_CGI/SAI）
RAI_CHANGE（12）	CRA が送信されない	2（START_REPORTING_RAI）
BOTH（12,13）	1（START_REPORTING_CGI/SAI）	1（START_REPORTING_CGI/SAI）

制限事項

1. GGSN では、ネットワーク要求更新済み PDP コンテキスト（NRUPC）応答で新しい ULI を受信しても、それが PCRF に報告されません。
2. GGSN では、専用ベアラーが削除されるか、コールがドロップされると、URI の変更は検出されません。

PDN タイプ IPv4v6 での動作の設定

この機能強化により、P-GW および GGSN において、MME または SGSN がセッション作成要求または PDP 作成要求で PDN タイプを IPv4v6 に設定し、かつデュアルアドレスフラグ（DAF）を False に設定した場合に、次の 4 つのオプションを有効にする新しい CLI 設定が提供されました。

1. オプション 1：現在のメソッドを使用して IPv6 アドレスを割り当て、セッション作成応答、または成功と原因コード #19「単一のアドレスベアラーのみによる新しい PDN タイプ」を含む PDP 作成応答で応答します。

2. オプション 2：IPv4 アドレスを割り当て、セッション作成応答、または成功と原因コード #19「単一のアドレスベアラーのみによる新しい PDN タイプ」を含む PDP 作成応答で応答します。
3. オプション 3：IPv6 アドレスを割り当て、セッション作成応答、または成功と原因コード #18「ネットワーク設定による新しい PDN タイプ」を含む PDP 作成応答で応答します。
4. オプション 4：IPv4 アドレスを割り当て、セッション作成応答、または成功と原因コード #18「ネットワーク設定による新しい PDN タイプ」を含む PDP 作成応答で応答します。

CLI が設定されていない場合、デフォルトの動作はオプション 1 です。ゲートウェイでは、同じ APN に対して複数の PDN 接続をサポートし、オプション 1、オプション 2、および 2 番目の PDN 接続を試みる UE の処理を実行します。APN ごとに異なる CLI を設定できます。

以前は、P-GW および GGSN で DAF False の IPv4v6 PDN に対してセッション作成要求または CPC を受信すると、割り当てられた PDN タイプに対するサポートは設定できず、セッション作成要求または PDP 作成要求で原因コードが返されていました。

PDN ゲートウェイの機能

ここでは、EPC E-UTRAN ネットワークにおける P-GW の機能について説明し、また、セッションのセットアップと切断のさまざまな段階におけるコール手順フローを示します。

P-GW は、次のネットワークフローをサポートします。

- eHRPD ネットワークにおける PMIPv6 PDN ゲートウェイコール/セッションプロシージャ
- LTE-SAE ネットワークにおける GTP PDN ゲートウェイコール/セッションプロシージャ

eHRPD ネットワークにおける PMIPv6 PDN ゲートウェイコール/セッションプロシージャ

この項では次のトピックについて説明します。

- IPv6/IPv4 アクセスによる初期アタッチ （115 ページ）
- ハンドオーバーなしの PMIPv6 ライフタイム延長 （117 ページ）
- UE によって開始される PDN 接続解除 （118 ページ）
- HSGW によって開始される PDN 接続解除 （119 ページ）
- P-GW によって開始される PDN 接続解除 （120 ページ）

IPv6/IPv4 アクセスによる初期アタッチ

このセクションでは、サブスクライバ（UE）の初期アタッチとセッション確立の手順について説明します。

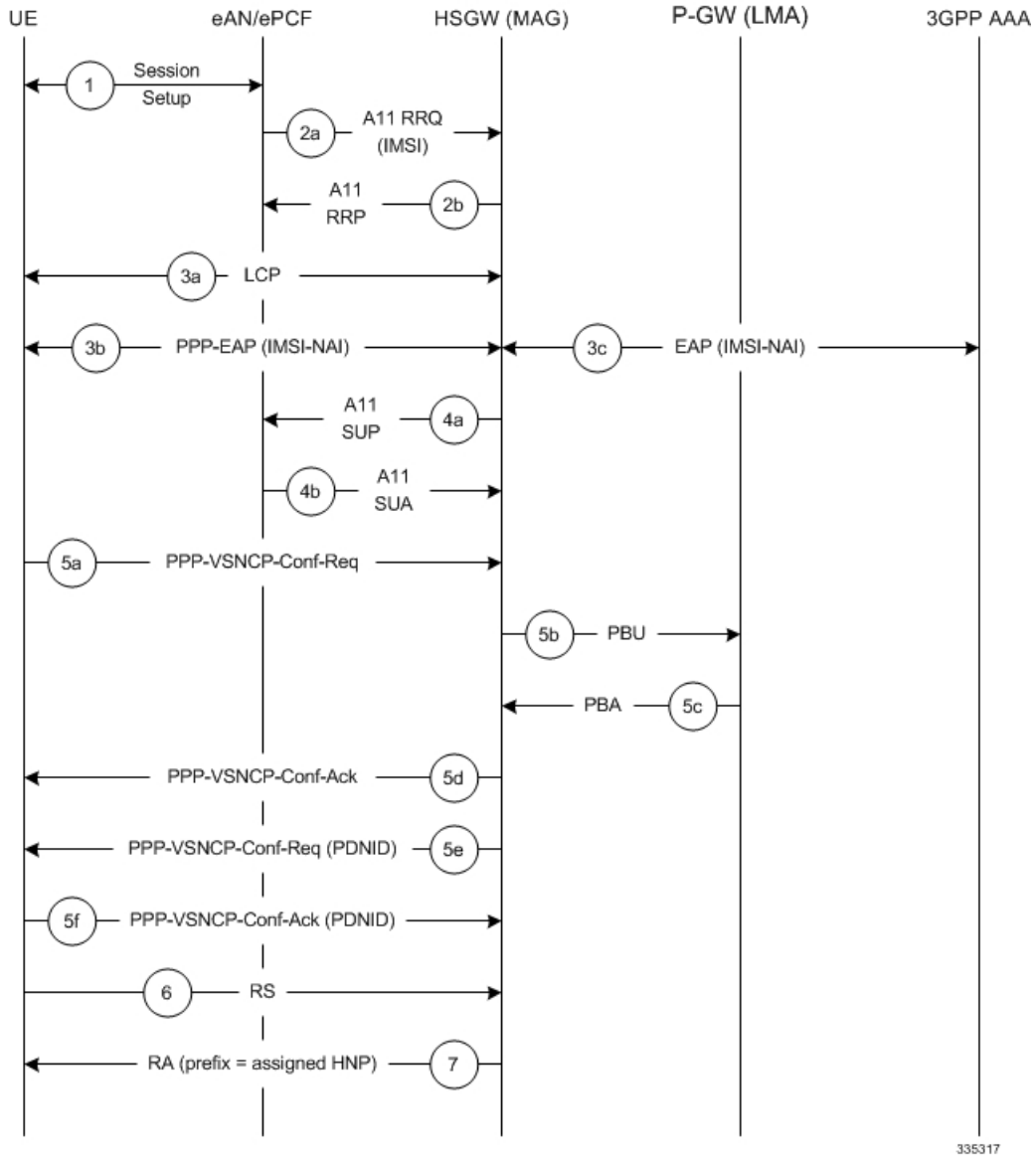


表 *7: IPv6/IPv4* アクセスコールフローによる初期アタッチの説明

ステップ	説明
1	サブスクライバ（UE）は eHRPD ネットワークにアタッチします。
2a	eAN/PCF は A11 RRQ を HSGW に送信します。eAN/PCF には、A11 RRQ 内に UE の実際の IMSI が含まれます。
2b	HSGW は A10 を確立し、A11 RRP で eAN/PCF に応答します。
3a	UE は、確立されたメイン A10 を介して HSGW との LCP ネゴシエーションを実行します。
3b	UE は EAP over PPP を実行します。

ステップ	説明
3c	UE と 3GPP AAA の間で EAP 認証が完了します。このトランザクション中に、HSGW は、AA サーバーからサブスクライバプロファイルを受信します。
4a	サブスクライバプロファイルを受信した後、HSGW は、A11 セッション更新メッセージで Qo プロファイルを eAN/PCF に送信します。
4b	eAN/PCF は、A11 セッション更新確認応答（SUA）で応答します。
5a	UE は、PPP-VSNCP-Conf-Req メッセージを HSGW に送信して、PDN 接続を開始します。この メッセージには、PDN の PDNID、APN、PDN-Type=IPv6/[IPv4]、PDSN アドレス、およびオプ ションで、UE がネットワークから受け取ることを想定している PCO オプションが含まれます
5b	HSGW は PBU を P-GW に送信します。
5c	P-GW は HSGW からの PBU を処理し、接続に HNP を割り当て、PBA で HSGW に応答します
5d	HSGW は、VSNCP 設定要求に対して VSNCP 設定確認応答で応答します。
5e	HSGW は、UE に PPP-VSNCP-Conf-Req を送信し、PPP VSNCP ネゴシエーションを完了します
5f	UE は、PPP-VSNCP-Conf-Ack を返すことで VSNCP ネゴシエーションを完了します。
6	UE は、オプションでルータ送信要求（RS）メッセージを送信します。
7	HSGW は、割り当てられたプレフィックスを使用してルータアドバタイズメント（RA）メッセ ージを送信します。

ハンドオーバーなしの PMIPv6 ライフタイム延長

ここでは、ハンドオーバーを発生させずに、P-GW によりセッション登録のライフタイムを延長する手順について説明します。

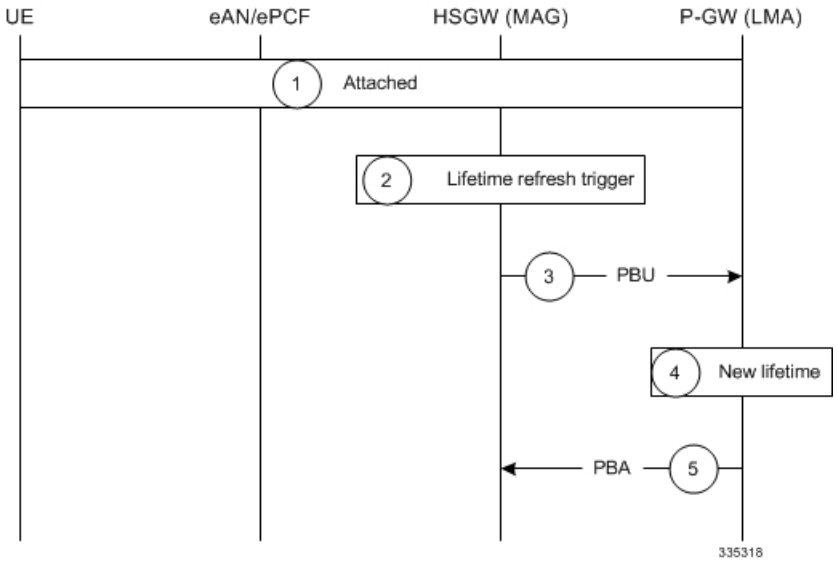


表 *8 : PMIPv6* ライフタイム延長（ハンドオーバーなし）コールフローの説明

ステップ	説明
1	UE が EPC に接続されており、割り当てられた HNP によって PDNID=x および APN の P-GW との PDN 接続が確立されています。
2	HSGW MAG サービス登録の有効期限が近づくと、LMA の更新要求がトリガーされます。
3	MAG サービスは、ライフタイム、MNID、APN、ATT=HRPD、HNP の各属性を使用して、P-GW LMA サービスにプロキシ バインディング アップデート（PBU）を送信します。
4	P-GW LMA サービスは、新しく付与されたライフタイムでバインディング キャッシュ エントリ（BCE）を更新します。
5	P-GW は Lifetime、MNID、APN の属性を持つプロキシ バインディング確認（PBA）で応答します。

UE によって開始される PDN 接続解除

このセクションでは、UE によるセッション解除の手順について説明します。

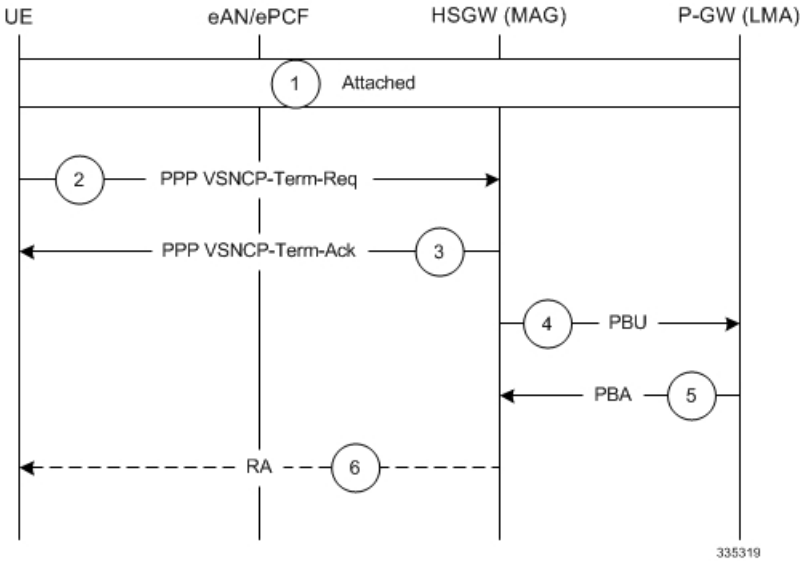


表 *9 : UE* コールフローによる *PDN* 接続解除の説明

ステップ	説明
1	UE が EPC に接続されており、割り当てられた HNP によって PDN-ID=x および APN の P-GW との PDN 接続が確立されています。
2	UE は PDN からの切断を決定し、PDNID=x で PPP VSNCP-Term-Req を送信します。

ステップ	説明
3	HSGW は PDN 接続の切断を開始し、PPP-VSNCP-Term-Ack を UE に（PDNID=x で）送信します。
4	HSGW は PMIP セッションの切断を開始するために、Lifetime=0、MNID、APN、ATT=HRPD、HNP の各属性を指定した PBU 登録解除を P-GW に送信します。PBU 登録解除メッセージにはバインドを作成した初期 PBU に存在していたすべてのモビリティオプションが含まれている要があります。
5	P-GW は HNP に基づいてバインディング キャッシュ エントリ（BCE）を検索し、バインドを除して、同じ属性（Lifetime=0、MNID、APN、ATT=HRPD、HNP）を指定した登録解除 PBA HSGW に応答します。
6	HSGW は、割り当てられた HNP とプレフィックス lifetime=0 を指定したルータアドバタイズント（RA）を必要に応じて送信します。

HSGW によって開始される PDN 接続解除

ここでは、HSGW によるセッション解除の手順について説明します。

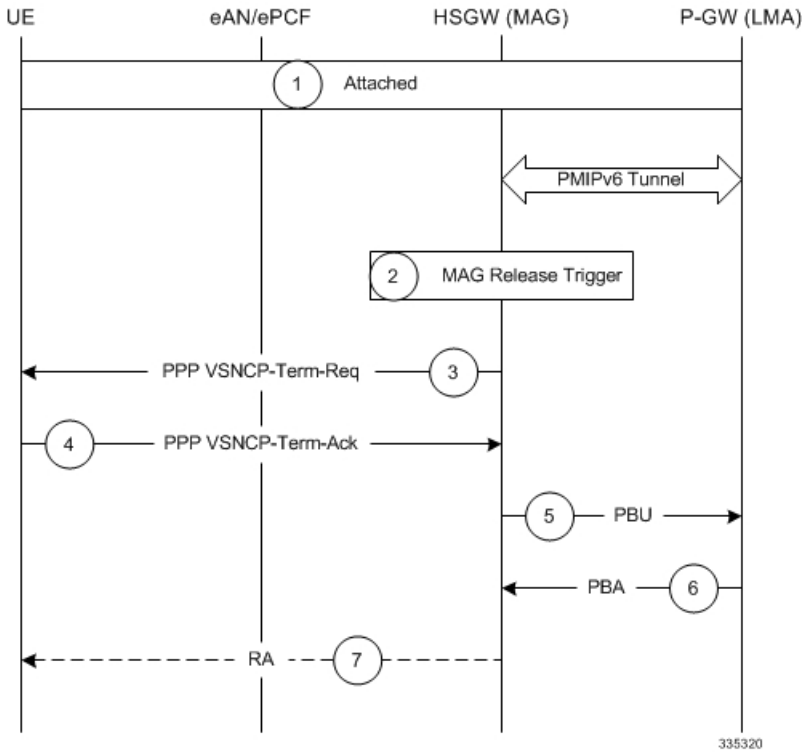


表 *10 : HSGW* コールフローによる *PDN* 接続解除の説明

ステップ	説明
1	UE が EPC に接続されており、割り当てられた HNP によって PDN-ID=x および APN の P-GW との PDN 接続が確立されています。
2	HSGW MAG サービスにより、PDNID=x の PDN 接続の切断がトリガーされます。
3	HSGW は PDNID=x を指定した PPP VSNCP-Term-Req を UE に送信します。
4	UE は VSNCP-Term-Ack（PDNID=x）で要求受信の確認応答を返します。
5	HSGW は PMIP セッションの切断を開始するために、Lifetime=0、MNID、APN、HNP の各属性を指定した PBU 登録解除を P-GW に送信します。PBU 登録解除メッセージには、バインドを作成した初期 PBU に存在していたすべてのモビリティオプションが含まれている必要があります。
6	P-GW は HNP に基づいて BCE を検索し、バインドを削除して、同じ属性（Lifetime=0、MNID、APN、ATT=HRPD、HNP）を指定した登録解除 PBA で HSGW に応答します。
7	HSGW は、割り当てられた HNP とプレフィックス lifetime=0 を指定したルータアドバタイズメント（RA）を必要に応じて送信します。

P-GW によって開始される PDN 接続解除

このセクションでは、P-GW によるセッション解除の手順について説明します。

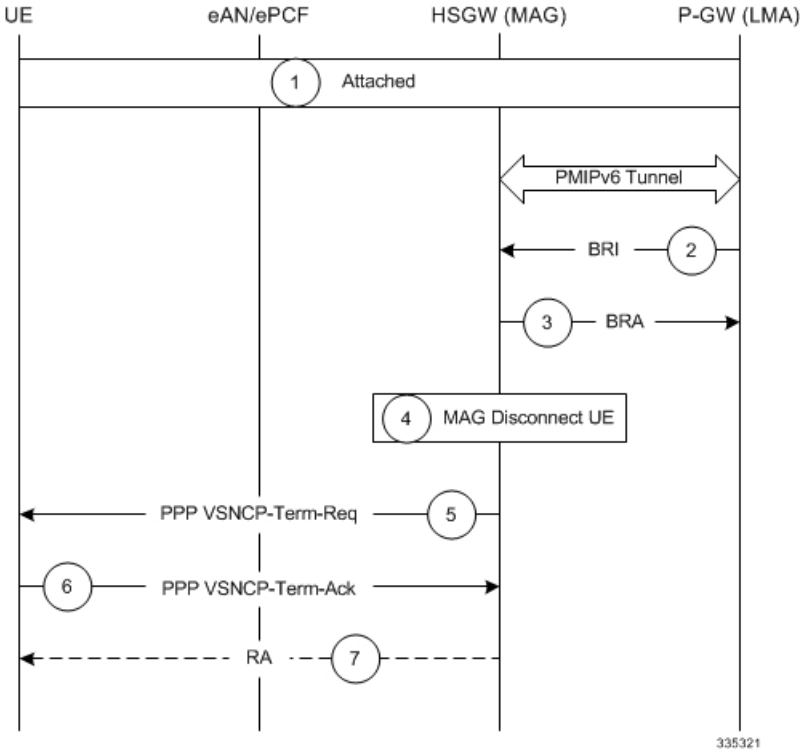


表 *11 : P-GW* コールフローによる *PDN* 接続解除の説明

ステップ	説明
1	UE が EPC に接続されており、割り当てられた HNP によって PDN-ID=x および APN の P-GW の PDN 接続が確立されています。
2	P-GW トリガーにより PDNID=x の PDN 接続が切断され、P-GW は、MNID、APN、HNP の各性を含むバインド失効通知（BRI）メッセージを HSGW に送信します。
3	HSGW は、同じ属性（MNID、APN、HNP）を含むバインド失効確認応答（BRA）メッセージBRI メッセージに応答します。
4	HSGW MAG サービスにより、PDNID=x の UE PDN 接続の切断がトリガーされます。
5	HSGW は PDNID=x を指定した PPP VSNCP-Term-Req を UE に送信します。
6	UE は VSNCP-Term-Ack（PDNID=x）で要求受信の確認応答を返します。
7	HSGW は、割り当てられた HNP とプレフィックス lifetime=0 を指定したルータアドバタイズント（RA）を必要に応じて送信します。

LTE-SAE ネットワークにおける GTP PDN ゲートウェイコール/セッションプロシージャ

この項では次のトピックについて説明します。

- サブスクライバ開始アタッチ（初回） （121 ページ）
- サブスクライバ開始デタッチ （125 ページ）

サブスクライバ開始アタッチ（初回）

このセクションでは、サブスクライバによる EPC ネットワークへの初回アタッチの手順について説明します。

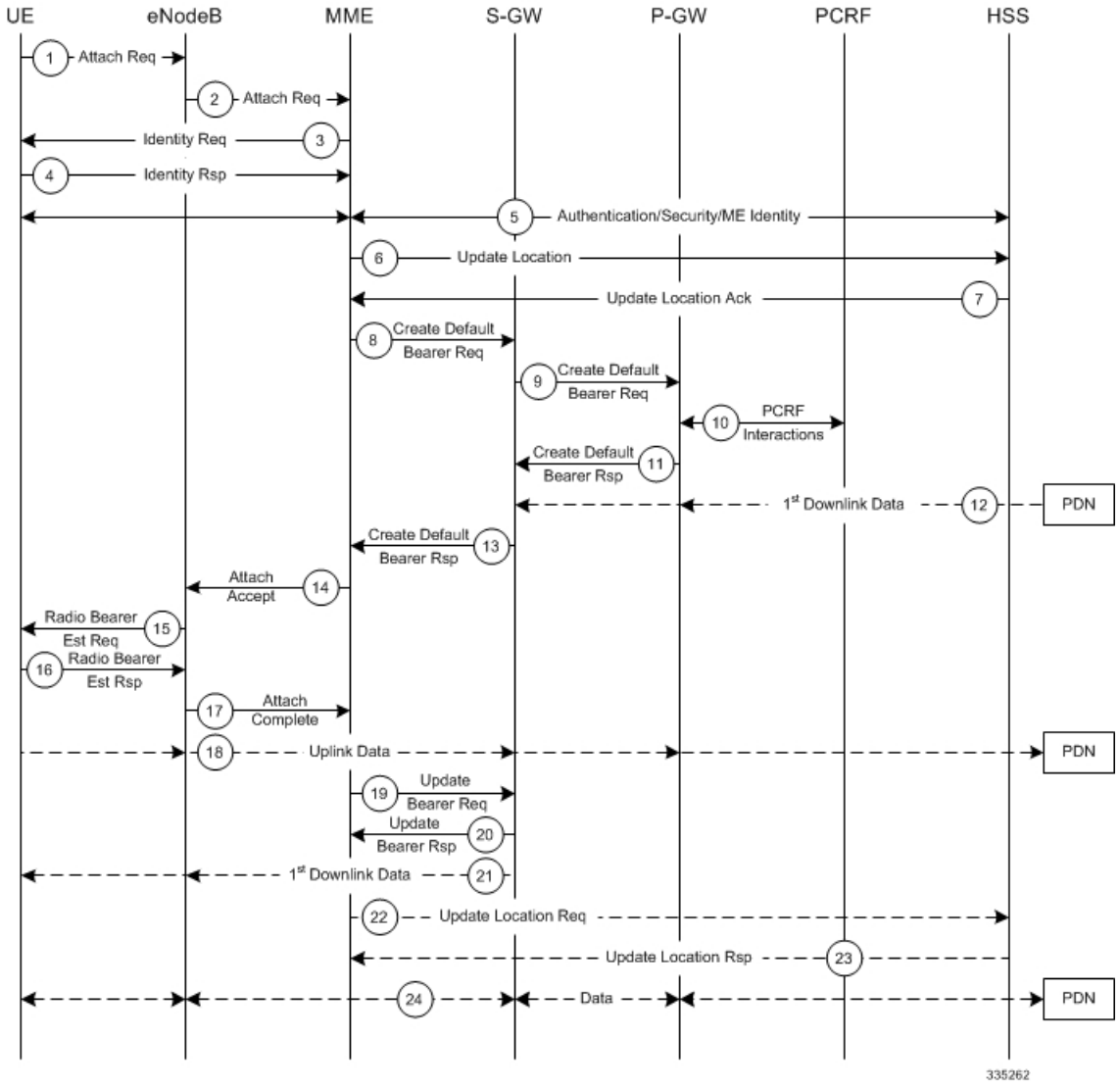


表 *12 :* サブスクライバ開始アタッチ（初回）コールフローの説明

ステップ	説明
1	UE は、アタッチ要求（IMSI または古い GUTI、最終アクセス TAI（使用可能な場合）、UE ネットワーク機能、PDN アドレス割り当て、プロトコル設定オプション、アタッチタイプ）メッセージを、eNodeB に対して選択されたネットワークの表示とともに送信することにより、アタッチ手順を開始します。UE に有効な GUTI がない場合は、IMSI が含められます。UE に有効な GUTI がある場合は、GUTI が含められます。

ステップ	説明
2	eNodeB は、GUTI および指定された選択済みネットワークから MME を取得します。その MM が eNodeB と関連付けられていない場合、eNodeB は「MME 選択機能」を使用して MME を選します。eNodeB は、S1-MME 制御メッセージ（初期 UE メッセージ）に含まれているアタッ要求メッセージを新しい MME に転送します。同時に、選択されたネットワークと、（新しい MME へのアタッチ要求メッセージが受信される）セルのグローバルに一意の E-UTRAN ID で る E-UTRAN エリアアイデンティティについての指示も転送します。
3	MME で UE が不明の場合、MME はアイデンティティ要求を UE に送信して、IMSI を要求し す。
4	UE は、アイデンティティ応答（IMSI）で応答します。
5	UE の UE コンテキストがネットワーク内のどこにも存在しない場合、認証は必須です。存在 る場合、この手順は任意です。ただし、少なくとも完全性チェックが開始され、初回アタッチ に ME アイデンティティが UE から取得されます。認証機能（この手順を実行した場合）には AKA 認証と、NAS プロトコルメッセージをさらに保護するための UE との NAS レベルのセキ リティ アソシエーションの確立が含まれます。
6	MME は、更新ロケーション（MME アイデンティティ、IMSI、ME アイデンティティ）を HS に送信します。
7	HSS は、更新ロケーション ACK を MME に送信することにより、更新ロケーションメッセー を確認応答します。このメッセージには、サブスクライバデータ（IMSI、サブスクリプショ データ）挿入要求も含まれています。サブスクリプションデータには、UE がアクセス権限を つすべての APN のリスト、それらの APN のうちどれがデフォルト APN かを示す表示、およ 許可された各 APN の「EPS サブスクライブ QoS プロファイル」が含まれます。更新ロケーシ ンが HSS によって拒否された場合、MME は該当する理由で UE からの接続要求を拒否します
8	MME が「サービング GW 選択機能」を使用して S-GW を選択し、UE に関連付けられたデフ ルトのベアラーに EPS ベアラーアイデンティティを割り当てます。PDN サブスクリプション ンテキストに P-GW アドレスが含まれていない場合、MME は「PDN GW 選択機能」の項で説 されているとおり、P-GW を選択します。次に、デフォルトベアラー作成要求（IMSI、MME ンテキスト ID、APN、RAT タイプ、デフォルトベアラー QoS、PDN アドレス割り当て、AMBR EPS ベアラーアイデンティティ、プロトコル設定オプション、ME アイデンティティ、ユーザ ロケーション情報）メッセージを選択された S-GW に送信します。
9	S-GW は EPS ベアラーテーブルに新しいエントリを作成し、デフォルトベアラー作成要求（IMSI APN、ユーザープレーンの S-GW アドレス、ユーザープレーンの S-GW TEID、コントロール レーンの S-GW TEID、RAT タイプ、デフォルトベアラー QoS、PDN アドレス割り当て、AMBR EPS ベアラーアイデンティティ、プロトコル設定オプション、ME アイデンティティ、ユーザ ロケーション情報）メッセージを P-GW に送信します。
10	ダイナミック PCC が展開される場合、P-GW は PCRF と対話して UE のデフォルト PCC ルー を取得します。IMSI、UE IP アドレス、ユーザーロケーション情報、RAT タイプ、AMBR は、 前のメッセージによって受信された場合、P-GW から PCRF に提供されます。

ステップ	説明
11	P-GW は、デフォルトベアラー作成応答（ユーザープレーンの P-GW アドレス、ユーザープレーンの P-GW TEID、コントロールプレーンの P-GW TEID、PDN アドレス情報、EPS ベアラーアイデンティティ、プロトコル設定オプション）メッセージを S-GW に返します。P-GW が、デフォルトベアラー作成要求で受信した PDN アドレス割り当てに基づいて PDN アドレスを割り当てた場合、PDN アドレス情報が含められます。PDN アドレス情報には、IPv4 用の IPv4 アドレスや、IPv6 用の IPv6 プレフィックスとインターフェイス識別子が含まれます。P-GW は、PDN アドレス割り当てで示された UE IP バージョン機能と、P-GW が PDN アドレス情報を割り当てる場合のオペレータのポリシーを判断に含めます。アタッチ手順の完了後に IP アドレスが UE によってネゴシエートされるかどうかは、デフォルトベアラー作成応答に示されます。
12	ダウンリンク（DL）データによって、S-GW へのフローを開始できます。S-GW はデータをバッファリングします。
13	S-GW は、デフォルトベアラー作成応答（PDN アドレス情報、ユーザープレーンの S-GW アドレス、ユーザープレーンの S-GW TEID、S-GW コンテキスト ID、EPS ベアラーアイデンティティ、プロトコル設定オプション）メッセージを新しい MME に返します。P-GW によって提供された場合は、PDN アドレス情報が含まれます。
14	新しい MME は、アタッチ承認（APN、GUTI、PDN アドレス情報、TAI リスト、EPS ベアラーアイデンティティ、セッション管理設定 IE、プロトコル設定オプション）メッセージを eNodeB に送信します。
15	eNodeB は、EPS 無線ベアラーアイデンティティを含む無線ベアラー確立要求を UE に送信します。ベアラー承認メッセージも UE に送信されます。
16	UE は、無線ベアラー確立応答を eNodeB に送信します。このメッセージには、アタッチ完了メッセージ（EPS ベアラーアイデンティティ）が含まれています。
17	eNodeB は、アタッチ完了（EPS ベアラーアイデンティティ）メッセージを MME に転送します。
18	アタッチが完了し、UE がデフォルトのベアラーを介してデータを送信します。この時点で、UE はアップリンクパケットを eNodeB に送信できます。その後 S-GW と P-GW にトンネリングされます。
19	MME は、ベアラー更新要求（eNodeB アドレス、eNodeB TEID）メッセージを S-GW に送信します。
20	S-GW は、ベアラー更新応答（EPS ベアラーアイデンティティ）メッセージを MME に送信して確認応答します。
21	S-GW は、バッファリングされたダウンリンクパケットを送信します。
22	MME がベアラー更新応答（EPS ベアラーアイデンティティ）メッセージを受信した後、EPS ベアラーが確立され、ユーザーが非 3GPP アクセスへのハンドオーバーを実行できることをサブスクリプションデータが示しており、MME が PDN サブスクリプションのコンテキストで HSS によって示された P-GW アドレスと異なる P-GW を選択した場合、MME は、非 3GPP アクセスによるモビリティのために、APN および P-GW アドレスを含むロケーション更新要求を HSS に送信します。

ステップ	説明
23	HSS は、APN と P-GW アドレスのペアを保存し、ロケーション更新応答を MME に送信します
24	双方向データが UE と PDN の間でやり取りされます。

サブスクライバ開始デタッチ

ここでは、サブスクライバによる EPC ネットワークからのデタッチ手順について説明します。

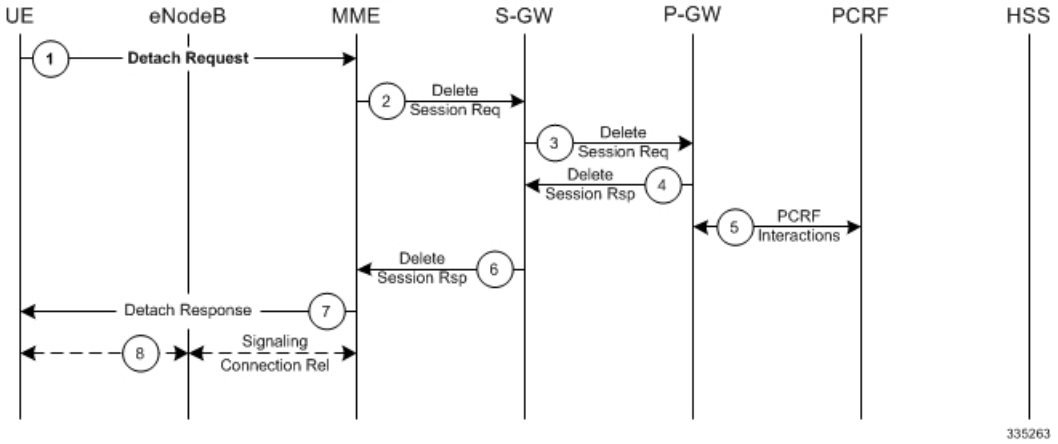


表 *13 :* サブスクライバ開始デタッチコールフローの説明

ステップ	説明
1	UE が、NAS メッセージのデタッチ要求（GUTI、Switch Off）を MME に送信します。Switch C は、デタッチの原因がスイッチオフの状況かどうかを示します。
2	この特定の UE に関する S-GW のアクティブな EPS ベアラーが、MME がベアラー削除要求（TEID）メッセージを S-GW に送信することによって非アクティブ化されます。
3	S-GW が、ベアラー削除要求（TEID）メッセージを P-GW に送信します。
4	P-GW は、ベアラー削除応答（TEID）メッセージで確認応答します。
5	PCRF がネットワークに適用されている場合、P-GW は PCRF と通信して、EPS ベアラーが解 されたことを PCRF に通知できます。
6	S-GW は、ベアラー削除応答（TEID）メッセージで確認応答します。
7	Switch Off で、デタッチがスイッチオフ状況によるものではないことが示されている場合、MM はデタッチ承諾メッセージを UE に送信します。
8	MME は、Cause = Detach で S1 Release コマンドを eNodeB に送信して、UE の S1-MME シグナ ング接続を解放します。

サポートされる標準

P-GW は、次の標準規格に準拠しています。

- リリース 12 3GPP の参考資料 （126 ページ）
- リリース 11 3GPP の参考資料 （126 ページ）
- リリース 10 3GPP の参考資料 （127 ページ）
- リリース 9 3GPP の参考資料 （127 ページ）
- リリース 8 3GPP の参考資料 （129 ページ）
- 3GPP2 の参考資料 （130 ページ）
- IETF リファレンス （130 ページ）
- オブジェクト管理グループ（OMG）の標準規格 （132 ページ）

リリース 12 3GPP の参考資料

重要 P-GW は現在、次のリリースの 12 3GPP 仕様に準拠しています。3GPP 仕様の大部分が 3GPP2 にも使用されています。3GPP2 に固有の仕様は、「*3GPP2* の参考資料」に記載されています。

- 3GPP TS 23.007：Restoration procedures
- 3GPP TS 23.401：General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402：Architecture enhancements for non-3GPP accesses
- 3GPP TS 29.060：General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.274：3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281：General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)

リリース 11 3GPP の参考資料

重要 P-GW は現在、次のリリースの 11 3GPP 仕様に準拠しています。3GPP 仕様の大部分が 3GPP2 にも使用されています。3GPP2 に固有の仕様は、「*3GPP2* の参考資料」に記載されています。

- 3GPP TS 23.007：Restoration procedures
- 3GPP TS 29.274：3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)

- 3GPP TS 23.401：General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402：Architecture enhancements for non-3GPP accesses
- 3GPP TS 29.060：General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.274：3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.281：General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)

リリース 10 3GPP の参考資料



重要 P-GW は現在、次のリリースの 10 3GPP 仕様に準拠しています。3GPP 仕様の大部分が 3GPP2 にも使用されています。3GPP2 に固有の仕様は、「*3GPP2* の参考資料」に記載されています。

- 3GPP TS 23.007：Restoration procedures
- 3GPP TS 23.203：Policy and charging control architecture; Stage 2
- 3GPP TS 23.401：General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402：Architecture enhancements for non-3GPP accesses
- 3GPP TS 29.212：Policy and Charging Control over Gx reference point
- 3GPP TS 29.274：3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP TS 29.281：GPRS Tunnelling Protocol User Plane (GTPv1-U)

リリース 9 3GPP の参考資料



重要 P-GW は現在、次のリリースの 9 3GPP 仕様に準拠しています。3GPP 仕様の大部分が 3GPP2 にも使用されています。3GPP2 に固有の仕様は、「*3GPP2* の参考資料」に記載されています。

- 3GPP TR 21.905：Vocabulary for 3GPP Specifications
- 3GPP TS 22.115：Service aspects; Charging and billing
- 3GPP TS 23.003：Numbering, addressing and identification
- 3GPP TS 23.007：Restoration procedures

- 3GPP TS 23.060：General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.203：Policy and charging control architecture
- 3GPP TS 23.207：End-to-end Quality of Service (QoS) concept and architecture
- 3GPP TS 23.216：Single Radio Voice Call Continuity (SRVCC); Stage 2
- 3GPP TS 23.228：IP Multimedia Subsystem (IMS); Stage 2
- 3GPP TS 23.401：General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402：Architecture enhancements for non-3GPP accesses
- 3GPP TS 24.008：Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 29.060：General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.061：Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP TS 29.212：Policy and Charging Control over Gx reference point
- 3GPP TS 29.214：Policy and Charging control over Rx reference point
- 3GPP TS 29.229：Cx and Dx interfaces based on Diameter protocol
- 3GPP TS 29.230：Diameter applications; 3GPP specific codes and identifiers
- 3GPP TS 29.272：Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
- 3GPP TS 29.273：3GPP EPS AAA Interfaces
- 3GPP TS 29.274：3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 29.275：Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3
- 3GPP TS 29.281：General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 29.282：Mobile IPv6 vendor specific option format and usage within 3GPP
- 3GPP TS 32.240：Telecommunication management; Charging management; Charging architecture and principles
- 3GPP TS 32.251：Telecommunication management; Charging management; Packet Switched (PS) domain charging
- 3GPP TS 32.298：Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP TS 32.299：Telecommunication management; Charging management; Diameter charging application

リリース 8 3GPP の参考資料



重要 P-GW は現在、次のリリース 8 3GPP 仕様に準拠しています。3GPP 仕様の大部分が 3GPP2 にも使用されています。3GPP2 に固有の仕様は、「*3GPP2* の参考資料」に記載されています。

- 3GPP TR 21.905：Vocabulary for 3GPP Specifications
- 3GPP TS 23.003：Numbering, addressing and identification
- 3GPP TS 23.007：Restoration procedures
- 3GPP TS 23.060：General Packet Radio Service (GPRS); Service description; Stage 2
- 3GPP TS 23.107：Quality of Service (QoS) concept and architecture
- 3GPP TS 23.203：Policy and charging control architecture
- 3GPP TS 23.401：General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP TS 23.402：Architecture enhancements for non-3GPP accesses
- 3GPP TS 23.869：Support for Internet Protocol (IP) based IP Multimedia Subsystem (IMS) Emergency calls over General Packet Radio Service (GPRS) and Evolved Packet Service (EPS)
- 3GPP TS 24.008：Mobile radio interface Layer 3 specification; Core network protocols
- 3GPP TS 24.229：IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3
- 3GPP TS 27.060：Mobile Station (MS) supporting Packet Switched Services
- 3GPP TS 29.061：Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP TS 29.210：Charging rule provisioning over Gx interface
- 3GPP TS 29.212：Policy and Charging Control over Gx reference point
- 3GPP TS 29.213：Policy and Charging Control signaling flows and QoS
- 3GPP TS 29.273：3GPP EPS AAA Interfaces
- 3GPP TS 29.274：Evolved GPRS Tunnelling Protocol for Control plane (GTPv2-C)
- 3GPP TS 29.275：Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols
- 3GPP TS 29.281：GPRS Tunnelling Protocol User Plane (GTPv1-U)
- 3GPP TS 29.282：Mobile IPv6 vendor specific option format and usage within 3GPP
- 3GPP TS 32.295：Charging management; Charging Data Record (CDR) transfer
- 3GPP TS 32.298：Telecommunication management; Charging management; Charging Data Record (CDR) encoding rules description

- 3GPP TS 32.299：Charging management; Diameter charging applications
- 3GPP TS 36.300：EUTRA and EUTRAN; Overall description Stage 2
- 3GPP TS 36.412：EUTRAN S1 signaling transport
- 3GPP TS 36.413：EUTRAN S1 Application Protocol (S1AP)

3GPP2 の参考資料

- X.S0057-0 v3.0 の『E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects』

IETF リファレンス

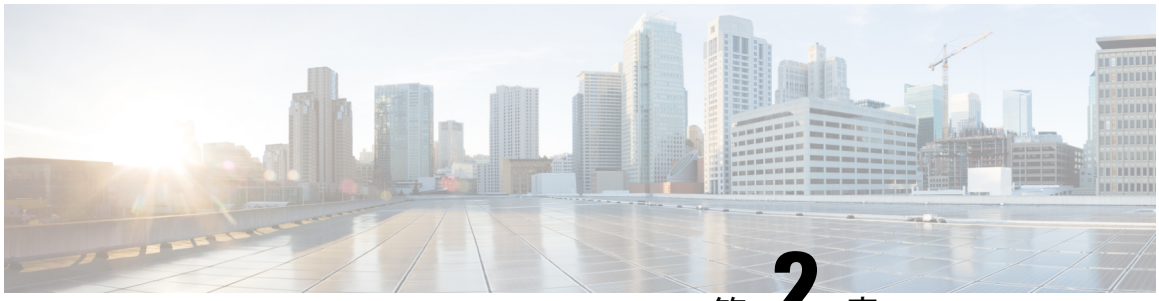
- RFC 768：User Datagram Protocol (STD 6)
- RFC 791：Internet Protocol (STD 5)
- RFC 1701：Generic Routing Encapsulation (GRE)
- RFC 1702：Generic Routing Encapsulation over IPv4 networks
- RFC 2131：Dynamic Host Configuration Protocol
- RFC 2460：Internet Protocol, Version 6 (IPv6) Specification
- RFC 2473：Generic Packet Tunneling in IPv6 Specification
- RFC 2698：A Two Rate Three Color Marker
- RFC 2784：Generic Routing Encapsulation (GRE)
- RFC 2890：Key and Sequence Number Extensions to GRE
- RFC 3162：RADIUS and IPv6
- RFC 3266：Support for IPv6 in Session Description Protocol (SDP)
- RFC 3319：Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
- RFC 3588：Diameter Base Protocol
- RFC 3589：Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5
- RFC 3602：The AES-CBC Cipher Algorithm and Its Use with IPSec
- RFC 3646：DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3715：IPSec-Network Address Translation (NAT) Compatibility Requirements
- RFC 3748：Extensible Authentication Protocol (EAP)

- RFC 3775：Mobility Support in IPv6
- RFC 3948：UDP Encapsulation of IPSec ESP Packets
- RFC 4004：Diameter Mobile IPv4 Application
- RFC 4005：Diameter Network Access Server Application
- RFC 4006：Diameter Credit-Control Application
- RFC 4187：Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
- RFC 4282：The Network Access Identifier
- RFC 4283：Mobile Node Identifier Option for Mobile IPv6 (MIPv6)
- RFC 4303：IP Encapsulating Security Payload (ESP)
- RFC 4306：Internet Key Exchange Protocol Version 2
- RFC 4739：Multiple Authentication Exchange in IKEv2 protocol
- RFC 4861：Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4862：IPv6 Stateless Address Autoconfiguration
- RFC 5094：Mobile IPv6 Vendor Specific Option
- RFC 5149：Service Selection for Mobile IPv6
- RFC 5213：Proxy Mobile IPv6
- RFC 5447：Diameter Mobile IPv6: Support for NAS to Diameter Server Interaction
- RFC 5555：Mobile IPv6 Support for Dual Stack Hosts and Routers
- RFC 5844：IPv4 Support for Proxy Mobile IPv6
- RFC 5845：Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- RFC 5846：Binding Revocation for IPv6 Mobility
- RFC 5996：Internet Key Exchange Protocol Version 2 (IKEv2)
- インターネットドラフト（draft-ietf-dime-qos-attributes-07）：QoS Attributes for Diameter
- インターネットドラフト（draft-ietf-mip6-nemo-v4traversal-06.txt）：Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)
- インターネットドラフト（draft-ietf-netlmm-grekey-option-01.txt）：GRE Key Option for Proxy Mobile IPv6, work in progress
- インターネットドラフト（draft-ietf-netlmm-pmip6-ipv4-support-02.txt）：IPv4 Support for Proxy Mobile IPv6
- インターネットドラフト（draft-ietf-netlmm-proxymip6-07.txt）：Proxy Mobile IPv6

- インターネットドラフト（draft-ietf-mext-binding-revocation-02.txt）：Binding Revocation for IPv6 Mobility, work in progress
- インターネットドラフト（draft-meghana-netlmm-pmipv6-mipv4-00.txt）：Proxy Mobile IPv6 and Mobile IPv4 interworking

オブジェクト管理グループ（OMG）の標準規格

- CORBA 2.6 Specification 01-09-35, Object Management Group



第 2 章

PDN ゲートウェイの設定

この章では、PDN ゲートウェイ（P-GW）の設定について説明します。

重要 この章にあるすべてのコマンドの情報は、『*Command Line Interface Reference*』で確認できます。

各ワイヤレスネットワークはそれぞれ異なるため、システムは、さまざまなワイヤレスネットワーク環境で動作できるように、さまざまなパラメータを使用して設計されます。この章では、システムを動作させるための最小限のパラメータセットのみを示します。P-GW 製品に固有のオプションの設定コマンドは、『*Command Line Interface Reference*』に記載されています。

この章では、次の手順について説明します。

- スタンドアロン eGTP P-GW としてのシステムの設定 （133 ページ）
- LTE-SAE ネットワークでのスタンドアロン PMIP P-GW としてのシステムの設定 （162 ページ）
- eHRPD ネットワークをサポートするスタンドアロン PMIP P-GW としてのシステムの設定 （182 ページ）
- P-GW でのオプション機能の設定 （203 ページ）

スタンドアロン eGTP P-GW としてのシステムの設定

この項では、テスト環境で eGTP P-GW として実行するようにシステムを設定するための一連の手順の概要と、関連する構成ファイルの例を示します。構成ファイルの完全な例については、付録「サンプル構成ファイル」を参照してください。ここでは次の内容について説明します。

- 必要な情報 （134 ページ）
- この設定が動作する仕組み （141 ページ）
- eGTP P-GW 設定 （143 ページ）

必要な情報

以降のセクションでは、P-GW を設定し、ネットワーク上で動作させるために必要な最小限の情報について説明します。プロセスをより効率的なものにするため、システムを設定する前にこの情報を用意しておくことを推奨します。

ここでは説明していないその他の設定パラメータがあります。これらのパラメータは、主にネットワークでの P-GW の動作の微調整に対応します。これらのパラメータの詳細については、『*Command Line Interface Reference*』[英語] の該当するセクションを参照してください。

必要なローカルコンテキスト設定情報

次の表に、P-GW でローカルコンテキストを設定するために必要な情報を示します。

表 *14 :* ローカルコンテキストの設定に必要な情報

必要な情報	説明
管理インターフェイスの設定	
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	管理インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
セキュリティ管理者名	システムに対して完全な権限を持つセキュリティ管理者の名前。
セキュリティ管理者のパスワード	オープンパスワードまたは暗号化パスワードを使用できます。
リモートアクセスタイプ	システムへのアクセスに使用するリモートアクセスプロトコルのタイプ（SSH など）。

必要な P-GW コンテキスト設定情報

次の表に、P-GW で P-GW コンテキストを設定するために必要な情報を示します。

表 *15 : P-GW* コンテキストの設定に必要な情報

必要な情報	説明
P-GW コンテキスト名	システムが P-GW コンテキストを認識するために使用する 1 ～ 79 文字（英字または数字）の識別文字列。
アカウンティングポリシー名	システムがアカウンティングポリシーを認識するために使用する 1 ～ 文字（英字または数字）の識別文字列。アカウンティングポリシーは Rf（オフライン課金）インターフェイスのパラメータを設定するため使用されます。
S5/S8 インターフェイスの設定（S-GW 間）	
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルーを設定するときに使用されます。
GTP-U サービスの設定	
GTP-U サービス名	システムが GTP-U サービスを認識するために使用する 1 ～ 63 文字（字または数字）の識別文字列。
IP address	S5/S8 インターフェイスの IPv4 アドレス。
P-GW サービス設定	
P-GW サービス名	システムが P-GW サービスを認識するために使用する 1 ～ 63 文字（字または数字）の識別文字列。 複数の P-GW サービスを使用する場合は、複数の名前が必要です。

必要な情報	説明
PLMN ID	MCC 番号：PLMN の識別子のモバイル国コード（MCC）部分（100 ～ 999 の整数値）。 MNC 番号：PLMN の識別子のモバイルネットワークコード（MNC）部分（00 ー 999 の 2 桁または 3 桁の整数値）。
eGTP サービスの設定	
eGTP サービス名	システムが eGTP サービスを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。

必要な PDN コンテキスト設定情報

次の表に、P-GW で PDN コンテキストを設定するために必要な情報を示します。

表 *16 : PDN* コンテキストの設定に必要な情報

必要な情報	説明
PDN コンテキスト名	システムが PDN コンテキストを認識するために使用する 1 ～ 79 文字（英字および/または数字）の識別文字列。
IP アドレスプールの設定	
IPv4アドレスプールの名前と範囲	システムが IPv4 プールを認識するために使用する 1 ～ 31 文字（英字と数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義される IPv4アドレスの範囲。
IPv6アドレスプールの名前と範囲	システムが IPv6 プールを認識するために使用する 1 ～ 31 文字（英字や数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義される IPv6アドレスの範囲。
アクセス制御リストの設定	
IPv4 アクセスリスト名	システムが IPv4 アクセスリストを認識するために使用する 1 ～ 47 文字（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。
IPv6 アクセスリスト名	システムが IPv6 アクセスリストを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。

必要な情報	説明
拒否/許可タイプ	タイプは次のとおりです。 • any • ホスト IP アドレスによる • IP パケットによる • 送信元 ICMP パケットによる • 送信元 IP アドレスマスキングによる • TCP/UDP パケットによる
アドレス再指定またはリダイレクトタイプ	タイプは次のとおりです。 • サーバーのアドレス再指定 • コンテキストのリダイレクト • CSS 配信シーケンスのリダイレクト • redirect css service コマンドで使用可能なキーワードとオプションついては、『Command Line Interface Reference』の • redirect nexthop
SGi インターフェイスの設定（IPv4 PDN へ/IPv4 PDN から）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
SGi インターフェイスの設定（IPv6 PDN へ/IPv6 PDN から）	

必要な情報	説明
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。

必要な AAA コンテキスト設定情報

次の表に、P-GW で AAA コンテキストを設定するために必要な情報を示します。

表 *17 : AAA* コンテキストの設定に必要な情報

必要な情報	説明
Gx インターフェイスの設定（PCRF 対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。

必要な情報	説明
Gx Diameter エンドポイントの設定	
エンドポイント名	Gx Diameter エンドポイントの設定がシステムによって認識される 1～63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Gx 送信元ホストがシステムによって認識される、1～255 文字（英字数字）の識別文字列。
元のホストアドレス	Gx インターフェイスの IP アドレス。
ピア名	上述の Gx エンドポイント名。
ピアレルム名	上述の Gx 発信元レルム名。
ピアのアドレスとポート番号	PCRF の IP アドレスとポート番号。
ルートエントリピア	上述の Gx エンドポイント名。
Gy インターフェイスの設定（オンライン課金サーバー対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1～79 文字（字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネトが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカドが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルーを設定するときに使用されます。
Gy Diameter エンドポイントの設定	

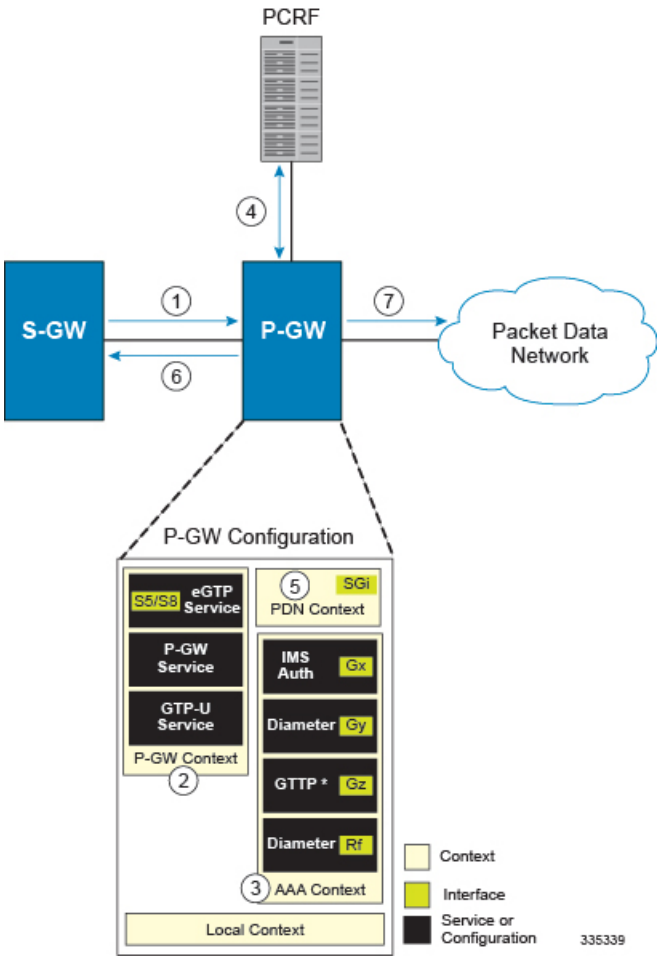
必要な情報	説明
エンドポイント名	Gy Diameter エンドポイントの設定がシステムによって認識される 1 ー 63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Gy 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字や数字）の識別文字列。
元のホストアドレス	Gy インターフェイスの IP アドレス。
ピア名	上述の Gy エンドポイント名。
ピアレルム名	上述の Gy 発信元レルム名。
ピアのアドレスとポート番号	OCS の IP アドレスとポート番号。
ルートエントリピア	上述の Gy エンドポイント名。
Gz インターフェイスの設定（オフライン課金サーバーに対する）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
Rf インターフェイスの設定（オフライン課金サーバーに対する）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。

必要な情報	説明
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネトが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカドが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルーを設定するときに使用されます。
Rf Diameter エンドポイントの設定	
エンドポイント名	Rf Diameter エンドポイントの設定がシステムによって認識される 1 ～63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Rf 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字数字）の識別文字列。
元のホストアドレス	Rf インターフェイスの IP アドレス。
ピア名	上述の Rf エンドポイント名。
ピアレルム名	上述の Rf 発信元レルム名。
ピアのアドレスとポート番号	OFCS の IP アドレスとポート番号。
ルートエントリピア	上述の Rf エンドポイント名。

この設定が動作する仕組み

次の図と補足テキストは、GTP LTE ネットワークから発信されるサブスクライバコールを処理するために、単一の送信元と接続先のコンテキストを持つこの設定がシステムによってどのように使用されるかを示しています。

図 *7: GTP P-GW* 構成要素



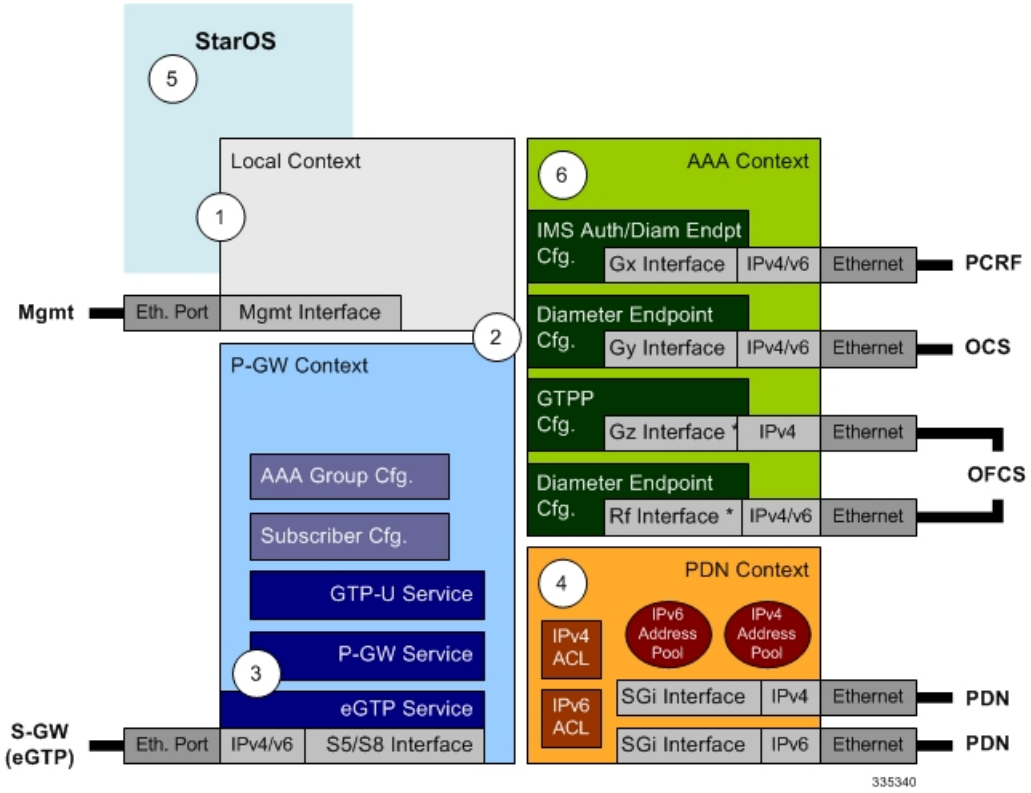
1. S-GW は、アクセスポイント名（APN）を含むセッション作成要求メッセージを P-GW に送信することにより、S5/S8 接続を確立します。
2. P-GW サービスは、セッションに AAA 機能を提供するために使用するコンテキストを決定します。このプロセスについては、『*System Administration Guide*』の「*Understanding the System Operation and Configuration*」の章にある「*How the System Selects Contexts*」の項で説明しています。
3. P-GW は、設定済みの Gx Diameter エンドポイントを使用して IP-CAN セッションを確立します。
4. P-GW は、IP-CAN セッションの確立を示すために CCRF に CC 要求（CCR）メッセージを送信し、PCRF は CC 応答（CCA）で確認応答します。
5. P-GW は APN 設定を使用して PDN コンテキストを選択します。選択した PDN コンテキストで設定された IP プールから IP アドレスが割り当てられます。
6. P-GW は、割り当てられたアドレスと追加情報を含むセッション作成応答メッセージで S-GW に応答します。

7. S5/S8 データプレーントンネルが確立され、P-GW は PDN との間でパケットを送受信できます。

eGTP P-GW 設定

スタンドアロン eGTP P-GW として動作するようにシステムを設定するには、次の手順を実行します。

図 *8 : eGTP P-GW* の設定可能項目



手順

ステップ 1 『*System Administration Guide*』[英語] に記載されている設定例を適用して、PSC のアクティブ化などのシステム設定パラメータを設定します。

ステップ 2 「初期設定 （144 ページ）」に記載されている設定例を適用して、コンテキストやサービスの作成などの初期設定パラメータを設定します。

ステップ 3 システムを eGTP P-GW として動作するように設定し、「P-GW サービス設定 （148 ページ）」に記載されている設定例を適用して、eGTP インターフェイスや IP ルートなどの基本的な P-GW パラメータを設定します。

ステップ 4 「P-GW PDN コンテキストの設定 （149 ページ）」の設定例を適用して、PDN コンテキストを設定します。

ステップ 5 「アクティブ課金サービス設定 （150 ページ）」の設定例を適用して、Gx インターフェイスのサポートのためのアクティブ課金サービスを有効にし、設定します。

ステップ 6 「ポリシーの設定 （152 ページ）」の設定例を適用して、AAA コンテキストを作成し、ポリシーのパラメータを設定します。

ステップ 7 「設定の確認と保存 （154 ページ）」の手順に従って、設定を確認して保存します。

初期設定

手順

ステップ 1 「ローカルコンテキストの変更 （144 ページ）」の設定例を適用して、ローカルシステム管理パラメータを設定します。

ステップ 2 「eGTP P-GW コンテキストの作成と設定 （145 ページ）」の設定例を適用して、eGTP サービスを配置したコンテキストを作成します。

ステップ 3 「P-GW コンテキストでの APN の作成と設定 （146 ページ）」の設定例を適用して、P-GW コンテキストで APN を作成および設定します。

ステップ 4 「P-GW コンテキストでの AAA グループの作成と設定 （147 ページ）」の設定例を適用して、P-GW コンテキストで AAA サーバーグループを作成および設定します。

ステップ 5 「eGTP サービスの作成と設定 （147 ページ）」の設定例を適用して、新しく作成されたコンテキスト内に eGTP サービスを作成します。

ステップ 6 「GTP-U サービスの作成と設定 （148 ページ）」の設定例を適用して、P-GW コンテキスト内に GTP-U サービスを作成および設定します。

ステップ 7 「P-GW PDN コンテキストの作成 （148 ページ）」の設定例を適用して、PDN へのインターフェイスが配置されるコンテキストを作成します。

ローカルコンテキストの変更

デフォルトサブスクライバを設定し、ローカルコンテキストでリモートアクセス機能を設定するには、次の例を使用します。

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
        exit
      server ftpd
        exit
      server telnetd
        exit
      subscriber default
        exit
      administrator <name> encrypted password <password> ftp
```

```
      ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
      exit
  port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
    end
```

eGTP P-GW コンテキストの作成と設定

次の例を使用して、P-GW コンテキストを作成し、S5 または S8 IPv4 インターフェイス（S-GW との間のデータトラフィック用）を作成し、S5 または S8 インターフェイスを設定済みのイーサネットポートにバインドします。

```
configure
  gtpp single-source
  context <pgw_context_name> -noconfirm
    interface <s5s8_interface_name>
      ip address <ipv4_address>
      exit
    gtpp group default
      gtpp charging-agent address <gz_ipv4_address>
      gtpp echo-interval <seconds>
      gtpp attribute diagnostics
      gtpp attribute local-record-sequence-number
      gtpp attribute node-id-suffix <string>
      gtpp dictionary <name>
      gtpp server <ipv4_address> priority <num>
      gtpp server <ipv4_address> priority <num> node-alive enable
      exit
    policy accounting <rf_policy_name> -noconfirm
      accounting-level {level_type}
      accounting-event-trigger interim-timeout action stop-start
      operator-string <string>
      cc profile <index> interval <seconds>
      exit
    exit
  subscriber default
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5s8_interface_name> <pgw_context_name>
    end
```

注：

- **gtpp single-source** が有効になり、各 AAA マネージャが独自の UDP ポートで要求を生成するのではなく、システムが単一の UDP ポートを使用して（AAA プロキシ機能によって）アカウンティングサーバーへの要求を生成できるようになりました。
- S5 または S8（P-GW から S-GW）インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。

- Rf（オフライン課金）インターフェイスのアカウンティングポリシーを設定します。アカウンティングレベルのタイプは、Flow、PDN、PDN-QCI、QCI、および Subscriber です。このコマンドの詳細については、『*Command Line Interface Reference*』の「*Accounting Profile Configuration Mode Commands*」の章を参照してください。
- Gz アカウンティングの GTPP グループを設定します。

P-GW コンテキストでの APN の作成と設定

次の設定を使用して、APN を作成します。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      associate accounting-policy <rf_policy_name>
      ims-auth-service <gx_ims_service_name>
      aaa group <rf-radius_group_name>
      dns primary <ipv4_address>
      dns secondary <ipv4_address>
      ip access-group <name> in
      ip access-group <name> out
      mediation-device context-name <pgw_context_name>
      ip context-name <pdn_context_name>
      ipv6 access-group <name> in
      ipv6 access-group <name> out
      active-charging rulebase <name>
      end
```

注：

- IMS 承認サービスは、AAA コンテキストで作成および設定されます。
- 複数の APN を、異なるドメイン名をサポートするように設定できます。
- 事前設定済みのアカウンティングポリシーをこの APN に関連付けるには、**associate accounting-policy** コマンドを使用します。アカウンティングポリシーは、P-GW コンテキストで設定されます。その例が「eGTP P-GW コンテキストの作成と設定（145 ページ）」で示されています。

Gz インターフェイスパラメータを含む APN を作成するには、次の設定を使用します。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      bearer-control-mode mixed
      selection-mode sent-by-ms
      accounting-mode gtpp
      gtpp group default accounting-context <aaa_context_name>
      ims-auth-service <gx_ims_service_name>
      ip access-group <name> in
      ip access-group <name> out
```

```
ip context-name <pdn_context_name>
active-charging rulebase <gz_rulebase_name>
end
```

注：

- IMS 承認サービスは、AAA コンテキストで作成および設定されます。
- 複数の APN を、異なるドメイン名をサポートするように設定できます。
- accounting-mode GTPP および GTPP group コマンドは、この APN を Gz アカウンティング用に設定します。

P-GW コンテキストでの AAA グループの作成と設定

RADIUS および Rf アカウンティングをサポートする AAA グループを作成および設定するには、次の例を使用します。

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter accounting endpoint <rf_cfg_name>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
    aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter accounting endpoint <rf_cfg_name>
      diameter accounting server <rf_cfg_name> priority <num>
      end
```

eGTP サービスの作成と設定

eGTP サービスを作成するには、次の設定例を使用します。

```
configure
  context <pgw_context_name>
    egtp-service <egtp_service_name> -noconfirm
      interface-type interface-pgw-ingress
      validation mode default
      associate gtpu-service <gtpu_service_name>
      gtpc bind address <s5s8_interface_address>
      end
```

注：

- 同じ ASR 5500 で P-GW サービスをコロケーションするには、**gtpc bind address** コマンドで、P-GW サービスがバインドされているのと同じ IP アドレスを使用する必要があります。

GTP-U サービスの作成と設定

次の設定例を使用して、GTP-U サービスを作成します。

```
configure
  context <pgw_context_name>
    gtpu-service <gtpu_service_name> -noconfirm
      bind ipv4-address <s5s8_interface_address>
      end
```

注：

- **bind** コマンドは、**ipv6-address** コマンドを使用して IPv6 アドレスとしても指定できます。

P-GW PDN コンテキストの作成

P-GW PDN コンテキストおよびイーサネット インターフェイスを作成し、インターフェイスを設定済みのイーサネットポートにバインドするには、次の例を使用します。

```
configure
  context <pdn_context_name> -noconfirm
    interface <sgi_ipv4_interface_name>
      ip address <ipv4_address>
    interface <sgi_ipv6_interface_name>
      ipv6 address <address>
      end
```

P-GW サービス設定

手順

ステップ 1 「P-GW サービスの設定 （148 ページ）」の設定例を適用して、P-GW サービスを設定します。

ステップ 2 「固定 IP ルートの設定 （149 ページ）」の設定例を適用して、eGTP サービングゲートウェイへの IP ルートを指定します。

P-GW サービスの設定

次の例を使用して、P-GW サービスを設定します。

```
configure
  context <pgw_context_name>
    pgw-service <pgw_service_name> -noconfirm
         plmn id mcc <id> mnc <id>
         associate egtp-service <egtp_service_name>
```

```
associate qci-qos-mapping <name>
end
```

注：

- QCI-QoS マッピング設定は AAA コンテキストで作成されます。詳細については、QCI-QoS マッピングの設定 （153 ページ）を参照してください。
- 同じ ASR 5500 で P-GW サービスをコロケーションするには、P-GW サービス内で **associate pgw-service** *name* コマンドを設定する必要があります。

固定 IP ルートの設定

次の例を使用して、eGTP サービングゲートウェイとのコントロールプレーンおよびユーザープレーンのデータ通信の IP ルートを設定します。

```
configure
  context <pgw_context_name>
    ip route <sgw_ip_addr/mask> <sgw_next_hop_addr> <pgw_intrfc_name>
    end
```

P-GW PDN コンテキストの設定

次の例を使用して、IP プールと APN を設定し、PDN コンテキストのインターフェイスにポートをバインドします。

```
configure
  context <pdn_context_name> -noconfirm
    interface <sgi_ipv4_interface_name>
      ip address <ipv4_address>
      exit
    interface <sgi_ipv6_interface_name>
      ip address <ipv6_address>
      exit
    ip pool <name> range <start_address end_address> public <priority>
    ipv6 pool <name> range <start_address end_address> public <priority>
    subscriber default
      exit
    ip access-list <name>
      redirect css service <name> any
      permit any
      exit
    ipv6 access-list <name>
      redirect css service <name> any
      permit any
      exit
      aaa group default
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <sgi_ipv4_interface_name> <pdn_context_name>
    exit
```

```
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <sgi_ipv6_interface_name> <pdn_context_name>
  end
```

アクティブ課金サービス設定

アクティブ課金を有効化および設定するには、次の例を使用します。

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule>
        .
        .
      <rule>
      exit
    ruledef default
      ip any-match = TRUE
      exit
    ruledef icmp-pkts
      icmp any-match = TRUE
      exit
    ruledef qci3
       icmp any-match = TRUE
      exit
    ruledef static
      icmp any-match = TRUE
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    charging-action icmp
      billing-action egcdr
      exit
    charging-action qci3
      content-id <id>
      billing-action rf
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft packet-filter qci3
      exit
    charging-action static
      service-identifier <id>
      billing-action rf
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft packet-filter qci3
```

```
      exit
    packet-filter <packet_filter_name>
      ip remote-address = { <ipv4/ipv6_address> | <ipv4/ipv6_address/mask> }
      ip remote-port { = <port_number> | range <start_port_number> to
<end_port_number> }
      exit
    rulebase default
             exit
    rulebase <name>
      <rule_base>
        .
        .
      <rule_base>
      exit
    rulebase <gx_rulebase_name>
      dynamic-rule order first-if-tied
      egcdr tariff minute <minute> hour <hour>(optional)
      billing-records egcdr
      action priority 5 dynamic-only ruledef qci3 charging-action qci3
      action priority 100 ruledef static charging-action static
      action priority 500 ruledef default charging-action icmp
      action priority 570 ruledef icmp-pkts charging-action icmp
      egcdr threshold interval <interval>
      egcdr threshold volume total <bytes>
      end
```

注：

- ルールベースとは、ルール定義および関連する課金アクションの集合です。
- 上記のように、複数のルール定義、課金アクション、およびルールベースを設定して、さまざまな課金シナリオをサポートできます。
- 課金アクションは、ルール定義が一致したときに実行するアクションを定義します。
- ルーティングルールや課金ルールの定義を作成および設定できます。作成できるルーティングルール定義の最大数は 256 です。課金ルール定義の最大数は 2048 です。
- Gz アカウンティングの場合、charge-action *qc13*、*icmp*、および *static* の例にある billing-action egcdr コマンドが必要です。
- Gz ルールベースの例では、オフライン課金用の Gz インターフェイスがサポートされます。Gz アカウンティングには、**billing-records egcdr** コマンドが必要です。その他のコマンドはすべてオプションです。



重要 専用ベアラーでアップリンクパケットを受信している場合は、専用ベアラーにインストールされているルールだけが照合されます。静的ルールは一致せず、一致しないパケットはドロップされます。

ポリシーの設定

手順

ステップ 1 「AAA コンテキストの作成と設定 （152 ページ）」の設定例を適用して、ポリシーとアカウンティングのインターフェイスを設定します。

ステップ 2 「QCI-QoS マッピングの設定 （153 ページ）」に記載されている設定例を適用して、QCI から QoS へのマッピングを作成し、設定します。

AAA コンテキストの作成と設定

次の例を使用して、Diameter サポートとポリシー制御を含む AAA コンテキストを作成および設定し、このコンテキストと PCRF、OCS、および OFCS 間のトラフィックをサポートしているインターフェイスにイーサネットポートをバインドします。

```
configure
  context <aaa_context_name> -noconfirm
    interface <gx_interface_name>
      ipv6 address <address>
      exit
    interface <gy_interface_name>
      ipv6 address <address>
      exit
    interface <gz_interface_name>
      ip address <ipv4_address>
      exit
    interface <rf_interface_name>
      ip address <ipv4_address>
      exit
    subscriber default
      exit
    ims-auth-service <gx_ims_service_name>
      p-cscf discovery table <#> algorithm round-robin
      p-cscf table <#> row-precedence <#> ipv6-address <pcrf_ipv6_adr>
      policy-control
        diameter origin endpoint <gx_cfg_name>
        diameter dictionary <name>
        diameter host-select table <#> algorithm round-robin
       diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

        exit
      exit
    diameter endpoint <gx_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv6_address>
      peer <gx_cfg_name> realm <name> address <pcrf_ipv4_or_ipv6_addr>
      route-entry peer <gx_cfg_name>
```

```
      exit
    diameter endpoint <gy_cfg_name>
      origin realm <realm_name>
      origin host <name> address <gy_ipv6_address>
      connection retry-timeout <seconds>
      peer <gy_cfg_name> realm <name> address <ocs_ipv4_or_ipv6_addr>
      route-entry peer <gy_cfg_name>
      exit
    diameter endpoint <rf_cfg_name>
      use-proxy
      origin realm <realm_name>
      origin host <name> address <rf_ipv4_address>
      peer <rf_cfg_name> realm <name> address <ofcs_ipv4_or_ipv6_addr>
      route-entry peer <rf_cfg_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gx_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gy_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gz_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <rf_interface_name> <aaa_context_name>
    end
```

注：

- **ims-auth-service** の下の **p-cscf table** コマンドでも、PCRF に IPv4 アドレスを指定できます。
- Gx インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。
- Gy インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。
- Rf インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。

QCI-QoS マッピングの設定

QCI 値を作成し、適用可能な QoS パラメータにマッピングするには、次の例を使用します。

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
```

```
qci 3 user-datagram dscp-marking <hex>
qci 9 user-datagram dscp-marking <hex>
end
```

注：

- 有効なライセンスキーがインストールされていない場合、P-GW は非標準の QCI 値をサポートしません。

  QCI 値 1 ～ 9 は、3GPP TS 23.203 で定義されている標準値です。P-GW はこれらの標準値をサポートします。

  3GPP リリース 8 以降では、通信事業者固有/非標準の QCI がサポートされ、キャリアは QCI 128- 254 を定義できます。

- 上記の設定は、1 つのキーワードの例のみを示しています。**qci** コマンドおよびサポートされるその他のキーワードの詳細については、『*Command Line Interface Reference*』の「*QCI - QOS Mapping Configuration Mode Commands*」[英語] の章を参照してください。

設定の確認と保存

Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

DHCP サービス設定

システムは、動的ホスト制御プロトコル（DHCP）を使用して PDP コンテキストに IP アドレスを割り当てるように設定できます。DHCP を使用した IP アドレスの割り当ては、APN での設定に従い、次の方法で行います。

DHCP プロキシ：システムはクライアント（MS）のプロキシとして機能し、クライアント（MS）に代わって DHCP 検出要求を開始します。DHCP 検出要求への応答で DHCP サーバーから割り当てられた IP アドレスを受信すると、受け取った IP アドレスを MS に割り当てます。割り当てられたこのアドレスは、システムの IP アドレスプールに設定されているアドレスと一致している必要があります。この手順全体は MS からは認識できません。

メモリ内のアドレス数が減少すると、システムは DHCP サーバーに追加のアドレスを要求します。メモリに保存されているアドレスの数が設定された制限を超えると、それらは DHCP サーバーに返却されます。

通信先 DHCP サーバーと IP アドレスの処理方法を指定するパラメータを最初に設定する必要があります。これらのパラメータは、DHCP サービスの一部として設定されます。

重要 ここでは、DHCP ベースの IP 割り当てのために DHCP サービスを設定する際に必要な最小限の命令セットについて説明します。追加の DHCP サーバーパラメータとこれらのコマンドの動作を設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*DHCP Service Configuration Mode Commands*」の章を参照してください。

以下の手順は、『システム管理ガイド』で説明されているシステムレベルの設定と、この章の「*eGTP P-GW* 設定」セクションで説明されている P-GW サービスがすでに設定済みであることを前提としています。

DHCP サービスを設定するには、次の手順を実行します。

手順

ステップ 1 システムコンテキストで DHCP サービスを作成し、「DHCP サービスの作成 （155 ページ）」の設定例を適用してバインドします。

ステップ 2 「DHCP サーバーパラメータ設定 （156 ページ）」の設定例を適用して、DHCP サーバーと、DHCP サーバーからの応答で受け入れられる最小および最大の許容リース時間を設定します。

ステップ 3 DHCPv6 サービス設定の確認 （161 ページ） の手順に従って、DHCP サービスの設定を確認します。

ステップ 4 「設定の確認と保存」セクションの説明に従って、設定を保存します。

DHCP サービスの作成

DHCP ベースのアドレス割り当てをサポートするように DHCP サービスを作成するには、次の例を使用します。

```
configure
   context <dest_ctxt_name>
      dhcp-service <dhcp_svc_name>
         bind address <ip_address> [nexthop-forwarding-address
<nexthop_ip_address> [mpls-label input <in_mpls_label_value> output
<out_mpls_label_value1> [out_mpls_label_value2]]]
         end
```

注：

- 適切に動作させるには、DHCP 機能を接続先コンテキスト内で設定する必要があります。
- オプションのキーワード **nexthop-forwarding-address** *<nexthop_ip_address>* **[mpls-label input** *<in_mpls_label_value>* **output** *<out_mpls_label_value1>* **[** *out_mpls_label_value2* **]]** により、MPLS トラフィックでの DHCP が適用されます。

DHCP サーバーパラメータ設定

DHCP ベースのアドレス割り当てをサポートするように DHCP サーバーパラメータを設定するには、次の例を使用します。

```
configure
   context <dest_ctxt_name>
      dhcp-service <dhcp_svc_name>
         dhcp server <ip_address> [priority <priority>
         dhcp server selection-algorithm {first-server | round-robin}
         lease-duration min <minimum_dur> max <max_dur>
         dhcp deadtime <max_time>
         dhcp detect-dead-server consecutive-failures <max_number>
         max-retransmissions <max_number>
         retransmission-timeout <dur_sec>
         end
```

注：

- 複数の DHCP サービスを設定できます。**dhcp server** コマンドを複数回入力することで、各サービスに複数の DHCP サーバーを構成できます。最大 225 の DHCP サービスを構成でき、それぞれの DHCP サービスには最大 8 つの DHCP サーバーを構成できます。
- **dhcp detect-dead-server** コマンドと **max-retransmissions** コマンドは、相互に連携して動作します。
- retransmission-timeout コマンドは **max-retransmissions** コマンドと連携して動作します。

DHCP サービス設定の確認

手順

ステップ 1 EXEC モードで次のコマンドを入力して、DHCP サーバーが正しく設定されていることを確認します。

```
show dhcp service all
```

このコマンドは、次に示すような出力を生成します。この例では、DHCP 名は *dhcp1* です。

```
Service name:                       dhcp1
Context:                                isp
Bind:                                   Done
Local IP Address:                       150.150.150.150
Next Hop Address:                       192.179.91.3
              MPLS-label:
               Input:                   5000
         Output:                        1566    1899
Service Status:                         Started
Retransmission Timeout:                 3000 (milli-secs)
Max Retransmissions:                    2
Lease Time:                             600 (secs)
Minimum Lease Duration:                 600 (secs)
Maximum Lease Duration:                 86400 (secs)
DHCP Dead Time:                         120 (secs)
DHCP Dead consecutive Failure:          5
```

```
DHCP T1 Threshold Timer:                50
DHCP T2 Threshold Timer:                88
DHCP Client Identifier:                 Not Used
DHCP Algorithm:                         Round Robin
DHCP Servers configured:
 Address: 150.150.150.150               Priority: 1
DHCP server rapid-commit:               disabled
DHCP client rapid-commit:               disabled
DHCP chaddr validation:                 enabled
```

ステップ 2 EXEC モードで次のコマンドを入力して、DHCP サービスのステータスを確認します。

show dhcp service status

DHCPv6 サービス設定

IPv6 の Dynamic Host Configuration Protocol（DHCP）が表示されるようにシステムを設定し、IPv6 ネットワークアドレスなどの設定パラメータを IPv6 ノードに渡すことができます。DHCPv6 の設定は APN 内で行います。

以下の手順は、『*System Administration Guide*』で説明されているシステムレベルの設定と P-GW PDN コンテキストの設定 （177 ページ）で説明されている APN がすでに設定済みであることを前提としています。

DHCPv6 サービスを設定するには、次の手順を実行します。

手順

ステップ 1 システムコンテキストで DHCPv6 サービスを作成し、DHCPv6 サービスの作成 （157 ページ）の設定例を適用してバインドします。

ステップ 2 DHCPv6 サーバーパラメータ設定 （158 ページ）の設定例を適用して、DHCPv6 サーバーや、更新時間、再バインド時間、優先ライフタイム、有効なライフタイムに関する設定可能なその他の値を設定します。

ステップ 3 DHCPv6 クライアントパラメータ設定 （159 ページ）の設定例を適用して、DHCPv6 クライアントや、最大再送信回数、サーバーのデッド回数、サーバーの復帰時間に関するその他の設定可能な値を設定します。

ステップ 4 DHCPv6 プロファイル設定 （159 ページ）の設定例を適用して、DHCPv6 プロファイルを設定します。

ステップ 5 DHCPv6 設定の関連付け （161 ページ）の設定例を適用して、DHCPv6 プロファイルの設定を APN に関連付けます。

ステップ 6 DHCPv6 サービス設定の確認 （161 ページ）の手順に従って、DHCPv6 サービスの設定を確認します。

ステップ 7 「設定の確認と保存」の章の説明に従って、設定を保存します。

DHCPv6 サービスの作成

DHCP ベースのアドレス割り当てをサポートするように DHCPv6 サービスを作成するには、次の例を使用します。

```
configure
  context <dest_ctxt_name>
    dhcpv6-service <dhcpv6_svc_name>
      bind address <ipv6_address> port <port>
      end
```

注：

- 適切に動作させるには、DHCPv6 機能を接続先コンテキスト内で設定する必要があります。
- ポートはリッスンポートを指定し、そのポートにバインドされたDHCPv6サーバーを起動するために使用されます。これはオプションであり、指定されていない場合、デフォルトのポートは 547 です。

（注） DHCPv6インターフェイスにはリンクローカルアドレスとユニキャストアドレスのみを使用します

DHCPv6 サーバーパラメータ設定

DHCPv6ベースのアドレス割り当てをサポートするようにDHCPv6サーバーパラメータを設定するには、次の例を使用します。

```
configure
  context <dest_ctxt_name>
    dhcpv6-service <dhcpv6_svc_name>
      dhcpv6-server
      renew-time <renewal_time>
      rebind-time <rebind_time>
      preferred-lifetime <pref_lifetime>
      valid-lifetime <valid_lifetime>
      end
```

注：

- **dhcp server** コマンドを複数回入力することで、複数の DHCP を設定できます。システムごとに（タイプに関係なく）最大 256 のサービスを設定できます。
- **renew-time** は、DHCP サービスによって割り当てられるプレフィックスの更新時間を設定します。デフォルトは 900 秒です。
- **rebind-time** は、DHCP サービスによって割り当てられるプレフィックスの再バインド時間を設定します。デフォルトは 900 秒です。
- **preferred-lifetime** は、DHCP サービスによって割り当てられるプレフィックスの優先ライフタイムを設定します。デフォルトは 900 秒です。
- **valid-lifetime** は、DHCP サービスによって割り当てられるプレフィックスの有効なライフタイムを設定します。デフォルトは 900 秒です。

DHCPv6 クライアントパラメータ設定

DHCPv6 ベースのアドレス割り当てをサポートするように DHCPv6 クライアントパラメータを設定するには、次の例を使用します。

```
configure
   context <dest_ctxt_name>
      dhcpv6-service <dhcpv6_svc_name>
         dhcpv6-client
            server-ipv6-address <ipv6_addr> port <port> priority <priority>
            max-retransmissions <max_number>
            server-dead-time <dead_time>
            server-resurrect-time <revive_time>
            end
```

注：

- DHCPv6 クライアントの設定には、IPv6 アドレス、ポート、および優先順位が必要です。ポートは DHCPv6 サーバーとの通信に使用されます。指定しない場合、デフォルトのポート 547 が使用されます。優先順位パラメータでは、試行するサーバーの優先順位を定義します。
- **max-retransmissions**：DHCPV6 クライアントが DHCPV6 サーバーに対して行う再送信の最大回数を設定します。デフォルトは 20 です。
- **server-dead-time**：PDN DHCPV6 サーバーは、クライアントから指定回数だけ試行しても応答しない場合、デッドと見なされます。デフォルトは 5 です。
- **server-resurrect-time**：PDN DHCPV6 サーバーは、指定された秒数のデッド状態後にアライブ状態と見なされます。デフォルトは 20 です。

DHCPv6 プロファイル設定

DHCPv6 プロファイルを設定するには、次の例を使用します。

```
configure
   context <dest_ctxt_name>
      dhcp-server-profile <server_profile>
         enable rapid-commit-dhcpv6
         process dhcp-option-from { AAA | LOCAL | PDN-DHCP } priority
<priority>
         dhcpv6-server-preference <pref_value>
         enable dhcpv6-server-unicast
         enable dhcpv6-server-reconf
         exit
      dhcp-client-profile <client_profile>
         dhcpv6-client-unicast
         client-identifier { IMSI | MSISDN }
         enable rapid-commit-dhcpv6
         enable dhcp-message-spray
         request dhcp-option dns-address
         request dhcp-option netbios-server-address
```

```
request dhcp-option sip-server-address
end
```

注：

- **dhcp-server-profile** コマンドは、サーバープロファイルを作成し、DHCP サーバープロファイル コンフィギュレーション モードを開始します。
- **enable rapid-commit-dhcpv6** コマンドは、DHCPv6 サーバーで高速コミットを有効にします。デフォルト設定は無効です。ネットワーク内に複数の DHCPv6 サーバーがある場合、rapid-commit-option を使用してこれを実行すると、UE のリソースすべてが確実に予約されます。
- **process dhcp-option-from** コマンドは、特定のクライアント要求に対して設定オプションを処理する順序を設定します。特定のクライアント設定の場合、値は AAA、PDN-DHCP-SERVER、LOCAL から取得できます。デフォルトでは、AAA が PDN-DHCP よりも優先され、PDN-DHCP は LOCAL の設定よりも優先されます。
- **dhcpv6-server-preference**：RFC-3315 に従って、DHCPv6-CLIENT は DHCPv6-SERVERS からのクエリへの応答を検討する前に、指定された時間だけ待機する必要があります。サーバーがプリファレンス値 255 で応答した場合、DHCPv6-CLIENT はそれ以上待つ必要はありません。デフォルト値は 0 で、1 ～ 255 の任意の整数を設定できます。
- **enable dhcpv6-server-unicast** コマンドは、DHCPv6 のサーバー ユニキャスト オプションを有効にします。デフォルトでは、無効になっています。
- **enable dhcpv6-server-reconf** コマンドは、サーバーからの再設定メッセージのサポートを設定します。デフォルトでは、無効になっています。
- **dhcpv6-client-unicast** コマンドを指定すると、クライアントはサーバーに向けてユニキャストアドレスでメッセージを送信できるようになります。
- **dhcp-client-profile** コマンドは、クライアントプロファイルを作成し、DHCP クライアント プロファイル コンフィギュレーション モードを開始します。
- **client identifier** コマンドは、外部 DHCP サーバーに送信されるクライアント識別子を設定します。デフォルトでは、IMSI が送信されます。もう 1 つの使用可能なオプションとして電話番号があります。
- **enable rapid-commit-dhcpv6** コマンドは、クライアントの高速コミットを設定します。デフォルトでは、DHCPv4 と DHCPv6 の両方で高速コミットオプションが有効になっています。
- **enable dhcp-message-spray** コマンドを指定すると、DHCP クライアントは、PDN 内で設定されているすべての DHCP サーバーに DHCP メッセージを配信できるようになります。デフォルトでは無効になっています。高速コミットで DHCP メッセージを送信できるサーバーは 1 つだけです。
- **request dhcp-option** コマンドは、DHCP クライアントが要求できる DHCP オプションを設定します。次のオプションを使用できます。
  - dns-address

- netbios-server-address
- sip-server-address

DHCPv6 設定の関連付け

DHCPv6 プロファイルを APN に関連付けるには、次の例を使用します。

```
configure
   context dest_ctxt_name
      apn apn_name
         dhcpv6 service-name dhcpv6_svc_name server-profile server_profile
client-profile client_profile
        dhcpv6 ip-address-pool-name dhcpv6_ip_pool allow-static-allocation

        dhcpv6 context-name <dest_ctxt>
        end
```

注：

- **dhcpv6 service-name** *dhcpv6_svc_name* **server-profile** *server_profile* **client-profile** *client_profile*：システムがDHCPv6サーバー コンフィギュレーションモードに移行できるようにします。このモードで DHCPv6 サーバーのパラメータを設定します。
- **dhcpv6 service-name** *dhcpv6_svc_name* **client-profile** *client_profile*：システムが DHCPv6 クライアント コンフィギュレーションモードに移行できるようにします。このモードでDHCPv6 クライアントのパラメータを設定します。
- **dhcpv6 ip-address-pool-name** *dhcpv6_ip_pool* **allow-static-allocation**：DHCPv6 プロファイルを APN と関連付けます。

（注） **allow-static-allocation** パラメータは、IPv6 プールを設定する場合にのみ使用します。

DHCPv6 サービス設定の確認

手順

ステップ 1 Exec モードで次のコマンドを入力して、DHCPv6 サーバーが正しく設定されていることを確認します。

```
show dhcpv6-service all
```

このコマンドは、次に示すような出力を生成します。この例では、DHCPv6 サービス名は *dhcp6-service* です。

```
Service name:               dhcpv6-service
Context:                            A
Bind Address:                       2092::192:90:92:40
```

```
Bind :                                Done
Service Status:                       Started
Server Dead Time:                     120 (secs)
Server Dead consecutive Failure:5
Server Select Algorithm:              First Server
Server Renew Time:                    400 (secs)
Server Rebind Time:                   500 (secs)
Server Preferred Life Time:           600 (secs)
Server Valid Life Time:               700 (secs)
Max Retransmissions:                  3 (secs)
Server Dead Tries:                    4 (secs)
Server Resurrect Time:                10 (secs)
ipv6_nd_flag:                         O_FLAG
DHCPv6 Servers configured:
          Address:                    2092::192:90:92:40 Priority: 1    enabled
```

ステップ 2 Exec モードで次のコマンドを入力して、DHCPv6 サービスのステータスを確認します。

show dhcpv6 status service *dhcpv6_service_name*

LTE-SAE ネットワークでのスタンドアロン PMIP P-GW としてのシステムの設定

ここでは、LTE-SAE テスト環境で P-MIP P-GW として動作するようにシステムを設定するための一連の手順の概要と、関連する構成ファイルの例を示します。構成ファイルの完全な例については、付録「サンプル構成ファイル」を参照してください。ここでは次の内容について説明します。

- 必要な情報 （162 ページ）必要な情報
- この設定が動作する仕組み （171 ページ）
- P-MIP P-GW（LTE）設定 （172 ページ）

必要な情報

以降のセクションでは、P-GW を設定し、ネットワーク上で動作させるために必要な最小限の情報について説明します。プロセスをより効率的なものにするため、システムを設定する前にこの情報を用意しておくことを推奨します。

ここでは説明していないその他の設定パラメータがあります。これらのパラメータは、主にネットワークでの P-GW の動作の微調整に対応します。これらのパラメータの詳細については、『*Command Line Interface Reference*』[英語] の該当するセクションを参照してください。

必要なローカルコンテキスト設定情報

次の表に、P-GW でローカルコンテキストを設定するために必要な情報を示します。

表 *18 :* ローカルコンテキストの設定に必要な情報

必要な情報	説明
管理インターフェイスの設定	
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	管理インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
セキュリティ管理者名	システムに対して完全な権限を持つセキュリティ管理者の名前。
セキュリティ管理者のパスワード	オープンパスワードまたは暗号化パスワードを使用できます。
リモートアクセスタイプ	システムへのアクセスに使用するリモートアクセスプロトコルのタイプ（SSH など）。

必要な P-GW コンテキスト設定情報

次の表に、P-GW で P-GW コンテキストを設定するために必要な情報を示します。

表 *19 : P-GW* コンテキストの設定に必要な情報

必要な情報	説明
P-GW コンテキスト名	システムが P-GW コンテキストを認識するために使用する 1 ～ 79 文字（英字または数字）の識別文字列。
アカウンティングポリシー名	システムがアカウンティングポリシーを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。アカウンティングポリシーは、Rf（オフライン課金）インターフェイスのパラメータを設定するために使用されます。
S5/S8 インターフェイスの設定（S-GW 間）	

必要な情報	説明
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
P-GW サービス設定	
P-GW サービス名	システムが P-GW サービスを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。 複数の P-GW サービスを使用する場合は、複数の名前が必要です。
LMA サービスの設定	
LMA サービス名	システムが LMA サービスを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。

必要な PDN コンテキスト設定情報

次の表に、P-GW で PDN コンテキストを設定するために必要な情報を示します。

表 *20 : PDN* コンテキストの設定に必要な情報

必要な情報	説明
P-GW コンテキスト名	システムが P-GW コンテキストを認識するために使用する 1 ～ 79 文字（英字と数字）の識別文字列。
IP アドレスプールの設定	

必要な情報	説明
IPv4アドレスプールの名前と範囲	システムが IPv4 プールを認識するために使用する 1 ～ 31 文字（英字数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義されるIPv4アドレスの範囲
IPv6アドレスプールの名前と範囲	システムが IPv6 プールを認識するために使用する 1 ～ 31 文字（英字数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義されるIPv6アドレスの範囲
アクセス制御リストの設定	
IPv4 アクセスリスト名	システムが IPv4 アクセスリストを認識するために使用する 1 ～ 47 文（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。
IPv6 アクセスリスト名	システムが IPv6 アクセスリストを認識するために使用する 1 ～ 79 文（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。
拒否/許可タイプ	タイプは次のとおりです。 • any • ホスト IP アドレスによる • IP パケットによる • 送信元 ICMP パケットによる • 送信元 IP アドレスマスキングによる • TCP/UDP パケットによる
アドレス再指定またはリダイレクトタイプ	タイプは次のとおりです。 • アドレス再指定サーバー • コンテキストのリダイレクト • CSS 配信シーケンスのリダイレクト • redirect css service コマンドで使用可能なキーワードとオプションついては、『Command Line Interface Reference』の • redirect nexthop

必要な情報	説明
SGi インターフェイスの設定（IPv4 PDN へ/IPv4 PDN から）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
SGi インターフェイスの設定（IPv6 PDN へ/IPv6 PDN から）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。

必要な AAA コンテキスト設定情報

次の表に、P-GW で AAA コンテキストを設定するために必要な情報を示します。

表 *21 : AAA* コンテキストの設定に必要な情報

必要な情報	説明
Gx インターフェイスの設定（PCRF 対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカドが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルーを設定するときに使用されます。
Gx Diameter エンドポイントの設定	
エンドポイント名	Gx Diameter エンドポイントの設定がシステムによって認識される 1 ～ 63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Gx 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字数字）の識別文字列。
元のホストアドレス	Gx インターフェイスの IP アドレス。
ピア名	上述の Gx エンドポイント名。
ピアレルム名	上述の Gx 発信元レルム名。
ピアのアドレスとポート番号	PCRF の IP アドレスとポート番号。
ルートエントリピア	上述の Gx エンドポイント名。
S6b インターフェイスの設定（3GPP AAA 対応）	

必要な情報	説明
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
S6b Diameter エンドポイントの設定	
エンドポイント名	S6b Diameter エンドポイント設定がシステムによって認識される 1 ー 63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameter アイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	S6b 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字や数字）の識別文字列。
元のホストアドレス	S6b インターフェイスの IP アドレス。
ピア名	上述の S6b エンドポイント名。
ピアレルム名	上述の S6b 発信元レルム名。
ピアのアドレスとポート番号	AAA サーバーの IP アドレスとポート番号。
ルートエントリピア	上述の S6b エンドポイント名。
Gy インターフェイスの設定（オンライン課金サーバー対応）	

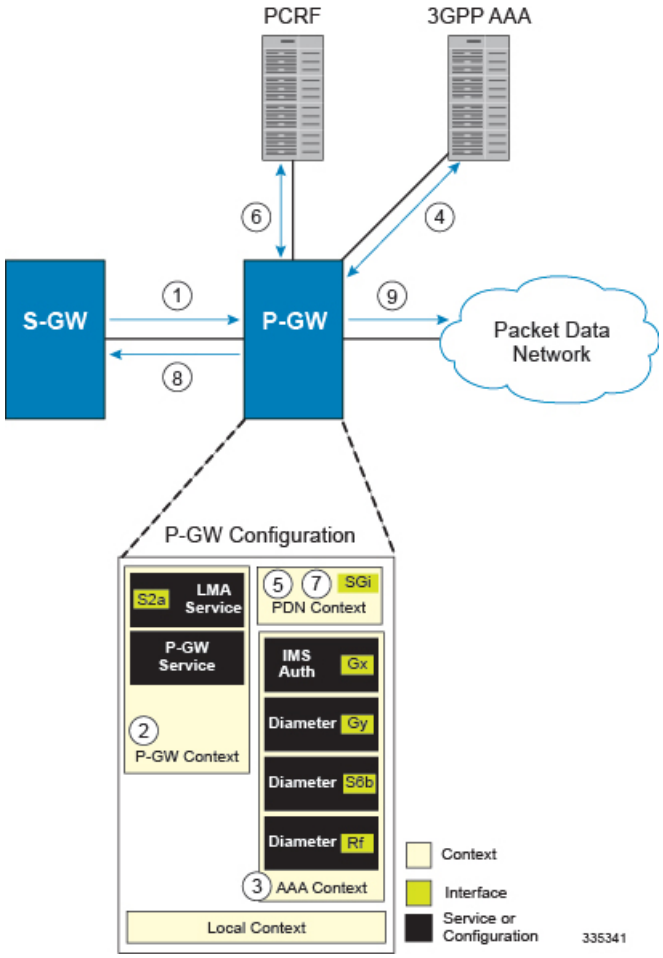
必要な情報	説明
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（ 字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 ア レス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネ トが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカ ドが取り付けられているシャーシスロット番号とその後に続くカード の物理コネクタの番号によって識別されます。たとえば、ポート 17/ は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルー を設定するときに使用されます。
Gy Diameter エンドポイントの設定	
エンドポイント名	Gy Diameter エンドポイントの設定がシステムによって認識される 1 ～ 63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはす ての Diameter メッセージに存在し、通常は会社名またはサービス名で す。
発信元ホスト名	Gy 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字 数字）の識別文字列。
元のホストアドレス	Gy インターフェイスの IP アドレス。
ピア名	上述の Gy エンドポイント名。
ピアレルム名	上述の Gy 発信元レルム名。
ピアのアドレスとポート番号	AAA サーバーの IP アドレスとポート番号。
ルートエントリピア	上述の Gy エンドポイント名。
Rf インターフェイスの設定（オフライン課金サーバーに対する）	

必要な情報	説明
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
Rf Diameter エンドポイントの設定	
エンドポイント名	Rf Diameter エンドポイントの設定がシステムによって認識される 1 ー 63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameter アイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Rf 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字や数字）の識別文字列。
元のホストアドレス	Rf インターフェイスの IP アドレス。
ピア名	上述の Rf エンドポイント名。
ピアレルム名	上述の Rf 発信元レルム名。
ピアのアドレスとポート番号	PCRF の IP アドレスとポート番号。
ルートエントリピア	上述の Rf エンドポイント名。

この設定が動作する仕組み

次の図と補足テキストは、PMIP LTE ネットワークから発信されるサブスクライバコールを処理するために、単一の送信元と接続先のコンテキストを持つこの設定がシステムによってどのように使用されるかを示しています。

図 *9 : LTE* ネットワークの *PMIP P-GW* の要素



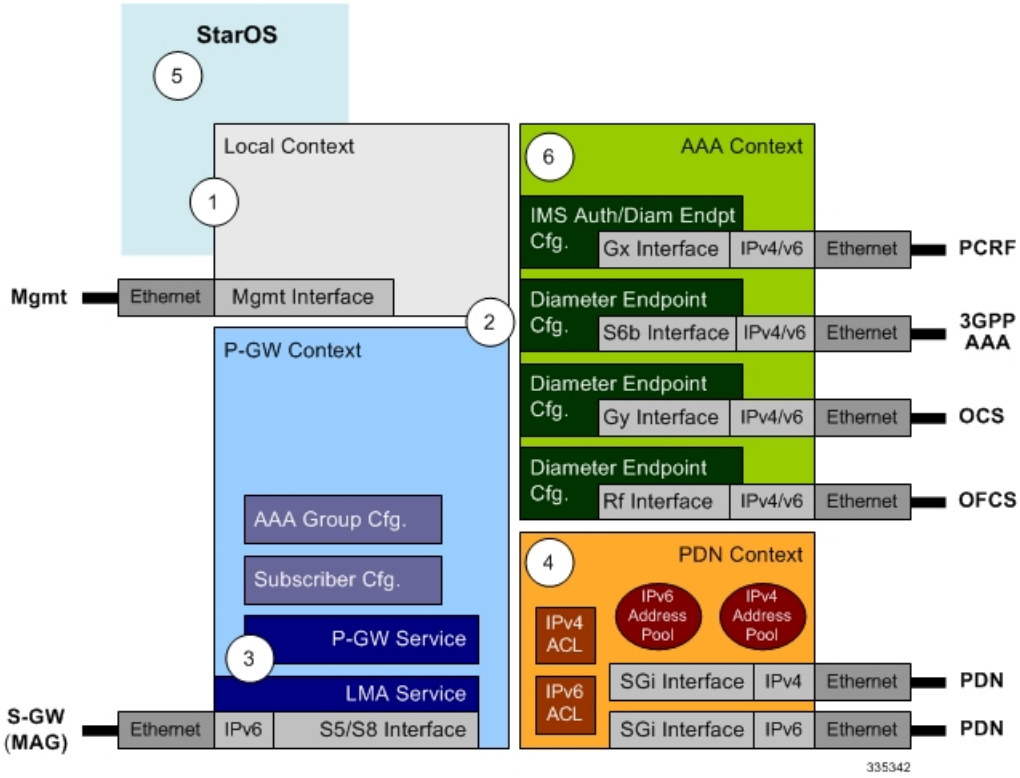
1. S-GW は、アクセスポイント名（APN）を含むセッション作成要求メッセージを P-GW に送信することにより、S5/S8 接続を確立します。
2. P-GW サービスは、セッションに AAA 機能を提供するために使用するコンテキストを決定します。このプロセスについては、『*System Administration Guide*』の「*Understanding the System Operation and Configuration*」の章にある「*How the System Selects Contexts*」の項で説明しています。
3. P-GW は、設定済みの Gx Diameter エンドポイントを使用して IP-CAN セッションを確立します。
4. P-GW は、IP-CAN セッションの確立を示すために CCRF に CC 要求（CCR）メッセージを送信し、PCRF は CC 応答（CCA）で確認応答します。

5. P-GW は APN 設定を使用して PDN コンテキストを選択します。選択した PDN コンテキストで設定された IP プールから IP アドレスが割り当てられます。
6. P-GW は、割り当てられたアドレスと追加情報を含むセッション作成応答メッセージで S-GW に応答します。
7. S5/S8 データプレーントンネルが確立され、P-GW は PDN との間でパケットを送受信できます。

P-MIP P-GW（LTE）設定

LTE-SAE ネットワーク環境でスタンドアロン P-MIP P-GW として動作するようにシステムを設定する場合は、次の図とその後の手順を確認してください。

図 *10 : PMIP P-GW（LTE）が設定可能*



手順

ステップ 1 『*System Administration Guide*』[英語] に記載されている設定例を適用して、PSC のアクティブ化などのシステム設定パラメータを設定します。

ステップ 2 「初期設定 （173 ページ）」に記載されている設定例を適用して、コンテキストやサービスの作成などの初期設定パラメータを設定します。

ステップ 3 システムを PMIP P-GW として動作するように設定し、「P-GW サービス設定 （176 ページ）」に記載されている設定例を適用して、PMIP インターフェイスや IP ルートなどの P-GW の基本的なパラメータを設定します。

ステップ 4 「P-GW PDN コンテキストの設定 （177 ページ）」の設定例を適用して、PDN コンテキストを設定します。

ステップ 5 「アクティブ課金サービス設定 （178 ページ）」の設定例を適用して、Gx インターフェイスのサポートのためのアクティブ課金サービスを有効にし、設定します。

ステップ 6 「AAA とポリシーの設定 （200 ページ）」の設定例を適用して、AAA コンテキストを作成し、AAA およびポリシーのパラメータを設定します。

ステップ 7 設定の確認と保存 （182 ページ） の手順に従って、設定を確認して保存します。

初期設定

手順

ステップ 1 「ローカルコンテキストの変更 （173 ページ）」の設定例を適用して、ローカルシステム管理パラメータを設定します。

ステップ 2 「P-MIP P-GW コンテキストの作成と設定 （174 ページ）」の設定例を適用して、P-GW サービスを配置したコンテキストを作成します。

ステップ 3 「P-GW コンテキストでの APN の作成と設定 （174 ページ）」の設定例を適用して、P-GW コンテキストで APN を作成および設定します。

ステップ 4 「P-GW コンテキストでの AAA グループの作成と設定 （175 ページ）」の設定例を適用して、P-GW コンテキストで AAA サーバーグループを作成および設定します。

ステップ 5 「LMA サービスの作成と設定 （176 ページ）」の設定例を適用して、新しく作成されたコンテキスト内のローカルモビリティアンカー（LMA）サービスを作成および設定します。

ステップ 6 「P-GW PDN コンテキストの作成 （176 ページ）」の設定例を適用して、PDN へのインターフェイスが配置されるコンテキストを作成します。

ローカルコンテキストの変更

デフォルトサブスクライバを設定し、ローカルコンテキストでリモートアクセス機能を設定するには、次の例を使用します。

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
        exit
      server ftpd
        exit
      server telnetd
        exit
```

```
      subscriber default
        exit
      administrator <name> encrypted password <password> ftp
      ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
      exit
  port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
    end
```

P-MIP P-GW コンテキストの作成と設定

次の例を使用して、P-GW コンテキストを作成し、S5 または S8 IPv6 インターフェイス（S-GW との間のデータトラフィック用）を作成し、S5 または S8 インターフェイスを設定済みのイーサネットポートにバインドします。

```
configure
  context <pgw_context_name> -noconfirm
    interface <s5s8_interface_name> tunnel
      ipv6 address <ipv6_address>
      tunnel-mode ipv6ip
      source interface <name>
      destination address <ipv6 address>
      exit
    exit

  policy accounting <rf_policy_name> -noconfirm
    accounting-level {level_type}
    accounting-event-trigger interim-timeout action stop-start
    operator-string <string>
    exit
  subscriber default
    exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5s8_interface_name> <pgw_context_name>
    end
```

注：

- S5 または S8（P-GW から S-GW）インターフェイスは、IPv6 アドレスである必要があります。
- Rf（オフライン課金）インターフェイスのアカウンティングポリシーを設定します。アカウンティングレベルのタイプは、Flow、PDN、PDN-QCI、QCI、および Subscriber です。このコマンドの詳細については、『*Command Line Interface Reference*』の「*Accounting Profile Configuration Mode Commands*」の章を参照してください。

P-GW コンテキストでの APN の作成と設定

次の設定を使用して、APN を作成します。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      ims-auth-service <gx_ims_service_name>
      aaa group <rf-radius_group_name>
      dns primary <ipv4_address>
      dns secondary <ipv4_address>
      ip access-group <name> in
      ip access-group <name> out
      mediation-device context-name <pgw_context_name>
      ip context-name <pdn_context_name>
      ipv6 access-group <name> in
      ipv6 access-group <name> out
      active-charging rulebase <name>
      end
```

注：

- IMS 承認サービスは、AAA コンテキストで作成および設定されます。
- 複数の APN を、異なるドメイン名をサポートするように設定できます。

P-GW コンテキストでの AAA グループの作成と設定

RADIUS および Rf アカウンティングをサポートする AAA グループを作成および設定するには、次の例を使用します。

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
    aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      end
```

LMA サービスの作成と設定

LMA サービスを作成するには、次の設定例を使用します。

```
configure
  context <pgw_context_name>
    lma-service <lma_service_name> -noconfirm
      no aaa accounting
      revocation enable
      bind address <s5s8_ipv6_address>
      end
```

注：

- **no aaa acounting** コマンドは、重複アカウンティングパケットを防止するために使用されます。
- 失効を有効にすると、MIP の失効が MAG とネゴシエートされて MIP バインディングが終了した場合に、MIP 登録の失効が可能になり、LMA は MAG に失効メッセージを送信できます。

P-GW PDN コンテキストの作成

P-GW PDN コンテキストおよびイーサネット インターフェイスを作成し、インターフェイスを設定済みのイーサネットポートにバインドするには、次の例を使用します。

```
configure
  context <pdn_context_name> -noconfirm
    interface <sgi_ipv4_interface_name>
      ip address <ipv4_address>
    interface <sgi_ipv6_interface_name>
      ipv6 address <address>
      end
```

P-GW サービス設定

手順

ステップ 1 「P-GW サービスの設定 （176 ページ）」の設定例を適用して、P-GW サービスを設定します。

ステップ 2 「固定 IP ルートの設定 （177 ページ）」の設定例を適用して、P-MIP サービングゲートウェイへの IP ルートを指定します。

P-GW サービスの設定

次の例を使用して、P-GW サービスを設定します。

```
configure
  context <pgw_context_name>
    pgw-service <pgw_service_name> -noconfirm
```

```
plmn id mcc <id> mnc <id>
associate lma-service <lma_service_name>
associate qci-qos-mapping <name>
authorize external
fqdn host <domain_name> realm <realm_name>
end
```

注：

- QCI-QoSマッピング設定はAAAコンテキストで作成されます。詳細については、「*QCI-QoS* マッピングの設定」の項を参照してください。
- 外部承認は、S6bインターフェイスを介して3GPP AAAサーバーによって実行されます。内部承認（APN）がデフォルトです。
- **fqdn host** コマンドは、S6bインターフェイスを介したP-GWと3GPP AAAサーバー間のメッセージで使用される、P-GWサービスの完全修飾ドメイン名を設定します。

固定 IP ルートの設定

P-GWとS-GW間のデータトラフィックのスタティックIPルートを設定するには、次の例に示すコマンドを使用します。

```
configure
  context <pgw_context_name>
    ipv6 route <ipv6_addr/prefix> next-hop <sgw_addr> interface
<pgw_sgw_intrfc_name>
    end
```

注：

- スタティック IP ルーティングは、ダイナミック ルーティング プロトコルを使用する設定には必要ありません。

P-GW PDN コンテキストの設定

次の例を使用して、IP プールと APN を設定し、PDN コンテキストのインターフェイスにポートをバインドします。

```
configure
  context <pdn_context_name> -noconfirm
    interface <pdn_sgi_ipv4_interface_name>
      ip address <ipv4_address>
      exit
    interface <pdn_sgi_ipv6_interface_name>
      ip address <ipv6_address>
      exit
    ip pool <name> range <start_address end_address> public <priority>
    ipv6 pool <name> range <start_address end_address> public <priority>
    subscriber default
    ip access-list <name>
      redirect css service <name> any
      permit any
```

```
    exit
  ipv6 access-list <name>
    redirect css service <name> any
    permit any
    exit
  aaa group default
    exit
  exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <pdn_ipv4_interface_name> <pdn_context_name>
  exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <pdn_ipv6_interface_name> <pdn_context_name>
  end
```

アクティブ課金サービス設定

アクティブ課金を有効化および設定するには、次の例を使用します。

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule>
        .
        .
      <rule>
      exit
    ruledef default
      ip any-match = TRUE
      exit
    ruledef icmp-pkts
      icmp any-match = TRUE
      exit
    ruledef qci3
       icmp any-match = TRUE
      exit
    ruledef static
      icmp any-match = TRUE
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    charging-action icmp
      billing-action egcdr
      exit
    charging-action qci3
```

```
      content-id <id>
      billing-action rf
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft packet-filter qci3
      exit
    charging-action static
      service-identifier <id>
      billing-action rf
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft packet-filter qci3
      exit
    packet-filter <packet_filter_name>
      ip remote-address = { <ipv4/ipv6_address> | <ipv4/ipv6_address/mask> }
      ip remote-port { = < port_number> | range <start_port_number> to
<end_port_number> }
      exit
    rulebase default
             exit
    rulebase <name>
      <rule_base>
        .
        .
      <rule_base>
      end
```

注：

- ルールベースとは、ルール定義および関連する課金アクションの集合です。
- 上記のように、複数のルール定義、課金アクション、およびルールベースを設定して、さまざまな課金シナリオをサポートできます。
- ルーティングルールや課金ルールの定義を作成および設定できます。作成できるルーティングルール定義の最大数は 256 です。課金ルール定義の最大数は 2048 です。
- 課金アクションは、ルール定義が一致したときに実行するアクションを定義します。



重要 専用ベアラーでアップリンクパケットを受信している場合は、専用ベアラーにインストールされているルールだけが照合されます。静的ルールは一致せず、一致しないパケットはドロップされます。

AAA とポリシーの設定

手順

ステップ 1 「AAA コンテキストの作成と設定 （180 ページ）」の設定例を適用して、AAA とポリシーのインターフェイスを設定します。

ステップ 2 「QCI-QoS マッピングの設定 （182 ページ）」の設定例を適用して、QCI から QoS へのマッピングを作成し、設定します。

AAA コンテキストの作成と設定

次の例を使用して、Diameter のサポートとポリシー制御を含む AAA コンテキストを作成および設定し、このコンテキストと PCRF 間のトラフィックをサポートしているインターフェイスにポートをバインドします。

```
configure
  context <aaa_context_name> -noconfirm
    interface <s6b_interface_name>
      ip address <ipv4_address>
      exit
    interface <gx_interface_name>
      ipv6 address <address>
      exit
    interface <gy_interface_name>
      ipv6 address <address>
      exit
    interface <rf_interface_name>
      ip address <ipv4_address>
      exit
    subscriber default
      exit
    ims-auth-service <gx_ims_service_name>
      p-cscf discovery table <#> algorithm round-robin
      p-cscf table <#> row-precedence <#> ipv6-address <pcrf_adr>
      policy-control
        diameter origin endpoint <gx_cfg_name>
        diameter dictionary <name>
        diameter host-select table <#> algorithm round-robin
       diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

        exit
      exit
    diameter endpoint <s6b_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv4_address>
      peer <s6b_cfg_name> realm <name> address <aaa_ipv4_addr>
      route-entry peer <s6b_cfg_name>
```

```
      exit
    diameter endpoint <gx_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv6_address>
      peer <gx_cfg_name> realm <name> address <pcrf_addr>
      route-entry peer <gx_cfg_name>
      exit
    diameter endpoint <gy_cfg_name>
      use-proxy
      origin realm <realm_name>
      origin host <name> address <gy_ipv6_address>
      connection retry-timeout <seconds>
      peer <gy_cfg_name> realm <name> address <ocs_ipv6_addr>
      route-entry peer <gy_cfg_name>
      exit
    diameter endpoint <rf_cfg_name>
      origin realm <realm_name>
      origin host <name> address <rf_ipv4_address>
      peer <rf_cfg_name> realm <name> address <ofcs_ipv4_addr>
      route-entry peer <rf_cfg_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s6b_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gx_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gy_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <rf_interface_name> <aaa_context_name>
    end
```

注：

- **ims-auth-service** の下の **p-cscf table** コマンドでも、PCRF に IPv4 アドレスを指定できます。
- S6b インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。
- Gx インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。
- Gy インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。

- Rf インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。

QCI-QoS マッピングの設定

QCI 値を作成し、適用可能な QoS パラメータにマッピングするには、次の例を使用します。

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
    qci 3 user-datagram dscp-marking <hex>
    qci 9 user-datagram dscp-marking <hex>
    end
```

注：

- 有効なライセンスキーがインストールされていない場合、P-GW は非標準の QCI 値をサポートしません。

  QCI 値 1 ～ 9 は、3GPP TS 23.203 で定義されている標準値です。P-GW はこれらの標準値をサポートします。

  3GPP リリース 8 以降では、通信事業者固有/非標準の QCI がサポートされ、キャリアは QCI 128- 254 を定義できます。

- 上記の設定は、1 つのキーワードの例のみを示しています。**qci** コマンドおよびサポートされるその他のキーワードの詳細については、『*Command Line Interface Reference*』の「*QCI - QOS Mapping Configuration Mode Commands*」[英語] の章を参照してください。

設定の確認と保存

Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

eHRPD ネットワークをサポートするスタンドアロン PMIP P-GW としてのシステムの設定

ここでは、テスト環境で eGTP P-GW として eHRPD のサポートを実行するようにシステムを設定するための一連の手順の概要と、関連する構成ファイルの例を示します。構成ファイルの完全な例については、付録「サンプル構成ファイル」を参照してください。ここでは次の内容について説明します。

- 必要な情報 （183 ページ）
- この設定が動作する仕組み （191 ページ）
- P-MIP P-GW（eHRPD）設定 （193 ページ）

必要な情報

以降のセクションでは、P-GW を設定し、ネットワーク上で動作させるために必要な最小限の情報について説明します。プロセスをより効率的なものにするため、システムを設定する前にこの情報を用意しておくことを推奨します。

ここでは説明していないその他の設定パラメータがあります。これらのパラメータは、主にネットワークでの P-GW の動作の微調整に対応します。これらのパラメータの詳細については、『*Command Line Interface Reference*』[英語] の該当するセクションを参照してください。

必要なローカルコンテキスト設定情報

次の表に、P-GW でローカルコンテキストを設定するために必要な情報を示します。

表 *22 :* ローカルコンテキストの設定に必要な情報

必要な情報	説明
管理インターフェイス コンフィギュレーション	
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	管理インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
セキュリティ管理者名	システムに対して完全な権限を持つセキュリティ管理者の名前。
セキュリティ管理者のパスワード	オープンパスワードまたは暗号化パスワードを使用できます。
リモートアクセスタイプ	システムへのアクセスに使用するリモートアクセスプロトコルのタイプ（SSH など）。

必要な P-GW コンテキスト設定情報

次の表に、P-GW で P-GW コンテキストを設定するために必要な情報を示します。

表 *23 : P-GW* コンテキストの設定に必要な情報

必要な情報	説明
P-GW コンテキスト名	システムが P-GW コンテキストを認識するために使用する 1 ～ 79 文字（英字または数字）の識別文字列。
アカウンティングポリシー名	システムがアカウンティングポリシーを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。アカウンティングポリシーは、Rf（オフライン課金）インターフェイスのパラメータを設定するために使用されます。
S2a インターフェイスの設定（HSGW 間）	
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
P-GW サービス設定	
P-GW サービス名	システムが P-GW サービスを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。 複数の P-GW サービスを使用する場合は、複数の名前が必要です。
PLMN ID	MCC 番号：PLMN の識別子のモバイル国コード（MCC）部分（100 ～ 999 の整数値）。 MNC 番号：PLMN の識別子のモバイルネットワークコード（MNC）部分（00 ー 999 の 2 桁または 3 桁の整数値）。
LMA サービスの設定	
LMA サービス名	システムが LMA サービスを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。

必要な PDN コンテキスト設定情報

次の表に、P-GW で PDN コンテキストを設定するために必要な情報を示します。

表 *24 : PDN* コンテキストの設定に必要な情報

必要な情報	説明
P-GW コンテキスト名	システムが P-GW コンテキストを認識するために使用する 1 ～ 79 文字（英字と数字）の識別文字列。
IP アドレスプールの設定	
IPv4アドレスプールの名前と範囲	システムが IPv4 プールを認識するために使用する 1 ～ 31 文字（英字数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義される IPv4 アドレスの範囲
IPv6アドレスプールの名前と範囲	システムが IPv6 プールを認識するために使用する 1 ～ 31 文字（英字数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義される IPv6 アドレスの範囲
アクセス制御リストの設定	
IPv4 アクセスリスト名	システムが IPv4 アクセスリストを認識するために使用する 1 ～ 47 文字（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。
IPv6 アクセスリスト名	システムが IPv6 アクセスリストを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。
拒否/許可タイプ	タイプは次のとおりです。 • any • ホスト IP アドレスによる • IP パケットによる • 送信元 ICMP パケットによる • 送信元 IP アドレスマスキングによる • TCP/UDP パケットによる

必要な情報	説明
アドレス再指定またはリダイレクトタイプ	タイプは次のとおりです。 • サーバーのアドレス再指定 • コンテキストのリダイレクト • CSS 配信シーケンスのリダイレクト • redirect css service コマンドで使用可能なキーワードとオプションについては、『Command Line Interface Reference』の • redirect nexthop
SGi インターフェイスの設定（IPv4 PDN へ/IPv4 PDN から）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
SGi インターフェイスの設定（IPv6 PDN へ/IPv6 PDN から）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。

必要な情報	説明
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。

必要な AAA コンテキスト設定情報

次の表に、P-GW で AAA コンテキストを設定するために必要な情報を示します。

表 *25 : AAA* コンテキストの設定に必要な情報

必要な情報	説明
Gx インターフェイスの設定（PCRF 対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
Gx Diameter エンドポイントの設定	
エンドポイント名	Gx Diameter エンドポイントの設定がシステムによって認識される 1 ～ 63 文字（英字や数字）の識別文字列。

必要な情報	説明
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Gx 送信元ホストがシステムによって認識される、1～255 文字（英字や数字）の識別文字列。
元のホストアドレス	Gx インターフェイスの IP アドレス。
ピア名	上述の Gx エンドポイント名。
ピアレルム名	上述の Gx 発信元レルム名。
ピアのアドレスとポート番号	PCRF の IP アドレスとポート番号。
ルートエントリピア	上述の Gx エンドポイント名。
S6b インターフェイスの設定（3GPP AAA 対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1～79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
S6b Diameter エンドポイントの設定	
エンドポイント名	S6b Diameter エンドポイント設定がシステムによって認識される 1 ー 63 文字（英字や数字）の識別文字列。

必要な情報	説明
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはす ての Diameter メッセージに存在し、通常は会社名またはサービス名で す。
発信元ホスト名	S6b 送信元ホストがシステムによって認識される、1 ～ 255 文字（英 や数字）の識別文字列。
元のホストアドレス	S6b インターフェイスの IP アドレス。
ピア名	上述の S6b エンドポイント名。
ピアレルム名	上述の S6b 発信元レルム名。
ピアのアドレスとポート番号	AAA サーバーの IP アドレスとポート番号。
ルートエントリピア	上述の S6b エンドポイント名。
Rf インターフェイスの設定（オフライン課金サーバーに対する）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（ 字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 ア レス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネ トが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカ ドが取り付けられているシャーシスロット番号とその後に続くカード の物理コネクタの番号によって識別されます。たとえば、ポート 17/ は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	管理インターフェイスから特定のネットワークへのスタティック IP ル トを設定するときに使用されます。
Rf Diameter エンドポイントの設定	
エンドポイント名	Rf Diameter エンドポイントの設定がシステムによって認識される 1 ～ 63 文字（英字や数字）の識別文字列。

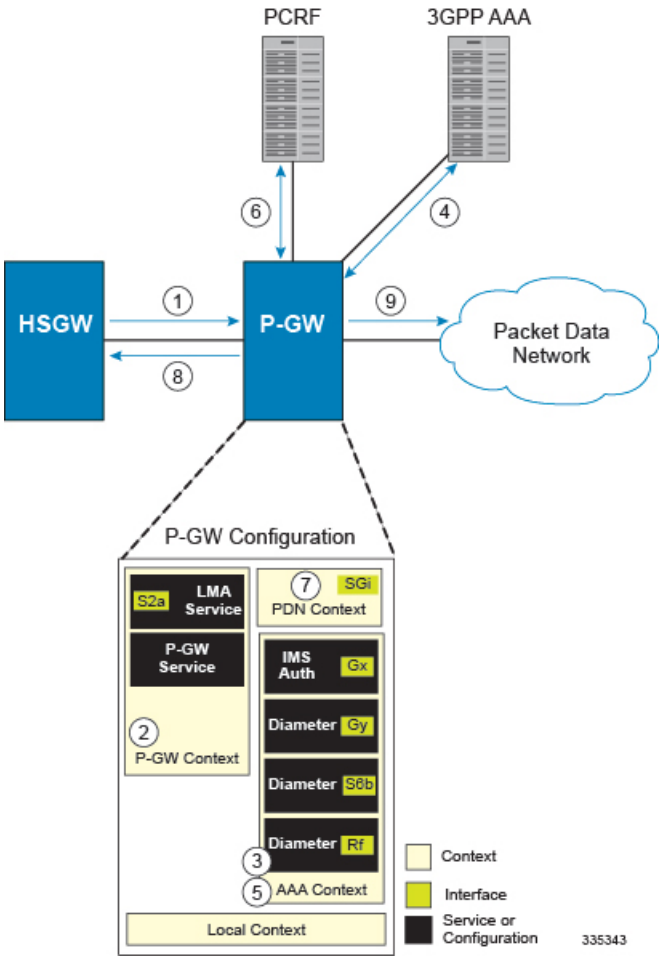
必要な情報	説明
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Rf送信元ホストがシステムによって認識される、1 ～ 255 文字（英字や数字）の識別文字列。
元のホストアドレス	Rf インターフェイスの IP アドレス。
ピア名	上述の Rf エンドポイント名。
ピアレルム名	上述の Rf 発信元レルム名。
ピアのアドレスとポート番号	OFCS の IP アドレスとポート番号。
ルートエントリピア	上述の Rf エンドポイント名。
Gy インターフェイスの設定（オンライン課金サーバー対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
Gy Diameter エンドポイントの設定	
エンドポイント名	Gy Diameter エンドポイントの設定がシステムによって認識される 1 ー 63 文字（英字や数字）の識別文字列。

必要な情報	説明
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Gy送信元ホストがシステムによって認識される、1 ～ 255 文字（英字数字）の識別文字列。
元のホストアドレス	Gy インターフェイスの IP アドレス。
ピア名	上述の Gy エンドポイント名。
ピアレルム名	上述の Gy 発信元レルム名。
ピアのアドレスとポート番号	OCS の IP アドレスとポート番号。
ルートエントリピア	上述の Gy エンドポイント名。

この設定が動作する仕組み

次の図と補足テキストは、GTP LTE ネットワークから発信されるサブスクライバコールを処理するために、単一の送信元と接続先のコンテキストを持つこの設定がシステムによってどのように使用されるかを示しています。

図 *11 : eHRPD* ネットワークをサポートする *PMIP P-GW* の要素



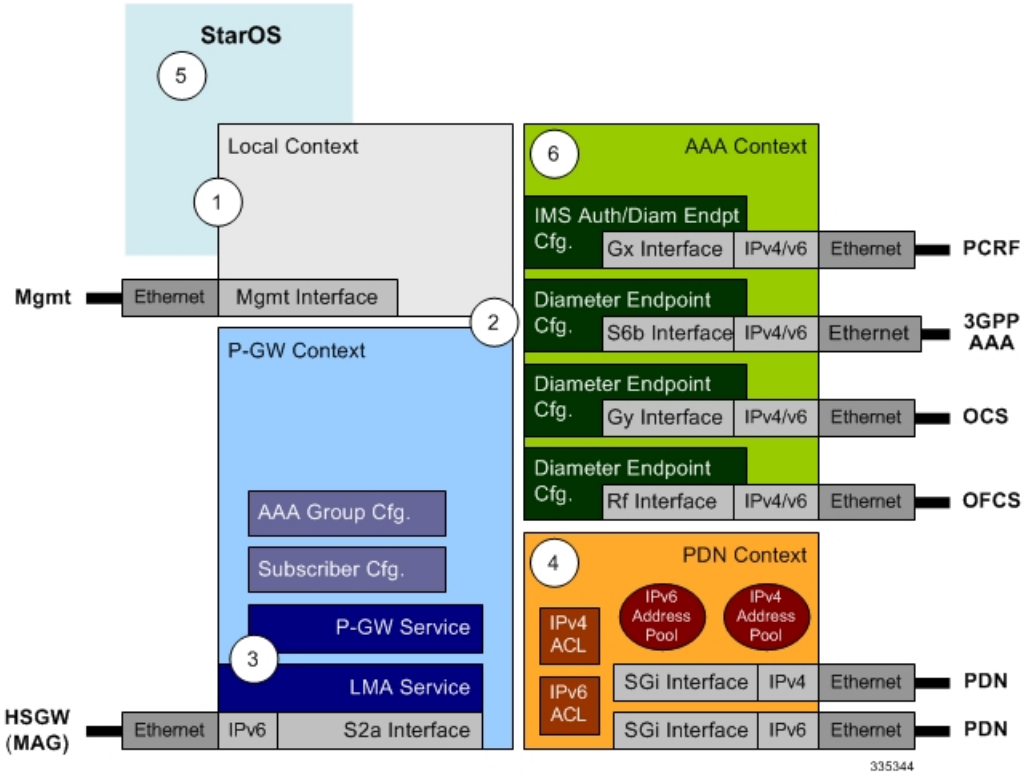
1. S-GW は、アクセスポイント名（APN）を含むセッション作成要求メッセージを P-GW に送信することにより、S5/S8 接続を確立します。
2. P-GW サービスは、セッションに AAA 機能を提供するために使用するコンテキストを決定します。このプロセスについては、『*System Administration Guide*』の「*Understanding the System Operation and Configuration*」の章にある「*How the System Selects Contexts*」の項で説明しています。
3. P-GW は、設定済みの Gx Diameter エンドポイントを使用して IP-CAN セッションを確立します。
4. P-GW は、IP-CAN セッションの確立を示すために CCRF に CC 要求（CCR）メッセージを送信し、PCRF は CC 応答（CCA）で確認応答します。
5. P-GW は APN 設定を使用して PDN コンテキストを選択します。選択した PDN コンテキストで設定された IP プールから IP アドレスが割り当てられます。
6. P-GW は、割り当てられたアドレスと追加情報を含むセッション作成応答メッセージで S-GW に応答します。

7. S5/S8 データプレーントンネルが確立され、P-GW は PDN との間でパケットを送受信できます。

P-MIP P-GW（eHRPD）設定

eHRPD ネットワーク環境でスタンドアロン P-MIP P-GW として動作するようにシステムを設定する場合は、次の図とその後の手順を確認してください。

図 *12 : P-MIP P-GW（eHRPD）設定*



手順

ステップ 1 『*System Administration Guide*』[英語] に記載されている設定例を適用して、PSC のアクティブ化などのシステム設定パラメータを設定します。

ステップ 2 「初期設定」に記載されている設定例を適用して、コンテキストやサービスの作成などの初期設定パラメータを設定します。

ステップ 3 システムを P-MIP P-GW として動作するように設定し、「P-GW サービス設定 （197 ページ）」に記載されている設定例を適用して、P-MIP インターフェイスや IP ルートなどの P-GW の基本的なパラメータを設定します。

ステップ 4 「P-GW PDN コンテキストの設定 （198 ページ）」の設定例を適用して、PDN コンテキストを設定します。

ステップ 5 「アクティブ課金サービス設定 （199 ページ）」の設定例を適用して、Gx インターフェイスのサポートのためのアクティブ課金サービスを有効にし、設定します。

ステップ 6 「AAA とポリシーの設定」の設定例を適用して、AAA コンテキストを作成し、AAA およびポリシーのパラメータを設定します。

ステップ 7 「設定の確認と保存 （203 ページ）」の手順に従って、設定を確認して保存します。

初期設定

手順

ステップ 1 「ローカルコンテキストの変更 （194 ページ）」の設定例を適用して、ローカルシステム管理パラメータを設定します。

ステップ 2 「P-MIP P-GW コンテキストの作成と設定 （195 ページ）」の設定例を適用して、P-GW サービスを配置したコンテキストを作成します。

ステップ 3 「P-GW コンテキストでの APN の作成と設定 （195 ページ）」の設定例を適用して、P-GW コンテキストで APN を作成および設定します。

ステップ 4 「P-GW コンテキストでの AAA グループの作成と設定 （196 ページ）」の設定例を適用して、P-GW コンテキストで AAA サーバーグループを作成および設定します。

ステップ 5 「LMA サービスの作成と設定 （197 ページ）」の設定例を適用して、新しく作成されたコンテキスト内に eGTP サービスを作成します。

ステップ 6 「P-GW PDN コンテキストの作成 （197 ページ）」の設定例を適用して、PDN へのインターフェイスが配置されるコンテキストを作成します。

ローカルコンテキストの変更

デフォルトサブスクライバを設定し、ローカルコンテキストでリモートアクセス機能を設定するには、次の例を使用します。

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
      exit
    server ftpd
      exit
    server telnetd
      exit
    subscriber default
      exit
    administrator <name> encrypted password <password> ftp
    ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
    exit
```

```
port ethernet <slot#/port#>
  no shutdown
  bind interface <lcl_cntxt_intrfc_name> local
  end
```

P-MIP P-GW コンテキストの作成と設定

次の例を使用して、P-GW コンテキストを作成し、S2a IPv6 インターフェイス（HSGW との間のデータトラフィック用）を作成し、S2a インターフェイスを設定済みのイーサネットポートにバインドします。

```
configure
  context <pgw_context_name> -noconfirm
    interface <s2a_interface_name> tunnel
      ipv6 address <address>
      tunnel-mode ipv6ip
        source interface <name>
        destination address <ipv4 or ipv6 address>
        exit
      exit
    policy accounting <rf_policy_name> -noconfirm
      accounting-level {level_type}
      accounting-event-trigger interim-timeout action stop-start
      operator-string <string>
      cc profile <index> interval <seconds>
      exit
    subscriber default
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s2a_interface_name> <pgw_context_name>
    end
```

注：

- S2a（P-GW から HSGW）インターフェイスは、IPv6 アドレスである必要があります。
- Rf（オフライン課金）インターフェイスのアカウンティングポリシーを設定します。アカウンティングレベルのタイプは、Flow、PDN、PDN-QCI、QCI、および Subscriber です。このコマンドの詳細については、『*Command Line Interface Reference*』の「*Accounting Profile Configuration Mode Commands*」の章を参照してください。

P-GW コンテキストでの APN の作成と設定

次の設定を使用して、APN を作成します。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      associate accounting-policy <rf_policy_name>
      ims-auth-service <gx_ims_service_name>
```

```
aaa group <rf-radius_group_name>
dns primary <ipv4_address>
dns secondary <ipv4_address>
ip access-group <name> in
ip access-group <name> out
mediation-device context-name <pgw_context_name>
ip context-name <pdn_context_name>
ipv6 access-group <name> in
ipv6 access-group <name> out
active-charging rulebase <name>
end
```

注：

- IMS 承認サービスは、AAA コンテキストで作成および設定されます。
- 複数の APN を、異なるドメイン名をサポートするように設定できます。
- 事前設定済みのアカウンティングポリシーをこの APN に関連付けるには、associate accounting-policy コマンドを使用します。アカウンティングポリシーは、P-GW コンテキストで設定されます。P-MIP P-GW コンテキストの作成と設定 （195 ページ） その例があります。

P-GW コンテキストでの AAA グループの作成と設定

RADIUS および Rf アカウンティングをサポートする AAA グループを作成および設定するには、次の例を使用します。

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
    aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
```

LMA サービスの作成と設定

LMA サービスを作成するには、次の設定例を使用します。

```
configure
   context <pgw_context_name>
      lma-service <lma_service_name> -noconfirm
         no aaa accounting
         revocation enable
         bind address <s2a_ipv6_address>
         end
```

注：

- **no aaa acounting** コマンドは、重複アカウンティングパケットを防止するために使用されます。
- 失効を有効にすると、MIP の失効が MAG とネゴシエートされて MIP バインディングが終了した場合に、MIP 登録の失効が可能になり、LMA は MAG に失効メッセージを送信できます。

P-GW PDN コンテキストの作成

P-GW PDN コンテキストおよびイーサネット インターフェイスを作成するには、次の例を使用します。

```
configure
   context <pdn_context_name> -noconfirm
      interface <sgi_ipv4_interface_name>
         ip address <ipv4_address>
         exit
      interface <sgi_ipv6_interface_name>
         ipv6 address <address>
         end
```

P-GW サービス設定

手順

ステップ 1 P-GW サービスの設定 （197 ページ）の設定例を適用して、P-GW サービスを設定します。

ステップ 2 固定 IP ルートの設定 （198 ページ）の設定例を適用して、HRPD サービングゲートウェイへの IP ルートを指定します。

P-GW サービスの設定

次の例を使用して、P-GW サービスを設定します。

```
configure
   context <pgw_context_name>
```

```
pgw-service <pgw_service_name> -noconfirm
  associate lma-service <lma_service_name>
  associate qci-qos-mapping <name>
  authorize external
  fqdn host <domain_name> realm <realm_name>
  plmn id mcc <id> mnc <id>
  end
```

注：

- QCI-QoS マッピング設定は AAA コンテキストで作成されます。詳細については、QCI-QoS マッピングの設定 （202 ページ）を参照してください。
- 外部承認は、S6b インターフェイスを介して 3GPP AAA サーバーによって実行されます。内部承認（APN）がデフォルトです。
- **fqdn host** コマンドは、S6b インターフェイスを介した P-GW と 3GPP AAA サーバー間のメッセージで使用される、P-GW サービスの完全修飾ドメイン名を設定します。

固定 IP ルートの設定

P-GW と HSGW 間のデータトラフィックのスタティック IP ルートを設定するには、次の例に示すコマンドを使用します。

```
configure
  context <pgw_context_name>
    ipv6 route <ipv6_addr/prefix> next-hop <hsgw_addr> interface
<pgw_hsgw_intrfc_name>
    end
```

注：

- スタティック IP ルーティングは、ダイナミック ルーティング プロトコルを使用する設定には必要ありません。

P-GW PDN コンテキストの設定

IP プールと IP アクセス制御リスト（ACL）を設定し、ポートを PDN コンテキストのインターフェイスにバインドするには、次の例に示すコマンドを使用します。

```
configure
  context <pdn_context_name> -noconfirm
    ip pool <name> range <start_address end_address> public <priority>
    ipv6 pool <name> range <start_address end_address> public <priority>
    subscriber default
      exit
    ip access-list <name>
      redirect css service <name> any
      permit any
      exit
    ipv6 access-list <name>
      redirect css service <name> any
      permit any
```

```
      exit
    aaa group default
      exit
        exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <pdn_sgi_ipv4_interface_name> <pdn_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <pdn_sgi_ipv6_interface_name> <pdn_context_name>
    end
```

アクティブ課金サービス設定

アクティブ課金を有効化および設定するには、次の例を使用します。

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule_definition>
        .
        .
      <rule_definition>
      exit
    ruledef <name>
      <rule_definition>
        .
        .
      <rule_definition>
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    packet-filter <packet_filter_name>
      ip remote-address = { < ipv4/ipv6_address> | <ipv4/ipv6_address/mask>
}
      ip remote-port { = < port_number> | range <start_port_number> to
<end_port_number> }
      exit
    rulebase default
```

```
exit
rulebase <name>
  <rule_base>
    .
    .
  <rule_base>
  end
```

注：

- ルールベースとは、ルール定義および関連する課金アクションの集合です。
- 最適化モードでのアクティブ課金により、ACS マネージャの一部ではなく、セッションマネージャの一部としてサービスを利用できるようになります。
- 上記のように、複数のルール定義、課金アクション、およびルールベースを設定して、さまざまな課金シナリオをサポートできます。
- ルーティングルールや課金ルールの定義を作成および設定できます。作成できるルーティングルール定義の最大数は 256 です。課金ルール定義の最大数は 2048 です。
- 課金アクションは、ルール定義が一致したときに実行するアクションを定義します。



重要 専用ベアラーでアップリンクパケットを受信している場合は、専用ベアラーにインストールされているルールだけが照合されます。静的ルールは一致せず、一致しないパケットはドロップされます。

AAA とポリシーの設定

手順

ステップ 1 「AAA コンテキストの作成と設定 （200 ページ）」の設定例を適用して、AAA とポリシーのインターフェイスを設定します。

ステップ 2 「QCI-QoS マッピングの設定 （202 ページ）」の設定例を適用して、QCI から QoS へのマッピングを作成し、設定します。

AAA コンテキストの作成と設定

次の例を使用して、Diameter サポートとポリシー制御を含む AAA コンテキストを作成および設定し、このコンテキスト、PCRF、3GPP AAA サーバー、オンライン課金サーバー、およびオフライン課金サーバー間のトラフィックをサポートするインターフェイスにポートをバインドします。

```
configure
  context <aaa_context_name> -noconfirm
```

```
interface <s6b_interface_name>
  ip address <ipv4_address>
  exit
interface <gx_interface_name>
  ipv6 address <address>
  exit
interface <rf_interface_name>
  ip address <ipv4_address>
  exit
interface <gy_interface_name>
  ipv6 address <address>
  exit
subscriber default
  exit
ims-auth-service <gx_ims_service_name>
  p-cscf discovery table <#> algorithm round-robin
  p-cscf table <#> row-precedence <#> ipv6-address <pcrf_adr>
  policy-control
    diameter origin endpoint <gx_cfg_name>
    diameter dictionary <name>
    diameter host-select table <#> algorithm round-robin
    diameter host-select row-precedence <#> table <#> host
<gx_cfg_name>
    exit
  exit
diameter endpoint <s6b_cfg_name>
  origin realm <realm_name>
  origin host <name> address <aaa_ctx_ipv4_address>
  peer <s6b_cfg_name> realm <name> address <aaa_ip_addr>
  route-entry peer <s6b_cfg_name>
  exit
diameter endpoint <gx_cfg_name>
  origin realm <realm_name>
  origin host <name> address <aaa_context_ip_address>
  peer <gx_cfg_name> realm <name> address <pcrf_ipv6_addr>
  route-entry peer <gx_cfg_name>
  exit
diameter endpoint <rf_cfg_name>
  origin realm <realm_name>
  origin host <name> address <aaa_ip_address>
  peer <rf_cfg_name> realm <name> address <ofcs_ip_addr>
  route-entry peer <rf_cfg_name>
  exit
diameter endpoint <gy_cfg_name>
  use-proxy
  origin realm <realm_name>
  origin host <name> address <aaa_ip_address>
  connection retry-timeout <seconds>
  peer <gy_cfg_name> realm <name> address <ocs_ip_addr>
  route-entry peer <gy_cfg_name>
  exit
```

```
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s6b_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gx_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gy_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <rf_interface_name> <aaa_context_name>
    end
```

注：

- **ims-auth-service** の下の **p-cscf table** コマンドでも、PCRF に IPv4 アドレスを指定できます。
- S6b インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。
- Gx インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。
- Gy インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。
- Rf インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。

QCI-QoS マッピングの設定

QCI 値を作成し、適用可能な QoS パラメータにマッピングするには、次の例を使用します。

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
    qci 3 user-datagram dscp-marking <hex>
    qci 9 user-datagram dscp-marking <hex>
    end
```

注：

- 有効なライセンスキーがインストールされていない場合、P-GW は非標準の QCI 値をサポートしません。

  QCI 値 1 ～ 9 は、3GPP TS 23.203 で定義されている標準値です。P-GW はこれらの標準値をサポートします。

3GPP リリース 8 以降では、通信事業者固有/非標準の QCI がサポートされ、キャリアは QCI 128- 254 を定義できます。

- 上記の設定は、1 つのキーワードの例のみを示しています。**qci** コマンドおよびサポートされるその他のキーワードの詳細については、『*Command Line Interface Reference*』の「*QCI - QOS Mapping Configuration Mode Commands*」[英語] の章を参照してください。

設定の確認と保存

EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

P-GW でのオプション機能の設定

この項の設定例はオプションであり、稼働中のネットワークでの P-GW の最も一般的な使用に対応するために提供されています。これらの例の目的は、テスト用の基本設定を提供することです。

S5 インターフェイスでの ACL ベースのノード間 IP セキュリティの設定

この項の設定例では、S5 インターフェイス上で IKEv2/IPSec ACL ベースのノード間トンネルエンドポイントを作成します。



重要 IP セキュリティ機能を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

暗号アクセス制御リストの作成および設定

次に、暗号 ACL（アクセス制御リスト）を設定する例を示します。この ACL では、IPSec トンネルを介したサブスクライバ データ パケットのルーティングに使用される一致基準が定義されます。

```
configure
  context <pgw_context_name> -noconfirm
    ip access-list <acl_name>
      permit tcp host <source_host_address> host <dest_host_address>
      end
```

注：

- この例の **permit** コマンドは、指定の送信元ホストの IPv4 アドレスを持つサーバーから、指定の宛先ホストの IPv4 アドレスを持つサーバーに、IPv4 トラフィックをルーティングします。

IPSec トランスフォームセットの作成および設定

IPSec トランスフォームセットの設定例を次に示します。このトランスフォームセットは、インターフェイス上のデータを保護するために使用されるプロトコルを決定するセキュリティアソシエーションを定義するために使用されます。

```
configure
  context <pgw_context_name> -noconfirm
    ipsec transform-set <ipsec_transform-set_name>
      encryption aes-cbc-128
      group none
      hmac sha1-96
      mode tunnel
      end
```

注：

- 暗号化アルゴリズム **aes-cbc-128**（Advanced Encryption Standard 暗号ブロック連鎖）は、システムに設定されている IPSec トランスフォームセットのデフォルトアルゴリズムです。
- **group none** コマンドは、暗号強度を含めず、Perfect Forward Secrecy を無効にすることを指定します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。
- **hmac** コマンドは、Encapsulating Security Payload（ESP）整合性アルゴリズムを設定します。**sha1-96** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。
- **mode tunnel** コマンドは、IP ヘッダーを含む IPSec ヘッダーでパケット全体をカプセル化するように指定します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。

IKEv2 トランスフォームセットの作成および設定

次の例では、IKEv2 トランスフォームセットを設定します。

```
configure
  context <pgw_context_name> -noconfirm
    ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
      end
```

注：

- 暗号化アルゴリズム **aes-cbc-128**、すなわち Advanced Encryption Standard 暗号ブロック連鎖は、システムに設定されている IKEv2 トランスフォームセットのデフォルトアルゴリズムです。
- **group 2** コマンドは、中程度のセキュリティを示すグループ 2 として Diffie-Hellman アルゴリズムを指定します。Diffie-Hellman アルゴリズムは、暗号指数の強度を制御します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。
- **hmac** コマンドは、Encapsulating Security Payload（ESP）整合性アルゴリズムを設定します。**sha1-96** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。
- **lifetime** コマンドは、セキュリティキーが存在できる時間を秒単位で設定します。
- **prf** コマンドは、秘密キーがないとランダムなビットストリングと区別できないスビットストリングを生成する IKE 疑似乱数関数を設定します。**sha1** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。
- NATT を使用した IKEv2 ACL モードはサポートされません。
- VRF を使用した IKEv2 はサポートされていません。

クリプトマップの作成と設定

次の例では、IKEv2 クリプトマップを設定します。

```
configure
  context <pgw_context_name>
    crypto map <crypto_map_name> ikev2-ipv4
      match address <acl_name>
      peer <ipv4_address>
      authentication local pre-shared-key key <text>
      authentication remote pre-shared-key key <text>
      ikev2-ikesa transform-set list  <name1> . . . name6>
      payload <name> match ipv4
        lifetime <seconds>
        ipsec transform-set list <name1> . . . <name4>
        exit
      exit
    interface <s5_intf_name>
      ip address <ipv4_address>
      crypto-map <crypto_map_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
```

```
bind interface <s5_intf_name> <pgw_context_name>
end
```

注：

- この例で使用するクリプトマップのタイプは、IPv4 アドレッシングの場合は IKEv2/IPv4 です。IKEv2/IPv6 クリプトマップも IPv6 アドレッシングに使用できます。
- **ipsec transform-set list** コマンドは、最大 4 つの IPsec トランスフォームセットを指定します。

APN を緊急として設定

このセクションの設定例では、VoLTE ベース E911 サポート用の緊急 APN を設定します。

APN コンフィギュレーション モードで、緊急 APN の名前を指定し、緊急非アクティブタイムアウトを次のように設定します。APN に P-CSCF FQDN サーバー名を設定することもできます。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      emergency-apn
      timeout emergency-inactivity <seconds>
      p-cscf fqdn <fqdn>
      end
```

注：

- デフォルトでは、APN は非緊急と見なされます。
- **timeout emergency-inactivity** コマンドは、緊急セッションでの非アクティブな状態をチェックするためのタイムアウト期間（秒単位）を指定します。<*seconds*> は 1 ～ 3600 の整数にする必要があります。
- デフォルトでは、緊急非アクティブタイムアウトは無効（0）になっています。
- **p-cscf fqdn** コマンドは、APN の P-CSCF FQDN サーバー名を設定します。<*fqdn*> は、1 ～ 256 文字の長さの文字列である必要があります。
- P-CSCF FQDN は、CLI で設定された P-CSCF IPv4 および IPv6 アドレスよりも重要です。

共通ゲートウェイ アクセス サポートの設定

この項では、同じ IP アドレッシング動作とサブスクライバ承認のための 3GPP AAA へのアクセスを使用して、複数のアクセスネットワーク（CDMA、eHRPD、および LTE）に加え、国際ローミング用の GSM/UMTS をサポートするためのいくつかの高度な機能設定について説明します。静的 IP アドレッシングを使用するサブスクライバは、アクセステクノロジーに関係なく、同じ IP アドレスを取得できます。

この設定は、HA、P-GW、および GGSN の論理サービスをサポートする共通ゲートウェイに 3Gおよび4Gアクセステクノロジーを組み合わせた統合ソリューションであり、サブスクライバは利用可能なアクセステクノロジーに関係なく、同じユーザーエクスペリエンスを得ることができます。



重要 この機能はライセンス対応のサポートであり、この設定に関連する一部のコマンドを使用するには、機能固有のセッションライセンスをシステムにインストールする必要がある場合があります。

以下の手順は、『*System Administration Guide*』で説明されているシステムレベルの設定と P-GW サービスがすでに設定済みであることを前提としています。

S6b およびその他の高度な機能を設定するには、次の手順を実行します。

1. Diameter エンドポイントの設定 （207 ページ）の設定例を適用して、Diameter エンドポイントを設定します。
2. AAA グループの設定 （207 ページ）の設定例を適用して、AAA グループを作成または変更します。
3. S6b を介した承認の設定 （208 ページ）の設定例を適用して、HSS を使用した承認を許可するように P-GW サービスを変更します。
4. オプションです。DNS クライアント設定 （208 ページ）の設定例を適用して、DNS クライアントパラメータを作成し、関連付けます。
5. オプションです。重複コールの受け入れ設定 （209 ページ）の設定例を適用して、同じ IP アドレスで受信した場合に重複コールを受け入れるように P-GW サービスを変更します。
6. 共通ゲートウェイ アクセス サポートの設定の確認 （209 ページ）の手順に従って、S6b の設定を確認します。
7. 「設定の確認と保存」の章の説明に従って、設定を保存します。

Diameter エンドポイントの設定

次の例を使用して、Diameter エンドポイントを設定します。

```
configure
  context <pgw_ctxt_name> -noconfirm
    diameter endpoint <s6b_endpoint_name>
      origin host <host_name> address <ip_address>
     peer <peer_name> realm <realm_name> address <ip_address> port <port_num>

    end
```

注：

- *<pgw_ctxt_name>* は、システム上の P-GW サービスを含むコンテキストの名前です。

AAA グループの設定

この機能に関して AAA グループを作成/変更するには、次の例を使用します。

```
configure
  context <fa_ctxt_name>
    aaa group <aaa_grp_name>
      diameter authentication dictionary aaa-custom15
        diameter authentication endpoint <s6b_endpoint_name>
        diameter authentication server <server_name> priority <priority>

        end
```

注：

- <*s6b_endpoint_name*> は、既存の Diameter エンドポイントの名前です。

S6b を介した承認の設定

3GPP AAA/HSS を使用した P-GW サービスで S6b インターフェイスを有効にするには、次の例を使用します。

```
configure
  context <pgw_ctxt_name>
    pgw-service <pgw_svc_name>
      plmn id mcc <number> mnc <number>
      authorize-with-hss
      fqdn host <host_name> realm <realm_name>
      end
```

注：

- <*pgw_svc_name*> には、システムで作成済みの P-GW サービス名を指定します。

DNS クライアント設定

3GPP AAA/HSS を使用した P-GW サービスで S6b インターフェイスを有効にするには、次の例を使用します。

```
configure
  context <pgw_ctxt_name>
    ip domain-lookup
    ip name-servers <ip_address/mask>
    dns-client <dns_name>
      bind address <ip_address>
      resolver retransmission-interval <duration>
      resolver number-of-retries <retrie>
      cache ttl positive <ttl_value>
      exit
    pgw-service <pgw_svc_name>
      default dns-client context
      end
```

注：

- <*pgw_svc_name*> には、システムで作成済みの P-GW サービス名を指定します。

重複コールの受け入れ設定

同じ IP アドレスの要求を含む重複セッションコールを受け入れるように P-GW サービスを設定するには、次の例に示すコマンドを使用します。

```
configure
  context <pgw_ctxt_name>
    pgw-service <pgw_svc_name>
      newcall duplicate-subscriber-requested-address accept
      end
```

注：

- <*pgw_svc_name*> には、システムで作成済みの P-GW サービス名を指定します。

共通ゲートウェイ アクセス サポートの設定の確認

1. EXEC モードで次のコマンドを入力して、共通ゲートウェイ アクセス サポートが正しく設定されていることを確認します。

   ```
   show pgw-service all
   ```

   このコマンドの出力は、次に示すサンプルのようになります。この例では、*PGW1* という名前の P-GW サービスが、*vpn1* コンテキストで設定されています。

   ```
   Service name:                  pgw1
   Context:                       cn1
   Associated PGW svc:            None
   Associated GTPU svc:           None
   Accounting Context Name:       cn1
   dns-client Context Name:       cn1
   Authorize:                     hss
   Fqdn-name:                     xyz.abc@starent.networks.com
   Bind:                          Not Done
   Local IP Address:              0.0.0.0          Local IP Port:
     2123
   Self PLMN:                     Not defined
   Retransmission Timeout:        5 (secs)
   ```

S5 インターフェイスでの動的なノード間 IP セキュリティの設定

この項の設定例では、S5 インターフェイス上で IPSec/IKEv2 動的ノード間トンネルエンドポイントを作成します。



重要 IP セキュリティ機能を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

IPSec トランスフォームセットの作成および設定

IPSec トランスフォームセットの設定例を次に示します。このトランスフォームセットは、インターフェイス上のデータを保護するために使用されるプロトコルを決定するセキュリティアソシエーションを定義するために使用されます。

```
configure
  context <pgw_context_name> -noconfirm
    ipsec transform-set <ipsec_transform-set_name>
      encryption aes-cbc-128
      group none
      hmac sha1-96
      mode tunnel
      end
```

注：

- 暗号化アルゴリズム **aes-cbc-128**（Advanced Encryption Standard 暗号ブロック連鎖）は、システムに設定されている IPSec トランスフォームセットのデフォルトアルゴリズムです。
- **group none** コマンドは、暗号強度を含めず、Perfect Forward Secrecy を無効にすることを指定します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。
- **hmac** コマンドは、Encapsulating Security Payload（ESP）整合性アルゴリズムを設定します。**sha1-96** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。
- **mode tunnel** コマンドは、IP ヘッダーを含む IPSec ヘッダーでパケット全体をカプセル化するように指定します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。

IKEv2 トランスフォームセットの作成および設定

次の例では、IKEv2 トランスフォームセットを設定します。

```
configure
  context <pgw_context_name> -noconfirm
    ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
      end
```

注：

- 暗号化アルゴリズム **aes-cbc-128**、すなわち Advanced Encryption Standard 暗号ブロック連鎖は、システムに設定されている IKEv2 トランスフォームセットのデフォルトアルゴリズムです。

- **group 2** コマンドは、中程度のセキュリティを示すグループ 2 として Diffie-Hellman アルゴリズムを指定します。Diffie-Hellman アルゴリズムは、暗号指数の強度を制御します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。
- **hmac** コマンドは、Encapsulating Security Payload（ESP）整合性アルゴリズムを設定します。**sha1-96** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。
- **lifetime** コマンドは、セキュリティキーが存在できる時間を秒単位で設定します。
- **prf** コマンドは、秘密キーがないとランダムなビットストリングと区別できないビットストリングを生成する IKE 疑似乱数関数を設定します。**sha1** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。

暗号テンプレートの作成と設定

次の例では、IKEv2 暗号テンプレートを設定します。

```
configure
  context <pgw_context_name> -noconfirm
    crypto template <crypto_template_name> ikev2-dynamic
      ikev2-ikesa transform-set list <name1> . . . <name6>
      ikev2-ikesa rekey
      payload <name> match childsa match ipv4
        ipsec transform-set list <name1> . . . <name4>
        rekey
        end
```

注：

- **ikev2-ikesa transform-set list** コマンドは、最大 6 つの IKEv2 トランスフォームセットを指定します。
- **ipsec transform-set list** コマンドは、最大 4 つの IPsec トランスフォームセットを指定します。

S5 IP アドレスの暗号テンプレートへのバインド

次の例は、暗号テンプレートへの S5 インターフェイスのバインドを設定します。

```
configure
  context <pgw_ingress_context_name> -noconfirm
    gtpu-service <gtpu_ingress_service_name>
      bind ipv4-address <s5_interface_ip_address> crypto-template
<sgw_s5_crypto_template>
      exit
    egtp-service <egtp_ingress_service_name>
      interface-type interface-pgw-ingress
      associate gtpu-service <gtpu_ingress_service_name>
```

```
      gtpc bind ipv4-address <s5_interface_ip_address>
      exit
    pgw-service <pgw_service_name> -noconfirm
      plmn id mcc <id> mnc <id> primary
      associate egtp-service <egtp_ingress_service_name>
      end
```

注：

- GTP-U および eGTP サービス設定の **bind** コマンドは、**ipv6-address** コマンドを使用して IPv6 アドレスとして指定することもできます。

セッション作成要求処理時のガードタイマーの設定

P-GW には、60 秒にハードコードされている既存のタイマー「session setup-timeout」があり、セッション作成のガードタイマーとして使用されます。このタイマーは、すべての APN に使用され、セッション作成のためにセッション作成要求を受信すると開始されます。

内部または外部の処理の問題や、Gx/Gy などの外部インターフェイスでの遅延により、セッション作成要求の処理が、エンドツーエンドのコールセットアップで予想される時間よりも長く実行される場合があります。タイマーの期限が切れたときにセッションの処理が完了していない場合、セッション作成要求の処理が停止し、P-GW は、対応する他のセッション（Gx/Gy など）をすべて停止して、内部のクリーンアップを行います。P-GW は、セッション作成失敗応答で応答し、S-GW で使用可能なリソースがないことを示します。遅延がない正常の場合は、セッション作成応答の送信中にタイマーが停止します。

以前にハードコードされたデフォルトのセッション セットアップ タイムアウト値である 60 秒を、設定可能な値で上書きできるようにする新しいCLI コマンドが導入されました。これは、エンドツーエンドのコールセットアップ時間に関してP-GWでコールセットアップ時間を微調整するのに役立ちます。

セッション タイムアウトの設定

次の設定例は、P-GW セッションのセットアップタイムアウトを設定可能にしています。

```
configure
  context  context_name
    pgw-service  service_name
      setup-timeout  timer-value
      [  default | no ] setup-timeout
      end
```

注：

- **setup-timeout**：セッションのセットアップタイムアウト時間を秒単位で指定します。タイマーが期限切れになる前に P-GW がセッション作成要求メッセージを処理できる場合、P-GW はタイマーを停止し、「成功」セッション作成応答を送信します。

  timer_value は、1 ー 120 の整数である必要があります。

  デフォルト：60 秒

- **default**：デフォルト値は 60 秒です。値が設定されていない場合、P-GW サービスはタイマーをデフォルト値に設定します。
- **no**：タイマーをデフォルト値の 60 秒に設定します。

GTP エコータイマーの設定

ASR 5500 P-GW の GTP エコー タイマーは、2 つの異なるタイプのパス管理（デフォルトとダイナミック）をサポートするように設定できます。このタイマーは、GTP-C と GTP-U の両方またはそのいずれかで設定できます。

デフォルトの GTP エコータイマーの設定

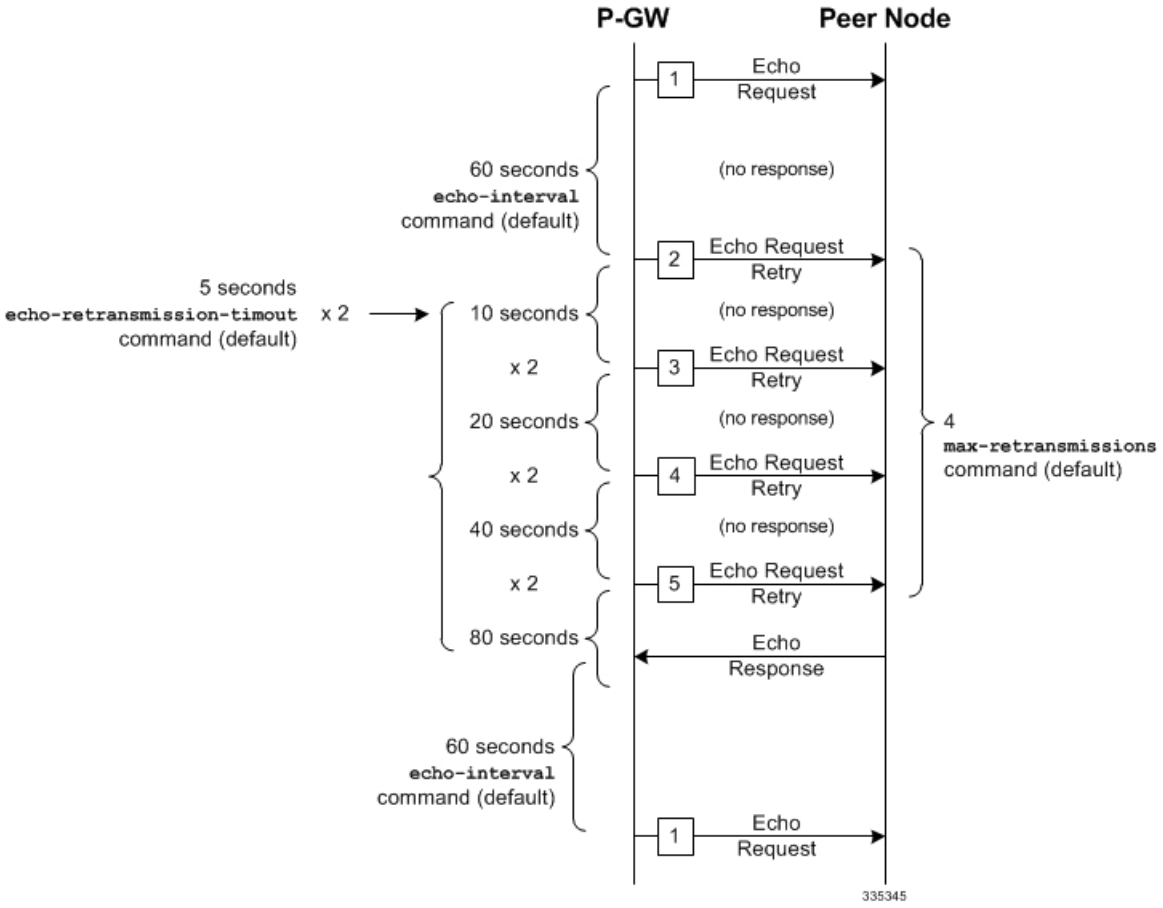
次の例では、デフォルトの eGTP-C および GTP-U インターフェイスのエコータイマーの設定について説明します。

eGTP-C

```
configure
     configure
          context <context_name>
               egtp-service <egtp_service_name>
                    gtpc echo-interval <seconds>
                    gtpc echo-retransmission-timeout <seconds>
                    gtpc max-retransmissions <num>
                    end
```

注：

- 次の図は、上記の例の 3 つの **gtpc** コマンドのデフォルト設定を使用した障害発生と回復シナリオを示しています。



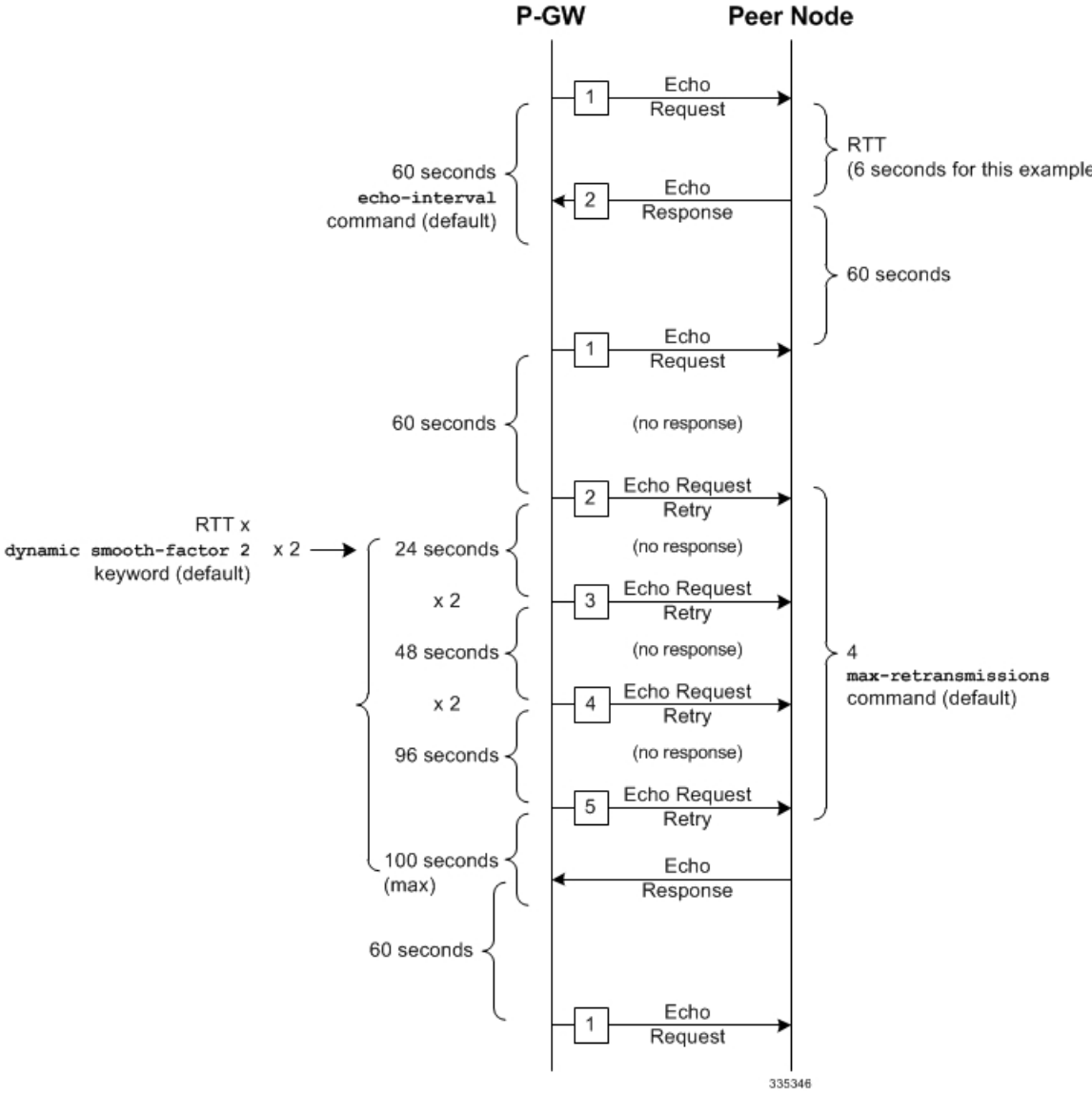
- 乗数（x2）はシステムのコードであり、設定できません。

GTP-U

```
configure
  configure
    context <context_name>
      gtpu-service <gtpu_service_name>
        echo-interval <seconds>
        echo-retransmission-timeout <seconds>
        max-retransmissions <num>
        end
```

注：

- 次の図は、上記の例にある 3 つの GTP-U コマンドのデフォルト設定を使用した障害発生と回復シナリオを示しています。



• 乗数（x2）はシステムのコードであり、設定できません。

動的 GTP エコータイマーの設定

次の例では、動的な eGTP-C および GTP-U インターフェイスのエコータイマーの設定について説明します。

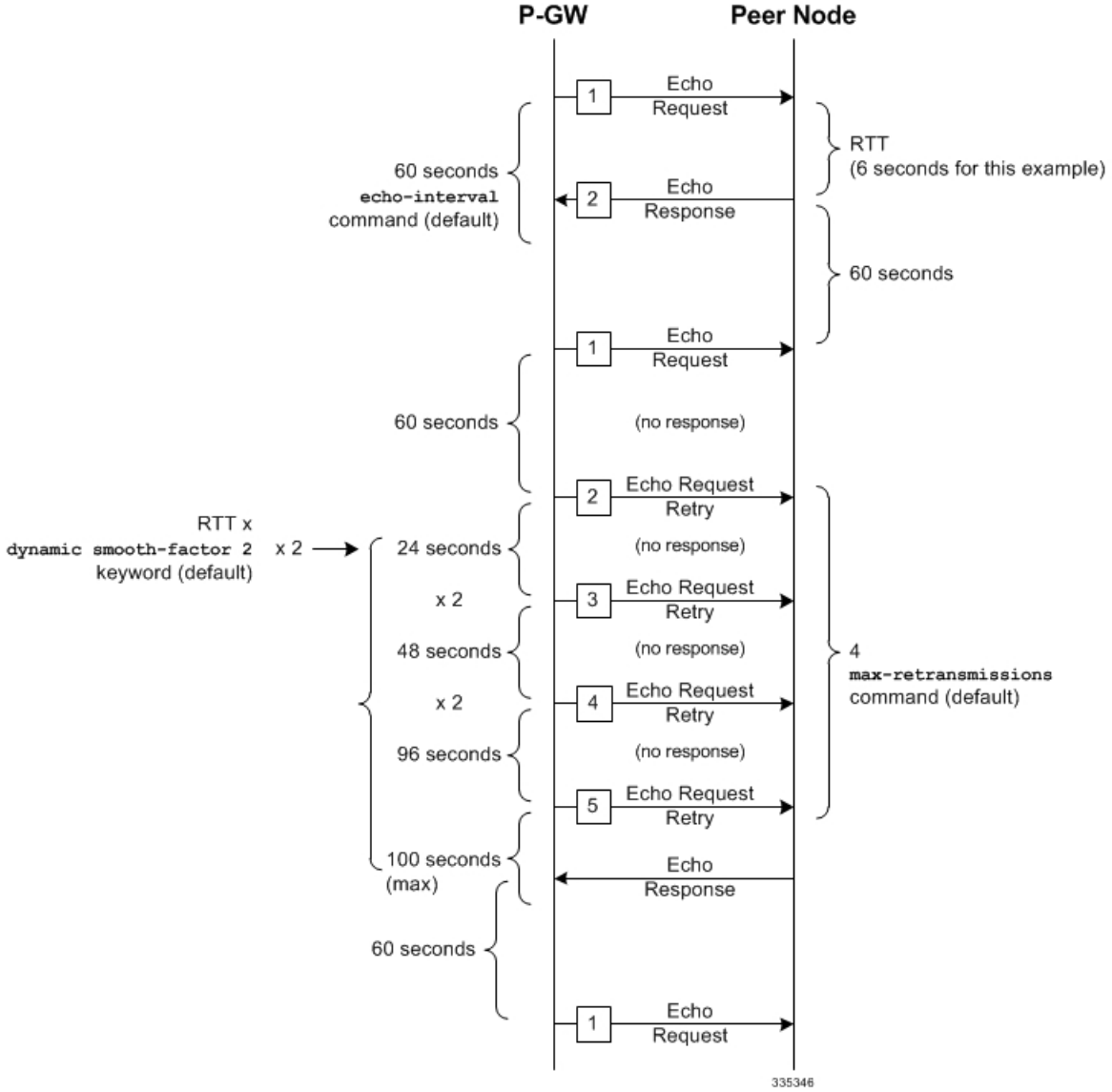
eGTP-C

```
configure
  configure
    context <context_name>
      egtp-service <egtp_service_name>
        gtpc echo-interval <seconds> dynamic smooth-factor <multiplier>
        gtpc echo-retransmission-timeout <seconds>
```

```
gtpc max-retransmissions <num>
end
```

注：

- 次の図は、上記の 3 つの **gtpc** コマンドのデフォルト設定と、6 秒のラウンドトリップタイマー（RTT）の例を使用した障害発生と回復のシナリオを示しています。



- 乗数（x2）と最大 100 秒はシステムコードであり、設定できません。

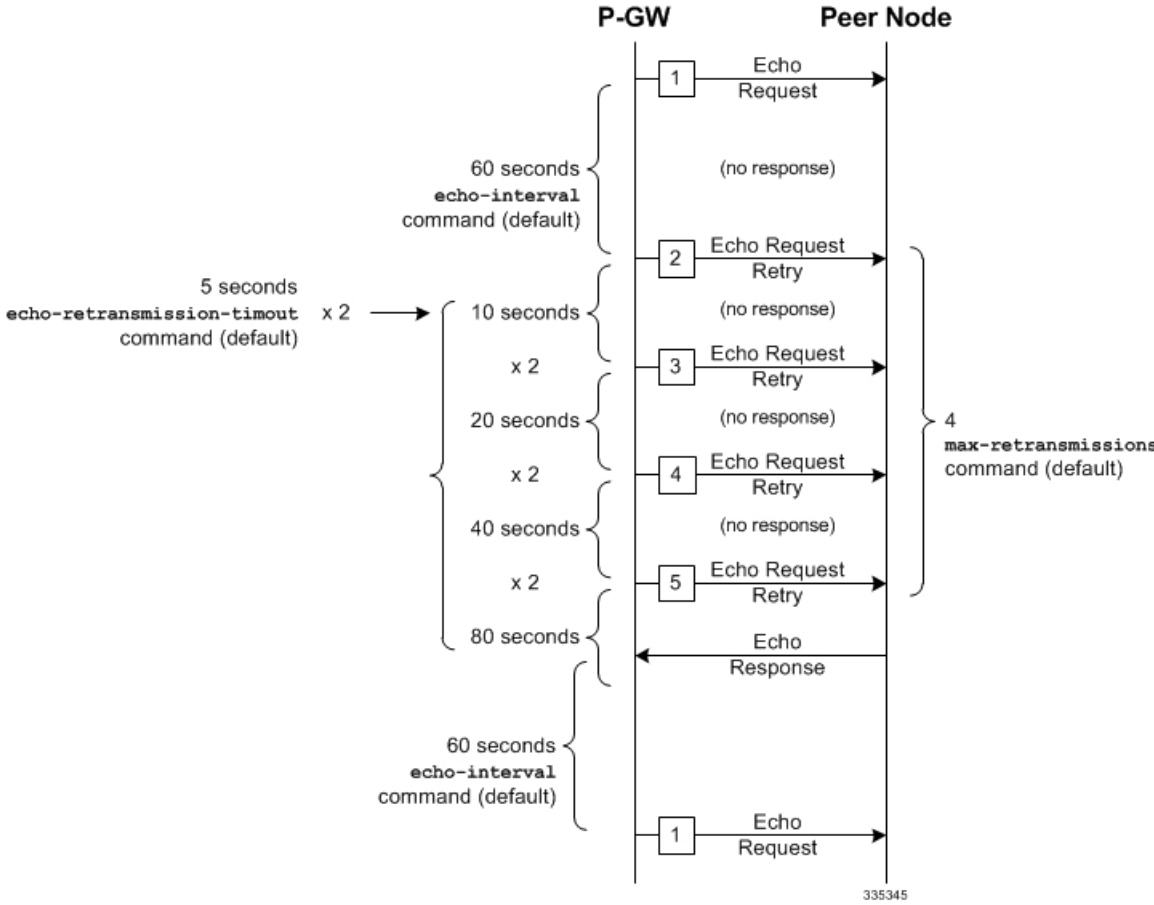
GTP-U

```
configure
  configure
    context <context_name>
      gtpu-service <gtpu_service_name>
        echo-interval <seconds> dynamic smooth-factor <multiplier>
```

```
echo-retransmission-timeout <seconds>
max-retransmissions <num>
end
```

注：

- 次の図は、上記の 3 つの **gtpc** コマンドのデフォルト設定と、6 秒のラウンドトリップタイマー（RTT）の例を使用した障害発生と回復のシナリオを示しています。



- 乗数（x2）と最大 100 秒はシステムコードであり、設定できません。

P-GW での GTPP オフラインアカウンティングの設定

デフォルトでは、P-GW サービスは GTPP アカウンティングをサポートします。GTPP オフライン課金機能を提供するには、次の例に示すパラメータを使用して P-GW を設定します。

```
configure
      gtpp single-source
      context <ingress_context_name>
            subscriber default
                  accounting mode gtpp
                  exit
            gtpp group default
                  gtpp charging-agent address <gz_ipv4_address>
                  gtpp echo-interval <seconds>
```

```
            gtpp attribute diagnostics
            gtpp attribute local-record-sequence-number
            gtpp attribute node-id-suffix <string>
            gtpp dictionary <name>
            gtpp server <ipv4_address> priority <num>
            gtpp server <ipv4_address> priority <num> node-alive enable
            exit
      policy accounting <gz_policy_name>
            accounting-level {type}
            operator-string <string>
            cc profile <index> buckets <num>
            cc profile <index> interval <seconds>
            cc profile <index> volume total <octets>
            exit
      exit
context <ingress_context_name>
      apn apn
            associate accounting-policy <gz_policy_name>
            exit
      interface <gz_interface_name>
            ip address <address>
            exit
      exit
port ethernet <slot_number/port_number>
      no shutdown
      bind interface <gz_interface_name> <ingress_context_name>
      end
```

注：

- **gtpp single-source** が有効になり、各 AAA マネージャが独自の UDP ポートで要求を生成するのではなく、システムが単一の UDP ポートを使用して（AAA プロキシ機能によって）アカウンティングサーバーへの要求を生成できるようになりました。
- **gtpp** は、**accounting mode** コマンドのデフォルトオプションです。
- コール制御プロファイルに設定されたアカウンティングモードは、この設定を上書きします。
- **accounting-level** のタイプは、Flow、PDN、PDN-QCI、QCI、および Subscriber です。このコマンドの詳細については、『*Command Line Interface Reference*』の「*Accounting Profile Configuration Mode Commands*」の章を参照してください。

GTP スロットリング機能の設定

GTP スロットリング機能を使用すると、通信事業者は P-GW/GGSN での着信/発信メッセージのレートを制御できます。

発信制御メッセージスロットリングの設定

次の設定は、発信制御メッセージスロットリングを有効にするのに役立ちます。

```
configure
  context context_name
  [no] gtpc overload-protection egress rlf-template rlf_template_name
```

```
throttling-overload-policy throttling_overload_policy_name
  end
```

着信制御メッセージスロットリングの設定

次の設定は、着信制御メッセージスロットリングを有効にするのに役立ちます。

```
configure
  context context_name
  [no] gtpc overload-protection ingress msg-rate msg_rate
[delay-tolerance msg_queue_delay ] [ queue-size queue_size ]
  end
```

ローカル QoS ポリシーの設定

この項の設定例では、ローカルQoSポリシーを作成します。ローカルQoSポリシーは、QoS、データ使用量、サブスクリプションプロファイル、サーバー使用率など、セッションのさまざまな側面をローカルに定義されたポリシーに従って制御するために使用されます。



重要 ローカル QoS ポリシー機能を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

ローカル QoS ポリシーの作成と設定

次の設定例では、P-GW でローカル QoS ポリシーを有効にします。

```
configure
  local-policy-service <name> -noconfirm
    ruledef <ruledef_name> -noconfirm
      condition priority <priority> <variable> match <string_value>
      condition priority <priority> <variable> match <int_value>
      condition priority <priority> <variable> nomatch <regex>
      exit
    actiondef <actiondef_name> -noconfirm
      action priority <priority> <action_name> <arguments>
      action priority <priority> <action_name> <arguments>
      exit
    actiondef <actiondef_name> -noconfirm
      action priority <priority> <action_name> <arguments>
      action priority <priority> <action_name> <arguments>
      exit
    eventbase <eventbase_name> -noconfirm
      rule priority <priority> event <list_of_events> ruledef <ruledef_name>
 actiondef <actiondef_name>
      end
```

注：

- 最大 16 のローカル QoS ポリシーサービスがサポートされます。
- パフォーマンス上の理由から、ローカル QoS ポリシーサービスでは ruledef の数を 256 以下にすることを推奨します。
- **condition** コマンドを複数回入力すると、ruledef の複数の条件を設定できます。一致する条件が見つかり、対応する条件が適用されるまで、優先順位に従って条件が検証されます。
- パフォーマンス上の理由から、ローカル QoS ポリシーサービスでは actiondef の数を 256 以下にすることを推奨します。
- **action** コマンドを複数回入力すると、actiondef の複数のアクションを設定できます。一致するアクションが見つかり、対応するアクションが適用されるまで、優先順位に従ってアクションが検証されます。
- 現在、1 つのイベントベースのみがサポートされており、「default」という名前にする必要があります。
- **rule** コマンドを複数回入力すると、イベントベースの複数のルールを設定できます。
- パフォーマンス上の理由から、イベントベースの数を 256 以下にすることを推奨します。
- ルールは優先順位に従って実行され、ルールが一致すると、actiondef で指定されたアクションが実行されます。イベント修飾子がルールに関連付けられている場合、ルールはその特定のイベントについてのみ照合されます。**continue** の修飾子がルールの最後にある場合、後続のルールも照合されます。それ以外の場合、ルールの評価は最初に一致した時点で終了します。

ローカル QoS ポリシーのバインド

オプション 1：次の設定例では、以前に設定済みのローカル QoS ポリシーをバインドしています。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      ims-auth-service <local-policy-service name>
      end
```

注：

- 最大 30 項目の承認サービスをシステムにグローバルに設定できます。設定するサービスの合計最大数にはシステムでの制限もあります。
- 緊急コールの場合に役立ちます。PCRF は関与しません。

オプション 2：次の設定例は、以前に設定済みのローカル QoS ポリシーまたは障害処理テンプレートをバインドする場合にも使用できます。

```
configure
  context <pgw_context_name> -noconfirm
```

```
ims-auth-service <auth_svc_name>
  policy-control
    associate failure-handling-template <template_name>
    associate local-policy-service <service_name>
    end
```

注：

- IMS 承認サービスに関連付けることができる障害処理テンプレートは 1 つだけです。このコマンドを発行する前に、障害処理テンプレートを設定する必要があります。
- 障害処理テンプレートは、Diameter アプリケーションで、result-code の示す失敗、tx-expiry、または response-timeout が発生したときに実行するアクションを定義します。アプリケーションは、テンプレートで指定されたアクションを実行します。障害処理テンプレートの詳細については、『*Command Line Interface Reference*』の「*Diameter Failure Handling Template Configuration Mode Commands*」の章を参照してください。
- ローカルポリシーへのフォールバックをサポートするには、障害処理テンプレートで「local-fallback」を選択する必要があります。
- PCRF で障害が発生した場合にローカルポリシーへのフォールバックをサポートするには、ローカルポリシーサービスを IMS 承認サービスに関連付ける必要があります。障害時には、ims-auth サービスに関連付けられているローカルポリシーテンプレートがフォールバック用に選択されます。

ローカル QoS ポリシーの確認

次の設定例では、ローカル QoS サービスが適用されているかどうかを確認します。

```
logging filter active facility local-policy level debug
logging active
show local-policy statistics all
```

注：

- コンソールポートや実稼働ノードではロギング機能を使用しないように、十分注意してください。

X.509 証明書ベースのピア認証の設定

ここにある設定例により、X.509 証明書ベースのピア認証が有効になります。これは、P-GW での IP セキュリティ用の認証方法として使用できます。



重要 IP セキュリティ機能を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

次の設定例により、P-GW での X.509 証明書ベースのピア認証が有効になります。

グローバル コンフィギュレーション モードで、次のように X.509 証明書と CA 証明書の名前を指定します。

```
configure
  certificate name <cert_name> pem url <cert_pem_url> private-key pem url
 <private_key_url>
  ca-certificate name <ca_cert_name> pem url <ca_cert_url>
  end
```

注：

- **certificate name** コマンドと **ca-certificate list ca-cert-name** コマンドは、使用される X.509 証明書と CA 証明書を指定します。
- 証明書および CA 証明書の PEM 形式のデータを指定することも、この例に示すように、指定した URL を介してファイルから情報を読み取ることもできます。

コンテキスト コンフィギュレーション モードで IPSec の暗号テンプレートを作成する場合、次のように、X.509 証明書と CA 証明書を暗号テンプレートにバインドし、X.509 証明書ベースのピア認証をローカルノードとリモートノードに対して有効にします。

```
configure
  context <pgw_context_name> -noconfirm
    crypto template <crypto_template_name> ikev2-dynamic
      certificate name <cert_name>
      ca-certificate list ca-cert-name <ca_cert_name>
      authentication local certificate
      authentication remote certificate
      end
```

注：

- システムごとに最大 16 の証明書と 16 の CA 証明書がサポートされます。サービスごとに 1 つの証明書がサポートされ、最大 4 つの CA 証明書を 1 つの暗号テンプレートにバインドできます。
- **certificate name** コマンドと **ca-certificate list ca-cert-name** コマンドは、証明書と CA 証明書を暗号テンプレートにバインドします。
- **authentication local certificate** コマンドと **authentication remote certificate** コマンドは、X.509証明書ベースのピア認証をローカルノードとリモートノードに対して有効にします。

RLF バイパス機能の設定

レート制限のバイパス機能は、既存の GTP スロットリング機能を拡張したものです。RLF 機能により、通信事業者はスロットリングされている一部のメッセージのバイパスを制御できるようになりました。

既存の CLI コマンド **gtpc overload-protection egress rlf-template rlf-temp** に新しいコマンドオプション **throttling-override-policy** が追加されました。これにより、設定されたメッセージタイプ、または緊急コールまたはプライオリティコールのすべてのメッセージ、または設定された

APNのコールのすべてのメッセージに対して、スロットリングを選択的にバイパスできます。新しい CLI コマンドモード **throttling-override-policy** も導入され、スロットリングのオーバーライドポリシーの汎用シンタックスが使用できるようになりました。

スロットリング オーバーライド ポリシー モードの設定

GTP-C スロットリング オーバーライド ポリシーを作成し、GTP-C スロットリング オーバーライド ポリシー モードを開始する場合、次の設定が役立ちます。

```
configure
   throttling-override-policy throttling-override-policy_name
```

注：

上記のコマンドシーケンスを入力すると、次のプロンプトが表示されます。

```
[local]host_name(config-throttling-override-policy)#
```

RLF バイパス機能の設定

次の設定では、レート制限機能をバイパスできるメッセージタイプを設定します。

```
configure
   throttling-override-policy  throttling-override-policy_name
     [  default | no ] egress bypass-rlf pgw { msg-type { cbr | dbr |
ubr | emergency-call | earp-pl-list {1 | 2 | 3 | 4 | 5 … | 15 }+ |
apn-names  <apn-name1>  <apn-name2>  <apn-name3>   }
     end
```

注：

- 空の throttling-override-policy が作成された場合、すべての設定可能な項目のデフォルト値はゼロまたは無効になります。
- throttling-override-policy が関連付けられていない場合、P-GW の **show service configuration** はそれを「n/a」と表示します。
- 追加できる throttling-override-policy の最大数は 1024 です。この制限は、RLF テンプレートの最大数と同じです。

例

次のコマンドは、P-GW ノードでベアラー作成要求メッセージタイプを設定して、スロットリングをバイパスするようにしています。

```
egress bypass-rlf pgw msg-type cbr
```

VoLTE セッションの自動修正

機能情報

要約データ

[ステータス（Status）]	変更された機能
導入されたリリース	21.2
変更されたリリース	該当なし
対象製品	P-GW
該当プラットフォーム	ASR 5500
デフォルト設定	無効
関連する CDETS ID	CSCvc72275
このリリースでの関連する変更点	N/A
関連資料	*P-GW Administration Guide* *Command Line Interface Reference*

マニュアルの変更履歴

重要 リリース 21.2 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

機能説明

スイッチオーバー後にIPマルチメディアサブシステム（IMS）セッションのダイナミックルールが失われると、VoLTE コールが影響を受けます。コールを回復するには、IMS セッションを手動でクリアして、正しいダイナミックルールでPDNを再確立する必要があります。VoLTE セッションの自動修正機能により、ダイナミックルールチェックが可能になります。これにより、P-GWがRAR（再承認要求）メッセージを受信したときに、手動による介入なしに、問題が自動的に特定され、修正されます。この機能は、チェックのトリガーとして「RAR」メッセージを使用するように設定された APN にのみ適用されます。

機能の仕組み

APN がポリシー制御および課金ルール機能（PCRF）から RAR メッセージを受信すると、再承認応答（RAA）メッセージがすぐに送信されます。この機能が有効になっている場合、P-GW で追加のチェックが実行され、デフォルトのベアラーに関連付けられたダイナミックルールがあるかどうかが確認されます。デフォルトのベアラーで Session Initiation Protocol（SIP）ルールが回復した場合は、他の専用ベアラーも回復されます。ダイナミックルールがデフォルトのベアラーに関連付けられていない場合、コールは終了されます。その後、原因コード「再アクティベーションが必要です」を含むベアラー削除要求がデフォルトのベアラーに送信されます。原因コードが確実に送信されるようにするには、「pdn-behavior ims」を使用して APN を設定する必要があります。続いて、Credit-Control-Request-Type（CCR-T）が PCRF および他の Diameter インターフェイス（s6b、Gy、および Rf）に送信されます。 したがって、異常が検出された場合の自動回復手順には、サブスクライバ接続の終了が含まれます。サブスクライバは後でネットワークに再接続する必要があります。スイッチオーバー後にダイナミックルールが失われたサブスクライバのモバイル発信またはモバイル着信コールは拒否されます。

VoLTE セッションの自動修正機能の設定

次の項では、この機能を有効または無効にするための設定コマンドについて説明します。

ダイナミックルールチェックの有効化または無効化

VoLTE セッションの自動修正のためのダイナミックルールチェックを有効にするために、新しい CLI コマンドの **pdn validate-post-switchover** が追加されました。この機能を有効にするには、ベース APN でこのコマンドを設定します。この機能は、自動リカバリが必要な VoLTE/IMS APN に対してのみ設定する必要があります。

この機能はデフォルトで無効に設定されています。

この機能を有効または無効にするには、以下のコマンドを入力します。

```
configure
  context <context_name>
    apn <apn_name>
      [no] pdn validate-post-switchover
      end
```

注：

- **no:** ベース APN で VoLTE セッションの設定済みの自動修正を無効にします。
- **pdn validate-post-switchover:** スイッチオーバー後の自動回復用のダイナミックルールを検証します。

モニタリングおよびトラブルシューティング

ここでは、VoLTE セッションの自動修正機能のサポートにおける show コマンドおよびその出力について説明します。

コマンドの表示

ここでは、この機能をモニターするために使用できるすべての show コマンドについて説明します。

show configuration apn

この機能が APN レベルで有効になっているかどうかを確認できるよう、上記の CLI コマンドが導入されました。「pdn validate-post-switchover」があれば、この機能は有効になっています。

show active-charging service statistics

このコマンドは、以下の出力を表示するように変更されました。

```
show active-charging service statistics
ACS Data Statistics:
  Packets Dropped due to System-Limit L4-Flows:                          0
  Packets Dropped - Invalid Len in IP Hdr(Dwlink):                       0
  Packets Dropped - Invalid Ver in IP Hdr(Dwlink):                       0
  Packets Not Processed due to Flow-limit:                               0
  Packets Not Processed due to CLP not found:                            0
  Packets Dropped CLP in Preservation Mode:                              0
  Total Pkts:                                                            0
  Total Collisions in data session hash:                                 0

ACS Reject Reason:
  RuleBase Mismatch  :                                                   0
  Bandwidth-Policy Mismatch  :                                           0
  CBB-Policy Mismatch  :                                                 0
  CF Policy Mismatch  :                                                  0
  No RuleBase configured in APN/Subs:                                    0
  No active rule in Rulebase/Subs:                                       0
  No Bandwidth-Policy configured in APN/Subs:                            0
  No Resources:                                                          0
  Max Sessions:                                                          0
  Reject Probability Exceeded:                                           0
  Rule Recovery Failed:                                                  0
  CDR Flow Control Initiated:                                            0

Protocol Reject stats:
  WTP Non-initial PDU:                                                   0
  WSP-CO Non-initial Connect PDU                                         0

Dynamic Rule Statistics:
  Total Subscribers:                0   Current Subscribers:             0
  Charging Msg Received:            0   Rule Defn Received:              0
  Installs Received:                0   Removes Received:                0
  Installs Succeeded:               0   Removes Succeeded:               0
  ADC Rules Received:               0   Total ADC Rules:                 0
  ADC Install Succeeded:            0   ADC Install Failed:              0
  ADC Custom Mute Received:         0   ADC Custom Unmute Received:      0
  ADC Start Sent:                   0   ADC Stop Sent:                   0
  L7 Rules Received:                0
  L7 Install Succeeded:             0   L7 Install Failed:               0
  Installs Failed:                  0   Removes Failed:                  0
  Install Failure Reason:
    No Resources:                   0   No Rulebase Match:               0
    No RuleName Match:              0   Rulebase Count Exceeded:         0
    Local Copy Failed:              0   Invalid Protocol:                0
    Invalid Source Mask:            0   Invalid Dest Mask:               0
    No Grp-of-Rdef Match:           0
```

```
    ADC Invalid Rule:               0   ADC Invalid Readdress:             0
    L7 Rule Invalid:                0
    L7 Protocol Invalid:            0   L7 Field Invalid:                  0
    L7 Operator Invalid:            0   L7 Value Invalid:                  0
    L7 Case-Sens Invalid:           0
  Remove Failure Reason:
    No RuleName Match:              0   No Grp-of-Rdef Match:              0
    Local Copy Failed:              0

Bandwidth Limiting Statistics:
    ITC Drops:
      Uplink Packets:                  0   Uplink Bytes:                  0
      Downlink Packets:                0   Downlink Bytes:                0
    Dynamic Rule Bandwidth Limiting Drops:
      Uplink Packets:                  0   Uplink Bytes:                  0
      Downlink Packets:                0   Downlink Bytes:                0
    Per-Bearer Bandwidth Limiting Drops:
      Uplink Packets:                  0   Uplink Bytes:                  0
      Downlink Packets:                0   Downlink Bytes:                0

Credit-Control Group Statistics:
  CC Dropped Uplink Packets:       0  CC Dropped Uplink Bytes:           0
  CC Dropped Downlink Packets:     0  CC Dropped Downlink Bytes:         0

Readdressing Failure Statistics (Packets):
  Non SYN Flow:                    0  Duplicate Key:                     0
  Dropped Pkts:                    0


First-request-only redirections:                                       0

Fallback Statistics:
  Bandwidth Policy Applied:                                            0
  Bandwidth Policy Failed:                                             0
```

バルク統計

このセクションでは、この機能をサポートするために追加、変更、または廃止されたすべてのバルク統計のリストを示します。

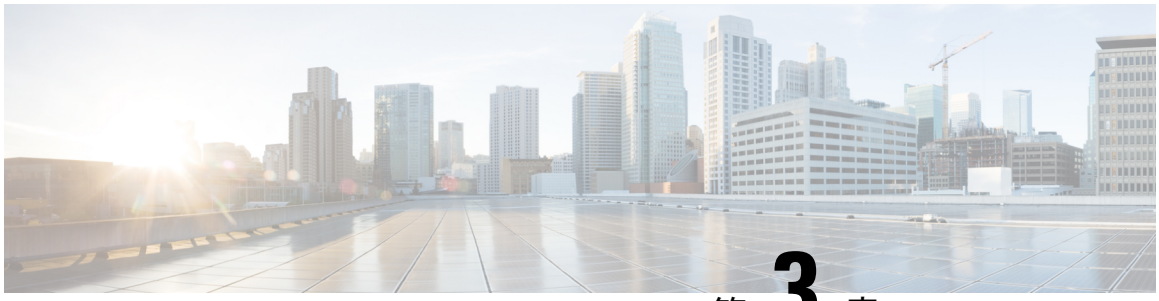
ECS スキーマ

このセクションでは、ダイナミックリカバリの失敗を示すために追加された新しいバルク統計を示します。

- dyn_rule_recovery_failure:

  ダイナミックルールリカバリの失敗により終了したセッションの合計数。
- dyn_rule_recovery_num_sess_not_terminated:

  ダイナミックルールがデフォルトベアラーにインストールされていなかったために、スイッチオーバー後に終了しなかったセッションの合計数。



第 3 章

サービスのモニタリング

この章では、コマンドラインインターフェイス（CLI）にある **show** コマンドを使用して、サービスのステータスとパフォーマンスをモニタリングする方法について説明します。これらのコマンドには関連するキーワードが多数あります。それらのキーワードを使用すると、現在のソフトウェア設定からコールのアクティビティやステータスに至るまで、システムのすべての側面に関する有益な情報が得られます。

この章で説明するキーワードの選択は、システムのモニタリングに関する最も有益で詳細な情報の提供を目的としています。これらのキーワードやその他の **show** コマンドキーワードの詳細については、『*Command Line Interface Reference*』[英語] を参照してください。

CLI に加えて、システムは、ステータスとアラームの状態を示す Simple Network Management Protocol（SNMP）トラップの送信をサポートしています。これらのトラップの詳細なリストについては、『*SNMP MIB Reference*』[英語] を参照してください。

この章では、次の事項について説明します。

- システムのステータスとパフォーマンスのモニタリング （229 ページ）
- 統計情報とカウンタのクリア （237 ページ）
- SAEGW および P-GW カウンタでの 64 ビット変換 （237 ページ）

システムのステータスとパフォーマンスのモニタリング

このセクションには、システム内のタスク、マネージャ、アプリケーション、およびその他のソフトウェアコンポーネントのステータスをモニターするために使用されるコマンドが含まれています。ほとんどのコマンドの出力に関する説明は、『*Counters and Statistics Reference*』に記載されています。

表 *26* : システムのステータスとパフォーマンスのモニタリングコマンド

手順	入力するコマンド
輻輳制御情報の表示	
輻輳制御の統計情報を表示	**show congestion-control statistics {a11mgr | ipsecmg**

手順	入力するコマンド
GTP 情報の表示	
特定のサービスの eGTP-C サービス統計情報を表示する	**show egtpc statistics egtpc-service** *name*
システム上のすべてのGTP-Uデータトラフィックの GTP-U サービス統計情報を表示する	**show gtpu statistics**
インフラストラクチャ DNS クエリの表示	
P-CSCF FQDN を解決するための インフラストラクチャ DNS クエリを確認する	**dns-client query client-name** *client_name* **query-type AAAA query-name** <*p-cscf.com*>
IP 情報の表示	
BGP ネイバーを表示する	
出力P-GWコンテキストでBGPネイバーを確認する	**context** *egress_pgw_context_name* **show ip bgp summary** （注） StarOS は次のアドレス範囲を Martian と見なし、この範囲に該当するBGPアップデートを拒否します。 また、StarOS ではBGPネットワークコマンドによる以下の範囲からの設定は許可されません。 • 127.x.x.x • 128.0.x.x • 191.255.x.x • 192.0.0.x • 223.255.255.x

手順	入力するコマンド
入力P-GWコンテキストでBGPネイバーを確認する	**context** *ingress_pgw_context_name* **show ip bgp summary** （注） StarOSは次のアドレス範囲をMartianと見なし、この範囲に該当するBGPアップデートを拒否します。 また、StarOSではBGPネットワークコマンドによる以下の範囲からの設定は許可されません。 • 127.x.x.x • 128.0.x.x • 191.255.x.x • 192.0.0.x • 223.255.255.x
IP接続状態の表示	
さまざまなコンポーネント/インターフェイスについてDiameterサーバーへのIP接続を確認する（すべてのピアはOPENまたはWAIT_DWR状態である必要があります）。	**show diameter peers full all |grep State**
IPインターフェイスステータスの表示	
IPインターフェイスが各コンテキストで稼働していることを確認する。	**show ip interface summary** **show ipv6 interface summary**
IPプール設定の表示	
IPv4プールが作成され、使用可能であることを確認する。	**context** *egress_pgw_context_name* **show ip pool summary**
IPv6プールが作成され、使用可能であることを確認する。	**context** *egress_pgw_context_name* **show ipv6 pool summary**
LMAサービス情報の表示	
特定のサービスのLMAサービス統計情報を表示する	**show lma-service statistics lma-service** *service_nam*
P-GWサービス情報の表示	
P-GWサービス統計情報を表示する	**show pgw-service statistics all**

手順	入力するコマンド
P-GW サービスを確認する	**context** *ingress_pgw_context_name* **show pgw-service all |grep Status** **show lma-service all |grep Status** **show egtp-service all |grep Status** **show gtpu-service all |grep State**
QoS/QCI 情報の表示	
QoS マッピングテーブルへの QoS クラスインデックスを表示する	**show qci-qos-mapping table all**
Rf アカウンティング情報の表示	
PGW が Rf アカウンティングレコードを送信していることを確認する： • 「Message sent」がゼロでないことを確認する。 • アクティブな課金セッションが存在することを確認する。	**show diameter accounting servers |grep Message** **show active-charging sessions all |more**
セッションサブシステムとタスク情報の表示	
セッションサブシステムとタスクの統計情報の表示 **重要** セッションサブシステムとその各種マネージャタスクの詳細については、『*System Administration Guide*』の付録「*System Software Task and Subsystem Descriptions*」を参照してください。	
AAA マネージャの統計情報を表示する	**show session subsystem facility aaamgr all**
AAA プロキシの統計情報を表示する	**show session subsystem facility aaaproxy all**
LMA マネージャの統計情報を表示する	**show session subsystem facility hamgr all**
セッションマネージャの統計情報を表示する	**show session subsystem facility sessmgr all**
セッション切断理由の表示	
詳細な出力でセッション切断の理由を表示する	**show session disconnect-reasons**
セッションリカバリ情報の確認	
セッション リカバリ ステータスを表示する	**show session recovery status [verbose]**
サブスクライバ情報の表示	
NAT 情報の表示	

手順	入力するコマンド
NAT ユーザーに割り当てられたプライベート IP を、割り当てられた他のパブリック IP とともに表示する	**show subscriber full username** *user_name*
このユーザーに割り当てられている NAT レルムを表示する	**show subscriber full username** *user_name* **|grep -i r**
特定の NAT IP アドレスのアクティブな課金フローを表示する	**show active-charging flows full nat required nat-ip** *ip_address*
セッションのリソースステータスの表示	
セッションのリソースステータスを表示する	**show resources session**
システム上の LMA サービスを使用しているサブスクライバの統計情報の表示	
システム上の特定の LMA サービスを使用しているサブスクライバの統計情報を表示する	**show subscribers lma-service** *service_name*
システム上の P-GW サービスを使用しているサブスクライバの統計の表示	
システム上の任意の P-GW サービスを使用しているサブスクライバの統計情報を表示する	**show subscribers pgw-only full**
サブスクライバ設定情報の表示	
ローカルに設定されたサブスクライバのプロファイル設定を表示する（サブスクライバが存在するコンテキストにある必要があります）	**show subscribers configuration username** *subscriber_name*
リモートで設定されたサブスクライバプロファイル設定を表示する	**show subscribers aaa-configuration username** *subscriber_name*
現在システムにアクセスしているサブスクライバの表示	
現在システムにアクセスしているサブスクライバのリストを表示する	**show subscribers all**
UE 接続ステータスの表示	

手順	入力するコマンド
UE が接続されていることを確認する： • APN 接続ごとに各ベアラーに対して 1 つのエントリがある IMSI を表示します。 • アクティブな課金セッションが存在することを確認する。 • ピアがアクティブであることを確認する。ピアは S-GW EGTP アドレスに対応している必要があります。 • 「Create Session Request」カテゴリと「Create Session Response」カテゴリが増加していることを確認する • 「Total Data Stats:」が増加していることを確認する eHRPD： • lma-sessions が存在することを確認する • 「Binding Updates Received:」カテゴリが増加していることを確認する	**show subscriber pgw-only imsi** *ue_imsi* **show active-charging sessions all |more** **show egtpc peers** **show egtpc statistics** **show gtpu statistics** **eHRPD のみ** **show lma-service session username** *user_name* **show lma-service statistics**

タイプがエラーおよび重大のシステムイベントログに IMSI/IMEI を含める

P-GW は、タイプがエラーおよび重大である次のシステムイベントログのイベントログ詳細に IMSI/IMEI を入力するように設定できます（利用可能な場合）。IMSI が利用できない場合、P-GW は IMEI の取得に最善を尽くします。

表 *27:* システムイベントログの詳細に *IMSI/IMEI* を含む新規および変更済みシステムイベントログ

イベント ログ	説明
新規イベント	
12225	「[IMSI <IMSI>] Misc Error3: s, error code d」形式の misc_error3 を表します。
12226	「[IMSI <IMSI>]Sessmgr-d Recover call from CRR failed for callid:0xx reason=s」形式中 recover_call_from_crr_failed1 エラーを表します。
12227	「[IMSI <IMSI>] Sessmgr-d Ran out of session handles」形式の aaa_create_session_failed_no_more_sessions1 エラーを表します。

イベント ログ	説明
140075	「[IMSI <IMSI>]s」形式の error_log1 を表します。
変更されたイベント	
139001	その他のさまざまな PGW エラーログを出力します。
191006	その他のさまざまな SAEGW エラーログを出力します。
10034	「[IMSI <IMSI>] default call fsm error: ostate=s(d) state=s(d) event=s(d)」形式の FSM を表します。
10035	「[IMSI <IMSI>] default call fsm invalid event: state=s(d) event=s(d)」形式の FSM INVALID イベントを表します。
12382	「[IMSI <IMSI>] Sessmgr-d: Request to s bearer rejected Reason: s」形式の SN_LE_SESSMGR_PGW_REJECT_BEARER_OP を表します。例：「[IMSI 112233445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress」。
12668	「[IMSI <IMSI>] Misc Error: Bad event in sessmgr fsm, event code d」形式の fsm_event_error を表します。
12774	「[IMSI <IMSI>] Local s TEID [lu] Collision: Clp Connect Time: lu, Old Clp Callid: d, Old Clp Connect Time: lu s」形式の pgw_purge_invalid_crr を表します。
12855	「[IMSI <IMSI>] NCQOS NRSPCA trig rcvd in invalid bcm mode.」形式の ncqos_nrspca_trig_err を表します。
12857	「[IMSI <IMSI>] NCQOS NRUPC Trig : TFT validation failed for nsapi <u>.」形式の ncqos_nrupc_tft_err を表します。
12858	「[IMSI <IMSI>] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi <u>.」形式の ncqos_nrxx_trig_already を表します。
12859	「[IMSI <IMSI>] NCQOS TFT check failed as TFT has invalid opcode for nsapi <u>:pf_id_bitmap 0xx and tft_opcode: d」形式の ncqos_nrxx_tft_check_fail を表します。
12860	「[IMSI <IMSI>] NCQOS Secondary ctxt with nsapi <u> rejected, due to <s>.」形式の ncqos_sec_rej を表します。
12861	「[IMSI <IMSI>] UPC Rejected for ctxt with nsapi <u>, due to <s>.」形式の ncqos_upc_rej を表します。
12862	「[IMSI <IMSI>] GGSN subsession invalid state state:<s>,[event:<s>]」形式の ggsn_subsession_invalid_state を表します。

イベント ログ	説明
11830	「[IMSI <IMSI>] Sessmgr-d Handoff from PGW-to-GGSN rejected, as GGSN doesnt support Deffered allocation for IPv4v6, dropping the call.」形式の gngp_handoff_rejected_for_pdn_ipv4v6 を表します。
11832	「[IMSI <IMSI>] Sessmgr-d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GBR bearer to be selected as Default bearer.」形式の gngp_handoff_rejected_no_non_gbr_bearer_for_def_bearer_selection を表します。
11834	「[IMSI <IMSI>] Sessmgr-d Handoff from GGSN-to-PGW rejected, as GGSN call with TEIDC <0xx> not found.」形式の gngp_handoff_from_ggsn_rejected_no_ggsn_call を表します。
12960	「[IMSI <IMSI>] Mismatch between PDP type of APN s and in create req. Rejecting call」形式の gtp_pdp_type_mismatch を表します。
11282	「[IMSI <IMSI>] s」形式の pcc_intf_error_info を表します。
11293	「[IMSI <IMSI>] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code d」形式の collision_error を表します。
11917	「[IMSI <IMSI>] Sessmgr d: Received invalid bearer binding request from ACS.」形式の rcvd_invalid_bearer_binding_req_from_acs を表します。
11978	「[IMSI <IMSI>] s」形式の saegw_uid_error を表します。
11994	「[IMSI <IMSI>] GGSN_INITIATE_SESS_SETUP_REQ is already fwded to PCC interface」形式の unwanted_pcc_intf_setup_req エラーを表します。
140005	「[IMSI <IMSI>] Invalid/unhandled UE event <s> in state <s>」形式の ue_fsm_illegal_event を表します。
140006	「[IMSI <IMSI>] Invalid/unhandled PDN event <s> in state <s>」形式の pdn_fsm_illegal_event を表します。
140007	「[IMSI <IMSI>] Invalid/unhandled EPSB event <s> in state <s>」形式の epsb_fsm_illegal_event を表します。
10726	「[IMSI <IMSI>] s」形式の saegwdrv_generic_error を表します。

タイプがエラーおよび重大のシステムイベントログに IMSI/IMEI を含めるよう P-GW を設定する

include-ueid キーワードが、グローバル コンフィギュレーション モードの **logging** コマンドに追加されました。有効にすると、前述のタイプがエラーおよび重大のシステムイベントで、ロギングの詳細に IMSI/IMEI が含められます（使用可能な場合）。

```
configure
    logging include-ueid
    no logging include-ueid
    end
```

注：

- **no** は、タイプがエラーおよび重大のシステムイベントログへの IMSI/IMEI の挿入を無効にします。
- **logging include-ueid** コマンドの現在の設定ステータスを表示するには、**show configuration** コマンドを使用します。
  - logging include-ueid（有効になっている場合）
  - no logging include-ueid（無効になっている場合）

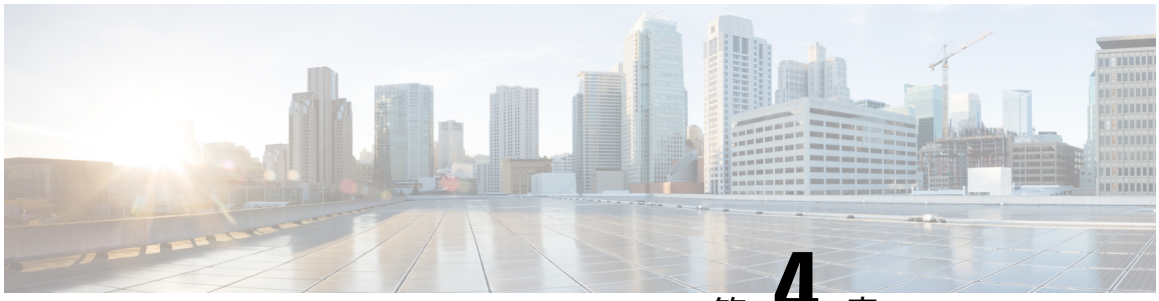
統計情報とカウンタのクリア

新しい情報を収集するために、定期的に統計情報とカウンタをクリアする必要がある場合があります。システムは、グループ化（PPP、MIPHA、MIPFA など）に基づいて統計情報とカウンタをクリアする機能を提供します。

統計情報とカウンタは、CLI **clear** コマンドを使用してクリアできます。このコマンドの使用方法の詳細については、『*Command Line Reference*』を参照してください。

SAEGW および P-GW カウンタでの 64 ビット変換

P-GW および SAEGW バルク統計カウンタの大部分は INT32 タイプであり、指定された期間中、正確な統計が表示されません。これらのカウンタは、指定された期間中にロールオーバーされます。ロールオーバーを回避し、カウンタのオーバーフローを阻止するために、バルク統計スキーマおよび SessMgr に Int32 から Int64 が導入されています。詳細については、『*Statistics and Counters Reference Guide*』[英語] を参照してください。



第 4 章

3GPP による Gx インターフェイスの変更

- 機能情報 （239 ページ）
- 変更された機能 （240 ページ）
- 制限事項 （240 ページ）

機能情報

要約データ

[ステータス（Status）]	変更された機能
導入されたリリース	21.1
変更されたリリース	21.2
対象製品	P-GW、SAEGW
該当プラットフォーム	ASR 5500
デフォルト設定	あり（顧客固有の Gx ディクショナリでのみ）
関連する CDETS ID	CSCvc99275
このリリースでの関連する変更点	N/A
関連資料	P-GW Administration Guide SAEGW Administration Guide

マニュアルの変更履歴

重要 リリース 21.2 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース	リリース日
このリリースで変更。	21.2	2017 年 4 月 27 日

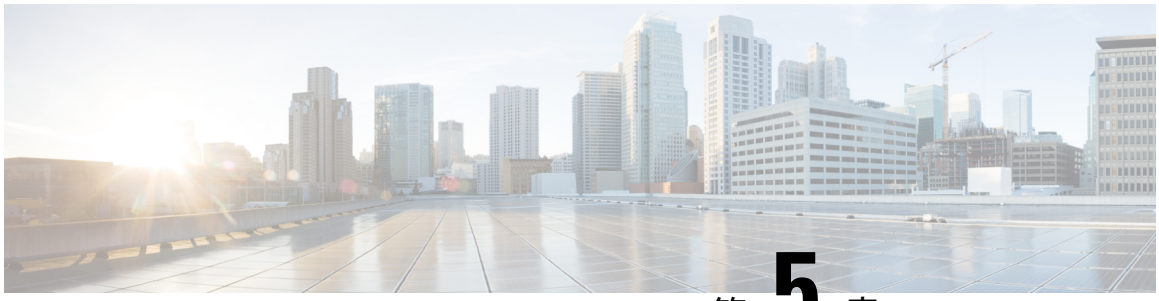
変更された機能

現在、P-GW は、ULI に変更がある場合にのみ、イベントトリガー Successful_Resource_Allocation に対して、3GPP-User-Location-Info AVP を CCR-U で送信します。この機能は、3GPP 仕様に準拠するように実装されています。この機能により、P-GW は、ULI に変更がない場合でも、イベントトリガー Successful_Resource_Allocation に対して 3GPP-User-Location-Info を CCR-U で送信します。Resource-Allocation-Notification AVP が Charging-Rule-Install AVP に含まれる場合、3GPP-User-Location-Information は PCRF に向けて送信される CCR-U に含まれます。

制限事項

この機能には次の制限があります。

1. この機能は、Diameter ディクショナリ dpca-custom8 で動作します。
2. ルールのインストールまたは変更中に、Resource-Allocation-Notification AVP を Charging-Rule-Install AVP 内に含める必要があります。



第 5 章

5G 非スタンドアロン

この章では、次のセクションで 5G 非スタンドアロン（NSA）機能について説明します。

- 機能の概要と変更履歴 （241 ページ）
- 機能説明 （243 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • S-GW • SAEGW
該当プラットフォーム	• ASR 5000 • ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A

関連資料	• *5G Non Standalone Solution Guide* • *AAA Interface Administration and Reference* • *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

SAEGW の 5G NSA ソリューションは、dcca-custom26 ディクショナリをサポートしています。	21.26
SAEGW の 5G NSA ソリューションは、GnGp ハンドオーバー中のセカンダリ RAT 使用状況 IE をサポートしています。	21.22
SAEGW の 5G NSA ソリューションは、dcca-custom1、dcca-custom7、および dcca-custom8 の各ディクショナリをサポートしています。	21.11
SAEGW の 5G NSA ソリューションは、次の機能をサポートしています。 • 拡張ビットレートの Gz への P-GW カスタムディクショナリのサポート • 拡張ビットレートの Gz への S-GW カスタムディクショナリのサポート • 拡張ビットレートの Gz および Rf への P-GW カスタムディクショナリのサポート • Gz CDR のセカンダリ RAT データ使用状況レポートにおける S-GW のサポート	21.10
SAEGW の 5G NSA ソリューションは、次の機能をサポートしています。 • Gz CDR のセカンダリ RAT データ使用状況レポートにおける P-GW のサポート • Rf CDR におけるセカンダリ RAT データ使用状況レポートでの P-GW のサポート • DCNR PDN の統計における S-GW および P-GW のサポート	21.9

5G NSA ソリューションは ASR 5000 プラットフォームで認定されています。	21.5
SAEGW の 5G NSA ソリューションは、次の機能をサポートしています。 • 機能ライセンス • 専用ベアラー • Gy インターフェイス • URLLC QCI	21.8
最初の導入。	21.6

機能説明



重要 5G NSA 機能は、リリース 21.8 以降でライセンス制御されます。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

SAEGW の 5G NSA ソリューションは、次の機能をサポートしています。

- **高スループット**

  5G NR は、最大 20 Gbps のダウンリンク データ スループットと最大 10 Gbps のアップリンク データ スループットを実現します。EPC の一部のインターフェイスは、5G スループットの処理（エンコード/デコード）をサポートしています。たとえば、NAS は最大 65.2 Gbps（APN-AMBR）、S5/S8/S10/S3（GTP-v2 インターフェイス）は最大 4.2 Tbps をサポートします。Diameter インターフェイス S6a と Gx は最大 4.2 Gbps のスループットをサポートし、S1-AP は最大 10 Gbps をサポートし、NAS は最大 10 Gbps（MBR、GBR）をサポートします。5G スループットをサポートするために、S6a、Gx、S1-AP、および NAS インターフェイスに新しい AVP/IE が導入されました。詳細については、「機能の仕組み」のセクションを参照してください。

- **P-GW での DCNR のサポート**：

  IMSA サービスで「Extended-BW-NR」機能を設定することにより、P-GW サービスでの DCNR 機能の設定をサポートします。「Feature-List-ID-2」の「Extended-BW-NR」機能ビットを PCRF に送信することにより、DCNR 機能サポートをアドバタイズします。MME/S-GW から 4.2Gbps を超える APN-AMBR 値を受信すると、AVP「Extended-APN-AMBR-UL」および「Extended-APN-AMBR-DL」を CCR メッセージで転送します。PCRF から拡張 AVP「Extended-APN-AMBR-UL」および「Extended-APN-AMBR-DL」を受信すると、これらをデコードします。

- MME/S-GW から 4.2 Gbps を超える MBR および GBR 値を受信すると、AVP 「Extended-Max-Requested-BW-UL」、「Extended-Max-Requested-BW-DL」、「Extended-GBR-UL」、および「Extended-GBR-DL」を送信します。PCRF からの受信時に、AVP「Extended-Max-Requested-BW-UL」、「Extended-Max-Requested-BW-DL」、「Extended-GBR-UL」、および「Extended-GBR-DL」をデコードします。拡張 QoS を使用して、専用ベアラーの確立をサポートします。AVP Extended-Max-Requested-BW-UL および「Extended-Max-Requested-BW-DL」を Gy レコードで送信します。

- **超低遅延のサポート**：

  超高信頼低遅延通信（URLLC）の 5G 要件をサポートします。3GPP では、URLCC QCI 80（非 GBR リソースタイプ）、QCI 82 および 83（GBR リソースタイプ）が導入されました。P-GW は、低遅延 eMBB アプリケーションで通常使用される URLLC QCI 80 を使用して、デフォルトのベアラーを確立します。P-GW は、URLLC QCI 82 および 83 を使用して専用ベアラーを確立します（非 GBR タイプの専用ベアラーを確立する場合は QCI 80 も使用）。通常、これは個別の自動化サービス（産業用自動化）によって使用されます。

- **ICSR のサポート**

  リリース 21.10 以降では、SAEGW での 5G NSA 用の ICSR がサポートされています。

- **DCNR 対応 UE 用の MME による S-GW と P-GW の動的な選択**

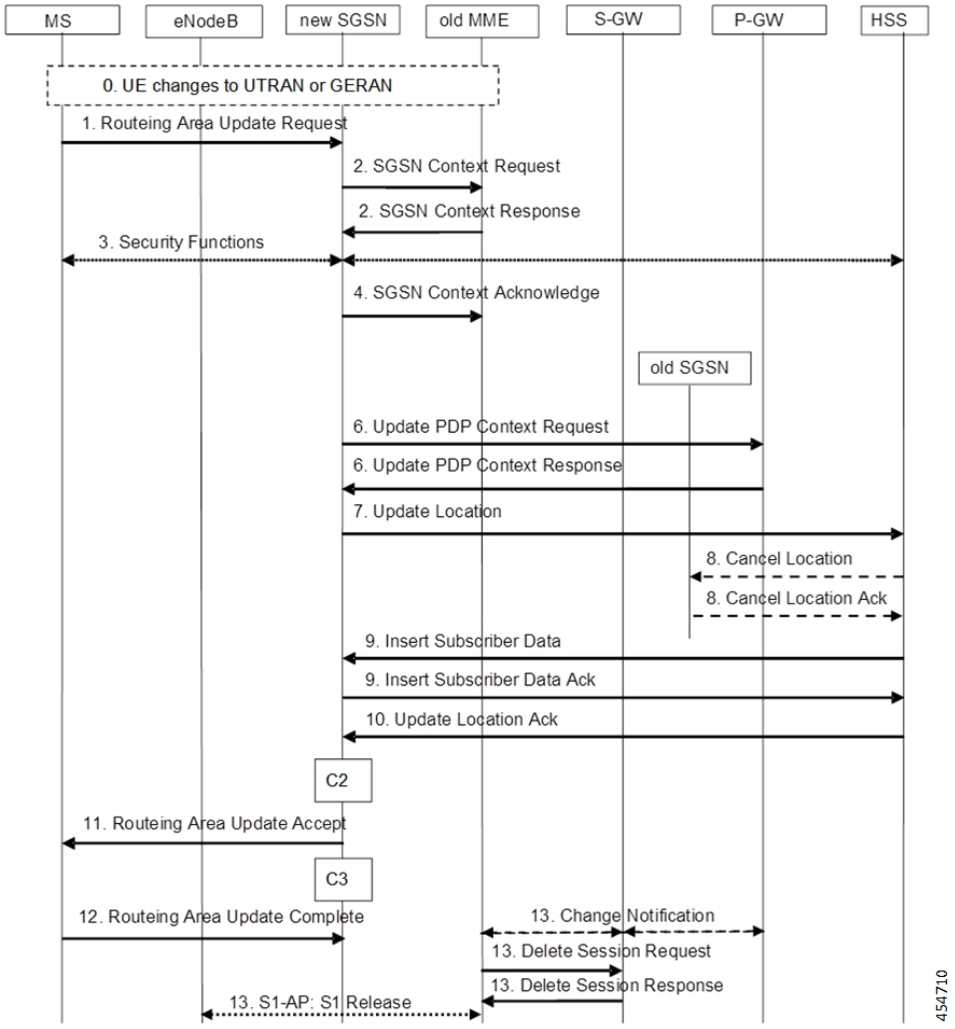
  DCNR 対応 UE が MME での登録を試み、すべての DCNR 検証が成功した場合（たとえば、MME での DCNR 機能設定、NR のアクセス制限を送信しない HSS など）、MME は「UP 機能選択通知フラグ」 IE を設定し、「セッション作成要求」メッセージで DCNR フラグを 1 に設定します。この機能は、SGW-C と PGW-C が NR を使用したデュアル接続をサポートする SGW-U と PGW-U を選択するのに役立つ CUPS アーキテクチャに関連しています。S-GW は S11 を介してこの IE を受信すると、この IE を S5 を介して P-GW に送信します。S-GW は、非 CUPS 展開で IE を受信した場合、IE を無視します。

- **P-GW セカンダリ RAT 使用状況データレポートの処理**：

  P-GW は、CDR のセカンダリ RAT データ使用状況レポートをサポートするために、Gz 用の custom24 および custom44 ディクショナリと、Rf 用の aaa-custom3、aaa-custom4 および aaa-custom6 ディクショナリをサポートしています。

GnGp ハンドオーバー中のセカンダリ RAT 使用状況のサポート

この機能は、4G から 3G へのハンドオーバー中に変更通知要求で報告されるセカンダリ RAT 使用状況をサポートします。このサポートは、GnGp ハンドオーバー中のセカンダリ RAT 使用による変更通知の処理に関するものです。この機能をサポートするように、次の図にステップ 13 が追加されています。使用状況は、次の CDR の生成時に報告される必要があります。



IMSI が不明

変更通知要求メッセージのセカンダリ RAT 使用状況 IE で指定された IMSI のコンテキストが見つからない場合は、原因値「IMSI/IMEI not known」を含む変更通知応答が返されます。

制限事項

この機能には以下の既知の制限があります。

- この機能は、セカンダリ RAT 使用状況 IE の処理のみをサポートします。
- 4Gから3Gへのハンドオーバー中に、専用ベアラーは保持され、デフォルトベアラーと専用ベアラー両方のセカンダリ RAT の使用状況が報告されます。

セカンダリ RAT データ使用状況レポートの有効化

セカンダリ RAT データ使用状況レポートを有効にするには、次の設定を使用します。

```
configure
  context context_name
    pgw-service service_name
      dcnr
      end
```



（注） P-GW サービスに関連付けられた GGSN サービスでは、先行する CLI を使用して DCNR を有効にする必要があります。

- **DCNR PDN の静的サポート**：

  DCNR PDN の S-GW および P-GW 統計のサポート

- **S-GW セカンダリ RAT 使用状況データレポートの処理**：

  S-GW は、Gz を介した CDR のセカンダリ RAT データ使用状況レポートをサポートするために、custom24 ディクショナリと custom6 ディクショナリをサポートしています。

- **Gz を介した P-GW カスタムディクショナリのサポート**：

  P-GW は、Custom44 ディクショナリと Custom24 ディクショナリをサポートしており、4.2Gbps を超える MBR、GBR、および APN-AMBR 値を受信した場合に、次の AVP の送信をサポートします。

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **複数プレゼンスレポートエリアのサポート**：

  S-GW は、S11/S4 および S5/S8 インターフェイスを介した Multiple-PRA アクションと Multiple-PRA 情報をサポートします。P-GW は、S5/S8 および Gx インターフェイスを介した Multiple-PRA アクションと Multiple-PRA 情報をサポートします。

- **Gz を介した S-GW カスタムディクショナリのサポート**：

  S-GW は、custom24 ディクショナリと custom6 ディクショナリをサポートしており、4.2Gbps を超える MBR、GBR、および APN-AMBR 値を受信した場合に、次の AVP の送信をサポートします。

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL

- Extended-GBR-DL
- Extended-APN-AMBR-UL
- Extended-APN-AMBR-DL

- **Gx を介した P-GW カスタムディクショナリのサポート**：

  P-GW は、dpca-custom15、dpca-custom11、dpca-custom23、dpca-custom19、および dpca-custom17 ディクショナリをサポートしており、4.2Gbps を超える GBR および APN-AMBR 値を受信した場合に、次の AVP の送信をサポートします。

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-DL
  - Extended-GBR-UL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **Gy を介した P-GW カスタムディクショナリのサポート**：

  P-GW は、dcca-custom1、dcca-custom7、dcca-custom8、dcca-custom13、および dcca-custom26 ディクショナリをサポートしており、4.2Gbps を超える GBR および APN-AMBR 値を受信した場合に、次の AVP の送信をサポートします。

  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-DL
  - Extended-GBR-UL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

- **Rf を介した P-GW カスタムディクショナリのサポート**：

  P-GW は、aaa-custom3、aaa-custom4、および aaa-custom6 ディクショナリをサポートしており、4.2Gbps を超える GBR および APN-AMBR 値を受信した場合に、次の AVP の送信をサポートします。

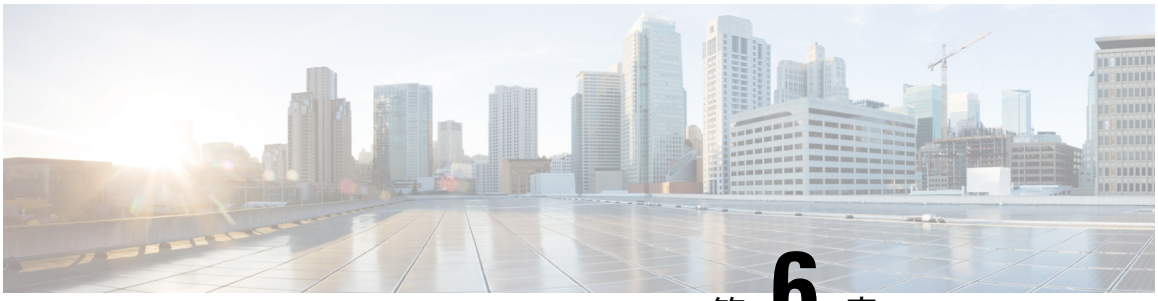
  - Extended-Max-Requested-BW-UL
  - Extended-Max-Requested-BW-DL
  - Extended-GBR-UL
  - Extended-GBR-DL
  - Extended-APN-AMBR-UL
  - Extended-APN-AMBR-DL

Multiple Presence Reporting Area

P-GW は、PCRF を使用する Gx インターフェイスを介した Feature-List-ID 2 の Multiple-Presence Reporting Area 機能のネゴシエーションをサポートします。CNO-ULI 機能は、P-GW や PCRF が Multiple-PRA をサポートしておらず、P-GW と PCRF の両方が CNO-ULI をサポートしている場合にのみ使用されます。



（注） この機能はリリース 21.9.1 で導入されました。詳細については、『*P-GW Administration Guide*』の「プレゼンスレポートエリア」の章を参照してください。



第 6 章

パイロットパケットへの ECPD ID とアカウント番号の追加

- 機能の概要と変更履歴 （249 ページ）
- 機能説明 （250 ページ）
- パイロットパケットの設定 （251 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• GGSN • P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *GGSN Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.25

機能説明

パイロットパケット機能は、サブスクライバの ID やサブスクライバの IP アドレスといったサブスクライバセッションに関する重要な情報を外部の要素に提供します。イベントトリガー中にサブスクライバが IP アドレスの割り当てまたは割り当て解除を行うと、「パイロット」パケットが生成されます。この情報を使用して、サブスクライバ分析などの新しいサービスが有効になり、UDP トランスポートで送信されます。

パイロットパケットは次の情報で構成され、タイプ、長さ、値（TLV）の形式になっています。

- 割り当て/割り当て解除フラグ
- MSISDN（MDN）
- IMSI
- 割り当て済み IPv4 アドレス
- 割り当て済み IPv6 アドレス
- 割り当て済み NAT IPv4アドレス
- NAT アドレスポートチャンクの開始
- NAT アドレスポートチャンクのサイズ
- サービス提供ネットワーク識別子
- 外部エージェントの IP アドレス
- NAI
- RAT タイプ

通信事業者は、パイロットパケットを持つネットワーク要素が SGi インターフェイスの Flexible-Services-Container TLV を介してエンタープライズレベルの情報を取得およびレポートできるようにします。

Flexible-Services-Container は、次のエンタープライズレベルの情報で構成されます。

- エンタープライズ カスタマー プロファイル データベース ID（ECPD ID）
- アカウント番号

例：ECPD ID = 3458312、アカウント番号 = 0442058164-00001

注

特記事項は次のとおりです。

- 新しい TLV が CLI で設定され、S6b が AAA メッセージで 受信した場合にのみ、P-GW はサブスクライバのパイロットパケットに新しい TLV を追加します。

- P-GW は再認証手順で受信した Flexible-Services-Container を無視します。
- P-GW や GGSN のサービスでは、エンタープライズ情報（ECPD ID とアカウント番号）の内容や解釈は必要ありません。データは P-GW や GGSN によって解析されず、パイロットパケットで透過的に渡されます。

パイロットパケットの設定

サードパーティのネットワーク要素へのサブスクライバセッションに関するキー情報を含むパイロットパケットを設定するには、次の設定を使用します。

```
configure
   context context_name
    pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type
 | serving-nw-id | flexible-services-container } | name server_name
source-ip-address source_ip_address destination-ip-address destination-ip_address
 destination-udp-port udp_port_value [ dscp-marking dscp-value ] | trigger
rat-change generate { nat-info-only | user-info-and-nat-info |
user-info-only } }
     default pilot-packet { attribute { foreign-agent-ip-address | nai
 | rat-type | serving-nw-id | flexible-services-container } | trigger
rat-change }
     no pilot-packet { attribute { foreign-agent-ip-address | nai |
rat-type | serving-nw-id | flexible-services-container } | name server_name
 | trigger rat-change }
     end
```

注：

- **pilot-packet { attribute flexible-services-container}**：パイロットパケットでオプションの flexible-services-container を送信します。
- **default pilot-packet { attribute flexible-services-container }**：パイロットパケットでオプションの flexible-services-container を送信しません。
- **no pilot-packet { attribute flexible-services-container }**：パイロットパケットでフレキシブルサービスコンテナ情報を無効にします。

設定の確認

パイロットパケットの設定を検証するには、次のコマンドを使用します。

- **show configuration**
- **show configuration verbose**

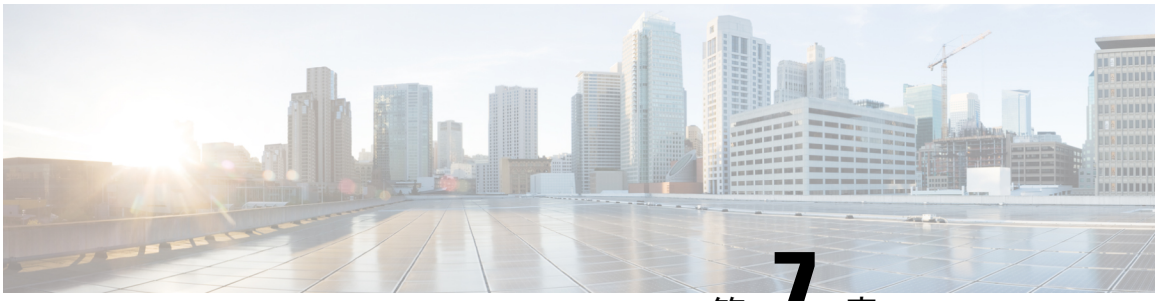
show configuration

このコマンドの出力には、次のフィールドが含まれています。

表 *28 : show config* コマンド出力の説明

フィールド	説明
flexible-services-container	オプションの TLV フレキシブル サービス コンテナがパイロットパケットで送信されることを示します。

show config verbose コマンドにも同様の フィールド出力が含まれています。



第 7 章

アドレスホールドタイマーのサポート

- 機能の概要と変更履歴 （253 ページ）
- 機能説明 （254 ページ）
- アップグレードおよびダウングレードプロセス （254 ページ）
- アドレスホールドタイマーの設定 （254 ページ）
- モニタリングおよびトラブルシューティング （255 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide* • *Command Line Interface Reference*

マニュアルの変更履歴

改訂の詳細	リリース
P-GW は、IPv6 のアドレスホールドタイマーの設定をサポートしています。	21.28.m14

機能説明

P-GW では、IPv4 の **address-hold-timer** パラメータが有効になっているときにアクティブなサブスクライバが切断されると、IP アドレスは保留状態になるか、まだ使用中と見なされます。この IP アドレスは、**address-hold-timer** の期限が切れるまで、**リリース**状態に戻りません。

そのため、指定された時間（秒単位）内に再接続したサブスクライバは、IP プールから同じ IP アドレスを取得できます。

このリリースのアドレスホールドタイマー機能では、CLI 設定による IPv6 プールがサポートされます。

show CLI 設定コマンドを使用して、次の情報を表示できます。

- USED、HOLD、FREE、RELEASE 状態のアドレスと、アドレスのリスト。
- アドレスホールドタイマーの状態を含むビジーアウト状態。
- 各状態の IP アドレスの累積数。

アップグレードおよびダウングレードプロセス

アドレスホールドタイマー CLI が設定されている場合、アップグレードの後、この機能は IPv6 プールに対して機能します。

IPv6 のアドレスホールドタイマー（AHT）を有効にしている場合、IPv6 の AHT がサポートされていないダウングレードの後、完全な IPv6 プール設定は無視されます。ダウングレード手順の前に、IPv6 のアドレスホールドタイマーが設定から削除されていることを確認してください。

アドレスホールドタイマーの設定

IPv6 アドレスホールドタイマーを有効にするには、次の設定例を使用します。

```
configure
  context context_name
    [ no ] ipv6 pool pool_name prefix ip_address/len public priority
address-hold-timer address_hold_timer_value
  end
```

注：

- **ipv6 pool** *pool_name* **prefix** *ip_address/len* **public** *priority* **address-hold-timer** *address_hold_timer_value*：IPv6 プールのアドレスホールドタイマーのサポートを有効にします。

address-hold-timer が有効な場合に、アクティブなサブスクライバが切断されると、IP アドレスは保持されているか、まだ使用中と見なされ、**address-hold-timer** が期限切れになるまで空き状態に戻りません。そのため、指定された時間（秒単位）内に再接続したサブスクライバは、IP プールから同じ IP アドレスを取得できます。

例：**Ipv6 pool PUBLIC1V6 prefix 5001::aaaa/48 public 0 address-hold-timer 120**

（注）

- **address-hold-timer** の値は、さまざまなキーワードや IPv6 プールで設定できます。ただし、アドレスホールドタイマーは、設定された最新の **address-hold-timer** の値を使用して設定されます。
- **address-hold-timer** の値は秒単位で設定されます。値 0 は、アドレスホールドタイマーが無効であることを意味します。
- P-GW では、アドレスホールドタイマー（AHT）のオンザフライ変更はサポートされていません。AHT が設定されている場合、進行中のコールは保留状態に移行しません。AHT が設定された後にコールが接続されると、IP は保留状態に移行します。

  オンザフライ アドレス ホールド タイマー（AHT）は、IPv4 プールと IPv6 プールで同様に動作します。

- **no**：特定のプールに設定されているアドレスホールドタイマーを削除します。例：`no ipv6 pool PUBLIC1V6 address-hold-timer`

モニタリングおよびトラブルシューティング

この項では、アドレスホールドタイマー機能のサポートに使用できる CLI コマンドに関する情報を提供します。

コマンドや出力の表示

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show ipv6 pool *pool_name*

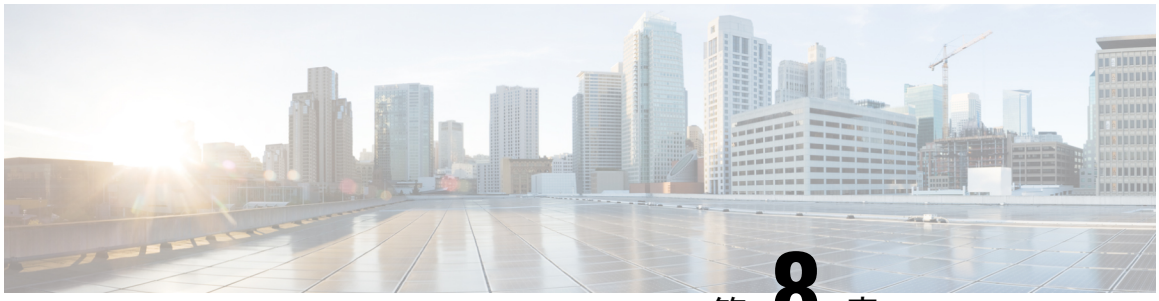
show ipv6 pool pool_name PUBLIC1V6 { free | used | release | hold | limit | wide } コマンドの出力が変更され、アドレスホールドタイマー CLI 統計が表示されるようになります。次に例を示します。

```
show ipv6 pool pool-name PUBLIC1V6
   Pool Name:     PUBLIC1V6
   Group Name:
   Pool Type:     Public        Priority: 0
```

```
    Pool Id:       2001          Vrf: n/a
    Pool Status:   Good
    Start Prefix:  5001::/64
    End Prefix:    5001:0:0:ffff::/64
        Addr-Hold-Timer: 100
        Total Prefix:  65536        Used Prefix: 0      Free Prefix: 65533       On-Hold
 Prefix: 1       Released Prefix: 2
        Pool Address Type: Normal
    Configured Prefix: 5001::aaaa/48
    User-Plane  ID   : N/A
    Virtual-FE  ID   : N/A
                 Nexthop Forwarding Address: Disabled
      Network Reachability Detection Server: Disabled
                  Suppress-Switchover-ADVS: Disabled
                   Allow-Static-Allocation: Disabled
                  Duplicate-Addr-Detection: Disabled
                         Send-Pilot-Packet: Enabled
                         Advertise-if-used: Disabled
      Addr-Hold-Timer-IPV6: 202                          Group Available Threshold:
Disabled    Clear: Disabled
                       Pool-Free Threshold: Disabled    Clear: Disabled
                       Pool-Used Threshold: Disabled    Clear: Disabled
              cip-local-pool-used Threshold: Disabled    Clear: Disabled
       cip-local-pool-in-use-addr Threshold: Disabled    Clear: Disabled
```

それぞれの説明は次のとおりです。

- **used**：**使用済み**状態のアドレスは、接続されたサブスクライバによって現在使用されているアドレスです。
- **hold**：ホールド状態のアドレスは、最近プールからリリースされたものの、**アドレスホールドタイマー**がまだ期限切れになっていないアドレスです。
- **free**：空き状態のアドレスは、サブスクライバによって現在使用されていないアドレスであり、このアドレスの以前のユーザーから保存された NAI および IMSI データを持ちません。
- **release**：リリース済み状態のアドレスは、プールからリリースされているアドレスであり、このアドレスのアドレスホールドタイマーは期限切れになっています。このアドレスは、以前のサブスクライバに関して保存された NAI および IMSI データを持ちます。
- **limit**：制限値が指定されていない場合、制限状態のアドレスについては、デフォルトの 100 個の IP アドレス情報が表示されます。
- **wide**：ワイド状態のアドレスは、80 列以上の書式になる可能性がある情報を表示するアドレスです。



第 8 章

APN バックオフタイマーのサポート

この章では、P-GW および SAEGW での APN バックオフタイマー機能の StarOS のサポートについて説明します。

- 機能説明 （257 ページ）
- P-GW/SAEGW での APN バックオフタイマーのサポートの設定 （259 ページ）
- 機能の監視 （261 ページ）

機能説明

以前は、P-GW で遅延耐性または優先順位の低いデバイスからのシグナリングトラフィック（優先順位の低いマシン間トラフィックなど）が区別されませんでした。

UE は、NAS や接続要求メッセージを介して MME にデバイスプロファイルを示すことができました。MME は、S5 インターフェイスのシグナリング優先順位表示情報要素（IE）を介して、この情報を P-GW に渡すことができました。一部の UE は、P-GW への S5 インターフェイスでのシグナリング優先順位表示 IE の送信をサポートしていなかった可能性があります。その結果、P-GW はシグナリングタイプを区別できませんでした。現在のリリースでは、P-GW はこれらのシグナリングタイプを区別できます。

さらに、過負荷状態のとき、P-GW は Low Access Priority Indicator（LAPI） デバイスからの新しいセッションを許可し、LAPI デバイスからのトラフィックを通常の UE と同じ優先順位で処理していました。現在の StarOS リリースでは、過負荷状態のときに、P-GW が LAPI として識別されたトラフィックをバックオフするように設定できます。APN 設定またはシグナリング優先順位表示 IE のいずれかに基づいて、この識別が行われます。

バックオフ タイマー アルゴリズムと R12 GTP-C 負荷/過負荷制御アルゴリズムが連携します。この機能のメリットは、優先順位の低いコールが拒否されることです。その結果、優先順位の高いコールの帯域幅を増やすことができます。

機能

APN バックオフタイマー機能をサポートするために、次の機能が導入されました。

1. セッション作成要求メッセージに含まれる、S5インターフェイスでのシグナリング優先順位表示 IE により、優先順位の低いデバイスが識別されます。
2. LAAPI APN を設定できます。その APN に着信するすべてのコールは LAPI コールと見なされます。
3. バックオフタイマーの値は、APN で設定されます。バックオフタイマーは、P-GW バックオフタイマー IE のセッション作成応答メッセージで送信されます。
4. 次の条件が満たされている場合、発生する APN 輻輳が原因でコールが拒否されます。設定されたバックオフタイマー値は、セッション作成応答メッセージのバックオフタイマー IE に挿入されます。
   - 上記の条件 1 または 2 により、着信コールが LAAPI として識別されている。
   - P-GW が過負荷状態になっている。
   - バックオフタイマーが設定されている。
5. M2M ライセンスがシステムに存在し、有効になっている必要があります。GTP-C 負荷/過負荷機能の設定と過負荷パラメータのバックエンドレポートは、M2M ライセンスで動作します。
6. 一部のディクショナリ（custom35 など）では、CDR に LAPI コール用の LAPI フィールドがあります。このフィールドは、シグナリング優先順位表示 IE により、コールが LAPI コールであることが示されている場合に入力されます。ただし、LAPI APN 設定によりコールのタイプが LAPI になっている場合、CDR に LAAPI フィールドを含めることはできません。
7. APN バックオフタイマー機能により拒否されたコールの数を示すために、バルク統計、カウンタ、および統計が APN および P-GW サービスレベルで導入されています。

GTP-C 過負荷機能と M2M ライセンス

P-GW/SAEGW が過負荷状態にあるかどうかを検出するために、GTP-C 過負荷機能のフレームワークが使用されています。過負荷設定と過負荷状態のレポートのみが有効になるように、M2M ライセンスに関連付けられています。ピアへの OCI の送信、スロットリング、ピアからの OCI の受信など、残りの過負荷機能は機能しません。そのため、以下の動作シナリオが考えられます。

コールが LAPI コールであり、バックオフタイマーが設定されており、P-GW が過負荷状態である場合は、次のように動作します。

- M2M ライセンスのみ：APN 輻輳が原因でコールが拒否されます。
- GTP-C 過負荷のみが有効：バックオフタイマーが設定できないため、該当しません。
- M2M と過負荷の両方が有効：APN 輻輳がコールが拒否されます。つまり、LAAPI は GTP-C 負荷/過負荷機能よりも優先されます。

コールが LAPI コールではない場合、またはバックオフタイマーが設定されておらず、P-GW が過負荷状態である場合は、次のように動作します。

- M2M ライセンスのみ有効：影響はありません。コールは正常に受け入れられます。
- 過負荷ライセンスのみ有効：コールは受け入れられます。OCI がセッション作成応答メッセージで送信されます。過負荷機能は正常に動作します。
- M2M と過負荷機能の両方が有効：コールは受け入れられます。OCI がセッション作成応答メッセージで送信されます。過負荷機能は正常に動作します。バックオフタイマー機能は無視されます。

ライセンス



重要 APN バックオフタイマー機能を使用するには、P-GW または SAEGW で M2M ライセンスを有効にする必要があります。ライセンスの詳細については、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

P-GW/SAEGW での APN バックオフタイマーのサポートの設定

ここでは、P-GW/SAEGW における APN バックオフタイマーのサポートの設定方法について説明します。この手順は、次の作業から構成されています。

1. LAPI 動作の設定
2. バックオフタイマーの設定
3. 設定の確認

LAPI 動作の設定

次の例を使用して、LAPI 動作を設定します。

```
configure
   apn apn_name
      pdn-behavior lapi
      end
```

LAPI 動作を無効にするには、次の手順を実行します。

```
configure
   apn apn_name
```

```
no pdn-behavior
end
```

注：

- **pdn-behavior lapi** は APN をLAPI APN として設定します。
- **no pdn-behavior** は LAPI APN 設定を無効にします。

⚠

注意 緊急 APN と **pdn-behavior lapi** の設定は相互に排他的であるため、同じ APN に設定しないでください。同じ APN で両方の設定が構成されている場合は、**pdn-behavior lapi** の設定が優先されます。その結果、両方の設定が構成され、システムが過負荷になっている場合、コールは拒否されます。

両方の設定が同じ APN で設定されているかどうかを確認するには、 *Exec* モードで **show configuration error verbose** コマンドを実行します。同じ APN で両方の設定が設定されている場合、 コマンド出力に 警告が含まれます。

APN バックオフタイマーとジッター値の設定

セッションごとに MME に返されるバックオフタイマー値にランダム性を導入するためには、P-GW で固定値とジッターが必要です。これは、バックオフタイマーが期限切れになった後のセッションストームを防ぐのに役立ちます。

APNバックオフタイマーとジッター値を設定するには、次の例に示すコマンドを使用します。

```
configure
  apn apn_name
    backoff timer-value seconds [ jitter seconds ]
    end
```

バックオフタイマー機能を無効にするには、次のコマンドを実行します。

```
configure
  apn apn_name
    no backoff timer-value
    end
```

注：

- **backoff timer-value** *seconds* では、バックオフタイマーの値を秒単位で設定します。有効なエントリは 0 ～ 576000 秒の整数です。デフォルト設定はありません。
- **jitter** *seconds* ではジッター値を秒単位で設定します。有効なエントリは 0 ～ 1000 秒です。デフォルト設定はありません。

設定の確認

設定を確認するには、次のコマンドを実行します。

「Exec モード」で **show apn name** *apn_name* コマンドを発行します。*apn_name* は、設定を表示する APN の名前です。

コマンド出力で、次のフィールドを探します。

- pdn behavior: <*lapi*> または <*no pdn-behavior*>
- Backoff Timer Value: <*seconds*> Jitter: <*seconds*>

設定が正しいことを確認します。設定のいずれかが正しくない場合は、この章の設定手順を使用して、正しくない設定を再設定してください。

機能の監視

この項では、通信事業者が APN バックオフタイマー機能をモニターできるようにするための情報を提供します。

バルク統計

APN スキーマ

APN バックオフタイマー機能をサポートするために、次のバルク統計が APN スキーマに追加されました。

- rej-pdn-backofftimer

P-GW スキーマ

APN バックオフタイマー機能をサポートするために、次のバルク統計が P-GW スキーマに追加されました。

- sessstat-rej-pdn-backofftimer

SAEGW スキーマ

APN バックオフタイマー機能をサポートするために、次のバルク統計が SAEGW スキーマに追加されました。

- pgw-sessstat-rej-pdn-backofftimer

show コマンドの出力

ここでは、P-GW と SAEGW 機能での APN バックオフタイマーのサポートをモニターするために使用できる、Exec モードの show コマンドと出力について説明します。

show apn name

このコマンドの出力が拡張され、設定済みのバックオフタイマー、ジッター、および PDN 動作の設定が表示されるようになりました。これらの設定は、M2M機能ライセンスが有効になっている場合にのみ表示されます。

- pdn behavior: lapi
- Backoff Timer Value: <*seconds*> Jitter: <*seconds*>

show apn statistics

このコマンドの出力が拡張され、設定されたバックオフタイマー値の結果として拒否された PDN の数が表示されるようになりました。

- バックオフアルゴリズムにより拒否された PDN の数：

show configuration apn name

このコマンドの出力で、オペレータに現在のAPNバックオフタイマーの設定が提示されます。

- pdn-behavior lapi（機能が有効になっている場合）
- backoff timer-value <*secs*> jitter <*secs*>

show pgw-service statistics

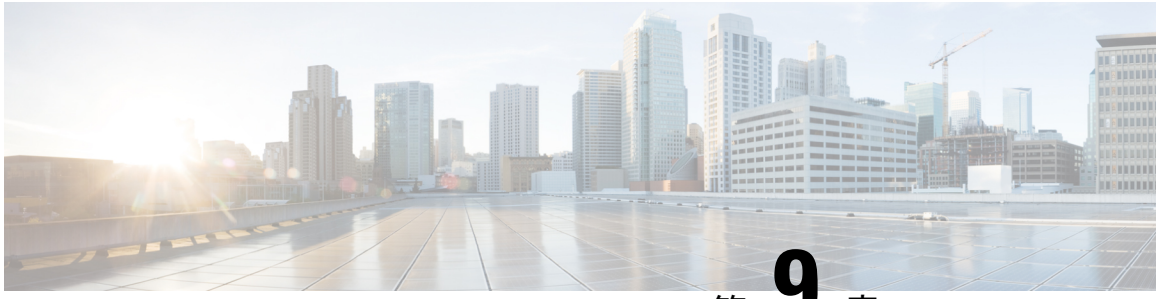
このコマンドの出力が拡張され、設定されたバックオフタイマー値によって拒否された PDN の総数が表示されるようになりました。

- 理由別の拒否された PDN：
  - APN バックオフタイマー

show session disconnect-reasons

APN バックオフタイマー機能をサポートするために、次の切断理由が追加されました。

- apn-congestion



第 9 章

CIoT デバイスの APN レートコントロール

この章は、次の内容で構成されています。

- 機能の概要と変更履歴 （263 ページ）
- 機能説明 （264 ページ）
- 機能の仕組み （264 ページ）
- 「CIoT デバイスの APN レート制御」機能の設定 （271 ページ）
- CIoT デバイスの APN レート制御機能のモニタリングおよび障害対応 （272 ページ）
- アカウンティングのサポート （273 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• C-SGN • P-GW
該当プラットフォーム	• UGP • VPC-DI • VPC-SI
機能のデフォルト	無効：ライセンスが必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *Statistics and Counters Reference* • *Ultra IoT C-SGN Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.15

機能説明

一般的なシナリオでは、CIoT 対応 UE ではデータパケットの送信頻度は低いですが、UE が短期間にデータパケットを頻繁に送信する珍しいケースもあります。このようなケースでは、ネットワークの輻輳が発生し、サービスに影響を与える場合があります。APN レートコントロールは、UE がデータパケットを送信するときにレートを制限するための 3GPP 標準準拠メカニズムの 1 つです。

APN レートコントロールにより、ホーム パブリック ランドモバイル ネットワーク（HPLMN）の通信事業者は、ダウンリンク（DL）とアップリンク（UL）で送信されるユーザーデータ量を制御できます。DL と UL の両方について、時間単位ごとのユーザーデータパケットの最大数や、時間単位ごとのユーザーデータオクテットの最大数でユーザーデータをポリシングすることで、これを実現します。

機能の仕組み

DL の APN レート コントロール ポリシングは P-GW または SCEF で実行され、UL の APN レート コントロール ポリシングは UE で実行されます。P-GW または SCEF は APN レートコントロール UL ポリシングも実行できます。詳細については、次を参照してください。

- UE の APN レートコントロール UL については、3GPP TS 24.301 を参照してください。
- SCEF の APN レートコントロールについては、3GPP TS 29.128 を参照してください。

（注） 既存の AMBR メカニズムは、無線効率と UE バッテリの寿命から考えて、CIoT デバイスの APN レートコントロールには適していません。たとえば、AMBR が 100 Kbps を超えると、毎日のデータ量が大きくなる可能性があります。

P-GW または Service Capability Exposure Function（SCEF）は、PCO 情報要素（IE）を使用して APN アップリンク レート コントロール コマンドを UE に送信します。APN アップリンク レートコントロールは、データ無線ベアラー（S1-U）またはシグナリング無線ベアラー（NAS データ PDU）のいずれかによってその APN で送信されるデータ PDU に適用されます。UE はこのアップリンク レート コントロール命令に準拠します。UE は、P-GW または SCEF から新しいレートコントロール命令を受信するまで、レートコントロール命令を有効と見なします。P-GW または SCEF は、UE に指示されたレートを超えるパケットを破棄または遅延させることにより、アップリンク レート コントロールを適用します。

APN レートコントロールの表示

APN レートコントロールの表示ステータスは、プロトコル設定オプション（PCO）または拡張プロトコル設定オプション（ePCO）の一部として送信されます。P-GW や MME がその機能交換の一環として ePCO をサポートする場合、P-GW や S-GW は、ePCO の一部として APN レート コントロール パラメータを送信します。これらのエンティティによって ePCO がサポートされていない場合、P-GW や S-GW は、PCO の一部として APN レート コントロール パラメータを送信します。

PCO または ePCO の一部として、APN レート コントロール パラメータが「追加パラメータリスト」として送信されます。特定の「コンテナ識別子」により、コンテナで伝送されるパラメータのタイプが識別されます。APN レートコントロールに関連する「コンテナ識別子」は次のとおりです。

- モバイルステーション（MS）からネットワーク方向：
  - 0016H（APN レート コントロール サポート インジケータ）
  - 0019H（例外データ サポート インジケータの追加 APN レートコントロール）
- ネットワークから MS 方向：
  - 0016H（APN レート コントロール パラメータ）
  - 0019H（例外データパラメータの追加 APN レートコントロール）

[container identifier] が APN レート コントロール サポート インジケータを示している場合、[container identifier contents] フィールドは空で、[length of container identifier contents] はゼロを示しています。[container identifier] フィールドが空でない場合は無視されます。この情報は、MS が APN レートコントロール機能をサポートしていることを示します。

[container identifier] が APN レート コントロール パラメータを示している場合、[container identifier contents] フィールドには APN レートコントロール機能のパラメータが含まれます。

[container identifier] が例外データの追加 APN レート コントロール サポート インジケータを示している場合、[container identifier contents] フィールドは空で、[length of container identifier contents] はゼロを示しています。[container identifier] フィールドが空でない場合は無視されます。この情報は、MS が例外データの追加 APN レートコントロール機能をサポートしていることを示します。

[container identifier] が例外データの追加 APN レート コントロール パラメータを示している場合、[container identifier contents] フィールドには例外データの追加 APN レートコントロール機能のパラメータが含まれます。

APN レート コントロール ステータス

APN レート コントロール ステータスは APN レートコントロール値の情報を保持する新しい IE であり、セッション作成要求（CSReq）、ベアラー削除要求（DBReq）、およびセッション削除応答（DSRes）の一部として追加されました。この IE は、UR 再接続時の CSReq の一部としてエンコードされ、現在のタイムアウト期間にサブスクライバで使用可能な残りの制限について P-GW に示します。

P-GW は、DBReq がデフォルトのベアラーにのみ送信されるときにこの IE を含め、UE が再度接続するときに使用できるようにします。さらに、P-GW は、DSRes が S-GW を介して MME に送信されるときに、この IE を含めます。

	ビット								
オクテット	8	7	6	5	4	3	2	1	
1	タイプ = 204（10 進数）								
2 ～ 3	長さ = n								
4	予備				インスタンス				
5 ～ 8	許可されるアップリンクパケットの数								
9 ～ 12	追加の例外レポートの数								
13 ～ 16	許可されるダウンリンクパケットの数								
17 ～ 24	APN レート コントロール ステータスの有効期間								
25 ～（n+4）	これらのオクテットは、明示的に指定されている場合にのみ存在します。								

オクテット 17 ー 24 は、1900 年 1 月 1 日の 00:00:00 に対する秒単位の時間としてコード化されます（うるう秒のない連続的な時間として計算され、共通の時間基準にトレース可能）。整数部分のバイナリエンコーディングが上位 32 ビットに入り、小数部分のバイナリエンコーディングが下位 32 ビットに入ります。小数部分は、1/2**32 秒の精度で表されます。

APN レート コントロール ステータス情報は、P-GW により S-GW 経由で MME に送信され、APN レートコントロールパラメータがモビリティ管理（MM）コンテキストに保存されます。これは、短い時間内に再確立が行われたされたときに、同じサブスクライバのレートコントロールを復元するのに役立ちます。パラメータは、時間単位の残りの期間で、残りメッセージとして扱われます。

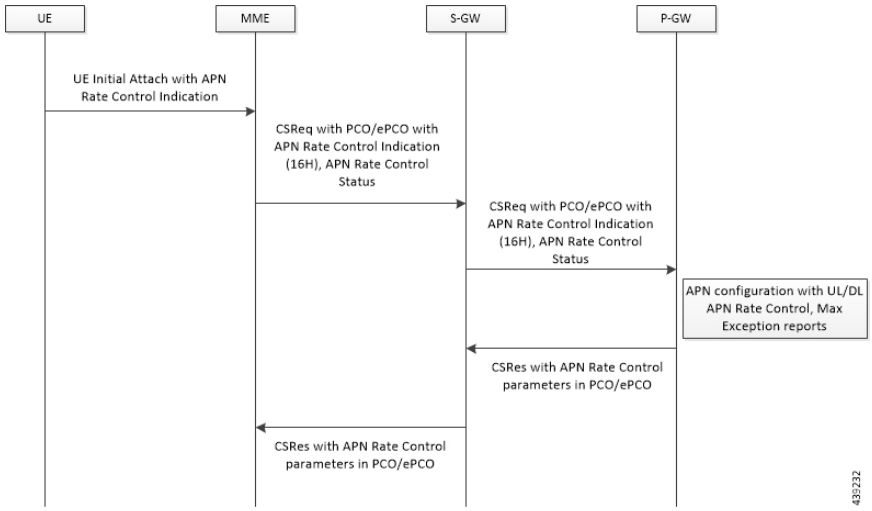
同じサブスクライバが（同じ APN の最初の PDN で）再確立した場合、MME は PCO または ePCO で P-GW に情報を返します。処理の間、P-GW は、最初のタイムアウトが完了するまで、ローカル設定ではなく MME から受信した値を使用します。

コール フロー

ここでは、この機能の主要なコールフローについて説明します。

CSReq 時の P-GW での APN レート制御処理

APN に対するサブスクライバの確立または再確立時に、MME は CSReq で APN レート制限の通知フラグ、追加の例外通知、および APN レート制御ステータスを送信します。



手順	説明
1	APN レート制御通知を含む UE 初期アタッチが、UE から MME に送信されます。
2	P-GW は、CSReq を受信すると、PCO で APN レート制御パラメータをエンコードしている間、および APN レート制御を適用している間、APN レート制御ステータスを考慮します。
3	P-GW では、APN レート制御を適用するための 2 つのオプションがあります。 **1.** 特定の APN に対する最初の PDN 接続がその後確立されると、P-GW/SCEF は以前に保存された APN レート制御ステータスを受信し、最初の APN レート制御の有効期間が期限切れになっていない場合は、受信した APN レート制御ステータスを適用し、関連するパラメータを（設定済みの APN レート制御パラメータの代わりに） PCO で UE に提供します。 **2.** 最初に適用されたパラメータが構成済みの APN レート制御パラメータと異なる場合、P-GW/SCEF は、最初の APN レート制御の有効期間が期限切れになった後に設定済みの APN レート制御パラメータを使用し、設定された APN レート制御パラメータを含む更新を UE に送信します。
4	P-GW は S-GW に CSRes を送信します。 P-GW は、APN レート制御パラメータを準備して PCO/ePCO にエンコードし、APN レート制御パラメータと例外データ用の追加の APN レート制御パラメータを含む CSRes メッセージを S-GW に返送します。
5	S-GW は、（ステップ 4 で P-GW から受信した）情報を MME に転送します。

APN レート制御パラメータは、アップリンク時間単位とサポートされているアップリンクレートに関する情報をエンコードします。

8	7	6	5	4	3	2	1	
予備				AER	アップリンク時間単位			オクテット 1
最大アップリンクレート								オクテット 2 〜オクテット 4

例外データ用の追加の APN レート制御パラメータは、追加の例外データについてサポートされているアップリンク時間単位とアップリンクレートに関する情報をエンコードします。

8	7	6	5	4	3	2	1	
予備					アップリンク時間単位			オクテット 1
例外データ用の追加のアップリンクレート								オクテット 2 〜オクテット 3

ここで、アップリンク時間単位は、次の形式に示すいずれかの値を取ることができます。

アップリンク時間単位（オクテット 1）	
ビット	
3 2 1	
0 0 0	制限なし
0 0 1	Minute
0 1 0	時間
0 1 1	日付
1 0 0	Week

最大アップリンクレート（オクテット 2 からオクテット 4）は、UE で制限されている時間単位あたり送信可能なメッセージの最大数をバイナリコードで表したものです。アップリンクの時間単位が「制限なし」に設定されている場合、UE が送信できる最大アップリンク データ量は制限されません。

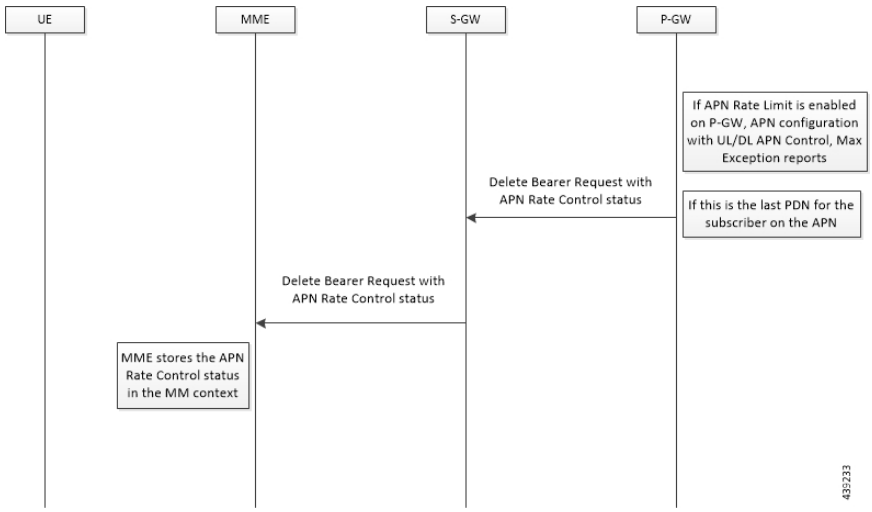
P-GW は、APN レート制御パラメータの UL APN レート制御情報について MME に通知します。この情報は、後で MME によって MM コンテキストで保存されます。

P-GW 側の APN レート制御は、方向ごとの「最大許容レート」に基づいています。P-GW が UE に「時間単位あたり許容される追加の例外レポートパケットの数」を提供した場合、「最大許容レート」は「時間単位あたりのパケット数」に「許可された追加の例外レポートパケットの数」を加えたものに等しくなります。それ以外の場合、「最大許容レート」は「時間単位あたりのパケット数」と等しくなります。

P-GW は、「最大許容レート」を超えるパケットを破棄または遅延させることにより、アップリンクレートを適用します。P-GW は、「最大許容レート」のダウンリンク部分を超えるパケットを破棄または遅延させることにより、ダウンリンクレートを適用します。

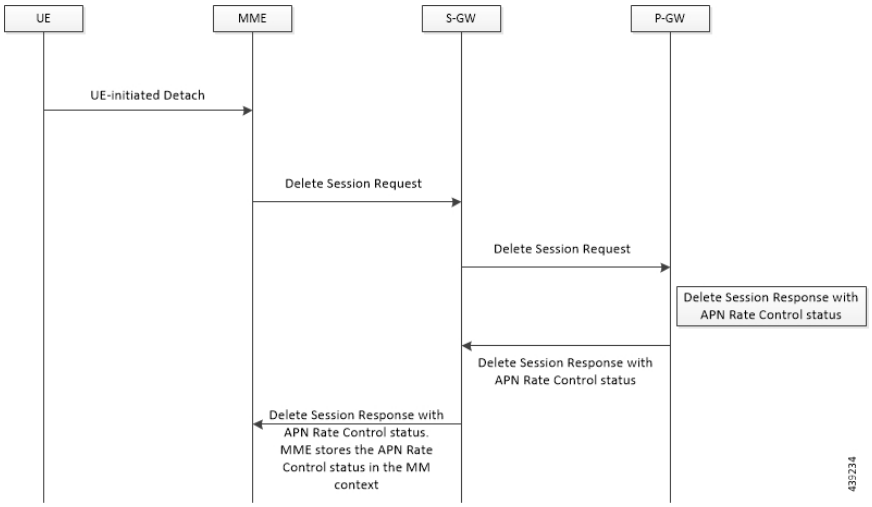
DBReq 時の P-GW での APN レート制御処理

ベアラーの削除時に、現在のベアラーがその指定された APN の PDN で最後のベアラーになることを P-GW が検出した場合、P-GW は、APN レート制御ステータスを、レート制限値の現在のクォータ（残りの時間単位の残りのメッセージ）とともに S-GW を介して MME に含めます。



DSRes での APN レート コントロール パラメータ

DSReq を受信すると、P-GW はサブスクライバをクリアし、APN レート コントロール ステータスを、その時点の残りのクォータおよびサブスクライバのメッセージとともに CSRes で MME に送信して、MM コンテキストを更新します。



ライセンス

CIoT デバイスの APN レート制御は、ライセンスによって制御される機能です。詳細については、シスコのアカウント担当者にお問い合わせください。

標準準拠

CIoT デバイスの APN レートコントロール機能は、以下の標準規格に準拠しています。

- 3GPP TS 29.274 v15.8.0：3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 23.401 v15.7.0：General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access

制限事項と考慮事項

「CIoT デバイスの APN レート制御」機能には、次の制約事項と制限があります。

- この機能は、最も高い優先順位を持ち、他の機能をチェックする前にレート制限が実行されているかどうかをチェックします。
- アップリンクとダウンリンクの両方のレート制限で、同じ時間単位（無制限、分、時間、日、または週）の値が使用されます。異なる値を受け入れることはありません。
- P-GW コールと Collapsed コールに適用されます。
- CIoT サブスクライバにのみ適用されます。CIoT サブスクライバを識別するために RAT タイプのチェックが実行されます。
- CIoT IP PDN にのみ適用されます。この機能は、非 IP PDN には適用されません。

- 再アタッチの場合、P-GW は、アップリンクレート制御操作を実行するために、サブスクライバに残されている APN レート制御パラメータを含む CSRes を UE に送信します。時間単位が期限切れになると、P-GW はクォータを更新しますが、更新されたクォータ値を UE と共有することはありません。UE は、初期アタッチ時にのみ P-GW で設定された APN レート制御値を取得します。
- 仮想 APN の概念がサブスクライバに適用されている場合は、Gi-APN レート制御パラメータが考慮されます。

「CIoT デバイスの APN レート制御」機能の設定

この機能を有効にするには、次の設定を使用します。

```
configure
   context context_name
      apn apn_name
        iot-rate-control time-unit { unrestricted | mins | hours | days
 | week } downlink packet-count dl_packet_count uplink packet-count
ul_packet_count aer aer_value
        end
```

注：

- **time-unit { unrestricted | mins | hours | days | week }**：時間単位のモードを指定します。
- **downlink**：APN レート制御をダウンリンク方向に適用します。
- **packet-count** *dl_packet_count*：許可されるダウンリンクパケットの数を指定します。*dl_packet_count* は、0 ～ 16777215 の整数である必要があります。整数 0 は、ダウンリンク方向のレート制御を無効にします。
- **uplink**：APN レート制御をアップリンク方向に適用します。
- **packet-count** *ul_packet_count*：許可されるアップリンクパケットの数を指定します。*ul_packet_count* は、0 ～ 16777215 の整数である必要があります。整数 0 は、アップリンク方向のレート制御を無効にします。
- **aer** *aer_value*：アップリンク方向の追加例外レポート（AER）の数を指定します。*aer_value* は、1 ～ 65535 の整数である必要があります。
- 以前に設定されている場合は、**no iot-rate-control** CLI コマンドを使用して機能を無効にします。

CIoT デバイスの APN レート制御機能のモニタリングおよび障害対応

ここでは、この機能のモニタリングや障害対応に使用できる CLI コマンドについて説明します。

show コマンドのサポート

この機能をサポートするために、次の show CLI コマンドを使用できます。

show apn statistics

この CLI コマンドの出力が拡張され、次の機能固有フィールドが表示されるようになりました。

- CIoT APN Rate Control：
  - Dropped UL packets：ドロップされた APN レート コントロール アップリンク パケットの総数を表示します。
  - Dropped DL packets：ドロップされた APN レート コントロール ダウンリンク パケットの総数を表示します。
  - Dropped UL bytes：ドロップされた APN レート コントロール アップリンク バイトの総数を表示します。
  - Dropped DL bytes：ドロップされた APN レート コントロール ダウンリンク バイトの総数を表示します。

show session subsystem facility sessmgr all debug-info

この CLI コマンドの出力が拡張され、次の機能固有フィールドが表示されるようになりました。

- CIoT APN Rate Control
  - Dropped UL packets：ドロップされた APN レート コントロール アップリンク パケットの総数を表示します。
  - Dropped DL packets：ドロップされた APN レート コントロール ダウンリンク パケットの総数を表示します。
  - Dropped UL bytes：ドロップされた APN レート コントロール アップリンク バイトの総数を表示します。
  - Dropped DL bytes：ドロップされた APN レート コントロール ダウンリンク バイトの総数を表示します。

show subscriber full all

この CLI コマンドの出力が拡張され、次の機能固有フィールドが表示されるようになりました。

- CIoT APN Rate Control：
  - Allowed UL limit：アップリンク方向に許可されたパケット数を表示します。
  - Allowed DL limit：ダウンリンク方向に許可されたパケット数を表示します。
  - Remaining UL limit：アップリンク方向の残りのパケット数を表示します。
  - Remaining DL limit：ダウンリンク方向の残りのパケット数を表示します。
  - Allowed Time unit：無制限、分、時間、日、または週モードのいずれかで設定された時間単位を表示します。
  - Status Validity Time：YYYY-MM-DD HH:MM:SS 形式で有効時間を表示します。

バルク統計

ここでは、CIoT デバイス機能の APN レートコントロールのバルク統計に関する情報を提供します。

APN スキーマ

CIoT デバイスの APN レート制御機能をサポートするために、APN スキーマで次のバルク統計が使用できます。

バルク統計	説明
apn-rate-control-ul-pkt-drop	ドロップされた APN レート制御アップリンクパケットの合計数を示します。
apn-rate-control-dl-pkt-drop	ドロップされた APN レート制御ダウンリンクパケットの合計数を示します。
apn-rate-control-ul-bytes-drop	ドロップされた APN レート制御アップリンクの合計バイト数を示します。
apn-rate-control-dl-bytes-drop	ドロップされた APN レート制御ダウンリンクの合計バイト数を示します。

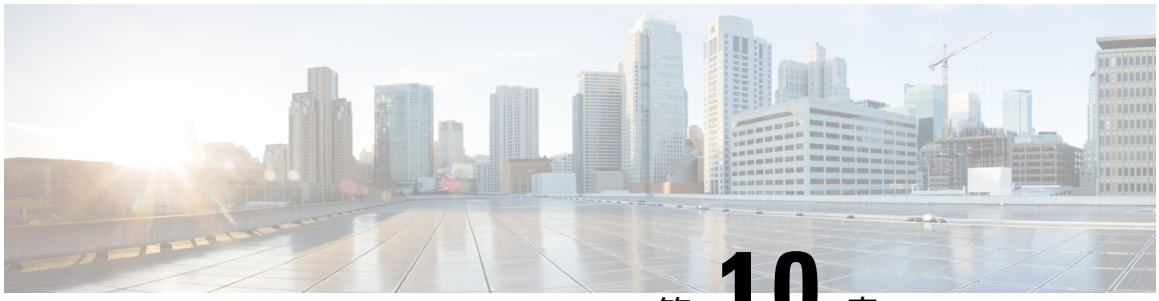
アカウンティングのサポート

CIoT デバイス機能の APN レート制御のサポートで使用可能な GTPP ディクショナリの詳細を次の表に示します。

CDR ディクショナリまたはフィールド	
ディクショナリの変更タイプ（新規または変更）：	変更内容
ディクショナリ名：	P-GW custom24 GTPP ディクショナリ
基づく 3GPP 仕様：	3GPP TS 32.299
適用可能なレコードタイプ：	G-CDR
適用可能な製品：	P-GW

次の CDR フィールドが P-GW custom24 GTPP ディクショナリに導入されました。

1. フィールド名：datapacketsFBCDownlink
   - 説明：ダウンリンクパケット数
   - 形式：整数
   - フィールドを設定する CLI コマンド：**gtpp fbc-downlink-pkt-cnt**
   - フィールドのデフォルト値：0
2. フィールド名：datapacketsFBCUplink
   - 説明：アップリンクパケット数
   - 形式：整数
   - フィールドを設定する CLI コマンド：**gtpp fbc-uplink-pkt-cnt**
   - フィールドのデフォルト値：0



第 10 章

主要なKPI統計のバックアップとリカバリ

この機能により、GGSN、P-GW、SAEGWや、S-GWカウンタをバックアップして、セッションマネージャ（SessMgr）の再起動後に主要なKPIカウンタ値をリカバリできます。

この章には次の情報が含まれます。

- 機能説明 （275 ページ）
- 機能の仕組み （275 ページ）
- 統計バックアップ機能の設定 （278 ページ）

機能説明

主要なKPI統計のバックアップとリカバリ機能が導入される前は、統計はバックアップされず、SessMgrタスクの再起動後に統計を回復できませんでした。この制限により、GGSN、P-GW、SAEGW、およびS-GWではタスクの再起動が発生するたびに統計が失われるため、KPIのモニタリングが問題でした。

KPIの計算では、2つの時間間隔のカウンタ値間の差分を取得し、その時間間隔で特定の手順が正常に処理された割合を決定します。SessMgrがクラッシュしてから回復すると、GGSN、P-GW、SAEGW、およびS-GWはカウンタ値を失い、ゼロにリセットされます。そのため、次の間隔でKPIを計算すると、その間隔については負の値になります。その結果、KPI値を使用してプロットされたグラフが表示されなくなり、運用チームがネットワークパフォーマンスの一貫したビューを取得して、本当に問題があるかどうかを判断することが困難になります。

この機能により、SessMgrの再起動が発生した場合でも信頼性の高いKPI計算を実行できます。

機能の仕組み

KPIの計算で使用される主要なカウンタのセットは、SessMgrタスクが再開された場合のリカバリのためにバックアップされます。バックアップされるカウンタは、複数のオペレータネットワークで通常使用されるKPIによって決定されます。

カウンタのバックアップは、設定によって有効化または無効化されます。設定では、カウンタがバックアップされる製品（GGSN、P-GW、SAEGW、S-GWまたはこれらの組み合わせ）と、カウンタをバックアップする時間間隔を指定します。

アーキテクチャ

この機能が有効になっている場合（以下の「統計情報バックアップ機能の設定」を参照）、GGSN、P-GW、SAEGW、およびS-GW（またはそのいずれか）は、SessMgrで保持されているカウンタのみをバックアップします。リカバリ機能は、機能が有効になっているときに必要に応じて自動的に実行されるため、設定や開始を行う必要はありません。

カウンタはSessMgrとペアになっているAAAMgrにバックアップされます。

チェックポインティング

ノードレベルの統計情報は、AAAMgrでチェックポインティングされます。特定の製品の統計情報がバックアップされると、関連するすべてのサービス（eGTP-CやGTP-Uなどの統計情報など）もチェックポインティングされます。

リカバリ

SessMgrが再起動すると、保存されているすべての統計情報をマッピングされたAAAMgrから受信することによってリカバリが実行され、復元された値が、サービスレベルごとに保持されているバックアップカウンタに追加されます。バックアップされたカウンタはセッションリカバリが完了した後にのみSessMgrにプッシュされるため、これはセッションリカバリ時間には影響しません。

セッションリカバリが完了したため、セッションマネージャはコールの処理を開始できます。このような場合、カウンタは引き続き増分されます。対応するカウンタのリカバリされた値は常に既存のカウンタに追加されます。ゲージカウンタはチェックポインティングされますが、リカバリされません。

統計情報収集の順序

チェックポイントメッセージングの上限は1 MBです。チェックポインティングするノードを選択する前に、使用可能なメモリがチェックされます。メモリが不足している場合は、ノード全体が廃棄されます。

1 MBの制限があるため、チェックポインティング対象のノード/統計情報は、次のように優先順位付けされます。

1. SAEGW統計情報：
   - P-GWおよびS-GWサービスノードレベルの収集された統計情報
2. P-GWサービスノード構成では、次の統計情報が保存されます。
   - P-GW、eGTP-C入力、GTP-U入力、インターフェイスごと（s2a、s2b、s5s8）、およびGGSN（関連付けられている場合）の収集された統計情報
   - SAEGWに関連付けられたP-GWサービスの収集されていない統計情報

3. S-GW サービスノード構成では、次の統計情報が保存されます。
   - S-GW、eGTP-C 入力/出力、および GTP-U 入力/出力の収集された統計情報
   - SAEGW に関連付けられた S-GW サービスの収集されていない統計情報
4. GGSN 統計情報：
   - GGSNサービスの収集された統計情報（P-GWサービスに関連付けられていない場合）
5. 収集されたセッション切断の理由（GGSN/P-GW/SAEGW/S-GWが有効になっている場合）

エラー処理

追加している新しい統計情報により 1 MB バッファのオーバーフローが発生する場合、そのサービスと対応するノードは含まれません。それ以降のノードのチェックポインティングもすべて停止されます。合計メモリ要件が 1 MB を超えた場合、エラーレベルのログにフラグが付けられます。

制限事項

- バックアップ間隔を指定する必要があり、カウンタは、指定された間隔でのみバックアップされます。たとえば、バックアップ間隔が 5 分に指定されている場合、カウンタは 5 分ごとにバックアップされます。バックアップがN分目で発生し、設定されたバックアップ間隔が 5 分ごとであると仮定すると、タスクのクラッシュが N＋4 分目で発生した場合、GGSN、P-GW、SAEGW、および/またはS-GWは、N分目にバックアップされた値のみを復元し、過去 4 分間のデータは失われます。
- SessMgr で保持されている統計のみがバックアップされます。他のマネージャの統計は、バックアップまたは復元されません。
- 次の統計はバックアップの対象になりません。
  - APN レベルの統計
  - eGTP-C APN-QCI の統計
  - DemuxMgr の統計
- CLI コマンド **clear statistics** は、AAAMgr のノード統計を削除するためのチェックポイントをトリガーしません。タイマーの期限が切れた後の新しいチェックポイントで、統計が上書きされます。
- 最大 1 MB の統計が AAAMgr に保存されます。最大サイズ制限後のサービスは、バックアップされません。
- バックアップ間隔をより短い期間に設定すると、チェックポイントのシステムオーバーヘッドが増加します。また、バックアップ間隔をより長い期間に設定すると、チェックポイントのシステムオーバーヘッドは減少しますが、1 MB のストレージ制限に達する可能性は高まります。

- SessMgr が AAAMgr から統計を復元する前に、SessMgr が再起動し、AAAMgr が再起動した場合、バックアップされた統計は失われます。
- この機能は、ICSR には適用されません。

統計バックアップ機能の設定

主要 KPI 統計のバックアップおよびリカバリ機能を有効にするには、GGSN、P-GW、SAEGW や、S-GW の統計のバックアップを設定する必要があります。

設定

以下の CLI コマンドを使用して、主要 KPI 統計のバックアップ機能を管理します。

イネーブル化

次のコマンドは、GGSN、P-GW、SAEGW、S-GW の統計のバックアップを設定し、主要な KPI 統計のバックアップとリカバリの機能を有効にします。

```
configure
     statistics-backup { ggsn | pgw | saegw | sgw }
     exit
```

バックアップ間隔の設定

次のコマンドは、統計のバックアップ間隔を分単位（0～60）で設定します。バックアップ間隔が指定されていない場合、デフォルト値の 5 分がバックアップ間隔として使用されます。

```
configure
     statistics-backup-interval minutes
     exit
```

重要 バックアップ間隔をより短い期間に設定すると、チェックポイントのシステムオーバーヘッドが増加します。また、バックアップ間隔をより長い期間に設定すると、チェックポイントのシステムオーバーヘッドは減少しますが、1 MB のストレージ制限に達する可能性は高まります。

モバイル IP を無効にすると、関連するすべてのコンフィギュレーション コマンド（グローバル コンフィギュレーション コマンドとインターフェイス コンフィギュレーション コマンドの両方）が削除されます。

次のコマンドは、GGSN、P-GW、SAEGW、S-GW の統計のバックアップを無効にするように GGSN、P-GW、SAEGW、S-GW を設定します。

```
configure
     no statistics-backup { ggsn | pgw | saegw | sgw }
     exit
```

統計バックアップ機能の設定の確認

show configuration コマンドまたは **show configuration verbose** コマンドを使用して、機能設定を表示します。

この機能が設定で有効になっている場合、**show configuration [verbose]** コマンドの出力に、次のような 2 つの行が表示されます。

```
statistics-backup  pgw
statistics-backup-interval 5
```

注：

- 表示される間隔は 5 分です。5 がデフォルトです。**statistics-backup-interval** コマンドが設定に含まれている場合、5 は設定された間隔（分）に置き換えられます。
- 機能を無効にするコマンドを入力すると、**show configuration [verbose]** コマンドによって生成される出力に statistics-backup の行は表示されません。



第 11 章

ベアラーの再確立

- 機能の概要と変更履歴 （281 ページ）
- ベアラー再確立の概要 （282 ページ）
- 機能の仕組み （282 ページ）
- S-GW から P-GW へのベアラー要求転送の変更の有効化 （283 ページ）
- P-GWによる、新しいイベント復元ベアラーを使用したローカルポリシーの呼び出し （283 ページ）
- コマンドと出力の表示 （285 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

表 *29 :* マニュアルの変更履歴

改訂の詳細	リリース
初版	21.19

ベアラー再確立の概要

UE リレーネットワークは、複数の RAN ノードおよび EPC ノードで構成されます。

一部の展開では、1 つの MME が、ユーザー UE MME とリレー UE MME の両方の役割を果たします。

UE リレーネットワークでは、System Architecture Evolution Gateway（SAEGW）が展開され、組み合わされた「リレー UE の SGW/P-GW」の役割を果たします。SAEGW は、ローカルポリシーのみを使用して設定されます（つまり、PCRF には接続しない）。

リレーノード UE からの初期アタッチ要求の一部として、P-GW（前述の SAEGW 内）は、デフォルトのベアラー（QCI6 など）の上に専用のベアラー（GBR 用の QCI-1、非 GBR 用の QCI5 など）を作成します。これは、この章の後のセクションで説明する適切なローカルポリシー設定に基づいて行われます。

RF 条件が劣化すると、リレーノード UE はマクロ eNB への RRC 接続を失います。結果として、マクロ eNB は、異常な原因（「UE との無線接続が失われた」、「未指定」など）による S1 リリース手順を開始します。これらのタイプの原因に対して、MME は通常、非 GBR ベアラーを保持し、GBR ベアラーを削除します。その結果、GBR ベアラー（QCI-1 ベアラーなど）は、MME によって削除されます。

RRC 接続が再確立されると、リレーノード UE が MME にサービス要求を送信します。MME は、以前に保持された非 GBR ベアラーをセットアップするために、初期コンテキストセットアップ要求をマクロ eNB に送信します。GBR ベアラーは保持されなかったため、MME は GBR ベアラーを再確立しません。その結果、完全な再アタッチ手順が発生するまで、リレーノード UE には GBR ベアラーがありません。

GBR ベアラーが再確立されないため、GBR トラフィックはデフォルトの非 GBR ベアラーを介して伝送され、音声パフォーマンスが低下します。

MME がベアラー変更要求を送信して、保存されている非 GBR ベアラーを再確立するときに、SAEGW は、この機能を使用して、以前に削除された GBR ベアラーを再確立できます。

機能の仕組み

SAEGW は、MME がベアラー変更要求を送信すると、以前に削除された GBR ベアラーを再確立して、保存されている非 GBR ベアラーを再確立します。

この動作は、SAEGW で 2 つの異なるメカニズムを使用して実現されます。

- SGW から P-GW へのベアラー変更要求の転送

• P-GW による、新しいイベント復元ベアラーを使用したローカルポリシーの呼び出し

S-GW から P-GW へのベアラー要求転送の変更の有効化

次の設定を使用して、S-GW から P-GW へのベアラー変更要求の強制転送を有効にします。

```
configure
   context context_name
      sgw-service service_name
         enable-bearer-restore
         end
```

S-GW サービスでは、**enable-bearer-restore** オプションが設定されるたびに、ベアラー変更要求が S-GW によって P-GW に転送されます。この転送は、S-GW サービスが SAEGW サービスに属している場合に発生します。

次に例を示します。

```
config
   context ingress
     sgw-service sgw-service
        enable-bearer-restore
```

（注）
- この CLI がない場合、S-GW は、特定の条件が満たされた場合にのみ、ベアラー変更要求メッセージを P-GW に転送します。次に例を示します。3GPP 仕様に準拠した RAT の変更、タイムゾーンの変更、URI の変更、ハンドオーバー通知フラグなど。
- ベアラー変更要求が不必要に P-GW に転送されないようにするために、**enable-bearer-restore** は、次のセクションで説明するように、**restore-bearer** イベントにローカルポリシーが設定されている場合にのみ使用する必要があります。

P-GW による、新しいイベント復元ベアラーを使用したローカルポリシーの呼び出し

eventbase でサポートされるイベントのリストが、restore-bearers で強化されています。このイベントは、P-GW が S-GW からベアラー変更要求を受信したときに呼び出されます。ローカルポリシーの設定で、**eventbase** に **restore-bearer** イベントがある場合、対応するルールが適用されます。

ローカルポリシーにないベアラーを再確立するには、次の設定を使用します。

```
configure
   local-policy-service local_policy_name
      eventbase eventbase_name
         [ no ] rule priority integer
```

event restore-bearers ruledef *ruledef_name* **actiondef** *actiondef_name*

end

ローカルポリシーの設定例を次に示します。

```
  local-policy-service local_policy
    ruledef apn_apn2
      condition priority 100 apn match apn2.com
    #exit
ruledef apn_apn1
      condition priority 100 apn match apn1.com
    #exit
    ruledef ded_bearer_creation_fail
      condition priority 100 apn match apn2.com
      condition priority 200 cause-code match 72 73 90 100 110
    #exit
    actiondef apn2_newcall
      action priority 100 allow-session
      action priority 500 activate-rule name apn2_dedicated_grp_of_rd
      action priority 600 activate-rule name apn2_qci1_dedicated_grp_of_rd
    #exit
    actiondef apn2_restore_bearer_config
      action priority 100 allow-session
      action priority 500 activate-rule name apn2_dedicated_grp_of_rd
      action priority 600 activate-rule name apn2_qci1_dedicated_grp_of_rd
    #exit
    actiondef apn2_retry_dedicated_bearer
      action priority 500 activate-rule name apn2_dedicated_grp_of_rd
      action priority 600 activate-rule name apn2_qci1_dedicated_grp_of_rd
      action priority 700 retry-count 4
      action priority 2000 allow-session
    #exit
actiondef apn1_newcall
      action priority 100 allow-session
    #exit
eventbase default
      rule priority 100 event new-call ruledef apn_apn1 actiondef apn1_newcall
      rule priority 200 event new-call ruledef apn_apn2 actiondef apn2_newcall
     rule priority 400 event rule-report-status ruledef ded_bearer_creation_fail actiondef
 apn2_retry_dedicated_bearer
      rule priority 600 event restore-bearers ruledef apn_apn2 actiondef
apn2_restore_bearer_config
    #exit
```

上記の設定で重要な点は、「new-call」イベントと「restore-bearers」イベントの両方で、actiondef が同じアクションで構成されていることです。その結果、欠落しているベアラー（QCI-1 GBR ベアラーなど）が確立されます。

「new-call」イベントの時点で、QCI-1（GBR）と QCI-5（非 GBR）の両方のベアラーが作成されます。「restore-bearer」イベントの時点で、ローカルポリシーは QCI-1 と QCI-5 の両方のベアラーを作成するアクションを返しますが、QCI-5 ベアラーはすでに存在するため（保存されているため）、QCI-1 ベアラーのみが確立されます。

コマンドと出力の表示

show saegw-service statistics all

このコマンドの出力には、enable-bearer-restore フラグにより SGW がベアラー変更要求を PGW に転送した回数が表示されます。

このコマンドの出力には、次のフィールドが含まれています。

MBR：ダイナミック ユーザー プレーン選択の統計を表示します。

- Attempted：enable-bearer-restore フラグによる S-GW と P-GW 間のベアラー変更要求が試行された回数を表示します。
- Successful：enable-bearer-restore フラグによる S-GW と P-GW 間のベアラー変更要求が成功した回数の合計を表示します。
- Failure：enable-bearer-restore フラグによる S-GW と P-GW 間のベアラー変更要求が失敗した回数の合計を表示します。
- Mismatch DNS response ：enable-bearer-restore フラグによる S-GW と P-GW 間の不一致 DNS 応答を表示します。
- Negative DNS response：enable-bearer-restore フラグによる S-GW と P-GW 間のネガティブ DNS 応答を表示します。
- DNS timed out：enable-bearer-restore フラグによる S-GW と P-GWD 間の DNS タイムアウトを表示します。

show local-policy statistics all

このコマンドの出力には、S-GW が P-GW にベアラー変更要求を送信したときのイベントベースのローカルポリシーに登録されているイベントのリストが表示されます。

このコマンドの出力には、次のフィールドが含まれています。

Restore Bearers：ローカルポリシー設定の restore-bearer の有効化と無効化を表示します。



第 12 章

IP プールごとの平均データレートのバルク統計

- 機能の概要と変更履歴 （287 ページ）
- 機能説明 （288 ページ）
- モニタリングおよびトラブルシューティング （288 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• GGSN • P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI
機能のデフォルト	有効、常時オン
このリリースでの関連する変更点	N/A
関連資料	*Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
IP プールグループの数が 2000 から 5000 に増加しました。	21.26
最初の導入。	21.3

機能説明

バルク統計のサポートが拡張され、IPプールごとのサブスクライバ平均データレート（すべてのセッションマネージャの累積）が取得されるようになりました。平均データレートは、システムに設定されているすべての IP プールで構成されます。

バルク統計の収集時間が、datarate-ippool スキーマで拡張されました。このスキーマは、構成時に最大 5000 の IP プールグループをサポートします。

モニタリングおよびトラブルシューティング

ここでは、この機能をサポートする show コマンドおよび使用可能なバルク統計を使ったモニタリングと障害対応の方法について説明します。

バルク統計

この機能では、次のバルク統計がサポートされています。

Datarate-IPPool スキーマ

次のバルク統計が Datarate-IPPool スキーマに追加されました。

- sess-datarate-ippool-name：平均データレートが取得される IP プールの名前を示します。
- sess-ave-rate-fuser-bps：アップリンク方向にユーザーから送られるIPプール単位の平均データレート（ビット/秒）を示します。
- sess-ave-rate-tuser-bps：アップリンク方向にユーザーに送られる IP プール単位の平均データレート（ビット/秒）を示します。
- sess-ave-rate-fuser-pps：アップリンク方向にユーザーから送られる IP プール単位の平均パケット/秒を示します。
- sess-ave-rate-tuser-pps：ダウンリンク方向にユーザーに送られるIPプール単位の平均パケット/秒を示します。

show コマンドと出力

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show bulkstats schema

表 *30 : show bulkstats schema* コマンド出力の説明

フィールド	説明
バルク統計サーバーの設定	
Server State	サーバーの状態（有効または無効）を示します。
File Limit	ファイルサイズの上限を KB 単位で示します。
Sample Interval	サンプリング間隔を示します。
Transfer Interval	転送間隔を示します。
Receiver Mode	レシーバーモードを示します。
Local File Storage	ローカルファイルストレージを示します。
バルク統計サーバーの統計	
Records awaiting transmission	送信を待機しているレコードの数を示します。
Bytes awaiting transmission	送信を待機しているバイト数を示します。
Total records collected	収集されたレコードの合計数を示します。
Total bytes collected	収集された合計バイト数を示します。
Total records transmitted	送信されたレコードの合計数を示します。
Total bytes transmitted	送信された合計バイト数を示します。
Total records discarded	破棄されたレコードの合計数を示します。
Total bytes discarded	破棄された合計バイト数を示します。
Last collection time required	必要な最後の収集時間を示します。
Last transfer time required	必要な最後の転送時間を示します。
詳細 n	
Remote File Format	リモートファイル形式（%date%-%time% など）
File Header	ファイルのヘッダー。
File Footer	ファイルのフッター。
ファイルごとの統計	
Records awaiting transmission	送信を待機しているレコードの数を示します。

フィールド	説明
Bytes awaiting transmission	送信を待機しているバイト数を示します。
Total records collected	収集されたレコードの合計数を示します。
Total bytes collected	収集された合計バイト数を示します。
Total records transmitted	送信されたレコードの合計数を示します。
Total bytes transmitted	送信された合計バイト数を示します。
Total records discarded	破棄されたレコードの合計数を示します。
Total bytes discarded	破棄された合計バイト数を示します。
Last transfer time required	必要な最後の転送時間を示します。
No successful data transfers	正常なデータ転送の合計数を示します。
No attempted data transfers	試行されたデータ転送の合計数を示します。

show bulkstats data

表 31 : show bulkstats data コマンド出力の説明

フィールド	説明
バルク統計サーバーの設定	
サーバの状態	サーバーの状態（有効または無効）を示します。
File Limit	ファイルサイズの上限を KB 単位で示します。
Sample Interval	サンプリング間隔を示します。
Transfer Interval	転送間隔を示します。
Receiver Mode	レシーバーモードを示します。
Local File Storage	ローカルファイルストレージを示します。
Historical Data Collection	履歴データ収集の状態（有効または無効）を示します。
バルク統計サーバーの統計	
Records awaiting transmission	送信を待機しているレコードの数を示します。
Bytes awaiting transmission	送信を待機しているバイト数を示します。
Total records collected	収集されたレコードの合計数を示します。

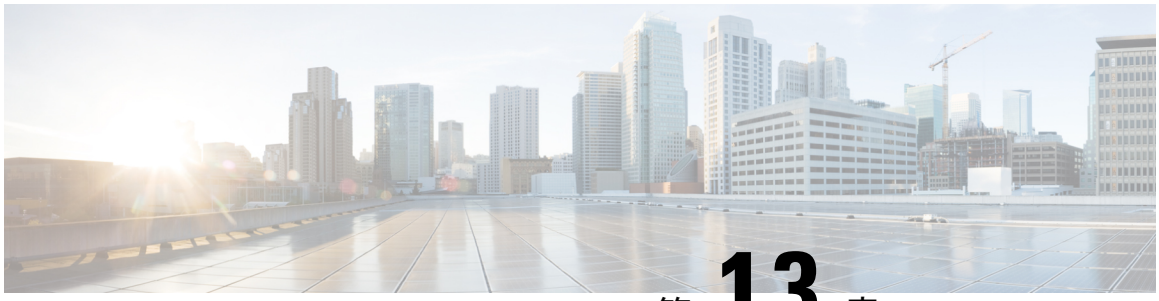
フィールド	説明
Total bytes collected	収集された合計バイト数を示します。
Total records transmitted	送信されたレコードの合計数を示します。
Total bytes transmitted	送信された合計バイト数を示します。
Total records discarded	破棄されたレコードの合計数を示します。
Total bytes discarded	破棄された合計バイト数を示します。
Last collection time required	必要な最後の収集時間を示します。
Last transfer time required	必要な最後の転送時間を示します。
No successful data transfers	正常なデータ転送の合計数を示します。
No attempted data transfers	試行されたデータ転送の合計数を示します。
詳細 n	
Remote File Format	リモートファイル形式（%date%-%time% など）
File Header	ファイルのヘッダー。
File Footer	ファイルのフッター。
バルク統計の受信者数	設定されているバルク統計収集サーバーの合計数を示します。
ファイルごとの統計	
Records awaiting transmission	送信を待機しているレコードの数を示します。
Bytes awaiting transmission	送信を待機しているバイト数を示します。
Total records collected	収集されたレコードの合計数を示します。
Total bytes collected	収集された合計バイト数を示します。
Total records transmitted	送信されたレコードの合計数を示します。
Total bytes transmitted	送信された合計バイト数を示します。
Total records discarded	破棄されたレコードの合計数を示します。
Total bytes discarded	破棄された合計バイト数を示します。
Last transfer time required	必要な最後の転送時間を示します。
No successful data transfers	正常なデータ転送の合計数を示します。
No attempted data transfers	試行されたデータ転送の合計数を示します。

フィールド	説明
ハンドオフ統計	
epdg-handoff-disc	LTE から Wi-Fi への HO 切断理由統計を設定します。
show epdg-service statistics handoff-disc-reasons	すべてのサービスで LTE から Wi-Fi への HO 切断理由に対応する統計を表示します。
clear epdg-service statistics handoff-disc-reasons	すべてのサービスで LTE から Wi-Fi への HO 切断理由に対応する統計を削除します。

show subscribers data-rate ip-pool <pool_name>

表 *32 : show subscribers data-rate ip-pool <pool_name>* コマンドの出力の説明

フィールド	説明
pk rate from user (bps)	最後のサンプリング期間中にサブスクライバからネットワークに送信されたデータについて取得されたピークデータレート（ビット/秒）。
peak rate to user (bps)	最後のサンプリング期間中にサブスクライバがネットワークから受信したデータについて取得されたピークデータレート（ビット/秒）。
ave rate from user (bps)	最後のサンプリング期間中にサブスクライバからネットワークに送信されたデータについて取得された平均データレート（ビット/秒）。
ave rate to user (bps)	最後のサンプリング期間中にサブスクライバがネットワークから受信したデータについて取得された平均データレート（ビット/秒）。
sust rate from user (pps)	最後の3つのサンプリング期間中にサブスクライバからネットワークに送信されたデータについて取得された平均データレート（パケット/秒）。
sust rate to user(pps)	最後の3つのサンプリング期間にサブスクライバがネットワークから受信したデータについて取得された平均データレート（パケット/秒）。



第 13 章

ARP 値別の GTP-C メッセージのバルク統計

この章では、P-GW、SAE-GW、および S-GW での、ARP 値による GTP-C メッセージのバルク統計機能に対する StarOS のサポートについて説明します。

- 機能説明 （293 ページ）
- パフォーマンス指標の変更 （294 ページ）

機能説明

「Long Term Evolution (LTE) Access Network Government Industry Requirements (GIR) for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority」に適合し、Voice over LTE（VoLTE）上の緊急通話をサポートするために、この機能にはいくつかのキーパフォーマンスインジケータ（KPI）が導入されています。この機能は、指定された間隔（分単位）に Enhanced Multimedia Priority Service（eMPS）セッションで受信された GTP-C メッセージの合計数の統計を収集するために使用されます。GTP-C メッセージのリストは、GIR のドキュメントに従って定義されます。この機能の一部として、次の処理が実行されます。

- S-GW は、NS/EP NGN-PS の使用に割り当てられた値のセットから選択された割り当ておよび保持プライオリティ（ARP）を含む、受信した GTP-C メッセージの総数のペグカウントを指定された間隔（分単位）で生成します。このペグカウントは、S-GW レベルで管理されます。
- P-GW は、NS/EP NGN-PS の使用に割り当てられた値のセットから選択された ARP を含む、受信した GTP-C メッセージの総数のペグカウントを指定された間隔（分単位）で生成します。このペグカウントは、特定の P-GW レベルで管理されます。
- GTP-C メッセージのペグカウントは、既存の GTP-C メッセージカウンタと同様にメッセージタイプ別に分類されます。バルク統計は、該当する S-GW および P-GW サービス、および S5、S8、S11、S4 インターフェイスによって分類されます。

eMPS セッション/メッセージのバルク統計が追加されました。

ピギーバックメッセージ

ピギーバックメッセージの場合、いずれかのメッセージが一致する ARP を含む場合、または最終的に非 eMPS セッションが eMPS セッションに変換される場合、両方のメッセージが eMPS メッセージとしてカウントされ、両方のメッセージに対応する統計が増分されます。

ベアラー変更要求が S-GW の S11 インターフェイスでベアラー作成応答と共にピギーバックされ、ベアラー作成応答が最終的に非 eMPS セッションから eMPS セッションに変換される場合、ベアラー変更応答の統計は増分されません。

バルク統計の収集とリセット

バルク統計は、eGTP-C スキーマと pgw-egtpc-s5s8 スキーマに追加されます。eGTP-C スキーマおよび pgw-egtpc-s5s8 スキーマのこれらの eMPS バルク統計は、次のバルク統計までの間のみ値を保持します。つまり、これらのバルク統計の値は、次のバルク統計までに交換された eMPS メッセージの数を示します。

制限事項

ここでは、この機能の既知の制限について説明します。

- ピアレベルと APN レベルの統計は収集されません。
- MPS 統計のリカバリはサポートされていません。
- eMPS セッションの ARP を使用した demux によって拒否された CSReq、DDNReq、および変更通知メッセージについては、MPS 統計は収集されません。
- 再試行または再送信されたメッセージについては、MPS 統計は収集されません。

ライセンス



重要 ARP 値による GTP-C メッセージのバルク統計を使用するには、有効なライセンスキーをインストールする必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

パフォーマンス指標の変更

S-GW 入力 S4 インターフェイス

次の CLI コマンドが変更され、S-GW 入力の S4 インターフェイスの eMPS セッション関連 GTP-C メッセージ統計が表示されるようになりました。

- **show egtpc statistics interface sgw-ingress interface-type s4**

- **interface-type**：インターフェイスレベルの GTP-C メッセージ統計を表示します
- **s4**：S4 インターフェイスのインターフェイスレベルの GTP-C メッセージ統計を表示します

- **show egtpc statistics egtp-service** *sgw_egtpc_service_name* **interface-type s4**
  - **s4**：S-GW eGTP-C インターフェイスのインターフェイスタイプ S4

上記の CLI コマンドの出力には、以下の新しいパラメータが表示されます。

- **eMPS 統計の合計**：eMPS セッションで送受信されたメッセージの累積 GTP-C メッセージ統計。
- **現在の間隔 eMPS 統計**：現在の統計収集間隔における、eMPS セッションで送受信されたメッセージの GTP-C メッセージ統計。統計の収集間隔は、バルク統計の収集間隔と同じになります。バルク統計の収集が設定されていない場合、現在の MPS 統計は MPS 統計の合計と同じになります。
- **セッション作成要求（合計 RX）**：このカウンタは、S4 インターフェイスで、MPS プロファイルで設定された ARP 値を含むセッション作成要求メッセージを受信したときに、S-GW によって増加されます。
- **セッション作成応答（合計 TX）**：このカウンタは、S4 インターフェイスで、MPS プロファイルで設定された ARP 値を含むセッション作成応答メッセージを送信したときに、S-GW によって増加されます。

S-GW 入力 S11 インターフェイス

次の CLI コマンドが変更され、S-GW 入力の S11 インターフェイスの eMPS セッション関連 GTP-C メッセージ統計が表示されるようになりました。

- **show egtpc statistics interface sgw-ingress interface-type s11**
  - **interface-type**：インターフェイスレベルの GTP-C メッセージ統計を表示します
  - **s11**：S11 インターフェイスのインターフェイスレベルの GTP-C メッセージ統計を表示します。

- **show egtpc statistics egtp-service** *sgw_egtpc_service_name* **interface-type s11**
  - **s11**：S-GW eGTP-C インターフェイスのインターフェイスタイプ S11

上記の CLI コマンドの出力には、以下の新しいパラメータが表示されます。

- **eMPS 統計の合計**：eMPS セッションで送受信されたメッセージの累積 GTP-C メッセージ統計。
- **現在の間隔 eMPS 統計**：現在の統計収集間隔における、eMPS セッションで送受信されたメッセージの GTP-C メッセージ統計。統計の収集間隔は、バルク統計の収集間隔と同じ

になります。バルク統計の収集が設定されていない場合、現在の MPS 統計は MPS 統計の合計と同じになります。

- **セッション作成要求（合計 RX）**：このカウンタは、S11 インターフェイスで、MPS プロファイルで設定された ARP 値を含むセッション作成要求メッセージを受信したときに、S-GW によって増分されます。
- **セッション作成応答（合計 TX）**：このカウンタは、S11 インターフェイスで、MPS プロファイルで設定された ARP 値を含むセッション作成応答メッセージを送信したときに、S-GW によって増分されます。
- **ベアラー変更要求（合計RX）**：このカウンタは、S11インターフェイスで、MPSプロファイルで設定されたARP値を含むベアラー変更要求メッセージを受信したときに、S-GWによって増分されます。
- **ベアラー変更応答（合計TX）**：このカウンタは、S11インターフェイスで、MPSプロファイルで設定されたARP値を含むベアラー変更応答メッセージを送信したときに、S-GWによって増分されます。
- **ベアラー作成要求（合計TX）**：このカウンタは、S11インターフェイスで、MPSプロファイルで設定されたARP値を含むベアラー作成要求メッセージを送信したときに、S-GWによって増分されます。
- **ベアラー作成応答（合計RX）**：このカウンタは、S11インターフェイスで、MPSプロファイルで設定されたARP値を含むベアラー作成応答メッセージを受信したときに、S-GWによって増分されます。
- **ダウンリンクデータ通知（合計 TX）**：このカウンタは、S11 インターフェイスで、MPS プロファイルで設定された ARP 値を含むダウンリンクデータ通知メッセージを送信したときに、S-GW によって増分されます。
- **ダウンリンクデータ通知確認（合計 RX）**：このカウンタは、S11 インターフェイスで、MPS プロファイルで設定された ARP 値を含むダウンリンクデータ通知確認メッセージを受信したときに、S-GW によって増分されます。
- **ベアラー更新要求（合計TX）**：このカウンタは、S11インターフェイスで、MPSプロファイルで設定されたARP値を含むベアラー更新要求メッセージを送信したときに、S-GWによって増分されます。
- **ベアラー更新応答（合計RX）**：このカウンタは、S11インターフェイスで、MPSプロファイルで設定されたARP値を含むベアラー更新応答メッセージを受信したときに、S-GWによって増分されます。

S-GW 出力の GTP ベース S5/S8 インターフェイス

次の CLI コマンドは、S-GW 出力の S5/S8 インターフェイスの eMPS セッション関連 GTP-C メッセージ統計を表示するように変更されています。

- **show egtpc statistics interface sgw-egress interface-type s5s8**

- **interface-type**：インターフェイスレベルの GTP-C メッセージ統計を表示します
- **s5s8**：S5/S8 インターフェイスのインターフェイスレベルの GTP-C メッセージ統計を表示します。

- **show egtpc statistics egtp-service** *sgw_egtpc_service_name* **interface-type sgw-s5s8**
  - **sgw-s5s8**：S-GW eGTP-C インターフェイスのインターフェイスタイプ S5/S8。

上記の CLI コマンドの出力には、以下の新しいパラメータが表示されます。

- **eMPS 統計の合計**：eMPS セッションで送受信されたメッセージの累積 GTP-C メッセージ統計。
- **現在の間隔 eMPS 統計**：現在の統計収集間隔における、eMPS セッションで送受信されたメッセージの GTP-C メッセージ統計。統計の収集間隔は、バルク統計の収集間隔と同じになります。バルク統計の収集が設定されていない場合、現在の MPS 統計は MPS 統計の合計と同じになります。
- **セッション作成要求（合計 TX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むセッション作成要求メッセージを送信したときに、S-GW によって増分されます。
- **セッション作成応答（合計 RX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むセッション作成応答メッセージを受信したときに、S-GW によって増分されます。
- **ベアラー変更要求（合計 TX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むベアラー変更要求メッセージを送信したときに、S-GW によって増分されます。
- **ベアラー変更応答（合計 RX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むベアラー変更応答メッセージを受信したときに、S-GW によって増分されます。
- **ベアラー作成要求（合計 RX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むベアラー作成要求メッセージを受信したときに、S-GW によって増分されます。
- **ベアラー作成応答（合計 TX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むベアラー作成応答メッセージを送信したときに、S-GW によって増分されます。
- **ベアラー更新要求（合計 RX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むベアラー更新要求メッセージを受信したときに、S-GW によって増分されます。
- **ベアラー更新応答（合計 TX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むベアラー更新応答メッセージを送信したときに、S-GW によって増分されます。

P-GW 入力の GTP ベース S5/S8 インターフェイス

次の CLI コマンドが変更され、P-GW 入力の S5 および S8 インターフェイスの eMPS セッション関連 GTP-C メッセージ統計が表示されるようになりました。

- **show egtpc statistics interface pgw-ingress interface-type s5s8**
- **show egtpc statistics egtp-service** *pgw_egtpc_service_name* **interface-type s5s8**
  - **s5s8**：P-GW eGTP-C インターフェイスのインターフェイスタイプ S5/S8。

上記の CLI コマンドの出力には、以下の新しいパラメータが表示されます。

- **eMPS 統計の合計**：eMPS セッションで送受信されたメッセージの累積 GTP-C メッセージ統計。
- **現在の間隔 eMPS 統計**：現在の統計収集間隔における、eMPS セッションで送受信されたメッセージの GTP-C メッセージ統計。統計の収集間隔は、バルク統計の収集間隔と同じになります。バルク統計の収集が設定されていない場合、現在の MPS 統計は MPS 統計の合計と同じになります。
- **セッション作成要求（合計 RX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むセッション作成要求メッセージを受信したときに、P-GW によって増加されます。
- **セッション作成応答（合計 TX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むセッション作成応答メッセージを送信したときに、P-GW によって増加されます。
- **ベアラー変更要求（合計 RX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むベアラー変更要求メッセージを受信したときに、P-GW によって増加されます。
- **ベアラー変更応答（合計 TX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むベアラー変更応答メッセージを送信したときに、P-GW によって増加されます。
- **ベアラー作成要求（合計 TX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むベアラー作成要求メッセージを受信したときに、P-GW によって増加されます。
- **ベアラー作成応答（合計 RX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むベアラー作成応答メッセージを受信したときに、P-GW によって増加されます。
- **ベアラー更新要求（合計 TX）**：このカウンタは、S5 または S8 インターフェイスで、MPS プロファイルで設定された ARP 値を含むベアラー更新要求メッセージを送信したときに、P-GW によって増加されます。

- **ベアラー更新応答（合計RX）**：このカウンタは、S5またはS8インターフェイスで、MPSプロファイルで設定されたARP値を含むベアラー更新応答メッセージを受信したときに、P-GW によって増加されます。

clear egtpc

インターフェイスレベルおよび eGTP-C サービスレベルで eMPS 統計をクリアするために、以下の CLI コマンドが変更されました。

- **clear egtpc statistics interface-type interface-pgw-ingress interface s5s8**：P-GW 入力タイプと S5 または S8 インターフェイスのすべての eGTP-C サービスについて、インターフェイス統計と eMPS 統計をクリアします。
- **clear egtpc statistics interface-type [interface-sgw-ingress | interface-sgw-egress] interface [s4 | s11 | sgw-s5s8]**：S-GW 入力タイプと S4 または S11 インターフェイス、または S-GW 出力タイプと S5 または S8 インターフェイスのすべての eGTP-C サービスについて、インターフェイス統計と eMPS 統計をクリアします。
- **clear egtpc statistics egtp-service** *pgw_egtpc_service_name* **interface [s5s8]**：すべての P-GW eGTP-C サービスと S5 または S8 インターフェイスについて、インターフェイス統計と eMPS 統計をクリアします。
- **clear egtpc statistics egtp-service** *sgw_egptc_service_name* **interface [s11 | s4 | sgw-s5s8]**：すべての S-GW eGTP-C サービスと S4 または S11 もしくは S5 または S8 インターフェイスについて、インターフェイス統計と eMPS 統計をクリアします。

P-GW eGTP-C S5/S8 スキーマ

この機能をサポートするために、次の新しいバルク統計変数が P-GW eGTP-C S5/S8 スキーマに追加されています。

- tun-recv-cresessreq-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって受信されたトンネルセッション作成要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-sent-cresessresp-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって送信されたトンネルセッション作成応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-recv-modbearerreq-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって受信されたトンネルベアラー変更要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-sent-modbearerresp-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって送信されたトンネルベアラー変更応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。

- tun-sent-crebearerreq-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって送信されたトンネルベアラー作成要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-recv-crebearerresp-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって受信されたトンネルベアラー作成応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-sent-updbearerreq-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって送信されたトンネルベアラー更新要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-recv-updbearerresp-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって受信されたトンネルベアラー更新応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。

eGTP-C スキーマ

この機能をサポートするために、次の新しいバルク統計変数が eGTP-C スキーマに追加されています。

- s11-tun-recv-cresesssreq-emps：インターフェイス s11 の eMPS サブスクライバに対してシステムによって受信されたトンネルセッション作成要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- s11-tun-sent-cresessresp-emps：インターフェイス s11 の eMPS サブスクライバに対してシステムによって送信されたトンネルセッション作成応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- s11-tun-recv-modbearerreq-emps：インターフェイス s11 の eMPS サブスクライバに対してシステムによって受信されたトンネルベアラー変更要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- s11-tun-sent-modbearerresp-emps：インターフェイス s11 の eMPS サブスクライバに対してシステムによって送信されたトンネルベアラー変更応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- s11-tun-sent-crebearerreq-emps：インターフェイス s11 の eMPS サブスクライバに対してシステムによって送信されたトンネルベアラー作成要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- s11-tun-recv-crebearerresp-emps：インターフェイス s11 の eMPS サブスクライバに対してシステムによって受信されたトンネルベアラー作成応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- s11-tun-sent-updbearerreq-emps：インターフェイス s11 の eMPS サブスクライバに対してシステムによって送信されたトンネルベアラー更新要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。

- s11-tun-recv-updbearerresp-emps：インターフェイス s11 の eMPS サブスクライバに対してシステムによって受信されたトンネルベアラー更新応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- s11-tun-sent-ddnreq-emps：インターフェイス s11 の eMPS サブスクライバに対してシステムによって送信されたダウンリンクデータ通知メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- s11-tun-recv-ddnack-emps：インターフェイス s11 の eMPS サブスクライバに対してシステムによって受信されたダウンリンクデータ通知確認応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- s4-tun-recv-cresessreq-emps：インターフェイス s4 の eMPS サブスクライバに対してシステムによって受信されたトンネルセッション作成要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- s4-tun-sent-cresessresp-emps：インターフェイス s4 の eMPS サブスクライバに対してシステムによって送信されたトンネルセッション作成応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-sent-cresessreq-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって送信されたトンネルセッション作成要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-recv-cresessresp-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって受信されたトンネルセッション作成応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-sent-modbearerreq-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって送信されたトンネルベアラー変更要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-recv-modbearerresp-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって受信されたトンネルベアラー変更応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-recv-crebearerreq-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって受信されたトンネルベアラー作成要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-sent-crebearerresp-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって送信されたトンネルベアラー作成応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。
- tun-recv-updbearerreq-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって受信されたトンネルベアラー更新要求メッセージの合計数。この統計は、現在のバルク統計間隔専用です。

- tun-sent-updbearerresp-emps：インターフェイス s5s8 の eMPS サブスクライバに対してシステムによって送信されたトンネルベアラー更新応答メッセージの合計数。この統計は、現在のバルク統計間隔専用です。



第 14 章

要約 PGW ローミングデータレートを出力するためのバルク統計

- 機能の概要と変更履歴 （303 ページ）
- 機能説明 （304 ページ）
- モニタリングおよびトラブルシューティング （304 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI
機能のデフォルト	有効、常時オン
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入	2024.02.0

機能説明

バルク統計のサポートが強化され、PLMNタイプ（ホーム、ローミング、訪問先）に基づいてユーザーのサブスクライバデータレートの概要が出力されるようになりました。

既存の **show subscribers pgw-only data-rate** コマンドに、次の plmn-type フィルタが追加され、サービスプロバイダーは PLMN タイプに基づいてサブスクライバのデータレートを取得できるようになりました。

- show subscribers pgw-only data-rate plmn-type home
- show subscribers pgw-only data-rate plmn-type roaming
- show subscribers pgw-only data-rate plmn-type visiting

これにより、ネットワーク内のローミングサブスクライバの合計数を把握でき、ローミング回線に対する請求処理の効率が向上します。

モニタリングおよびトラブルシューティング

ここでは、この機能をサポートする show コマンドおよび使用可能なバルク統計を使ったモニタリングと障害対応の方法について説明します。

show コマンドと出力

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show sub pgw-only data-rate

このコマンドを使用して、PGW サブスクライバの統合データレートを表示します。

フィールド	説明
Peak rate from user(bps)	最後のサンプリング期間中にサブスクライバからネットワークに送信されたデータについて取得されたピークデータレート（ビット/秒）。サンプリング期間は 30 秒です。
Peak rate to user(bps)	最後のサンプリング期間中にサブスクライバがネットワークから受信したデータについて取得されたピークデータレート（ビット/秒）。サンプリング期間は 30 秒です。
ave rate from user(bps)	最後のサンプリング期間中にサブスクライバからネットワークに送信されたデータについて取得された平均データレート（ビット/秒）。サンプリング期間は 30 秒です。

ave rate to user(bps)	最後のサンプリング期間中にサブスクライバがネットワークから受信したデータについて取得された平均データレート（ビット/秒）。サンプリング期間は 30 秒です。
sust rate from user(bps)	直近 3 回のサンプリング期間中にサブスクライバからネットワークに送信されたデータについて取得された平均データレート（ビット/秒）。サンプリング期間は 30 秒です。
sust rate to user(bps)	直近 3 回のサンプリング期間中にサブスクライバがネットワークから受信したデータについて取得された平均データレート（ビット/秒）。サンプリング期間は 30 秒です。
Peak rate from user(pps)	ユーザーからパケットを受信する速度（パケット/秒）。サンプリング期間は 30 秒です。
peak rate to user(pps)	ユーザーにパケットが送信される速度（パケット/秒）。サンプリング期間は 30 秒です。
ave rate from user(pps)	ユーザーからパケットを受信する平均速度（パケット/秒）。サンプリング期間は 30 秒です。
ave rate to user(pps)	ユーザーにパケットが送信される平均速度（パケット/秒）。サンプリング期間は 30 秒です。
sust rate from user(pps)	ユーザーからパケットを受信する持続速度（パケット/秒）。サンプリング期間は 30 秒です。
sust rate to user(pps)	ユーザーにパケットが送信される持続速度（パケット/秒）。サンプリング期間は 30 秒です。

次の show コマンドを使用すると、ホーム、ローミング、訪問などの PLMN タイプで同様な P-GW ローミングデータレートの詳細を表示できます。

- **show subscribers pgw-only data-rate plmn-type** *home*：P-GW ホームサブスクライバのデータレートを表示します。
- **show subscribers pgw-only data-rate plmn-type** *roaming*：P-GW ローミングサブスクライバのデータレートを表示します。
- **show subscribers pgw-only data-rate plmn-type** *visiting*：P-GW 訪問サブスクライバのデータレートを表示します。

バルク統計

この機能では、次のバルク統計がサポートされています。

PGW スキーマ

次のバルク統計が PGW スキーマに追加されました。

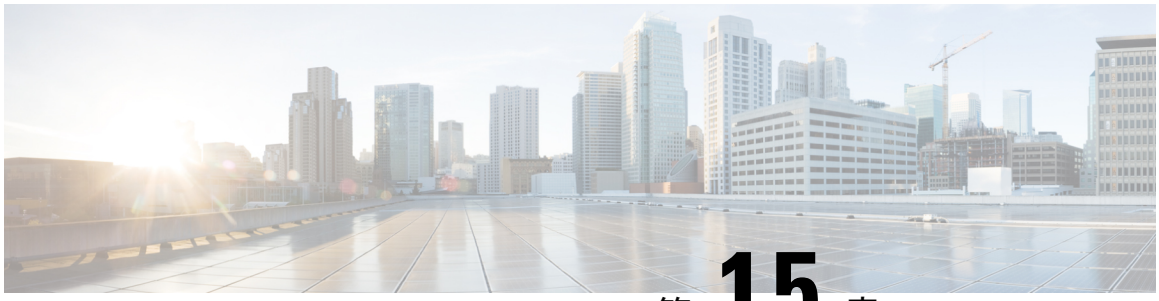
変数	説明
pgw-only data-rate のバルク統計変数	
pgw-subs-total	サブスクライバ数の合計を表示します。
pgw-data-active	アクティブなサブスクライバ数の合計を表示します。
pgw-data-dormant	休止のサブスクライバ数の合計を表示します。
pgw-data-fromuseravg-bps	ユーザーからの平均データレートをビット/秒単位で表示します。
pgw-data-touseravg-bps	ユーザーへの平均データレートをビット/秒単位で表示します。
pgw-data-fromuserpeak-bps	ユーザーからのピークデータレートをビット/秒単位で表示します。
pgw-data-touserpeak-bps	ユーザーへのピークデータレートをビット/秒単位で表示します。
pgw-data-fromusersust-bps	ユーザーからの平均データレートをビット/秒単位で表示します。
pgw-data-tousersust-bps	ユーザーへの持続的データレートをビット/秒単位で表示します。
pgw-data-fromuserpeak-pps	ユーザーからのピークデータレートをパケット/秒単位で表示します。
pgw-data-touserpeak-pps	ユーザーへのピークデータレートをパケット/秒単位で表示します。 **タイプ**：ゲージ
pgw-data-fromuseravg-pps	ユーザーからの平均データレートをパケット/秒単位で表示します。

変数	説明
pgw-data-touseravg-pps	ユーザーへの平均データレートをパケット/秒単位で表示します。
pgw-data-fromusersust-pps	ユーザーからの持続的データレートをパケット/秒単位で表示します。
pgw-data-tousersust-pps	ユーザーへの持続的データレートをパケット/秒単位で表示します。 **タイプ**：ゲージ
plmn-type ホームでの pgw-only data-rate のバルク統計変数	
pgw-subs-total-home	ホームサブスクライバ数の合計を表示します。
pgw-data-active-home	アクティブなホームサブスクライバ数の合計を表示します。
pgw-data-dormant-home	休止のホームサブスクライバ数の合計を表示します。
pgw-data-fromuseravg-bps-home	ユーザーからの平均データレートをビット/秒単位で表示します。
pgw-data-touseravg-bps -home	ユーザーへの平均データレートをビット/秒単位で表示します。
pgw-data-fromuserpeak-bps-home	ユーザーからのピークデータレートをビット/秒単位で表示します。
pgw-data-touserpeak-bps-home	ユーザーへのピークデータレートをビット/秒単位で表示します。
pgw-data-fromusersust-bps-home	ユーザーからの平均データレートをビット/秒単位で表示します。
pgw-data-tousersust-bps-home	ユーザーへの持続的データレートをビット/秒単位で表示します。

変数	説明
pgw-data-fromuserpeak-pps-home	ユーザーからのピークデータレートをパケット/秒単位で表示します。
pgw-data-touserpeak-pps-home	ユーザーへのピークデータレートをパケット/秒単位で表示します。
pgw-data-fromuseravg-pps-home	ユーザーからの平均データレートをパケット/秒単位で表示します。
pgw-data-touseravg-pps -home	ユーザーへの平均データレートをパケット/秒単位で表示します。
pgw-data-fromusersust-pps-home	ユーザーからの持続的データレートをパケット/秒単位で表示します。 **タイプ**：ゲージ
pgw-data-tousersust-pps-home	ユーザーへの持続的データレートをパケット/秒単位で表示します。
plmn-type ローミングでの pgw-only data-rate のバルク統計変数	
pgw-subs-total-roaming	ローミングサブスクライバ数の合計を表示します。
pgw-data-active-roaming	アクティブなローミングサブスクライバ数の合計を表示します。
pgw-data-dormant-roaming	休止のローミングサブスクライバ数の合計を表示します。
pgw-data-fromuseravg-bps-roaming	ユーザーからの平均データレートをビット/秒単位で表示します。 **タイプ**：ゲージ
pgw-data-touseravg-bps-roaming	ユーザーへの平均データレート（ビット/秒単位）。

変数	説明
pgw-data-fromuserpeak-bps-roaming	ユーザーからのピークデータレート（ビット/秒）。
pgw-data-touserpeak-bps-roaming	ユーザーへのピークデータレート（ビット/秒）。
pgw-data-fromusersust-bps-roaming	ユーザーからの平均データレート（ビット/秒）。
pgw-data-tousersust-bps-roaming	ユーザーへの持続的データレート（ビット/秒）。
pgw-data-fromuserpeak-pps-roaming	ユーザーからのピークデータレート（パケット/秒）。
pgw-data-touserpeak-pps-roaming	ユーザーへのピークデータレート（パケット/秒）。
pgw-data-fromuseravg-pps-roaming	ユーザーからの平均データレート（パケット/秒）。
pgw-data-touseravg-pps -roaming	ユーザーへの平均データレート（ビット/秒）。
pgw-data-fromusersust-pps-roaming	ユーザーからの持続的データレート（パケット/秒）。
pgw-data-tousersust-pps-roaming	ユーザーへの持続的データレート（パケット/秒）。
plmn-type 訪問での pgw-only data-rate のバルク統計変数	
pgw-subs-total-visiting	訪問サブスクライバ数の合計を表示します。
pgw-subs-total-visiting	訪問サブスクライバ数の合計を表示します。
pgw-data-dormant-visiting	休止の訪問サブスクライバ数の合計を表示します。
pgw-data-fromuseravg-bps-visiting	ユーザーからの平均データレートをビット/秒単位で表示します。
pgw-data-touseravg-bps -visiting	ユーザーへの平均データレート（ビット/秒単位）。

変数	説明
pgw-data-fromuserpeak-bps-visiting	ユーザーからのピークデータレートをビット/秒単位で表示します。
pgw-data-touserpeak-bps-visiting	ユーザーへのピークデータレートをビット/秒単位で表示します。
pgw-data-fromusersust-bps-visiting	ユーザーからの平均データレートをビット/秒単位で表示します。
pgw-data-tousersust-bps-visiting	ユーザーへの持続的データレートをビット/秒単位で表示します。
pgw-data-fromuserpeak-pps-visiting	ユーザーからのピークデータレートをパケット/秒単位で表示します。
pgw-data-touserpeak-pps-visiting	ユーザーへのピークデータレートをパケット/秒単位で表示します。
pgw-data-fromuseravg-pps-visiting	ユーザーからの平均データレートをパケット/秒単位で表示します。
pgw-data-touseravg-pps -visiting	ユーザーへの平均データレートをパケット/秒単位で表示します。
pgw-data-fromusersust-pps-visiting	ユーザーからの持続的データレートをパケット/秒単位で表示します。
pgw-data-tousersust-pps-visiting	ユーザーへの持続的データレートをパケット/秒単位で表示します。



第 15 章

VRFに基づくIPプールの一括ビジーアウト

- 機能の概要と変更履歴 （311 ページ）
- IP プールのビジーアウト （312 ページ）
- VRF を使用した IPv4 プールのビジーアウトの有効化 （312 ページ）
- VRF を使用した IPv6 プールのビジーアウトの有効化 （314 ページ）
- IPv4 プールでの VRF による一括ビジーアウトの無効化 （315 ページ）
- IPv6 プールでの VRF による一括ビジーアウトの無効化 （316 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：有効にするには設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
初版	2024.03.0

IP プールのビジーアウト

ビジーアウトにより、現在のコンテキストで IP プールからのアドレスが解放されると、そのアドレスが使用できなくなります。

IP プールの一括ビジーアウト

IP プールの一括ビジーアウトは、次の項目をビジーアウトするために使用されます。

- コンテキスト内のすべての IP プール
- 特定のアドレス範囲
- 特定の IPv4/IPv6 プール：プール内のアドレスの範囲、または特定の IP プール内のアドレスのグループ、または IP アドレスの範囲または複数の IP アドレスプールのグループ。

VRF 名による IP プールの一括ビジーアウト

P-GW では、VRF 名オプションを使用して busyout ip pool を設定することで、その VRF に関連付けられているすべての IP プールをビジーアウトできます。

たとえば、vrf_1 という名前の VRF に関連付けられている「n」個の IP プールがある場合、vrf_1 では、設定 **busyout ip pool vrf** *vrf_1* は、「n」個すべての IP プールをビジーアウト状態に設定します。この **busyout ip pool vrf** 設定により、各プールが個別にビジーアウトとしてマークされるのを避けることができます。

VRF を使用した IPv4 プールのビジーアウトの有効化

CLI プロシージャを使用して、複数の IPv4 プールのビジーアウト設定を有効にすることができます。

手順

ステップ 1 VRF に基づいて IPv4 プールのビジーアウトを設定します。 *vrf_name* では大文字と小文字が区別され、1 ー 63 文字で値を入力する必要があります。

busyout ip pool vrf *vrf_name*

例：

```
[local]qvpc-si# config
[local]qvpc-si(config)# context context_name
[egress]qvpc-si(config-ctx)# busyout ip pool vrf vrf_name
[egress]qvpc-si(config-ctx)# end
```

ステップ 2 IPv4 IP プールでビジーアウト構成が配置されている場合に、ビジーアウト IPv4 プールが設定されているかどうかを確認します。

show ip pool summary vrf *vrf_name*

例：

```
[ISP1]laas-setup# show ip pool summary vrf mpls-vrf-1
context ISP1:
+-----Type:    (P) - Public    (R) - Private    (N) - NAT
|              (S) - Static    (E) - Resource   (O) - One-to-One NAT
|              (M) - Many-to-One NAT
|
|+----State:   (G) - Good      (D) - Pending Delete   (R)-Resizing
||             (I) - Inactive
||
||++--Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+-Busyout: (B) - Busyout configured
|||||
|||||
vvvvv Pool Name                         Start Address   Mask/End Address Used    Avail
----- --------------------------------- --------------- ---------------  ----------------
RG00B PRIVATEPOOL3                      10.140.150.0    255.255.255.0    0        254
RG00B PRIVATEPOOL2                      10.140.140.0    255.255.255.0    0        254
RG00B PRIVATEPOOL1                      31.33.0.0       255.255.0.0      0        65534
RG00B privatepool-1                     10.160.0.0      255.248.0.0      0        524286

Total Pool Count: 5
Total Pool Kernel Routes: 9    Max Pool Kernel Routes: 6000
Total Pool Explicit Host Routes: 0    Max Pool Explicit Host Routes: 24000

ISP1]laas-setup# show ip pool summary vrf mpls-vrf-1 wide
context ISP1:
+-----Type:    (P) - Public    (R) - Private    (N) - NAT
|              (S) - Static    (E) - Resource   (O) - One-to-One NAT
|              (M) - Many-to-One NAT
|
|+----State:   (G) - Good      (D) - Pending Delete   (R)-Resizing
||             (I) - Inactive
||
||++--Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+-Busyout: (B) - Busyout configured
|||||
|||||
vvvvv Pool Name                         Start Address   Mask/End Address Used     Hold     Quarantine
  Avail    Rel      Free     Group Name
----- --------------------------------- --------------- ---------------  -------- -------- -----------
 -------- -------- -------- --------------------------------
RG00B PRIVATEPOOL3                      10.140.150.0    255.255.255.0    0        0        0
    254      0        254
RG00B PRIVATEPOOL2                      10.140.140.0    255.255.255.0    0        0        0
    254      0        254
RG00B PRIVATEPOOL1                      31.33.0.0       255.255.0.0      0        0        0
    65534    0        65534
RG00B privatepool-1                     10.160.0.0      255.248.0.0      0        0        0
    524286   0        524286   int41
```

VRF を使用した IPv6 プールのビジーアウトの有効化

CLI プロシージャを使用して、IPv6 プールのビジーアウト設定を有効にすることができます。

手順

ステップ 1 VRF に基づいて複数の IPv6 プールのビジーアウトを有効にします。 *vrf_name* では大文字と小文字が区別され、1 ー 63 文字で値を入力する必要があります。

busyout ipv6 pool vrf *vrf_name*

例：

```
[local]qvpc-si# config
[local]qvpc-si(config)# context context_name
[egress]qvpc-si(config-ctx)# busyout ipv6 pool vrf vrf_name
[egress]qvpc-si(config-ctx)# end
```

ステップ 2 IPv6 IP プールでビジーアウト構成が配置されている場合に、ビジーアウト IPv6 プールが設定されているかどうかを確認します。

show ipv6 pool summary vrf *vrf_name*

例：

```
[ISP1]laas-setup# show ipv6 pool summary vrf mpls-vrf-1
context ISP1:
+-----Type:    (P) - Public    (R) - Private
|              (S) - Static    (H) - Shared
|
|+----State:   (G) - Good      (D) - Pending Delete   (R)-Resizing
||             (I) - Inactive
||
||++--Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+-Addr-Type: (N) - Normal  (T) 6to4
|||||
|||||+-Busyout: (B) - Busyout configured
||||||
||||||
vvvvvv Pool Name            Start Prefix                          End Prefix
              Used     Avail
------ -------------------- ------------------------------------
---------------------------------------  -------- --------
RG00NB PRIVATEV6            7001::/64                             7001:0:0:ffff::/64
              0        65536
RG00NB PRIVATEV61           8001::/64                             8001:0:0:ffff::/64
              0        65536
RG00NB PRIVATEV62           6001::/64                             6001:0:0:ffff::/64
              0        65536

Total Pool Count: 3
[ISP1]laas-setup# show ipv6 pool summary vrf mpls-vrf-1 wide
context ISP1:
+-----Type:    (P) - Public    (R) - Private
|              (S) - Static    (H) - Shared
```

```
|
|+----State:   (G) - Good      (D) - Pending Delete   (R)-Resizing
||             (I) - Inactive
||
||++--Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+-Addr-Type: (N) - Normal  (T) 6to4
|||||
|||||+-Busyout: (B) - Busyout configured
||||||
||||||
vvvvvv Pool Name            Start Prefix                            End Prefix
              Used     Avail
------ -------------------- ---------------------------------------
----------------------------------------  -------- --------
RG00NB PRIVATEV6            7001::/64                               7001:0:0:ffff::/64
              0        65536
RG00NB PRIVATEV61           8001::/64                               8001:0:0:ffff::/64
              0        65536
RG00NB PRIVATEV62           6001::/64                               6001:0:0:ffff::/64
              0        65536
Total Pool Count: 3
```

IPv4 プールでの VRF による一括ビジーアウトの無効化

CLI 手順を使用した VRF 設定によって、一括ビジーアウトを無効にすることができます。

（注） VRF のビジーアウト前に、IP プールがすでにビジーアウトとしてマークされていて、VRF に関連付けられている場合、VRF を設定または設定解除しても、IP プールのビジーアウトステータスは同じままです。

手順

VRF に基づいて IPv4 プールのビジーアウトを無効にするには、**no** を入力します。この VRF に関連付けられているプールがビジーアウトとしてマークされている場合、IP プールはビジーアウトのままになります。

no busyout ip pool vrf *vrf_name*

例：

```
[local]qvpc-si# config
[local]qvpc-si(config)# context egress
[egress]qvpc-si(config-ctx)# no busyout ip pool vrf vrf_name
[egress]qvpc-si(config-ctx)# end
```

（注）
vrf_name では大文字と小文字が区別され、1 ー 63 文字の値を入力する必要があります。

IPv4 プールのビジーアウト設定が正常に無効になりました。

IPv6 プールでの VRF による一括ビジーアウトの無効化

CLI プロシージャを使用して、複数の IPv6 プールのビジーアウト設定を無効にすることができます。

（注） VRF のビジーアウト前に、IP プールがすでにビジーアウトとしてマークされていて、VRF に関連付けられている場合、VRF を設定または設定解除しても、IP プールのビジーアウトステータスは同じままです。

手順

VRF に基づいて IPv6 プールのビジーアウトを無効にするには、**no** を入力します。この VRF に関連付けられているプールがビジーアウトとしてマークされている場合、IP プールはビジーアウトのままになります。

no busyout ipv6 pool vrf *vrf_name*

例：

```
[local]qvpc-si# config
[local]qvpc-si(config)# context egress
[egress]qvpc-si(config-ctx)# no busyout ipv6 pool vrf vrf_name
[egress]qvpc-si(config-ctx)# end
```

（注）
vrf_name では大文字と小文字が区別され、1 ～ 63 文字の値を入力する必要があります。

IPv6 プールのビジーアウト設定が正常に無効になりました。



第 16 章

コールトランザクションを記録および生成する機能

- 機能の概要と変更履歴 （317 ページ）
- 機能説明 （318 ページ）
- 機能の仕組み （318 ページ）
- RTT の設定 （332 ページ）
- モニタリングおよびトラブルシューティング （334 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• ePDG • P-GW • SaMOG
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *ePDG Administration Guide* • *P-GW Administration Guide* • *SaMOG Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
P-GW と SaMOG は、履歴コールトランザクションを記録および生成する機能をサポートしています。付加的な RTT レコードスキーマが追加されました。	21.27
追加された RTT レコードスキーマ	21.26
最初の導入。	20.0

機能説明

リージョンおよびネットワーク オペレーション センター（NOC）は、リアルタイムツール（RTT）を使用してネットワークの問題をデバッグし、ユーザーの動作を把握します。ePDG、P-GW、および SaMOG におけるすべてのコールトランザクションは、RTT ファイルで生成されます。ePDG、P-GW、および SaMOG は、SSH File Transfer Protocol（SFTP）を介して外部サーバーに RTT ファイルを転送します。カンマ区切り値（.CSV）形式の RTT ファイルは、圧縮または非圧縮形式で転送されます。転送は、設定に基づいて外部サーバー（顧客ネットワーク内のサーバーなど）に、直接または Cisco Collector サーバーを介して行われます。

（注） RTT レコードスキーマとその手順番号は、ゲートウェイ RTT 用に一般化されています。特定の RTT レコードスキーマの詳細については、シスコのアカウント担当者にお問い合わせください。

機能の仕組み

このセクションでは、RTT の手順とスキーマについて説明します。

RTT 手順

次の表に、ePDG、P-GW、および SaMOG に固有の RTT 手順を示します。

手順番号	手順名	適用性
1	S5/S8/S2b GTP セッション作成	P-GW、ePDG、SaMOG
2	S5/S8/S2b GTP ベアラー作成	P-GW、ePDG、SaMOG
3	S5/S8/S2b GTP セッション削除	P-GW、ePDG、SaMOG

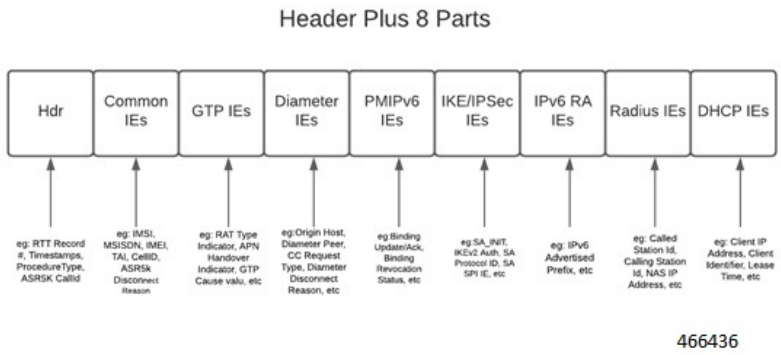
手順番号	手順名	適用性
4	S5/S8/S2b GTP ベアラー削除	P-GW、ePDG、SaMOG
5	GTP ベアラー変更	P-GW
6	S5/S8/S2b GTP ベアラー更新	P-GW、ePDG、SaMOG
7	S6b/SWm – Diameter AAR/ AAA	P-GW、ePDG、SaMOG
8	S6b/SWm – Diameter RAR/RAA	P-GW、ePDG、SaMOG
9	S6b/SWm – Diameter セッション終了	P-GW、ePDG、SaMOG
10	S6b/SWm – セッション中止	P-GW、ePDG、SaMOG
11	Diameter Gx – CCR-I/CCA-I	P-GW
12	Diameter Gx – CCR-U/CCA-U	P-GW
13	Diameter Gx – CCR-T/CCA-T	P-GW
14	Diameter Gx – RAR/RAA	P-GW
15	Diameter Gy – CCR-I/CCA-I	P-GW
16	Diameter Gy – CCR-U/CCA-U	P-GW
17	Diameter Gy – CCR-T/CCA-T	P-GW
18	Diameter Gy – RAR/RAA	P-GW
19	PMIPv6 S2a – バインディング更新/確認応答	P-GW
20	PMIPv6 S2a 失効更新/確認応答	P-GW
21	SWu – IKEv2 SA INIT/応答	ePDG
22	SWu – IKEv2 認証要求/応答	ePDG
23	SWu – IKEv2 情報要求/応答	ePDG
24	SWm – Diameter EAP 要求/応答	ePDG、SaMOG
25	ePDG ルーターアドバタイズメント	ePDG、SaMOG
26	SWu – CREATE_CHILD_SA 要求/応答	ePDG
27	Radius – WLC-SaMOG アクセス要求/チャレンジ	SaMOG
28	Radius – WLC-SaMOG アクセス要求/承認	SaMOG
29	Radius – WLC-SaMOG 接続解除要求/応答	SaMOG

手順番号	手順名	適用性
30	Radius – WLC-SaMOG アカウンティング要求/応答	SaMOG
31	Radius – SaMOG-Radius サーバーアカウンティング要求/応答	SaMOG
32	WLC – SaMOG DHCP 検出/オファー	SaMOG
33	WLC – SaMOG DHCP 要求/確認応答/否定応答	SaMOG
34	WLC – SaMOG DHCP リリース/確認応答/否定応答	SaMOG

RTT レコードスキーマ

次の図は、ePDG、P-GW、および SaMOG の RTT スキーマの詳細を示しています。最初の 6 つの IE（IPv6RA IE に送られる共通 IE）は、ePDG、P-GW、SaMOG に共通です。最後の 2 つのフィールドである [Radius IE] と [DHCP IE] は、SaMOG に固有です。

図 *13 : RTT* レコードスキーマ



RTT スキーマにはヘッダーがあり、その後に 8 つの情報要素（IE）ブロックが続きます。8 つのブロックにグループ化された 220 の IE があります。スキーマ 1 ～ 170 は ePDG に固有です。スキーマ 1 ～ 170 + 10（180）の CUPS スキーマは P-GW に固有であり、スキーマ 171 ～ 220 は SaMOG に固有です。CUPS スキーマの詳細については、『*Ultra Packet Core CUPS User Plane Administration Guide*』を参照してください。RTT レコードスキーマ IE の完全なリストについては、シスコのアカウント担当者にお問い合わせください。

RTT レコードキーマの一覧を次の表に示します。

IE	説明	書式例	関連する手順
1	ゲートウェイ RTT レコード番号	<proclet-type> | <instance-id> | <RTT-record-#> のカウンタ	すべて
2	ゲートウェイの RTT バージョン番号	R20.0 のバージョン 3	すべて

IE	説明	書式例	関連する手順
3	手順番号	CFS 表 1 で定義	すべて
4	ゲートウェイ名	シャーシのホスト名	すべて
5	手順開始時刻（GMT）	UTC の時刻（ミリ秒の精度で表示）	すべて
6	手順終了時刻（GMT）	UTC の時刻（ミリ秒の精度で表示）	すべて
7	ASR5K CallID	内部 CallID。例：[376efb10]	すべて
8	GW 名	RTT レコードが生成されるゲートウェイ名（ePDG/P-GW/SaMOG）。	All
9 ～ 10	予約済み		
11	IMSI	例：[311480076488840]	1、11、12、13、22、24、27、28、30、32、33、34
12	[MSISDN]	例：[19728256305]	1、5、7、15、16、17
13	IMEISV	例：[9900028823793406]	1、11、15
14	TAI：MCC/MNC/TAC	例：文字列 [311-480-0x3B00]	1 ～ 6、11、12、15、16

IE	説明	書式例	関連する手順
15	Cell ID	ECI。例：[0xE70D01]	1 ～ 6、11、12、15、16
16	ASR5.5K 切断理由	セッション切断の内部理由（タイムアウト、エラーなど）。 詳細については、『*Statistics and Counters Reference Guide*』[英語] を参照してください。	すべて（保留中のエラー）
17	MAC Address	UE デバイスの MAC アドレス。SaMOG RADIUS コールフローの場合、この属性は calling-station-ID と同じです。例：0034567890AB	24、27、28、29、30、31、32、33、34
18 ～ 20	予約済み		
21	サービス提供ネットワーク	MCC MNC。例：[311480]	1、5
22	無線アクセス技術	TS29.274で定義。例：[6 = E-UTRAN]	22
23	ハンドオーバーインジケータ	指示属性の HI フィールド、例：[0 = New PDN; 1 = Handover]	1、5
24	SGW/HSGW/ePDG/SaMOG 制御 TEID	ピアのトンネル識別子。例：[0x26B609F0]	1、2、5
25	PGW 制御 TEID	PGW のトンネル識別子。例：0x084BC005	1 および 2
26	AN GW アドレス	リモート GW の IP アドレス：HSGW または SGW	1、2、5
27	アクセス ポイント名	文字列、例： [Customerims.mnc311.mcc480.3 gppnetwork.org]	1
28	フレーム IP アドレス	UE が割り当てた IPv4 アドレス	1、11、12、13

IE	説明	書式例	関連する手順
29	フレーム IPv6 アドレス	UE が割り当てた IPv6 プレフィックス/アドレス	1、11、12、13
30	アップリンク AMBR	Kbps 単位。例：[0-4294967295]	1、6
31	ダウンリンク AMBR	Kbps 単位。例：[0-4294967295]	1、6
32	PCO DNS IPv6 アドレス：プライマリ	プライマリ DNS サーバーの IPv6 アドレス。	1
33	PCO DNS IPv6アドレス：セカンダリ^ターシャリ	DNS のセカンダリ IPv6 アドレス^ターシャリ IPv6 アドレス	1
34	PCO DNS IPv4 アドレス：プライマリ	IPv4 アドレス	1
35	PCO DNS IPv4 アドレス：セカンダリ	DNS のセカンダリ IPv4 アドレス^ターシャリ IPv6 アドレス	1
36	EPS ベアラー ID のリスト（成功）	各ベアラー ID は「|」で区切る必要があります。 例：1 | 3 | 5	1、2、4、5、6
37	リンクされたベアラー ID	TS29.274 に基づく。例：[0-15]	2、3、4、5
38	アップリンク MBR	kbps 単位。MBR 例：1234 | 3456 | 567 各ベアラーの MBR は「|」で区切る必要があります。IE 37 と同じ順序です。	1、6
39	ダウンリンク MBR	アップリンク MBR と同じ	1、6
40	アップリンク GBR	kbps 単位。GBR。例：1234 | 3456 | 567 各ベアラーの MBR は「|」で区切る必要があります。IE 37 と同じ順序です。	1、6
41	ダウンリンク GBR	アップリンク GBR と同じ	1、6
42	GTP 原因値	TS29.274 要求に基づく/承認/拒否の原因。例：[1-255]	1 ～ 6
43	ピギーバック レコード インジケータ	ピギーバック メッセージ レコードの明示的な表示、例：(0=no; 1=yes)	2、5
44	予約済み		
45	SGW/HSGW/ePDG/SaMOG データ TEID	ピアのトンネル識別子、例：[0x26B609F0]	1、2、5

IE	説明	書式例	関連する手順
46	PGW データ TEID	P-GWのトンネル識別子、例：[0x084BC005]	1 および 2
47 〜 50	予約済み		
51	セッション ID	認証セッションのセッション ID、例： UTF8 文字列 [0006-diamproxy.WSBOMAGJPNC. S6b.vzims.com; 21604107; 449305093; 536f9359-503]	7 〜 18、24
52	認証アプリケーション ID	例：[S6b = 16777999 , Gx = 16777238, Gy = 4]	7 〜 18、24
53	PGW ホスト（発信元ホスト）	PGW の FQDN、例：[0004-diamproxy. WSBOMAGJPNC. Gy.vzims. com]	7 〜 18、24
54	Diameter ピアアドレスレルム	3GPP AAA、PCRF OCS レルムの FQDN、例：[Customerims.com]	7 〜 18、24
55	宛先ピアホスト	3GPP AAA、PCRF、OCS ホストの FQDN、例：[njbbpcrf1a.vzims.com]	7 〜 18、24
56	CC 要求タイプ	例：列挙型 [1-3, for I, U, T]	11、12、13、15、16、17
57	CC 要求番号	例：[0]	11、12、13、15、16、17
58	結果コード	RFC3588 に基づく Diameter 結果コード、例：[2001]	7 〜 18、24
59	送信元状態 ID	例：[1366695723]	7 〜 18
60	サービスの選択	承認用の APN 名を提供するために使用される AVP、例：[Customerinternet]	12、24
61	課金ゲートウェイ機能ホスト	CGF の FQDN、例：[cgf1.NEE29.vzims.com]	5、7

IE	説明	書式例	関連する手順
62	課金グループ ID	各ベアラーの課金 ID は「|」で区切られます。IE 37 と同じ順序であり、その後に 44 が続きます。	5、7
63	サーバー名（CSCF アドレス）	IMS APN のみ、例：[pcscf1.CTX07.vzims.com]	7
64	フレームプール	IPv4 アドレスの割り当て元のプール名、例：[int41]	7
65	Framed-IPv6-Pool	IPv6 プレフィックスの割り当て元のプール名、例：[ims61]	7
66	認証要求タイプ	TS29.273 および 29.212 に基づく。例：列挙型 [1-3]	7、24
67	再認証要求タイプ	TS29.273 および 29.212 に基づく。例：列挙型 [0-1]	8、14、18
68	Diameter の終了原因	TS29.273 および 29.212 に基づく。例：列挙型 [1-8]	9、13、17
69	QoS クラス識別子	QCI、例：[8]	11、12、15、16
70	IP-CAN タイプ	例：[5 = 3GPP-EPS]	11、12、14
71	イベント トリガー	TS29.212、一連のパイプ区切りトリガーに基づく、例：[1 = QOS_CHANGE]	11 および 12
72	予約済み IE/未使用		
73	課金ルール削除	削除された課金ルールの名前、例：文字列 [RTRRule3300]	12
74	課金ルールインストール	インストールされている課金ルールの名前、例：文字列 [RTRRule3300]	11
75	複数サービスインジケータ	TS32.299 に基づく、例：列挙型 [0-1]	15、16、17
76	Multiple Services Credit Control 評価グループ	評価グループの識別子、例：[3300]	15、16、17
77	Multiple Services Credit Control 付与サービスユニット	CC 合計オクテット、例：[524288000]	15
78 ～ 80	予約済み		
81	EAP Auth-Session-State	例：STATE_MAINTAINED (0)	24

IE	説明	書式例	関連する手順
82	WLAN ユーザー名	例：0311150123456701@ wlan.mnc150。 mcc311.3 gppnetwork.org	24
83	RAT タイプ	例：0 = WLAN	24
84	訪問ネットワーク識別子	例：mnc150.mcc311.3gppnetwork.org	24
85	EAP マスターセッションキー	MSK	24
86	APN 設定	PDN タイプ | サービス = 選択 | ゲートウェイ	24
87 ～ 90	予約済み		
91	MAG IP アドレス	MAG IP アドレス	19 および 20
92	LMA IP Address	LMA IP Address	19 および 20
93	IMSI-NAI	例：6311480000021024@nai.epc. mnc480. mcc311.3 gppnetwork.org	19 および 20
94	サービス選択のモビリティオプション	EPS APN名 に設定、3GPP TS 23.003 の形式、例：Customerims	19 および 20
95	ホーム ネットワーク プレフィックス オプション	動的または静的に割り当てられたプレフィックスと、UE に割り当てられた IID	19 および 20
96	IPv4 アドレス要求	アドレス/プレフィックス、例：209.165.200.225/32	19
97	IPv4 アドレス確認応答	ステータス：アドレス/プレフィックス、例：0:209.165.200.225/32	19
98	IPv4 デフォルトルータ	IPv4 アドレス、例：209.165.200.226	19
99	アップリンク GRE キー	16 進数、例：0x004D90CC	19
100	ダウンリンク GRE キー	16 進数、例：0xCC904D00	19
101	課金特性	16 進数、例：0×0A	19
102	課金識別子	16 進数、例：0x5E9BD665	19
103	サービス提供ネットワーク	MCC-MNC	19
104	ベースステーション ID	16 進数、例：001C0001008A	19

IE	説明	書式例	関連する手順
105	MEID	10 進数文字列、例：99000044001930	
106	バインディングシーケンス番号	バインディング更新およびACK用の16ビット符号なし整数	19
107	Lifetime	バインディングユニットが期限切れと見なされる前の IME を表す 16 ビット符号なし整数。例0x0708	19
108	ハンドオフ インジケータ オプション	HO インジケータ 例0x01 = new attachment	19
109	Access Technology Type（ATT）	例0x09 = eHRPD	19
110	プロキシ バインディング ステータス	BU 処理の状態を示す 8 ビット符号なし整数。	19
111	PCO DNS IPv6 アドレス	DNS IPv6 アドレス、複数の場合の形式 = "Addr1|Addr2"	19
112	PCO DNS IPv4 アドレス	DNS IPv4 アドレス、複数の場合の形式 = "Addr1|Addr2"	19
113	P-CSCF アドレス	P-CSCF IPv6 アドレス、複数の場合の形式 = "Addr1!Addr2"	19
114	バインディング失効ステータス	BRI 処理の結果を示す 8 ビットの符号なし整数。128 未満の値は、成功を示します	20
115	バインディング失効シーケンス番号	BRI および BRA メッセージと一致するシーケンス番号	20
116	失効トリガー	トリガーの UE ごとまたはグローバルな理由を示す 8 ビットの符号なし整数	20
117	失効フラグ	16 進数、例：0x4	20
118 ～ 130	予約済み		
131	UE IP アドレス	UE IP アドレス	21、22、23、26
132	SA_INIT の UE UDP ポート	SA_INIT の UE UDP 送信元ポート	21、22、23、26
133	ePDG アドレス	SA_INIT の ePDG IP アドレス	21、22、23、26

IE	説明	書式例	関連する手順
134	ePDG ポート	SA_INIT 用の ePDG UDP ポート（例：IKE の場合は 4500）	21、22、23、26
135	イニシエータ SPI	イニシエータ（UE）SPI	21、22、26
136	レスポンダ SPI	レスポンダ（ePDG）SPI	21、22、26
137	トランスフォーム ヘッダー タイプおよび ID	TypeID によりネゴシエートされた値が入力されます。 x|y|z|w|U (Enc/prf/Integrity/Dhg/ESN) 値がネゴシエートされていない場合は、-1 が入力されます。例：IIKE_Auth に PRF は存在しません。 値はこれらのプロトコルの IANA 標準の番号になります。	21、22、26
138	KE DH グループ	Diffie Hellman グループ番号	21、26
139	通知メッセージタイプ	例：NAT_Detection IP タイプ（必要に応じて区切る）は x|y|z^a|b|c と区切られます。この x/y/z はプロシージャ要求で通知され、a/b はプロシージャ応答で通知されます。要求と応答のいずれにも通知がない場合、デリミタ^の前または後のいずれかが空白になります。	21、26
140	IDi	識別イニシエータ：RFC822 アドレス、例：0311150123456701@wlan.mnc150. mcc311 3gppnetwork.org	22
141	IDr	識別レスポンダ：IKEv2 FQDN ID、例：apncf.w-apn. mnc150.mcc311. pub。3gppnetwork.org	22
142	TSi	プロトコルタイプ | アドレス範囲 | ポート範囲 （TS が複数ある場合は ^ で区切ることができます）	22
143	TSr	プロトコルタイプ | アドレス範囲 | ポート範囲 （TS が複数ある場合は ^ で区切ることができます）	22
144	EAP メッセージステータスコード	例：SUCCESS これは、応答の最後の値と見なされます	22、27、28
145	EAP メッセージ ID	EAP メッセージ ID	22、27
146	EAP タイプ	例：AKA (0x17) for ePDG EAP-AKA (0x17)	22、27、28

IE	説明	書式例	関連する手順
147	設定済みの属性認証方式	文字列としての共有キー。例：local_method|remote_method（local/remote は PSK/EAP/CERT）。	22
148	IKEv2 設定属性（内部 IP4/IPv6）	例：UE アドレス x^y（x は IPv4、y は IPv6）	22
149	IKEv2_CFG_ ATTRIBUTE_INTERNAL_ IP4_NETMASK	例：255.255.255.255	22
150	IKEv2_CFG_ ATTRIBUTE_ INTERNAL_DNS_ IPV4	x^y^z（x、y、z は IPv4 アドレス）。IKE_Auth_reply で指定可能な最大 3 つのエントリ。	22
151	IKEv2_CFG_ ATTRIBUTE_ INTERNAL_DNS_ IPV6	x^y^z（x、y、z は IPv6 アドレス）。IKE_Auth_reply で指定可能な最大 3 つのエントリ。 この IE はありません。新しい IE を追加する必要があります	22
152	P-CSCF IPv4	x^y^z（x、y、z は IPv4 アドレス）。IKE_Auth_reply で指定可能な最大 3 つのエントリ。	
153	P-CSCF IPv6	x^y^z（x、y、z は IPv6 アドレス）。IKE_Auth_reply で指定可能な最大 3 つのエントリ。	22
154	SA プロトコル ID	例：ESP (0x03)	22
155	SA SPI UE	例：0x020000BA	22
156	SA SPI ePDG	SA SPI UE に似ています。この IE はありません。追加する必要があります	
157	情報要求タイプ	削除、DPD など。	23
158	IKEv2 通知 - エラーコード	SWu コールフローごとの IKEv2 標準エラーコードおよびカスタマーのカスタムコード：最後に受信/送信された通知エラーコードが更新されました。設定されている場合は Verison のカスタムコード、それ以外の場合は標準コードになります。	21、22、23、26
159 ～ 160	予約済み		
161	アドバタイズされた IPv6 プレフィックス	ルータアドバタイズメントの一部としてアドバタイズされた IPv6 プレフィックス	25
162 ～ 170	予約済み		

IE	説明	書式例	関連する手順
171	着信側 -ステーション ID	SSIDに追加された「-」で区切られたオクテット値を使用して、ブリッジまたはアクセスポイントの MAC アドレスを ASCII 形式で保存します。例：mac64-d9-89-43- d4-a0: grp123456789123456789	27、28、30、31
172	Service-Type	ユーザーが要求したサービスのタイプまたは指定されたサービスのタイプを示します。例：02 (Framed)。	27、28、30、31
173	NAS-Port-Type	ユーザーを認証するNASの物理ポートのタイプを示します。例：19 (Wireless_IEEE_802_11)	27、28、30、31
174	NAS-Port-ID	ユーザーを認証する NAS のポートを識別します。例：10	27、28、30、31
175	NAS-IP-Address	ユーザー認証を要求する NAS の識別用 IP アドレスを示します。例：192.168.15.51	27、28、29、30、31
176	NAS-IPv6-Address	ユーザー認証を要求する NAS の IP アドレスを示します。例：2405:200:816:945::2:ed9e	27、28、29、30、31
177	NAS-Identifier	要求を送信した NAS を識別する文字列を示します。例：samog_wlc	27、28、29、30、31
178	Acct-Session-ID	セッションがログファイルの開始レコードと終了レコードに一致することを示します。	27、28、29、30、31
179	Acct-Multi-Session-ID	ログファイル内の複数の関連セッションをリンクするための一意のアカウンティング ID を示します。相互にリンクされた各セッションの Acct-Session-Id は一意ですが、Acct-Multi-Session-Id は同じです。	27、28、29、30、31
180	NAS-Port	ユーザーを認証する NAS の物理ポート番号を示します。例 1	27、28、30、31

IE	説明	書式例	関連する手順
181	Framed-MITU	ユーザーに対して設定する最大伝送ユニット（MTU）を示します。例：1300	27 および 28
182	予約済み		
183	Framed-IP-Address	ユーザーに割り当てられているアドレスを示します。例：1,2,3,5	29、30、31
184	Acct-Termination_Cause	セッション終了の原因を示します。例：1（ユーザー要求の場合）。	29
185	Framed-IPv6-Prefix	ユーザーの IPv6 プレフィックスを示します。例：1:2:3:5::/64 または 1:2:3:5::	29、30、31
186	Tunnel-Type	トンネリングプロトコルを示します。例：14（VLAN の場合）。	27、28、30、31
187	Tunnel-Medium-Type	プロトコル作成の転送メディアを示します。例：06（IEEE-802 の場合）	27、28、30、31
188	Tunnel-Private-Group-ID	指定されたトンネリングセッションのグループ ID	27、28、30、31
189	Acct-Output-Packets	送信されたパケット数。例：20	30、31
190	Acct-Input-Packets	受信されたパケット数。例：24	30、31
191	Acct-Status-Type	ユーザーサービスの開始または終了を示します。例：1（開始）2（停止）。	30、31
192	Acct-Session-Time	ユーザーがサービスを受けた秒数を示します。Acct-Status-Type が Stop に設定されているアカウンティング要求レコードにのみ表示されます。	30、31
193 ～ 205	予約済み		
206	Transaction ID	トランザクション ID。例：0x7df10d5d	32、33
207	Client IP Address	アドレス 13.0.0.2 を介してクライアントに割り当てられる IP アドレス	32、33、34

IE	説明	書式例	関連する手順
208	要求された IP アドレス	DHCP要求メッセージでクライアントによって要求されたIPアドレス。（DHCP オプション：requested ip addr(50) : 13.0.0.2	33
209	デフォルト GW	デフォルトゲートウェイの IP アドレス例：DHCP オプション - default gateway(03) : 25.8.0.1	32、33
210	Primary DNS Server	プライマリ DNS サーバーの IP アドレス例：DHCP オプション - primary dns server(06) : 49.45.0.1	32、33
211	Secondary DNS Server	セカンダリ DNS サーバーの IP アドレス例：DHCP オプション - secondary dns server(06) : 4.5.6.7	32、33
212	リース時間	リース時間の IP アドレス。例：DHCP オプション - lease time(51) : Infinite / 2000 in seconds	32、33
213	サーバー ID	DHCP サーバー識別子例：DHCP オプション - server identifier(54) : 10.70.150.223	32、33
214	サブネット マスク	サブネットマスクのIPアドレス例：DHCPオプション - subnet mask(01) : 255.255.0.0	32、33
215	エラーメッセージ	例：DHCP Option-message (56) : Invalid requested IP	33、34
216 ～ 220	予約済み		

（注） スキーマ 1 ～ 170 は、ePDG に固有です。スキーマ 1 ～ 170 + 10 CUP スキーマは PGW に固有であり、スキーマ 171 ～ 220 は SaMOG に固有です。

RTT の設定

ここでは、ePDG、P-GW、および SaMOG の RTT 設定情報について説明します。

コールトランザクションを記録および生成するための RTT の設定

RTT がコールトランザクションを記録および生成できるようにするには、次の設定コマンドを使用します。

```
configure
  context context_name
```

```
    [ epdg-service | pgw-service | samog-service ] service_name
      [ no ] reporting-action event-record
end
```

注：

- **reporting-action event-record**：RTT によるイベントレポートを有効にします。
- **no**：RTT によるイベントレポートを無効にします。

セッション イベント モジュールでの RTT の設定

次の設定を使用して、ePDG、P-GW、および SaMOG で RTT 機能を設定します。

```
configure
  context context_name
    session-event-module
      event transfer-mode push primary url URL_addressfile name file_name
 | rotation volume volume_size | rotation time rotation_time | compression
compression_type | extension extension_type
       event use-harddisk
       event remove-file-after-transfer
       event push-interval interval_time
    end
```

注：

- **transfer-mode**：RTT での転送モードを有効にします。
- **push primary url***URL_address*：レコードが転送される外部サーバーの場所を指定します。
- **file name** *file_name*：レコードが保存される RTT ファイル名を指定します。*file_name* には、1 ～ 31 文字の英数字を指定できます。
- **rotation volume** *volume_size*：RTT ファイルは、このボリュームに基づいて生成されます。51200 ～ 62914560 の整数を入力します。
- **rotation time** *rotate_time*：RTT ファイルは、この時間に基づいて生成されます。30 ～ 86400 秒の整数を入力します。

（注） RTT ファイルは、ローテーションボリュームまたはローテーション時間に基づいて内部的に生成されます。

- **compression**：ファイル圧縮タイプを指定します。有効にすると、RTT ファイルが Gzip ファイルとして生成されます。それ以外の場合は、通常のファイルとして生成されます。
- **extension***extension_type*：RTT ファイル拡張子（.csv）を指定します。
- **event use-harddisk**：RTT ファイル生成用のストレージスペースとしてハードディスクを指定します。

- **event remove-file-after-transfer**：ファイルを外部サーバーにプッシュした後に削除する RTT ファイルを指定します。
- **event push-interval**：RTT ファイルが外部サーバーに転送されるプッシュ間隔時間を指定します。

モニタリングおよびトラブルシューティング

この項では、この機能をサポートするために show コマンドを使用して監視およびトラブルシューティングする方法について説明します。

show コマンドと出力

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show samog-service name

表 *33 : show samog-service name* コマンド出力の説明

フィールド	説明
レポートアクション	
イベントの記録	RTT機能が有効になっているかどうかを示します。

show event-record statistics

表 *34 : show event-record statistics* コマンド出力の説明

フィールド	説明
Total Number of Event Records	イベントレコードの合計数（GTPv2 + Diameter + IKE + RA + Radius + DHCP。
GTPv2 Event Records	GTPv2 レコードの合計数。
CSR	CSR（セッション作成要求）イベントの合計数。
CBR	CBR（ベアラー作成要求）イベントの合計数。
DSR	DSR（セッション削除要求）イベントの合計数。
DBR	DBR（ベアラー削除要求）イベントの合計数。
UBR	UBR（ベアラー更新要求）イベントの合計数。

フィールド	説明
IPV6 RA Event Records	IPV6 RA イベントレコードの合計数。
RA Prefix	RA プレフィックスイベントの総数。
Diameter Event Records	Diameter イベントレコードの合計数（S6b + SWm + STa + Gx + Gy）。
ePDG イベント	
IKEv2 Event Records	IKE イベントの総数。
IKE_SA_INIT	IKE_SA_INIT イベントの合計数。
IKE_AUTH	IKE_AUTH イベントの合計数。
IKE_INFORMATION	IKE_INFORMATION イベントの合計数。
CREATE_CHILD_SA	CREATE_ChiLD_SA イベントの合計数。
SaMOG イベント	
Radius Auth Event Records	RADIUS 認証イベントレコードの合計数。
Access Req/Challenge	RADIUS認証アクセス要求のチャレンジイベントレコードの合計数。
Access Req/Accept	RADIUS 認証アクセス要求の承認イベントレコードの合計数。
Disconnect Req	RADIUS 認証切断要求イベントレコードの合計数。
Radius Accounting Event Records	RADIUS アカウンティング イベント レコードの合計数。
Accounting Req from WLC	WLCからのRADIUSアカウンティングイベントレコードの合計数。
Accounting Req to Radius Server	RADIUS サーバーへの RADIUS アカウンティング イベント レコードの合計数。
STa Procedures	STa インターフェイス固有イベントの合計数。
AAR	AAR（AA-Request）イベントの合計数。
RAR	RAR（再承認要求）イベントの合計数。
ASR	ASR （セッション中止要求）イベントの合計数。
STR	STR （セッション終了要求）イベントの合計数。

フィールド	説明
DER	DER（DE-Request）イベントの合計数。
DHCP Event Records	DHCP イベントレコードの合計数。
Discover/Offer	DHCPv4 検出オファーイベントレコードの合計数。
Release/Ack	DHCPv4 リリース ACK イベントレコードの合計数。
Request/Ack	DHCPv4 要求 ACK イベントレコードの合計数。

バルク統計

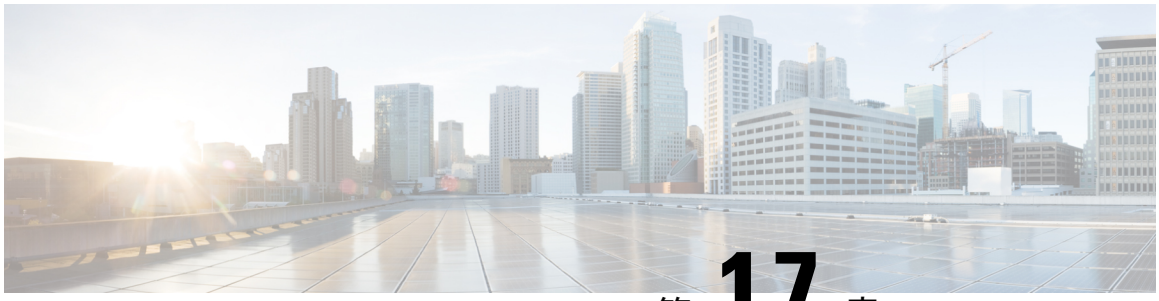
この機能の一部として、次のバルク統計が SaMOG スキーマに追加されています。

SaMOG スキーマ

表 *35 : SaMOG* スキーマのバルク統計変数

変数	説明
sess-samog-total-number-event-records	SaMOG セッションイベントレコードの合計数。
sess-samog-total-s2a-event-records	SaMOG S2a イベントレコードの合計数。
sess-samog-total-csr-event-records	SaMOG CSR イベントレコードの合計数。
sess-samog-total-cbr-event-records	SaMOG CBR イベントレコードの合計数。
sess-samog-total-dsr-event-records	SaMOG DSR イベントレコードの合計数。
sess-samog-total-dbr-event-records	SaMOG DBR イベントレコードの合計数。
sess-samog-total-ubr-event-records	SaMOG UBR イベントレコードの合計数。
sess-samog-total-ipv6-ra-event-records	SaMOG IPv6 RA イベントレコードの合計数。
sess-samog-total-ra-prefix-event-records	SaMOG RA プレフィックス イベント レコードの合計数。
sess-samog-total-dhcpv4-event-records	SaMOG DHCPv4 イベントレコードの合計数。
sess-samog-total-dhcpv4-disc-offer-event-records	SaMOG DHCPv4 ディスカバリ オファー イベントレコードの合計数数。
sess-samog-total-dhcpv4-req-ack-event-records	SaMOG DHCPv4 要求の確認応答イベントレコードの合計数。

変数	説明
sess-samog-total-dhcpv4-rel-ack-event-records	SaMOG DHCPv4 リリースの確認応答イベントレコードの合計数。
sess-samog-total-rad-auth-event-records	SaMOG RADIUS 認証イベントレコードの合計数。
sess-samog-total-rad-auth-acc-req-chal-event-records	SaMOG RADIUS 認証アクセス要求のチャレンジイベントレコードの合計数。
sess-samog-total-rad-auth-acc-req-acpt-event-records	SaMOG RADIUS 認証アクセス要求が承認されたイベントレコードの合計数。
sess-samog-total-rad-auth-disc-req-event-records	SaMOG RADIUS 認証切断要求イベントレコードの合計数。
sess-samog-total-rad-acct-event-records	SaMOG RADIUS アカウンティング イベント レコードの合計数。
sess-samog-total-rad-acct-wlc-event-records	ワイヤレス LAN コントローラからの SaMOG RADIUS アカウンティング イベント レコードの合計数。
aaa-samog-total-rad-acct-aaa-event-records	AAA に送られた SaMOG RADIUS アカウンティング イベント レコードの合計数。
aaa-samog-total-sta-event-records	SaMOG STa イベントレコードの合計数。
aaa-samog-total-sta-aar-event-records	SaMOG STa AAR イベントレコードの合計数。
aaa-samog-total-sta-der-event-records	SaMOG STa DER イベントレコードの合計数。
aaa-samog-total-sta-asr-event-records	SaMOG STa ASR イベントレコードの合計数。
aaa-samog-total-sta-rar-event-records	SaMOG STa RAR イベントレコードの合計数。
aaa-samog-total-sta-str-event-records	SaMOG STa STR イベントレコードの合計数。



第 17 章

Cisco Ultra Traffic Optimization

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （339 ページ）
- 概要 （341 ページ）
- Cisco Ultra Traffic Optimization の仕組み （341 ページ）
- Cisco Ultra Traffic Optimization の設定 （375 ページ）
- モニタリングおよびトラブルシューティング （380 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • Ultra Gateway Platform
機能のデフォルト	無効：ライセンスが必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide*

マニュアルの変更履歴

重要 リリース 21.2 および N5.1 よりも前に導入された機能の変更履歴の詳細は示されません。

改訂の詳細	リリース
このリリースでは、P-GW は、Cisco Ultra Traffic Optimization の show コマンドをサポートしており、UDP および TCP スプリットのアップリンクとダウンリンクの Rx/Tx パケット統計を表示するように出力が拡張されています。	21.23
このリリースでは、Cisco Ultra Traffic Optimization P-GW は、トラフィックの高スループット（4G または 5G）最適化をサポートしています。	21.22
このリリースでは、P-GW は最適化ライブラリでの MBR/GBR 処理をサポートしています。	21.21
このリリースでは、Cisco Ultra Traffic Optimization の設定可能なポリシーパラメータの範囲が変更されています。	21.20.4
このリリースでは、次の 3 つの新しいパラメータが大規模 TODR に追加されています。 **1.** International Mobile Subscriber Identity（IMSI） **2.** フロー ID およびフロー ID リスト **3.** ユーザーロケーション情報（ULI） 詳細については、「大規模 *TODR* の機能拡張」のセクションを参照してください。	21.19.1
Cisco Ultra Traffic Optimization ライブラリバージョンが 3.0.9 から 3.0.11 にアップグレードされました。	21.14.2
このリリースでは、新しいキーワード **large-flows-only** および **managed-large-flows-only** が **data-record** コマンドの一部として導入され、CUTO ライブラリがそれぞれの統計を外部サーバーにストリーミングできるようになりました。 この機能拡張をサポートする新しいバルク統計が追加されました。	21.14
このリリースでは、Cisco Ultra Traffic Optimization ソリューションが拡張され、TCP トラフィックの既存のサポートとともに、基本的な Quick UDP Internet Connections（QUIC）UDP トラフィックをサポートするようになりました。	21.3.17
Cisco Ultra Traffic Optimization 関連の設定を有効にするためにシャーシを再起動する必要がなくなりました。	21.3.x
Cisco Ultra Traffic Optimization ソリューションのためのマルチポリシーのサポート。	21.6

改訂の詳細	リリース
Cisco Ultra Traffic Optimization ソリューションが、Ultra Gateway Platform（UGP）でサポートされています。	21.6
Cisco Ultra Traffic Optimization ソリューションが拡張され、TCP トラフィックの既存のサポートとともに、基本的な Quick UDP Internet Connections（QUIC）UDP トラフィックをサポートするようになりました。	21.5
Cisco Ultra Traffic Optimization 関連の設定を有効にするためにシャーシを再起動する必要がなくなりました。	21.5
最初の導入。	21.2

概要

高帯域幅のバルクデータフローのシナリオでは、さまざまなワイヤレスネットワークの状態とポリシー（シェーピング、スロットリング、特に RAN において輻輳を引き起こすその他のボトルネックなど）によって、ユーザーエクスペリエンスに影響が及びます。これにより、TCP は鋸歯状のアルゴリズムを適用して輻輳制御を行い、ユーザーエクスペリエンスが影響を受けます。また、システム全体のキャパシティが十分に活用されなくなります。

Cisco Ultra Traffic Optimization ソリューションは、TCP および HTTP トラフィックのクライアントレスの最適化を提供します。このソリューションは Cisco P-GW と統合されており、次の利点があります。

- 既存のセルサイトのキャパシティが増加し、より多くのトラフィックを送信できます。
- 1 秒あたりのビット数が増えることで、ユーザーの Quality of Experience（QoE）が向上します。
- 特にネットワークの輻輳時に、サブスクライバごとのスループットを即座に安定させ、最大化できます。

Cisco Ultra Traffic Optimization の仕組み

Cisco Ultra Traffic Optimization は、ネットワークの負荷が高い/輻輳が発生しているときにビデオトラフィックをシェーピングすることで、そのメリットを実現します。ゲートウェイを通過する個々のビデオフローをモニターおよびプロファイルし、機械学習アルゴリズムを使用して、そのフローが輻輳したチャネルを通過しているかどうかを判断します。Cisco Ultra Traffic Optimization は、検出された輻輳の程度に応じて、ビデオフローをさまざまなレベルと時間に制御し、ビデオトラフィックの配信を輻輳が少ない時間帯に効率的に調整します。その際、品質を維持するために、引き続き十分な帯域幅をビデオに提供します。その結果、HD ビデオを維持しながら、ネットワーク遅延を減少させ、ユーザースループットを向上させることができ

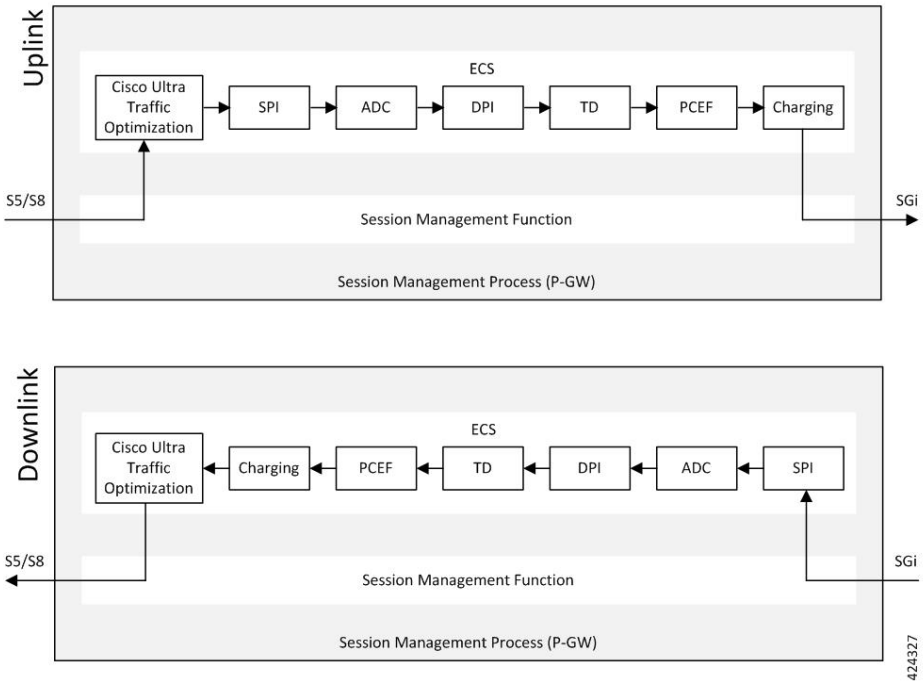
ます。Cisco Ultra Traffic Optimization では、どのような形であれ、パケットがドロップされたり、データペイロードが変更されることはありません。

Cisco Ultra Traffic Optimization は、アプリケーションの検出と制御（ADC）などの標準の Cisco P-GW 機能と統合され、モバイル通信事業者は、トラフィックのアプリケーションタイプや、APN、QCI、およびその他の一般的なトラフィックの詳細に基づいて最適化ポリシーを定義できます。Cisco Ultra Traffic Optimization は、無線ネットワークに完全に対応しており、eNodeB セル単位で管理できます。

アーキテクチャ

StarOS には高度に最適化されたパケット処理フレームワークの Cisco Ultra Traffic Optimization エンジンが搭載されており、ユーザーパケット（ダウンリンク）はオペレーティングシステムのユーザースペースで処理されます。P-GW のさまざまな機能を含む高速パケット処理は、ユーザースペースで実行されます。Cisco Ultra Traffic Optimization エンジンは、StarOS の明確に定義されたアプリケーション プログラミング インターフェイス（API）を使用して、Cisco P-GW のパケット処理パスに統合されています。

次の図は、トラフィックの最適化による P-GW パケットフローの概要を示しています。



ライセンス

Cisco Ultra Traffic Optimization は、シスコのライセンスソリューションです。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスの

インストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

制限事項と制約事項

- P-GW が Cisco Ultra Traffic Optimization エンジンに送信するために選択する値は、ベアラー GBR とベアラー MBR から関連付けられた値です。
- 現在の実装では、トラフィックの最適化のために、ダウンリンク GBR と MBR のみがエンジンに送信されます。
- UDP および QUICベースのトラフィック最適化は、ポート 443 でのみサポートされます。
- トラフィック最適化のデータレコードは、EDR と同じフォルダに生成されます。また、ファイルローテーション条件は EDR と同様になります。
- ライブラリを静的にリンクせずに動的にロードするプロビジョニングは制限されています。
- OP は、「フローごと」のレベルの GBR と MBR で機能してフローを最適化します。ただし、P-GW は、ベアラーレベルの GBR および MBR の送信のみをサポートします。
- 最適化ライブラリ機能への GBR および MBR 値の送信は、P-GW 製品にのみ適用されます。

トラフィック最適化データレコードの処理

トラフィック最適化データレコード（TODR）は、Cisco Ultra Traffic Optimization エンジンのアイドルタイムアウトの期限切れ時にのみ生成されます。P-GW からのセッションまたはフローに関連する統計は、この TODR に含まれていません。データレコードは、トラフィック最適化統計用の個別のファイルであり、外部分析プラットフォームで使用できます。

大規模 TODR の機能拡張

21.19.1 以降のリリースでは、次の 3 つの新しいパラメータが大規模 TODR に追加されています。

1. International Mobile Subscriber Identity（IMSI）
2. フロー ID およびフロー ID リスト
3. ユーザーロケーション情報（ULI）

   フロー ID は、エンドポイント検出および応答に表示される ACS フロー ID（「sn-flow-id」属性）を関連付けるために使用され、その後、ULI が RAN カウンタに関連付けられます。

（注） これらの新しいフィールドは、非 VPP ベースの P-GW および SAEGW で生成された大規模 TODR でのみ使用できます。

大規模 TODR の機能拡張

大規模 TODR の機能拡張を有効にするには、次の設定を使用します。

```
configure
  active-charging service service_name
    traffic-optimization-profile
      data-record
        enhanced-large-todr [ imsi | acs-flow-id | uli ]
        end
```

例 1：すべてのフィールドを表示する場合

```
enhanced-large-todr
```

例 2：IMSI と ULI を表示する場合

```
enhanced-large-todr imsi
enhanced-large-todr uli
```

コマンドと出力の表示

```
show active-charging traffic-optimization info
```

出力例 1：

```
[local]laas-setup# show active-charging traffic-optimization info
        Version   : 3.1.1
        Mode      : Active
        Configuration:
                Data Records(TODR): ENABLED     TODR Type: ALL_FLOWS
                Statistics Options: DISABLED
                EFD Flow Cleanup Interval: 1000(milliseconds)
                Statistics Interval: 60(seconds)
                Enhanced Large TODR: DISABLED
[local]laas-setup#
```

IMSI と ULI の出力例 2：

```
[local]laas-setup# show active-charging traffic-optimization info
        Version   : 3.1.1
        Mode      : Active
        Configuration:
                Data Records(TODR): ENABLED     TODR Type: ALL_FLOWS
                Statistics Options: DISABLED
                EFD Flow Cleanup Interval: 1000(milliseconds)
                Statistics Interval: 60(seconds)
                Enhanced Large TODR: ENABLED, Fields: imsi uli
[local]laas-setup#
```

このコマンドの出力には、次のフィールドが含まれています。

- Enhanced Large TODR

既存の大規模 TODR の機能拡張

1. **IMSI を使用した大規模 TODR**

   IMSI：International Mobile Subscriber Identity を示します。

   信頼できるビルドの場合、IMSI 値は 0 です。

2. **ACS Flow ID**

   [ACS Flow ID] は新しく導入されたフィールドです。大量のフローが存在する可能性があるため、TODR の一部として最大 20 フローに制限されます。

   acs_flow_id_count：この TODR に存在する ACS フロー ID の数。最大 20 の ACS フロー ID が存在します。

   acs_flow_id_list：個別の ACS フロー ID のリスト。たとえば、acs_flow_id1、acs_flow_id2 などです。

   1. **EDR ACS Flow ID**

      EDR では、各 ACS フロー ID は、次に示すように EDR 設定で属性「sn-flow-id」を有効にすると出力されます。

      ```
      config
      active-charging service ACS
          edr-format EDR_SN
          delimiter comma
            attribute sn-flow-id priority 10
            rule-variable bearer 3gpp imsi priority 15
            rule-variable bearer qci priority 20
      ```

      ACS フロー ID は、EDR で **92:30278:14786055** の形式で出力されます。

      - 92 はセッション マネージャ インスタンスです。
      - 30278 はセッションハンドルまたはセッション番号です。
      - 14786055 は ACS フロー ID です。

   2. **TODR ACS Flow ID**

      TODR ACS フロー ID は、お客様が TODR を EDR に関連付けることができるように、EDR と同じ形式にする必要があります。したがって、acs_flow_id1、acs_flow_id2 などのリスト acs_flow_id_list 内の各フロー ID は、`smgr instance:session handle: flow id` として TODR に出力される必要があります。

      たとえば **92:30278:14786055** です。

      - 92 はセッション マネージャ インスタンスです。
      - 30278 はセッションハンドルまたはセッション番号です。
      - 14786055 は ACS フロー ID です。

3. **ULI**

元の要件は ECGI を出力することでしたが、すべてのシナリオをカバーしているわけではありません。たとえば、PGW が 4G から 3G に移動するコールのアンカーである場合、ECGI では矛盾します。ユーザーが現在 3G にいるため、ULI（ユーザーロケーション情報）は ECGI ではなく CGI を示すからです。通常、MME は ULI で発生した変更を SGW 経由で PGW に通知します。この機能は、ECGI のスーパーセットである ULI をサポートします。

新しいフィールドは ULI と呼ばれますが、ULI は複数の識別子で構成される可変長の複雑な IE です。詳細については、3GPP TS 29.274 を参照してください。

図 *14*：ユーザーロケーション情報（*ULI*）

Octets	Bits 8	7	6	5	4	3	2	1
1	Type = 86 (decimal)							
2 to 3	Length = n							
4	Spare				Instance			
5	Spare		LAI	ECGI	TAI	RAI	SAI	CGI
a to a+6	CGI							
b to b+6	SAI							
c to c+6	RAI							
d to d+4	TAI							
e to e+6	ECGI							
f to f+4	LAI							
g to (n+4)	These octet(s) is/are present only if explicitly specified							

ULI は 1 つ以上の識別子で構成できます。たとえば、UIC に TAI と ECGI の両方が含まれる場合がありますが、こうした識別子をサポートすることで問題が生じます。ULIはパケットレベルごとに存在し、合計長は 8 バイトを超えます。また、バイト配列を渡す必要があり、パフォーマンスに影響を与えるためです。この課題を克服するために、URI を複合タイプ（たとえば、TAI と ECGI の組み合わせ）として形成すると、ECGI 部分のみが TODR に表示されます。これは、URI の識別子部分が `uint64_t`（8 バイト）に格納されるようにするために行われます。具体的には次のとおりです。

1. TAI と ECGI の両方が複合タイプとして存在する場合、ECGI のみが表示されます。
2. CGI と RAI の両方が複合タイプとして存在する場合、CGI のみが表示されます。
3. SAI と RAI の両方が複合タイプとして存在する場合、RAI のみが表示されます。

すべての TODR は、2 秒の精度で複数のフェーズを持つことができます。ULI は次のようにフェーズ属性のリストに が追加されます。

1. *ULI*：新しく導入されたフィールド。

   ULI Details

   ECGI は、次の図に示すように ULI に保存されます。次の形式で出力する必要があります。

   ULI タイプ：ULI 値

   ULI タイプは次のいずれかになります。

   - 1–CGI

- 2–SAI
- 4–RAI
- 8–TAI
- 16–ECGI

ECGI は、次の図に示すように ULI に保存されます。次の形式で出力する必要があります。

ULI タイプ：**ULI 値**

ULI タイプが ECGI である場合の例を次に示します。

16:0x21635401234567

この 16 は、ULI タイプが ECGI であることを表します

0x21635401234567 は ECGI の 16 進数表現です。

MCC は「123」です。つまり、MCC の 3 桁は「1」、「2」、「3」です。MNC は「456」です。 つまり、MNC の 3 桁は「4」、「5」、「6」です

ECI は 10 進数で「19088743」（16 進数で「1234567」）です

図 *15 : ECGI* フィールド

Octets	Bits 8	7	6	5	4	3	2	1
e	MCC digit 2				MCC digit 1			
e+1	MNC digit 3				MCC digit 3			
e+2	MNC digit 2				MNC digit 1			
e+3	Spare				ECI			
e+4 to e+6	ECI (E-UTRAN Cell Identifier)							

属性とファイル形式のリスト

トラフィック最適化のすべての TODR 属性は、単一の CLI コマンドで有効化されます。出力は常にカンマ区切りで、厳密な形式で示されます。

標準 TODR

標準 TODR の形式を次に示します。

```
instance_id,flow_type,srcIP,dstIP,policy_id, proto_type, dscp,
flow_first_pkt_rx_time_ms,flow_last_pkt_rx_time_ms,flow_cumulative_rx_bytes
```

例：

```
1,0,173.39.13.38,192.168.3.106,0,1,0,
 1489131332693,1489131335924,342292
```

それぞれの説明は次のとおりです。

- *instance_id*：インスタンス ID。

- *flow_type*：標準フロー（0）
- *srcIP*：送信元 IP アドレスを示します。
- *dstIP*：宛先 IP アドレスを示します。
- *policy_id*：トラフィック最適化ポリシー ID を示します。
- *proto_type*：使用されている IP プロトコルを示します。IP プロトコルは TCP および UDP です。
- *dscp*：アップストリームパケットの DSCP コードを示します。
- *flow_first_pkt_rx_time_ms*：トラフィックの最適化中に最初のパケットが検出されたときのタイムスタンプを示します。
- *flow_last_pkt_rx_time_ms*：トラフィックの最適化中に最後のパケットが検出されたタイムスタンプを示します。
- *flow_cumulative_rx_bytes*：このフローによって転送されたバイト数を示します。

大規模 TODR

次に、大きな TODR の出力例を示します。

```
19,1,404005123456789,22.22.0.1,209.165.200.225.8,custom1,2,0,1588858362158,1588858952986,16420806,1588858364162,419,351,7000,0,0,1,
19:2:15,2,0,0,2,1,1,16:0x12546300012345,
1588858364162,80396,1472,0,0,0,2,1,16:0x12546300012345,1588858366171,146942,1937,7000,0,0,2
```

それぞれの説明は次のとおりです。

- *instance_id*：インスタンス ID。
- *flow_type*：大規模フロー（1）
- *imsi_id*： International Mobile Subscriber Identity を示します。
- *srcIP*：送信元 IP アドレスを示します。
- *dstIP*：宛先 IP アドレスを示します。
- *policy_name*：設定されたトラフィック最適化ポリシーの名前を識別します。
- *policy_id*：トラフィック最適化ポリシー ID を示します。
- *proto_type*：使用されている IP プロトコルを示します。IP プロトコルは TCP および UDP です。
- *dscp*：アップストリームパケットの DSCP コードを示します。
- *flow_first_pkt_rx_time_ms*：トラフィックの最適化中に最初のパケットが検出されたときのタイムスタンプを示します。
- *flow_last_pkt_rx_time_ms*：トラフィックの最適化中に最後のパケットが検出されたときのタイムスタンプを示します。

- *flow_cumulative_rx_bytes*：このフローによって転送されたバイト数を示します。
- *large_detection_time_ms*：大規模フローが検出されたときのタイムスタンプを示します。
- *avg_burst_rate_kbps*：測定されたすべてのバーストの平均レートを Kbps 単位で示します。
- *avg_eff_rate_kbps*：平均有効レートを Kbps 単位で示します。
- *final_link_peak_kbps*：大規模フローの存続期間中に検出された最大のリンクピークを示します。
- *recover_capacity_bytes*：この大規模フローの回復済みキャパシティを Kbps 単位で示します。
- *recover_capacity_ms*：この大規模フローの回復済みキャパシティのタイムスタンプを示します。
- *acs_flow_id_count*：この TODR に存在する ACS フロー ID の数を示します。最大 20 の ACS フロー ID が存在します。
- *acs_flow_id_list*：個別の ACS フロー ID のリストを示します。たとえば、acs_flow_id1、acs_flow_id2 などです。
- *Phase_count*：大規模フローのフェーズ数を示します。
- *min_gbr_kbps*：最小保証ビットレート（GBR）を Kbps 単位で示します。
- *max_gbr_kbps*：最大保証ビットレート（MBR）を Kbps 単位で示します。
- *Phase_count_record*：このレコードに存在するフェーズの数を示します。
- *end_of_ Phases*：0（フェーズの終了ではない）または 1（フェーズの終了）。
- 大規模なフローのフェーズ属性：
  - *Phase_type*：フェーズのタイプを示します。このフィールドは、フローが次の 3 つの可能な状態のいずれかであったことを示します。各状態は数値で表されます。
    - 0 - 増加フェーズ（フローが以前アイドルだった場合）
    - 1 - 測定フェーズ（必須）
    - 2 - フロー制御フェーズ（測定フェーズで輻輳が検出された場合）
  - *uli_type*：ULI のタイプを示します。
  - *Phase_start_time_ms*：フェーズの開始時刻のタイムスタンプを示します。
  - *burst_bytes*：バーストサイズをバイト単位で示します。
  - *burst_duration_ms*：バースト期間をミリ秒単位で示します。
  - *link_peak_kbps*：フロー存続期間中のフローのピークレートを示します。

- *flow_control_rate_kbps*：フロー制御が試行されたときのレートを示します（非フロー制御フェーズの場合は 0）。このフィールドは、フローが「フロー制御フェーズ」の場合にのみ有効です。
- *max_num_queued_packets*：キューに入れられたパケットの最大数を識別します。
- *policy_id*：トラフィック最適化ポリシー ID を識別します。

最適化ライブラリへの GBR および MBR 値の送信

P-GW は次を送信します。

- トラフィック最適化の分類選択に基づく GBR および MBR 値
- 最適化ライブラリへのフローレベルの GBR および MBR 値
- 最適化ライブラリへのダウンリンク GBR と MBR のみ

P-GW は、最適化ライブラリに、非 GBR ベアラー上のフローとしてゼロ GBR 値を渡します。

最適化ライブラリは、送信元 IP、宛先 IP、およびプロトコル IP（3 タプル）に基づいて論理フローを維持します。一方、P-GW は、送信元 IP、宛先 IP、送信元ポート、宛先ポート、およびプロトコル IP（5 タプル）に基づいて、GBR および MBR の値を最適化ライブラリに渡します。したがって、複数の StarOS の 5 タプルエントリが、最適化ライブラリの同じ 3 タプルエントリに属することができます。最適化ライブラリは以下を使用します。

- 上限値として、同じ 3 タプルエントリに属するすべての MBR 値の最小値。
- 下限値として、同じ 3 タプルエントリに属するすべての GBR 値の最大値。

高スループットトラフィック最適化のサポート

Cisco Ultra Traffic Optimization 機能が強化され、トラフィックの最適化を通じてサブスクライバをサポートします。高スループットトラフィック最適化サポート機能により、5G サブスクライバのトラフィック（高スループット）の最適化のサポートが追加されています。この機能により、スループット特性（4G または 5G に基づく）に応じて、トラフィック最適化パラメータを自動的に切り替えることもできます。

（注） これはライセンスで供与される機能です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

既存の Cisco Ultra Traffic Optimization のシングルフローロジックが強化され、リアルタイムのプロファイルパケットパターン（たとえば、4G LTE 対 5G mm および波トラフィックパターン）に応じてアルゴリズムが動的に切り替わります。

Cisco Ultra Traffic Optimization ライブラリが更新され、トラフィック最適化ポリシーに 2 つの別個のポリシーパラメータセットが導入されました。

- ベースポリシーパラメータ：これらのパラメータは、通常のスループット（4Gスループットなど）を検出したときに、Cisco Ultra Traffic Optimization アルゴリズムによって適用されます。これらは「基本」ポリシーパラメータと呼ばれます。これらのパラメータは、高スループットトラフィック最適化サポート機能が導入される前に存在していたパラメータと同じものです。
- 拡張ポリシーパラメータ：これらのパラメータは、フローの高スループット（5G スループットなど）を検出したときに、Cisco Ultra Traffic Optimization アルゴリズムによって適用されます。これらは「拡張」ポリシーパラメータと呼ばれます。

同じポリシーに含まれる 2 つの別個のポリシーパラメータセットは、スループットに変更があった場合、セッションマネージャの介入を必要とせずに、一方のセットからもう一方のセットに迅速に切り替わります。

そのため、同じポリシー内で2つの別個のポリシーパラメータセットを設定すると、Cisco Ultra Traffic Optimization アルゴリズムがスループットの変化に合わせて自動的、動的、かつ即時に調整されるという要件を満たすことができます。このスループットの変化は、たとえば、UE が 5G または高速 4G のカバレッジエリアに入ったときなど、RAN 特性の変化によって発生する可能性があります。

高スループット最適化サポートの仕組み

Cisco Ultra Traffic Optimization アルゴリズムは、トラフィックをモニターし、次のロジックに基づいて、基本ポリシーパラメータと拡張ポリシーパラメータの間を自動的に移行します。

1. 基本ポリシーから始めます。
2. 測定フェーズのバーストレートが拡張リンクプロファイルの初期レートより大きい場合は、拡張ポリシーに移行します。
3. 測定フェーズのバーストレートが基本リンクプロファイルの最大レートより小さい場合は、基本ポリシーに移行します。
4. すべての測定フェーズについて、手順 2 と 3 を繰り返します。

.

トラフィック最適化のためのマルチポリシーのサポート

Cisco Ultra Traffic Optimization エンジンは、複数のポリシーのトラフィック最適化をサポートし、必要な場所でトラフィックの最適化を実行します。デフォルトでは、2 つの事前設定済みポリシーを含む最大 32 のポリシーがサポートされます。通信事業者は、各トラフィック最適化ポリシーで複数のパラメータを設定できます。

この機能には、次の機能が含まれます。

- デフォルトでは、トラフィック最適化は、サービススキーマを使用する特定のサブスクライバ、ベアラー、またはフローの TCP および UDP データに対して有効になっています。

重要 ポート 443 は、UDP または QUIC ベースのトラフィック最適化をサポートしています。

- ポリシーの選択は、設定した優先順位によって変わります。トラフィック最適化ポリシーに優先順位を付けるために、トリガー条件が使用されます。優先順位は、トラフィック最適化ポリシーが適用される具体的な場所に関係なく設定できます。設定した優先順位に基づいて、トラフィック最適化ポリシーを別のポリシーでオーバーライドできます。
- サービススキーマの下でトラフィック最適化ポリシーをトリガーアクションに関連付ける設定。
- ロケーショントリガーに対するトラフィック最適化ポリシーを選択する設定。現在、ローカルポリシーサービスコンフィギュレーションモードでは、ECGI 変更検出のみがサポートされています。

重要 ロケーション変更トリガーは、IPSG ではサポートされていません。

重要 セッションリカバリ（SR）またはシャーシ間セッションリカバリ（ICSR）後に、フローのポリシー ID は回復されません。

重要 マルチポリシーサポート機能を使用するには、同じ Cisco Ultra Traffic Optimization ライセンスキーをインストールする必要があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

マルチポリシーサポートの仕組み

ポリシーの選択

シスコの Ultra Traffic Optimization エンジンには、Managed と Unmanaged の 2 つのデフォルトポリシーが用意されています。Unmanaged ポリシーが選択されている場合、トラフィックの最適化は実行されません。

Managed ポリシーが選択されている場合は、トラフィックの最適化が、デフォルトのパラメータを使用して実行されます。トリガーアクションでポリシーが指定されておらず、ポリシーを

指定せずにトラフィックの最適化が有効になっている場合は、Managedポリシーが適用されます。

Managedポリシーが選択されている場合は、トラフィックの最適化が、デフォルトのパラメータを使用して実行されます。トリガーアクションでポリシーが指定されておらず、ポリシーを指定せずにトラフィックの最適化が有効になっている場合は、Managedポリシーが適用されます。

- セッション セットアップ トリガー：トリガーアクションがサービススキーマのセッションセットアップにのみ適用される場合、そのトリガーアクションは、新しいセッションにのみ適用されます。
- ベアラー セットアップ トリガー：トリガーアクションがベアラーセットアップにのみ適用される場合、そのトリガーアクションにおける変更は、新しく作成されたベアラーとそのフローに適用されます。
- フロー作成トリガー：フロー作成に対応するトリガー条件では、トリガー条件 any-match に加えて、rule-name、local-policy-rule、またはIPプロトコルに基づいて条件を追加できます。

トリガー条件が原因で既存のフローでのトラフィックの最適化が無効になっている場合、トラフィック最適化エンジンは、デフォルトの Unmanaged ポリシーをそれらに適用します。

ポリシーの削除

ポリシープロファイルを削除する前に、トラフィック最適化ポリシーへのすべての関連付けを削除する必要があります。

ポリシーの削除の詳細については、「トラフィック最適化ポリシーの設定」の項を参照してください。

マルチポリシーサポートの設定

次の項では、マルチポリシーサポートに必要な設定について説明します。

トラフィック最適化プロファイルの設定

トラフィック最適化プロファイルを設定するには、次の CLI コマンドを使用します。

```
configure
  require active-charging
  active-charging service service_name
    traffic-optimization-profile profile_name
      data-record[ large-flows-only | managed-large-flows-only ]
      no data record
      [ no ] efd-flow-cleanup-interval cleanup_interval
      [ no ] stats-interval stats_interval
      [ no ] stats-options { flow-analyst [ flow-trace ] | flow-trace
 [ flow-analyst ] }
      end
```

注：

- **require active-charging**：アクティブ課金サービスの設定要件を有効にします。



重要　このコマンドを設定した後で、設定を保存してからシャーシをリロードし、コマンドを有効にする必要があります。設定ファイルを保存してシャーシをリロードする方法については、使用している展開の『*System Administration Guide*』を参照してください。

- **data-record**：トラフィック最適化データレコードの生成を有効にします。

  large-flows-only：大規模フローのトラフィック最適化データレコードの生成を有効にします。

  managed-large-flows-only：管理対象大規模フローのトラフィック最適化データレコードの生成を有効にします。

  キーワード**large-flows-only** および **managed-large-flows-only** を **data-record** とともに設定すると、CUTO ライブラリが、**stats-options** コマンドの一部として、それぞれの統計を外部サーバーにストリーム配信できるようになります。オペレータは、**stats-options** キーワード **flow-trace** および **flow-analyst** と **data-record** コマンドの組み合わせを設定することが可能で、それに応じて CUTO ライブラリに通知できます。



（注）　上記の 2 つのキーワードのいずれかをデータレコードの一部として設定できます。設定すると、CUTO ライブラリがそれぞれの統計をストリーム配信できるようになります。

  data-record コマンドのデフォルトの動作は、上記の導入の影響を受けません。どのオプションも設定しなかった場合、既存の動作として、すべての標準フローと大規模フローに対して TODR が生成されます。

- **efd-flow-cleanup-interval**：EFD フローのクリーンアップ間隔を設定します。間隔値は、10 ～ 5000 ミリ秒の整数です。
- **stats-interval**：フロー統計の収集とレポートの間隔を秒単位で設定します。間隔値は、1 ～ 60 秒の整数です。
- **stats-options**：フロー統計を収集するためのオプションを設定します。外部サーバーへのストリームが Flow Trace か Flow Analyst、またはその両方である必要があるかどうかのみを指定します。



（注）　21.6 リリース以降、**heavy-session** コマンドは廃止されます。

トラフィック最適化ポリシーの設定

トラフィック最適化ポリシーを設定するには、次の CLI コマンドを使用します。

```
configure
  require active-charging
  active-charging service service_name[extended]
    [ no ] traffic-optimization-policy policy_name[extended]
      bandwidth-mgmt { backoff-profile [ managed | unmanaged ] [
min-effective-rate effective_rate [ min-flow-control-rate flow_rate ] |
min-flow-control-rate flow_rate [ min-effective-rate effective_rate ] ] |
min-effective-rate effective_rate [ backoff-profile [ managed | unmanaged
 ] [ min-flow-control-rate flow_rate ] | min-flow-control-rate control_rate
 [ backoff-profile [ managed | unmanaged ] ] | min-flow-control-rate [
 [ backoff-profile [ managed | unmanaged ] [ min-effective-rate
effective_rate ] | [ min-effective-rate effective_rate ] [ backoff-profile [
 managed | unmanaged ] ] }
      extended-bandwidth-mgmt { backoff-profile [ managed | unmanaged
 ] [ min-effective-rate effective_rate [ min-flow-control-rate flow_rate ]
| min-flow-control-rate flow_rate [ min-effective-rate effective_rate ] ] |
 min-effective-rate effective_rate [ backoff-profile [ managed | unmanaged
 ] [ min-flow-control-rate flow_rate ] | min-flow-control-rate control_rate
 [ backoff-profile [ managed | unmanaged ] ] | min-flow-control-rate [
 [ backoff-profile [ managed | unmanaged ] [ min-effective-rate
effective_rate ] | [ min-effective-rate effective_rate ] [ backoff-profile [
 managed | unmanaged ] ] }
      [ no ] bandwidth-mgmt
      [ no ] extended-bandwidth-mgmt
     curbing-control { max-phases max_phase_value [ rate curbing_control_rate
 [ threshold-rate threshold_rate [ time curbing_control_duration ] ] ] | rate
curbing_control_rate [ max-phases [ threshold-rate threshold_rate [ time
curbing_control_duration ] ] ] | threshold-rate [ max-phases max_phase_value [
 rate curbing_control_rate [ time curbing_control_duration ] ] ] | time [
max-phases max_phase_value [ rate curbing_control_rate [ threshold-rate
threshold_rate] ] ] }
      extended-curbing-control { max-phases max_phase_value [ rate
curbing_control_rate [ threshold-rate threshold_rate [ time curbing_control_duration
 ] ] ] | rate curbing_control_rate [ max-phases [ threshold-rate threshold_rate
 [ time curbing_control_duration ] ] ] | threshold-rate [ max-phases
max_phase_value [ rate curbing_control_rate [ time curbing_control_duration ] ] ]
| time [ max-phases max_phase_value [ rate curbing_control_rate [ threshold-rate
 threshold_rate] ] ] }
      [ no ] curbing-control
      [ no ] extended-curbing-control
      heavy-session { standard-flow-timeout [ threshold threshold_value
 | threshold threshold_value [ standard-flow-timeout timeout_value ] }
      extended-heavy-session { standard-flow-timeout [ threshold
threshold_value | threshold threshold_value [ standard-flow-timeout timeout_value
 ] }
      [ no ] heavy-session
      [ no ] extended-heavy-session
      link-profile { initial-rate initial_seed_value [ max-rate
max_peak_rate_value [ peak-lock ] ] | max-rate [ initial-rate initial_seed_value
 [ peak-lock ] ] | peak-lock [ initial-rate initial_seed_value [ max-rate
max_peak_rate_value ] ] }
```

```
        extended-link-profile { initial-rate initial_seed_value [ max-rate
 max_peak_rate_value [ peak-lock ] ] | max-rate [ initial-rate
initial_seed_value [ peak-lock ] ] | peak-lock [ initial-rate initial_seed_value
 [ max-rate max_peak_rate_value ] ] }
        [ no ] link-profile
        [ no ] extended-link-profile
        session-params { tcp-ramp-up tcp_rampup_duration [ udp-ramp-up
udp_rampup_duration ] | udp-ramp-up udp_rampup_duration [ tcp-ramp-up
tcp_rampup_duration ] }
        extended-session-params { tcp-ramp-up tcp_rampup_duration [
udp-ramp-up udp_rampup_duration ] | udp-ramp-up udp_rampup_duration [ tcp-ramp-up
 tcp_rampup_duration ] }
        [ no ] session-params
        [ no ] extended-session-params
        end
```

注：

- ポリシー名の後に **extended** キーワードを使用した場合にのみ、**extended-bandwidth-mgmt** などの「**extended-***」パラメータを表示できます。
- **no**：設定されたパラメータをデフォルト値で上書きします。通信事業者は、ポリシープロファイルを削除する前に、ポリシープロファイル内の関連付けられているポリシーをすべて削除する必要があります。これを実行しないと、次のエラーメッセージが表示されます。

  ```
  Failure: traffic-optimization policy in use, cannot be deleted.
  ```

- **bandwidth-mgmt**：基本帯域幅管理パラメータを設定します。
  - **backoff-profile**：バックオフ率の全体的なアグレッシブネスを決定します。
  - **managed**：トラフィックのモニタリングとトラフィックの最適化の両方を有効にします。
  - **unmanaged**：トラフィックのモニタリングのみを有効にします。
  - **min-effective-rate**：有効な最小シェーピングレートを Kbps 単位で設定します。
  - **min-flow-control-rate**：輻輳時に大量のセッションフローを制御するために許可される最小レートを Kbps 単位で設定します。
- **extended-bandwidth-mgmt**：拡張帯域幅管理パラメータを設定します。
  - **backoff-profile**：バックオフ率の全体的なアグレッシブネスを決定します。
  - **managed**：トラフィックのモニタリングとトラフィックの最適化の両方を有効にします。
  - **unmanaged**：トラフィックのモニタリングのみを有効にします。
  - **min-effective-rate**：有効な最小シェーピングレートを Kbps 単位で設定します。

- **min-flow-control-rate**：輻輳時に大量のセッションフローを制御するために許可される最小レートを Kbps 単位で設定します。

- **curbing-control**：基本抑制フローの制御関連パラメータを設定します。
  - **max-phases**：ターゲットのシェーピングレートが **threshold-rate** を下回る連続フェーズを設定して、抑制フローの制御をトリガーします。。
  - **rate**：動的レートではなく、固定レート（Kbps）で抑制フローの制御を設定します。
  - **threshold-rate**：抑制をトリガーする最小ターゲット シェーピング レートを Kbps 単位で設定します。。
  - **time**：フロー制御フェーズの期間をミリ秒単位で設定します。

- **extended-curbing-control**：拡張抑制フローの制御関連パラメータを設定します。
  - **max-phases**：ターゲットのシェーピングレートが **threshold-rate** を下回る連続フェーズを設定して、抑制フローの制御をトリガーします。拡張パラメータの場合、最大位相値は 2 ～ 10 の整数です。デフォルト値は基本パラメータの値を継承します。
  - **rate**：動的レートではなく、固定レート（Kbps）で抑制フローの制御を設定します。拡張パラメータの場合、制御レート値は 0 ～ 100000 kbps の整数です。デフォルト値は基本パラメータの値を継承します。
  - **threshold-rate**：抑制をトリガーする最小ターゲット シェーピング レートを kbps 単位で設定します。拡張パラメータの場合、しきい値レートは 100 ～ 100000 kbps の整数です。デフォルト値は基本パラメータの値を継承します。
  - **time**：フロー制御フェーズの期間をミリ秒単位で設定します。

    拡張パラメータの場合、フロー制御期間の値は 0 ～ 600000 の整数です。デフォルト値は基本パラメータの値を継承します。

- **heavy-session**：基本ヘビーセッションの検出パラメータを設定します。
  - **standard-flow-timeout**：標準フローの期限切れのアイドルタイムアウトをミリ秒単位で設定します。
  - **threshold**：ヘビーセッションの検出しきい値をバイト単位で設定します。このしきい値に達すると、フローがモニターされ、管理される可能性があります。。

- **extended-heavy-session**：拡張ヘビーセッションの検出パラメータを設定します。
  - **standard-flow-timeout**：標準フローの期限切れのアイドルタイムアウトをミリ秒単位で設定します。。
  - **threshold**：ヘビーセッションの検出しきい値をバイト単位で設定します。このしきい値に達すると、フローがモニターされ、管理される可能性があります。

- **link-profile**：基本リンクのプロファイルパラメータを設定します。

- **initial-rate**：トラフィックセッションで取得されたピークレートの初期シード値を Kbps 単位で設定します。
- **max-rate**：トラフィックセッションで許可される最大学習ピークレートを Kbps 単位で設定します。
- **peak-lock**：初期リンクピークレート設定で利用可能なリンクピークレートで確認します。

- **extended-link-profile**：拡張リンクのプロファイルパラメータを設定します。
  - **initial-rate**：トラフィックセッションで取得されたピークレートの初期シード値を Kbps 単位で設定します。
  - **max-rate**：トラフィックセッションで許可される最大学習ピークレートを Kbps 単位で設定します。
  - **peak-lock**：初期リンクピークレート設定で利用可能なリンクピークレートで確認します。

- **session-params**：基本セッションパラメータを設定します。
  - **tcp-ramp-up**：TCP トラフィックのランプアップフェーズ期間をミリ秒単位で設定します。
  - **udp-ramp-up**：UDP トラフィックのランプアップフェーズ時間をミリ秒単位で設定します。。

- **extended-session-params**：拡張セッションパラメータを設定します。
  - **tcp-ramp-up**：TCP トラフィックのランプアップフェーズ期間をミリ秒単位で設定します。
  - **udp-ramp-up**：UDP トラフィックのランプアップフェーズ時間をミリ秒単位で設定します。。



重要 **require active-charging** コマンドを設定した後で、設定を保存してからシャーシをリロードし、コマンドを有効にする必要があります。設定ファイルを保存してシャーシをリロードする方法については、使用している展開の『*System Administration Guide*』を参照してください。

基本および拡張セットパラメータの範囲とデフォルト値、および Cisco Ultra Traffic Optimization ライブラリでパラメータを設定する際の検証範囲と値を次の表に示します。

パラメータカテゴリ（基本/拡張）	パラメータ	基本パラメータの範囲。	デフォルト値（基本パラメータ）	拡張パラメータの範囲	デフォルト値（拡張パラメータ）	範囲/値のチェック	備考
bandwidth-mgmt/extended-bandwidth-mgmt	**backoff-profile**	**managed/unmanaged**	**managed**	**managed/unmanaged**	基本パラメータ値を継承	基本パラメータ値との一致が必要	基本パラメータ値とは異なる値を入力すると、基本パラメータの値と該当するメッセージが表示されます。
	min-effective-rate	100 ～ 100000 kbps	600	100 ～ 500000 kbps	45000	すべての範囲を許可	
	min-flow-control-rate	100 ～ 100000 kbps	250	100 ～ 500000 kbps	1000	すべての範囲を許可	

パラメータカテゴリ（基本/拡張）	パラメータ	基本パラメータの範囲。	デフォルト値（基本パラメータ）	拡張パラメータの範囲	デフォルト値（拡張パラメータ）	範囲/値のチェック	備考
curbing-control / extended-curbing-control	**max-phases**	2 ～ 10	2	2 ～ 10	基本パラメータ値を継承	すべての範囲を許可	
	rate	0 ～ 100000 kbps	0	0 ～ 100000 kbps	基本パラメータ値を継承	すべての範囲を許可	
	threshold-rate	100 ～ 100000 kbps	600	100 ～ 100000 kbps	基本パラメータ値を継承	すべての範囲を許可	
	time	0 ～ 600000 ミリ秒	0	0 ～ 600000 ミリ秒	基本パラメータ値を継承	すべての範囲を許可	
heavy-session / extended- heavy-session	**standard-flow-time out**	100 ー 10000 ミリ秒	500	100 ー 10000 ミリ秒	基本パラメータ値を継承	すべての範囲を許可	
	threshold	100000 ～ 100000000 バイト	3000000	100000 ～ 100000000 バイト	基本パラメータ値を継承	すべての範囲を許可	

パラメータカテゴリ（基本/拡張）	パラメータ	基本パラメータの範囲。	デフォルト値（基本パラメータ）	拡張パラメータの範囲	デフォルト値（拡張パラメータ）	範囲/値のチェック	備考
link-profile / **extended-link-profile**	**initial-rate**	100 ～ 100000 kbps	7000	100 ～ 500000 kbps	50000	基本パラメータの最大レート以上が必要	基本パラメータ値とは異なる値を入力すると、基本パラメータの値と該当するメッセージが表示されます。
	max-rate	100 ～ 100000 kbps	15,000	100 ～ 500000 kbps	100000	基本パラメータの最大レート以上が必要	基本パラメータ値とは異なる値を入力すると、基本パラメータの値と該当するメッセージが表示されます。
	peak-lock	enabled/disabled	disabled	enabled/disabled	disabled	どちらでも許可	

パラメータカテゴリ（基本/拡張）	パラメータ	基本パラメータの範囲。	デフォルト値（基本パラメータ）	拡張パラメータの範囲	デフォルト値（拡張パラメータ）	範囲/値のチェック	備考
session-params / extended-session- params	**tcp-ramp-up**	0 ～ 10000 ミリ秒	2000	0 ～ 10000 ミリ秒	2000	すべての範囲を許可	
	udp-ramp-up	0 ～ 10000 ミリ秒	2000	0 ～ 10000 ミリ秒	2000	すべての範囲を許可	

トラフィック最適化ポリシー：デフォルト値

```
Bandwidth-Mgmt:

   Backoff-Profile          : Managed
   Min-Effective-Rate       : 600 (kbps)
   Min-Flow-Control-Rate    : 250 (kbps)

Curbing-Control:

   Time                     : 0 (ms)
   Rate                     : 0 (kbps)
   Max-Phases               : 2
   Threshold-Rate           : 600 (kbps)

Heavy-Session:

   Threshold                : 3000000(bytes)
   Standard-Flow-Timeout    : 500 (ms)

Link-Profile:

   Initial-Rate             : 7000 (kbps)
   Max-Rate                 : 15000 (kbps)
   Peak-Lock                : Disabled

Session-Params:

   Tcp-Ramp-Up              : 2000 (ms)
   Udp-Ramp-Up              : 2000 (ms)
```

トリガーアクションとトラフィック最適化ポリシーの関連付け

トリガーアクションをトラフィック最適化ポリシーに関連付けるには、次のCLIコマンドを使用します。

```
configure
   require active-charging
   active-charging service service_name
      trigger-action trigger_action_name
        traffic-optimization policy policy_name
```

```
[ no ] traffic-optimization
end
```

注：

- **traffic-optimization policy**：トラフィック最適化ポリシーを設定します。
- **no**：設定されたトラフィック最適化ポリシーを削除します。

TCP と UDP の有効化

トラフィック最適化のために TCP および UDP プロトコルを有効にするには、次の CLI コマンドを使用します。

```
configure
  require active-charging
  active-charging service service_name
    trigger-condition trigger_condition_name
      [ no ] ip protocol = [ tcp | udp ]
      end
```

注：

- **no**：アクティブ課金サービスに関する設定を削除します。
- **ip**：IP 設定を確立します。
- **protocol**：IP パケットで転送されるプロトコルを示します。
- **tcp**：IP パケットで転送される TCP プロトコルを示します。
- **udp**：IP パケットで転送される UDP プロトコルを示します。



重要 このコマンドを設定した後で、設定を保存してからシャーシをリロードし、コマンドを有効にする必要があります。設定ファイルを保存してシャーシをリロードする方法については、使用している展開の『*System Administration Guide*』を参照してください。

マルチポリシーをサポートするためのサービススキーマの設定

サービススキームフレームワークは、APN、ルールベース、QCI、およびルールレベルでのトラフィック最適化を実現します。マルチポリシーサポート機能を搭載した21.6では、通信事業者がサービススキーマフレームワークでのトラフィック最適化を利用して、複数のポリシーを設定し、目的の場所に応じたトラフィック最適化を設定できます。

サービススキーマフレームワークは、コールセットアップ時間、ベアラー作成時間、またはフロー作成時間のいずれかでトリガーできるトリガー条件に基づいてアクションを関連付ける場合に役立ちます。

セッション セットアップ トリガー

ワイルドカード設定の **any-match = TRUE** は、このトリガーでサポートされている唯一の条件であり、サブスクライバのすべてのフローに適用できます。

セッショントリガーを設定するには、次の設定を使用します。

```
configure
    active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
         exit
      service-scheme service_scheme_name
         trigger sess-setup
            priority priority_value trigger-condition trigger_condition_name1
 trigger-action trigger_action_name
             exit
      subs-class sub_class_name
         apn = apn_name
         exit
      subscriber-base subscriber_base_name
        priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
         end
```

設定例

次に、セッション セットアップ トリガーの設定例を示します。

```
service-scheme SS1
     trigger sess-setup
       priority 1 trigger-condition sess-setup trigger-action sess-setup
     #exit
   trigger-condition sess-setup
     any-match = TRUE
   #exit
   trigger-action sess-setup
     traffic-optimization policy sess-setup
   #exit
```

ベアラー作成トリガー

QCIに関連するトリガー条件をこのトリガーに使用できるため、これは特定のベアラーのすべてのフローに適用されます。

次の設定を使用して、ベアラー作成トリガーを設定します。

```
configure
  active-charging service service_name
     service-scheme service_scheme_name
        trigger bearer-creation
          priority priority_value trigger-condition trigger_condition_name2
trigger-action trigger_action_name
```

```
    exit
  trigger-condition trigger_condition_name2
    qci = qci_value
    exit
  trigger-action bearer-creation
    traffic-optimization policy bearer-creation
    exit
```

設定例

次に、ベアラー作成トリガーの設定例を示します。

```
service-scheme SS1
      trigger bearer-creation
        priority 1 trigger-condition bearer-creation trigger-action bearer-creation
      #exit
    trigger-condition bearer-creation
      qci = 1 to 2
    #exit
    trigger-action bearer-creation
      traffic-optimization policy bearer-creation
    #exit
```

フロー作成トリガー

ここではルール名やQCIに関連するトリガー条件を使用できるため、このトリガーは特定のフローに関連しています。

次の設定を使用して、フロー作成トリガーを設定します。

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name
 trigger-action trigger_action_name
         exit
         trigger-condition trigger_condition_name
         ip-protocol = protocol_type
         rule-name = rule_name
            **Multi-line or All-lines**
         exit
```

設定例

デフォルトの Cisco Ultra Traffic Optimization ポリシーを使用したフロー作成トリガーの設定例を以下に示します。

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition TC5 trigger-action TA4
    #exit
    trigger-condition TC5
      ip protocol = tcp
      ip protocol = udp
      multi-line-or all-lines
    #exit
```

```
    trigger-action TA4
      traffic-optimization
    #exit
```

設定：*ecgi-change*

ecgi-change の設定例を以下に示します。

ACS 設定でのトリガー条件とトリガーアクション

```
configure
active-charging-service ACS
   trigger-action TA1
      traffic-optimization policy flow-create-ecgi-change
    #exit
    trigger-condition TC4
      local-policy-rule = ruledef-ecgi
    #exit
 end
```

サービススキーマ設定

```
configure
active-charging-service ACS
    service-scheme SS1
      trigger flow-create
        priority 2 trigger-condition TC4 trigger-action TA1
      #exit
    subs-class SC1
      any-match = TRUE
    #exit
    subscriber-base SB1
      priority 1 subs-class SC1 bind service-scheme SS1
    #exit
end
```

ローカルポリシー設定

```
local-policy-service LP
    ruledef anymatch
      condition priority 1 imsi match *
    #exit
    ruledef ecgi-1
     condition priority 1 ecgi mcc 111 mnc 444 eci match 1AE7F0A 1AE7F0B 1AE7F28 1AE7F29
 1AE7F46 1AE7F47 1AEAC00 1AEAC01 1AEAC02 1AEAC0A 1AEAC0B 1AEAC0C 1AEAC14 1AEAC15 1AEAC16
 1AEAC28 1AEAC29 1AEAC2A 1AEAC46 1AEAC47 1AEAC48 1AEAC50 1AEAC51 1AEAC52 1AEAC6E 1AEAC6F
 1AEAC70 1AEAC78 1AEAC79 1AEAC7A
    #exit
    ruledef ecgi-10
     condition priority 1 ecgi mcc 300 mnc 235 eci match 1F36C52 1F36C6E 1F36C6F 1F36C70
 1F36C78 1F36C79 1F36C7A
    #exit
    ruledef ecgi-2
     condition priority 1 ecgi mcc 111 mnc 444 eci match 1AEBE01 1AEBE02 1AEBE0B 1AEBE0C
 1AEBE15 1AEBE16 1AEBE29 1AEBE2A 1AEBE47 1AEBE48 1AEBF00 1AEBF01 1AEBF02 1AEBF0A 1AEBF0B
 1AEBF0C 1AEBF14 1AEBF15 1AEBF16 1AEBF1E 1AEBF1F 1AEBF20 1AEBF28 1AEBF29 1AEBF2A 1AEBF46

    #exit
    ruledef ecgi-3
     condition priority 1 ecgi mcc 111 mnc 444 eci match 1AEBF47 1AEBF48 1AEBF50 1AEBF51
 1AEBF52 1AEBF6E 1AEBF6F 1AEBF70 1AEBF78 1AEBF79 1AEBF7A 1AF0E00 1AF0E01 1AF0E02 1AF0E0A
 1AF0E0B 1AF0E0C 1AF0E14 1AF0E15 1AF0E16 1AF0E28 1AF0E29 1AF0E2A 1AF0E46
```

```
    #exit
    ruledef ecgi-4
     condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF0E47 1AF0E48 1AF4A0A 1AF4A0B
 1AF4A14 1AF4A15 1AF4A28 1AF4A29 1AF4A46 1AF4A47 1AF4D00 1AF4D01 1AF4D0A 1AF4D0B 1AF4D14
 1AF4D15 1AF4D28 1AF4D29 1AF4D46 1AF4D47 1AF4D50 1AF4D51 1AF4D6E 1AF4D6F
    #exit
    ruledef ecgi-5
     condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF4D78 1AF4D79 1AF7200 1AF7201
 1AF7202 1AF720A 1AF720B 1AF720C 1AF7214 1AF7215 1AF7216 1AF721E 1AF721F 1AF7444 1AF7228
 1AF7229 1AF722A 1AF7246 1AF7247 1AF7248 1AF7250 1AF7251 1AF7252 1AF726E
    #exit
    ruledef ecgi-6
     condition priority 1 ecgi mcc 111 mnc 444 eci match 1AF726F 1AF7270 1B04C00 1B04C01
 1B04C02 1B04C03 1B04C0A 1B04C0B 1B04C0C 1B04C0D 1B04C14 1B04C15 1B04C16 1B04C17 1B04C1E
 1B04C1F 1B04C20 1B04C21 1B04C28 1B04C29 1B04C2A 1B04C2B 1B04C46 1B04C47
    #exit
    ruledef ecgi-7
     condition priority 1 ecgi mcc 111 mnc 444 eci match 1B04C48 1B04C49 1B04C50 1B04C51
 1B04C52 1B04C53 1B04C6E 1B04C6F 1B04C70 1B04C71 1B04C78 1B04C79 1B04C7A 1B04C7B 1B05300
 1B05301 1B05302 1B0530A 1B0530B 1B0530C 1B05314 1B05315 1B05316 1B05328 1B05329
    #exit
    ruledef ecgi-8
     condition priority 1 ecgi mcc 111 mnc 444 eci match 1B0532A 1B05346 1B05347 1B05348
 1B32F00 1B32F01 1B32F02 1B32F0A 1B32F0B 1B32F0C 1B32F14 1B32F15 1B32F16 1B32F28 1B32F29
 1B32F2A 1B32F46 1B32F47 1B32F48 1B76400 1B76401 1B76402 1B7640A 1B7640B 1B7640C 1B76428

    #exit
    ruledef ecgi-9
     condition priority 1 ecgi mcc 111 mnc 444 eci match 1B76429 1B7642A 1B76446 1B76447
 1B76448 1F36C00 1F36C01 1F36C02 1F36C0A 1F36C0B 1F36C0C 1F36C14 1F36C15 1F36C16 1F36C1E
 1F36C1F 1F36C20 1F36C28 1F36C29 1F36C2A 1F36C46 1F36C47 1F36C48 1F36C50 1F36C51
    #exit
    actiondef activate_lp_action
      action priority 1 activate-lp-rule name ruledef-tai
    #exit
    actiondef activate_lp_action1
      action priority 3 event-triggers ecgi-change
    #exit
    actiondef ecgi_change
      action priority 1 activate-lp-rule name ruledef-ecgi
    #exit
    eventbase default
      rule priority 1 event new-call ruledef anymatch actiondef activate_lp_action1
continue
      rule priority 11 event new-call ruledef ecgi-1 actiondef ecgi_change continue
      rule priority 12 event new-call ruledef ecgi-2 actiondef ecgi_change continue
      rule priority 13 event new-call ruledef ecgi-3 actiondef ecgi_change continue
      rule priority 14 event new-call ruledef ecgi-4 actiondef ecgi_change continue
      rule priority 15 event new-call ruledef ecgi-5 actiondef ecgi_change continue
      rule priority 16 event new-call ruledef ecgi-6 actiondef ecgi_change continue
      rule priority 17 event new-call ruledef ecgi-7 actiondef ecgi_change continue
      rule priority 18 event new-call ruledef ecgi-8 actiondef ecgi_change continue
      rule priority 19 event new-call ruledef ecgi-9 actiondef ecgi_change continue
      rule priority 20 event new-call ruledef ecgi-10 actiondef ecgi_change continue
      rule priority 21 event ecgi-change ruledef ecgi-1 actiondef ecgi_change continue
      rule priority 22 event ecgi-change ruledef ecgi-2 actiondef ecgi_change continue
      rule priority 23 event ecgi-change ruledef ecgi-3 actiondef ecgi_change continue
      rule priority 24 event ecgi-change ruledef ecgi-4 actiondef ecgi_change continue
      rule priority 25 event ecgi-change ruledef ecgi-5 actiondef ecgi_change continue
      rule priority 26 event ecgi-change ruledef ecgi-6 actiondef ecgi_change continue
      rule priority 27 event ecgi-change ruledef ecgi-7 actiondef ecgi_change continue
      rule priority 28 event ecgi-change ruledef ecgi-8 actiondef ecgi_change continue
      rule priority 29 event ecgi-change ruledef ecgi-9 actiondef ecgi_change continue
      rule priority 30 event ecgi-change ruledef ecgi-10 actiondef ecgi_change continue
```

```
    #exit
  #exit
end
```

トラフィック最適化ポリシーの設定

```
configure
active-charging-service ACS
traffic-optimization-policy Config:
    traffic-optimization-policy flow-create-ecgi-change
      heavy-session threshold 400000
    #exit
end
```

ローカルポリシー設定



重要 ローカルポリシーを設定するには、ローカルポリシー意思決定エンジンのライセンスが必要です。特定のライセンス要件に関する詳細については、シスコのアカウント担当者にお問い合わせください。

ここでは、ロケーションに応じたトラフィック最適化ポリシーの設定について説明します。

次の設定例を使用して、eCGI 変更ルールを有効にします。

```
configure
   active-charging service service_name
      local-policy-service service_name
         ruledef ruledef_name
            condition priority priority_value ecgi mccmcc_value mnc mnc_value
eq eq_value
            exit
         actiondef actiondef_name1
            action priority priority_value event-triggers actiondef_name2
            exit
         actiondef actiondef_name2
            action priority priority_value activate-lp-ruleruledef_name
            exit
         eventbase eventbase_name
            rule priority priority_value event event_name ruledef ruledef_name
actiondef actiondef_name1continue
            rule priority priority_value event event_name ruledef ruledef_name
actiondef actiondef_name1continue
            exit
```

サービススキームの設定

```
configure
   active-charging service service_name
       service-scheme service_scheme_name
          trigger flow-create
             priority priority_value trigger-condition trigger_condition_name
 trigger-action trigger_action_name
```

```
    exit
trigger condition trigger_condition_name
    local-policy-rule = rule_name
    exit
trigger action trigger_action_name
    traffic-optimization policy policy_name
    exit
```

L7 ルールの設定



重要 L7 ルールを設定するには、アプリケーション検出制御ライセンスが必要です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

L7 ルールを設定するには、次の CLI を使用します。

```
configure
   active-charging service service_name
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name
 trigger-action trigger_action_name
         trigger-condition trigger_condition_name
            rule-name = rule_name
            rule-name = rule_name
               **Multi-line or All-lines**
         trigger-action trigger_action_name
            traffic-optimization policy policy_name
            exit
```

設定例

次に L7 ルールの設定例を示します。

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition TC6 trigger-action TA6
    #exit
    trigger-condition TC6
      rule-name = whatsapp
      rule-name = http
      multi-line-or all-lines
    #exit
    trigger-action TA6
      traffic-optimization policy flow-create-L7-Rules
    #exit
```

Ookla Speedtest

「L7 ルールの設定 （369 ページ）」で説明されている設定情報を使用してください。

設定例

次に、Ookla Speedtest の設定例を示します。

```
service-scheme SS1
     trigger flow-create
       priority 1 trigger-condition ookla trigger-action ookla
     #exit
   trigger-condition ookla
     rule-name = speedtest
   #exit
   trigger-action ookla
     no traffic-optimization
   #exit
```

ロケーションおよびアプリベースの設定

設定例

```
service-scheme SS1
   trigger flow-create
     priority 1 trigger-condition TC3 trigger-action TA2
   #exit
   trigger-condition TC3
     local-policy-rule = ruledef-ecgi
     rule-name = youtube
     rule-name = whatsapp
     multi-line-or all-lines
   #exit
   trigger-action TA2
     traffic-optimization policy flow-create-ecgi-change
   #exi
```

TCP と *UDP* の無効化による選択的設定

設定例

```
service-scheme SS1
    trigger flow-create
      priority 1 trigger-condition tcponly trigger-action tcponly
      priority 2 trigger-condition udponly trigger-action udponly
    #exit
    trigger-condition tcponly
      ip protocol = tcp
    #exit
    trigger-condition udponly
      ip protocol = udp
    #exit
    trigger-action tcponly
      no traffic-optimization
    #exit
    trigger-action udponly
      no traffic-optimization
    #exit
```

L7/ADC およびロケーショントリガーベースの設定

設定例

この設定例では、通信事業者が Speedtest のトラフィック最適化を常に無効にするシナリオについて説明します。この設定では、ロケーションに関係なくトラフィックの最適化が無効になります。特定のロケーション（ECGI）に対して特定のポリシーを適用し（Speedtest を除く）、任意のトリガー条件によって設定された他のポリシーをオーバーライドします。

また、特定のポリシー最適化（例：YouTube）では、ポリシーの選択に次のように優先順位が付けられます。

```
Service Scheme Configuration:
service-scheme SS1
trigger flow-create
  priority 1 trigger-condition speedtest-tc trigger-action speedtest-ta
  priority 2 trigger-condition location-tc trigger-action location-ta
  priority 3 trigger-condition youtube-tc trigger-action youtube-ta
  #exit
  trigger-condition location-tc
    local-policy-rule = ruledef-ecgi
  #exit
  trigger-action location-ta
    traffic-optimization policy flow-create-ecgi-change
  #exit
  trigger-condition speedtest-tc
    *rule-name = speedtest
  #exit
  trigger-action speedtest-ta
    no traffic-optimization
  #exit
  trigger-condition youtube-tc
    rule-name = youtube
  #exit
  trigger-action youtube-ta
    traffic-optimization policy youtube-policy
  #exit
* Provided rule-name = speedtest, is configured such that it always detects this traffic.
```

Cisco Ultra Traffic Optimization バルク統計の機能拡張

機能説明

この StarOS 21.23 リリースでは、次の show コマンドとバルク統計スキーマのカウンタが拡張され、Cisco Ultra Traffic Optimization ソリューションの UDP および TCP スプリットのアップリンクとダウンリンクの Rx および Tx パケット統計が表示されるようになりました。

- show active-charging traffic-optimization counters sessmgr all
- show active-charging traffic-optimization counters tcp sessmgr all
- show active-charging traffic-optimization counters udp sessmgr all

モニタリングおよびトラブルシューティング

コマンドと出力の表示

show active-charging traffic-optimization counters sessmgr all

次の show コマンドで、CUTO コントロールプレーンの統計を表示できます。

表 *36 : show active-charging traffic-optimization counters sessmgr all*

フィールド	説明
CUTO Control Plane Stats：	
Total Active Streams	アクティブなストリームの合計数を表示します。
Active TCP Streams	受信されたアクティブな TCP アップリンクおよびダウンリンクストリームの合計数を表示します。
Active UDP(QUIC) Streams	送信されたアクティブな UDP アップリンクおよびダウンリンクストリームの合計数を表示します。

次の show コマンドでも同様の出力を表示できます。

- **show active-charging traffic-optimization counters tcp sessmgr all**
- **show active-charging traffic-optimization counters udp sessmgr all**

show bulkstats variables ecs

次の ECS レベルの統計変数が Cisco Ultra Traffic Optimization 機能に追加されています。

表 *37 : ECS* スキーマのバルク統計変数

変数	説明	データ タイプ
cuto-tcp-uplink-rx	**説明**：Cisco Ultra Traffic Optimization のために UE から受信された TCP パケットの合計数を示します。 **タイプ**：カウンタ **トリガー**：Cisco Ultra Traffic Optimization のために UE から TCP パケットが受信されるたびに増分されます。 **可用性**：アクティブ課金サービスごと。	Int64

変数	説明	データ タイ
cuto-tcp-uplink-tx	**説明**：Cisco Ultra Traffic Optimization のために UE に送信された TCP パケットの合計数を示します。 **タイプ**：カウンタ **トリガー**：Cisco Ultra Traffic Optimization のために UE に TCP パケットが送信されるたびに増分されます。 **可用性**：アクティブ課金サービスごと。	Int64
cuto-tcp-dnlink-rx	**説明**：Cisco Ultra Traffic Optimization のためにインターネットから受信された TCP パケットの合計数を示します。 **タイプ**：カウンタ **トリガー**：Cisco Ultra Traffic Optimization のためにインターネットから TCP パケットが受信されるたびに増分されます。 **可用性**：アクティブ課金サービスごと。	Int64
cuto-tcp-dnlink-tx	**説明**：Cisco Ultra Traffic Optimization のためにインターネットに送信された TCP パケットの合計数を示します。 **タイプ**：カウンタ **トリガー**：Cisco Ultra Traffic Optimization のためにインターネットに TCP パケットが送信されるたびに増分されます。 **可用性**：アクティブ課金サービスごと。	Int64
cuto-udp-uplink-rx	**説明**：Cisco Ultra Traffic Optimization のために UE から受信された UDP パケットの合計数を示します。 **タイプ**：カウンタ **トリガー**：Cisco Ultra Traffic Optimization のために UE から UDP パケットが受信されるたびに増分されます。 **可用性**：アクティブ課金サービスごと。	Int64

変数	説明	データ タイプ
cuto-udp-uplink-tx	**説明**：Cisco Ultra Traffic Optimization のために UE に送信されたUDPパケットの合計数を示します。 **タイプ**：カウンタ **トリガー**：Cisco Ultra Traffic Optimization のために UE に UDP パケットが送信されるたびに増分されます。 **可用性**：アクティブ課金サービスごと。	Int64
cuto-udp-dnlink-rx	**説明**：Cisco Ultra Traffic Optimization のためにインターネットから受信された UDP パケットの合計数を示します。 **タイプ**：カウンタ **トリガー**：Cisco Ultra Traffic Optimization のためにインターネットから UDP パケットが受信されるたびに増分されます。 **可用性**：アクティブ課金サービスごと。	Int64
cuto-udp-dnlink-tx	**説明**：Cisco Ultra Traffic Optimization のためにインターネットに送信された UDP パケットの合計数を示します。 **タイプ**：カウンタ **トリガー**：Cisco Ultra Traffic Optimization のためにインターネットに UDP パケットが送信されるたびに増分されます。 **可用性**：アクティブ課金サービスごと。	Int64

バルク統計

次のバルク統計が ECS スキーマに追加されました。

ECS スキーマ

表 *38 : ECS* スキーマのバルク統計変数

変数	説明
cuto-tcp-uplink-rx	Cisco Ultra Traffic Optimization のために UE から受信された TCP パケットの合計数を示します。
cuto-tcp-uplink-tx	Cisco Ultra Traffic Optimization のために UE に送信された TCP パケットの合計数を示します。

変数	説明
cuto-tcp-dnlink-rx	Cisco Ultra Traffic Optimization のためにインターネットから受信された TCP パケットの合計数を示します。
cuto-tcp-dnlink-tx	Cisco Ultra Traffic Optimization のためにインターネットに送信された TCP パケットの合計数を示します。
cuto-udp-uplink-rx	Cisco Ultra Traffic Optimization のために UE から受信された UDP パケットの合計数を示します。
cuto-udp-uplink-tx	Cisco Ultra Traffic Optimization のために UE に送信された UDP パケットの合計数を示します。
cuto-udp-dnlink-rx	Cisco Ultra Traffic Optimization のためにインターネットから受信された UDP ダウンリンクパケットの合計数を示します。
cuto-dnlink-forward	Cisco Ultra Traffic Optimization ライブラリによって転送されたダウンリンク方向のデータパケットの合計数を示します。
cuto-dnlink-tx	Cisco Ultra Traffic Optimization ライブラリによって送信されたダウンリンクパケットの合計数を示します。
cuto-dnlink-rx	Cisco Ultra Traffic Optimization ライブラリによって受信されたダウンリンクパケットの合計数を示します。
cuto-dnlink-hold	Cisco Ultra Traffic Optimization ライブラリによって保持されたダウンリンク方向のデータパケットの合計数を示します。

Cisco Ultra Traffic Optimization の設定

ここでは、Cisco Ultra Traffic Optimization ソリューションのサポートを有効にする方法について説明します。

トラフィック最適化のロード

Cisco Ultra Traffic Optimization をソリューションとしてロードするには、グローバル コンフィギュレーション モードで次の設定コマンドを使用します。

```
configure
   require active-charging traffic-optimization
   end
```



重要　このコマンドを設定した後で、設定を保存してからシャーシをリロードし、コマンドを有効にする必要があります。設定ファイルを保存してシャーシをリロードする方法については、使用している展開の『*System Administration Guide*』を参照してください。



重要　トラフィックの最適化の有効化や無効化は、サービススキームフレームワークを介して行うことができます。



重要　**require active-charging traffic-optimization** CLI コマンドを設定した後は、シャーシをリロードしてコマンドを有効にする必要があります。設定ファイルを保存してシャーシをリロードする方法については、使用している展開の『*System Administration Guide*』を参照してください。



重要　21.3 および 21.5 以降のリリースでは、シャーシ再起動の依存関係が無効になりました。Cisco Ultra Traffic Optimization エンジンがデフォルトでロードされます。Cisco Ultra Traffic Optimization のコンフィギュレーション CLI は、ライセンスが有効になっている場合に使用できます。そのため、**traffic-optimization** キーワードは廃止されました。

Cisco Ultra Traffic Optimization 設定プロファイルの有効化

Cisco Ultra Traffic Optimization プロファイルを有効にするには、ACS コンフィギュレーションモードで次の設定コマンドを使用します。

```
configure
   active-charging service service_name
      traffic-optimization-profile
      end
```

注：

- 上記の CLI コマンドは、新しいコンフィギュレーション モードであるトラフィック最適化プロファイル設定を有効にします。

動作モードの設定

次の CLI コマンドを使用して、トラフィック最適化プロファイル コンフィギュレーション モードでの Cisco Ultra Traffic Optimization エンジンの動作モードを設定します。

```
configure
   active-charging service service_name
      traffic-optimization-profile
         mode [ active | passive ]
         end
```

注：

- **mode**：トラフィック最適化の動作モードを設定します。
- **active**：パケットに対してトラフィックの最適化とフローモニタリングの両方が実行されるアクティブモード。
- **passive**：フロー制御は実行されず、パケットのモニタリングが行われるパッシブモード。

サービス スキーム フレームワークを使用した Cisco Ultra Traffic Optimization 設定プロファイルの有効化

サービス スキーム フレームワークは、APN、ルールベース、QCI、およびルールレベルでのトラフィック最適化を可能にするために使用されます。サービス スキーム フレームワークには、主要な 2 つの構造があります。

- **サブスクライバベース**：これは、サブスクライバクラスの設定に基づいて、サブスクライバをサービススキームに関連付ける場合に役立ちます。
  - **subs-class**：subs-class で定義された条件により、ルールベース、APN、v-APN 名に基づいてサブスクライバを分類できます。条件は組み合わせて定義でき、それらの評価では OR 演算子と AND 演算子の両方がサポートされます。
- **サービススキーム**：これは、コールセットアップ時間、ベアラー作成時間、またはフロー作成時間のいずれかでトリガーできるトリガー条件に基づいてアクションを関連付ける場合に役立ちます。
  - **trigger-condition**：すべてのトリガーにおいて、trigger-action の適用は trigger-condition で定義された条件に基づきます。
  - **trigger-actions**：分類されたフローで実行されるアクションを定義します。これらのアクションには、トラフィック最適化、スロットル抑制などがあります。

セッション セットアップ トリガー

ワイルドカード設定の **any-match = TRUE** は、このトリガーでサポートされている唯一の条件であり、サブスクライバのすべてのフローに適用できます。

設定例を以下に示します。

```
configure
   active-charging service service_name
     service-scheme service_scheme_name
```

```
            trigger sess-setup
               priority priority_value trigger-condition trigger_condition_name1
 trigger-action trigger_action_name
               exit
            trigger-condition trigger_condition_name1
               any-match = TRUE
               exit
            trigger-action sess-setup
            traffic-optimization policy sess-setup
               exit
```

ベアラー作成トリガー

QCIに関連するトリガー条件をこのトリガーに使用できるため、これは特定のベアラーのすべてのフローに適用されます。

以下に設定例を示します。

```
configure
   active-charging service service_name
      trigger-action trigger_action_name
         traffic-optimization
         exit
      trigger-condition trigger_condition_name1
         any-match = TRUE
         exit
      trigger-condition trigger_condition_name2
         qci = qci_value
         exit
      service-scheme service_scheme_name
         trigger bearer-creation
            priority priority_value trigger-condition trigger_condition_name2
 trigger-action trigger_action_name
               exit
         exit
      subs-class sub_class_name
         apn = apn_name
         exit
      subscriber-base subscriber_base_name
        priority priority_value subs-class sub_class_name bind service-scheme
 service_scheme_name
         end
```

フロー作成トリガー

ここではルール名やQCIに関連するトリガー条件を使用できるため、このトリガーは特定のフローに関連しています。

以下に設定例を示します。

```
configure
   active-charging service service_name
```

```
trigger-action trigger_action_name
   traffic-optimization
   exit
trigger-condition trigger_condition_name1
   any-match = TRUE
   exit
trigger-condition trigger_condition_name2
   qci = qci_value
   exit
trigger-condition trigger_condition_name3
   rule-name = rule_name
   exit
service-scheme service_scheme_name
   trigger bearer-creation
      priority priority_value trigger-condition trigger_condition_name3
trigger-action trigger_action_name
       exit
   exit
subs-class sub_class_name
   apn = apn_name
   exit
subscriber-base subscriber_base_name
  priority priority_value subs-class sub_class_name bind service-scheme
service_scheme_name
   end
```

注：

- *trigger_condition_name3* には、ルールのみ、QCI のみ、ルールと QCI の両方、ルールと QCI のいずれかを含めることができます。

トラフィック最適化の各種レベル、および対応するサブスクライバクラスの設定とトリガーを次の表に示します。

トラフィック最適化レベル	サブスクライバクラスの設定とトリガー
すべてのコールまたはフローに適用可能	**subs-class** *sc1* **any-match = TRUE** **exit** セットアップのトリガー条件は、**any-match = TRUE** です。
ルールベースのすべてのコールまたはフローに適用可能	**subs-class** *sc1* **rulebase = prepaid** **exit** セットアップのトリガー条件は、**any-match = TRUE** です。

トラフィック最適化レベル	サブスクライバクラスの設定とトリガー
APN のすべてのコールまたはフローに適用可能	**subs-class** *sc1* **apn = cisco.com** **exit** セットアップのトリガー条件は、**any-match = TRUE** です。
ベアラーのすべてのフローに適用可能	**trigger-condition** *TC1* **qci = 1** **exit** ベアラー作成のトリガー条件は TC1 です。
特定のフローに適用可能	**trigger-condition** *TC1* **qci = 1** **rule-name = tcp** **multi-line-or all-lines** **exit** フロー作成のトリガー条件は TC1 です。



重要 LTE から eHRPD へのハンドオーバーの場合、QCI は eHRPD では無効であるため、サービススキームでトリガー条件としてルール名を設定することを推奨します。

TODR の生成

ACS コンフィギュレーションモードで次の CLI コマンドを使用して、トラフィック最適化データレコード（TODR）の生成を有効にします。

```
configure
   active-charging service service_name
      traffic-optimization-profile
         data-record
         end
```

注：

- 以前に設定されている場合は、**no data-record** コマンドを使用して TODR の生成を無効にします。

モニタリングおよびトラブルシューティング

ここでは、P-GW 上の Cisco Ultra Traffic Optimization ソリューションのモニタリングとトラブルシューティングに使用できるコマンドについて説明します。

Cisco Ultra Traffic Optimization Show コマンドと出力

このセクションでは、Cisco Ultra Traffic Optimization をサポートするために導入された show コマンドとフィールドについて説明します。

show active-charging traffic-optimization counters

show active-charging traffic-optimization counters sessmgr { all | instance *number* **}** CLI コマンドが導入されました。ここで、

- **counters** は、Cisco Ultra Traffic Optimization エンジンからの集約フローカウンタ/統計情報を表示します。



重要 このCLIコマンドはライセンスに依存し、ライセンスがロードされている場合にのみ表示されます。

新しいフィールドとカウンタを以下に示します。

- Traffic Optimization Flows:
  - Active Normal Flow Count
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count
  - Base Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Extended Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count
  - Total Normal Flow Count
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
  - Base Policy:
    - Total Large Flow Count

- Total Managed Large Flow Count
- Total Unmanaged Large Flow Count

- Extended Policy:
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count

- Total IO Bytes
- Total Large Flow Bytes
- Total Recovered Capacity Bytes
- Total Recovered Capacity ms

上記のコマンドを実行すると、マルチポリシーサポート機能に関する次のフィールドが表示されます。



重要 このCLIコマンドはライセンスに依存し、ライセンスがロードされている場合にのみ表示されます。

- TCP トラフィック最適化フロー：
  - Active Normal Flow Count
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count
  - Base Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count

  - Extended Policy:
    - Active Large Flow Count
    - Active Managed Large Flow Count
    - Active Unmanaged Large Flow Count

  - Total Normal Flow Count
  - Total Large Flow Count

- Total Managed Large Flow Count
- Total Unmanaged Large Flow Count
- Base Policy:
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
- Extended Policy:
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
- Total IO Bytes
- Total Large Flow Bytes
- Total Recovered Capacity Bytes
- Total Recovered Capacity ms

• UDP トラフィック最適化フロー：

- Active Normal Flow Count
- Active Large Flow Count
- Active Managed Large Flow Count
- Active Unmanaged Large Flow Count
- Base Policy:
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count
- Extended Policy:
  - Active Large Flow Count
  - Active Managed Large Flow Count
  - Active Unmanaged Large Flow Count

•
- Total Normal Flow Count
- Total Large Flow Count
- Total Managed Large Flow Count

- Total Unmanaged Large Flow Count
- Base Policy:
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
- Extended Policy:
  - Total Large Flow Count
  - Total Managed Large Flow Count
  - Total Unmanaged Large Flow Count
- Total IO Bytes:
- Total Large Flow Bytes
- Total Recovered Capacity Bytes
- Total Recovered Capacity ms

show active-charging traffic-optimization info

この show コマンドは、Exec モードで導入されています。引数の説明は、次のとおりです。

- **traffic-optimization**：すべてのトラフィック最適化オプションを表示します。
- **info**：Cisco Ultra Traffic Optimization エンジンの情報を表示します。

この CLI コマンドの出力には、バージョン、モード、および設定値が表示されます。

次に、新しいフィールド/カウンタを示します。

- Version:
- Mode:
- Configuration:
  - Data Records (TODR)
  - Statistics Options
  - EFD Flow Cleanup Interval
  - Statistics Interval

show active-charging traffic-optimization policy

上記のコマンドを実行すると、マルチポリシーサポート機能に関する次のフィールドが表示されます。

- Policy Name
- Policy-Id
- Bandwidth-Mgmt
  - Backoff-Profile
  - Min-Effective-Rate
  - Min-Flow-Control-Rate
- Extended-Bandwidth-Mgmt
  - Backoff-Profile
  - Min-Effective-Rate
  - Min-Flow-Control-Rate
- Curbing-Control
  - Time
  - Rate
  - Max-phases
  - Threshold-Rate
- Extended-Curbing-Control
  - Time
  - Rate
  - Max-phases
  - Threshold-Rate
- Heavy-Session
  - Threshold
  - Standard-Flow-Timeout
- Extended-Heavy-Session
  - Threshold
  - Standard-Flow-Timeout
- Link-Profile
  - Initial-Rate
  - Max-Rate
  - Peak-Lock

- Extended-Link-Profile
  - Initial-Rate
  - Max-Rate
  - Peak-Lock
- Session-Params
  - Tcp-Ramp-Up
  - Udp-Ramp-Up
- Extended-Session-Params
  - Tcp-Ramp-Up
  - Udp-Ramp-Up

バルク統計

大規模な管理対象フローをサポートするために、次のバルク統計が ECS スキーマに追加されました。

バルク統計	説明
tcp-active-base-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-base-large-flow カウントの数値を示します。
tcp-active-base-managed-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-base-managed-large-flow カウントの数値を示します。
tcp-active-base-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-base-unmanaged-large-flow カウントの数値を示します。
tcp-active-ext-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-ext-large-flow カウントの数値を示します。
tcp-active-ext-managed-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-ext-managed-large-flow カウントの数値を示します。
tcp-active-ext-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-ext-managed-large-flow カウントの数値を示します。

バルク統計	説明
tcp-total-base-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-base-large-flow カウントの数値を示します。
tcp-total-base-managed-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-base-managed-large-flow カウントの数値を示します。
tcp-total-base-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-base-unmanaged-large-flow カウントの数値を示します。
tcp-total-ext-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-ext-managed-large-flow カウントの数値を示します。
tcp-total-ext-managed-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-ext-managed-large-flow カウントの数値を示します。
tcp-total-ext-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-ext-unmanaged-large-flow カウントの数値を示します。
udp-active-base-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-base-large-flow カウントの数値を示します。
udp-active-base-managed-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-base-managed-large-flow カウントの数値を示します。
udp-active-base-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-base-unmanaged-large-flow カウントの数値を示します。
udp-active-ext-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-ext-large-flow カウントの数値を示します。
udp-active-ext-managed-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-ext-managed-large-flow カウントの数値を示します。

バルク統計	説明
udp-active-ext-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-ext-unmanaged-large-flow カウントの数値を示します。
udp-total-base-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-base-large-flow カウントの数値を示します。
udp-total-base-managed-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-base-managed-large-flow カウントの数値を示します。
udp-total-base-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-base-unmanaged-large-flow カウントの数値を示します。
udp-total-ext-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-ext-large-flow カウントの数値を示します。
udp-total-ext-managed-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-ext-managed-large-flow カウントの数値を示します。
udp-total-ext-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-ext-unmanaged-large-flow カウントの数値を示します。
tcp-active-normal-flow-count	Cisco Ultra Traffic Optimization の TCP active-normal-flow カウントの数値を示します。
tcp-active-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-large-flow カウントの数値を示します。
tcp-active-managed-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-managed-large-flow カウントの数値を示します。
tcp-active-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-unmanaged-large-flow カウントの数値を示します。
tcp-total-normal-flow-count	Cisco Ultra Traffic Optimization の TCP total-normal-flow カウントの数値を示します。
tcp-total-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-large-flow カウントの数値を示します。

バルク統計	説明
tcp-total-managed-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-managed-large-flow カウントの数値を示します。
tcp-total-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-unmanaged-large-flow カウントの数値を示します。
tcp-total-io-bytes	Cisco Ultra Traffic Optimization の TCP total-IO のバイト数を示します。
tcp-total-large-flow-bytes	Cisco Ultra Traffic Optimization の TCP total-large-flow のバイト数を示します。
tcp-total-recovered-capacity-bytes	Cisco Ultra Traffic Optimization の TCP total-recovered キャパシティのバイト数を示します。
tcp-total-recovered-capacity-ms	Cisco Ultra Traffic Optimization の TCP total-recovered キャパシティをミリ秒単位で示します。
udp-active-normal-flow-count	Cisco Ultra Traffic Optimization の UDP active-normal-flow カウントの数値を示します。
udp-active-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-large-flow カウントの数値を示します。
udp-active-managed-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-managed-large-flow カウントの数値を示します。
udp-active-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-unmanaged-large-flow カウントの数値を示します。
udp-total-normal-flow-count	Cisco Ultra Traffic Optimization の UDP total-normal-flow カウントの数値を示します。
udp-total-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-large-flow カウントの数値を示します。
udp-total-managed-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-managed-large-flow カウントの数値を示します。

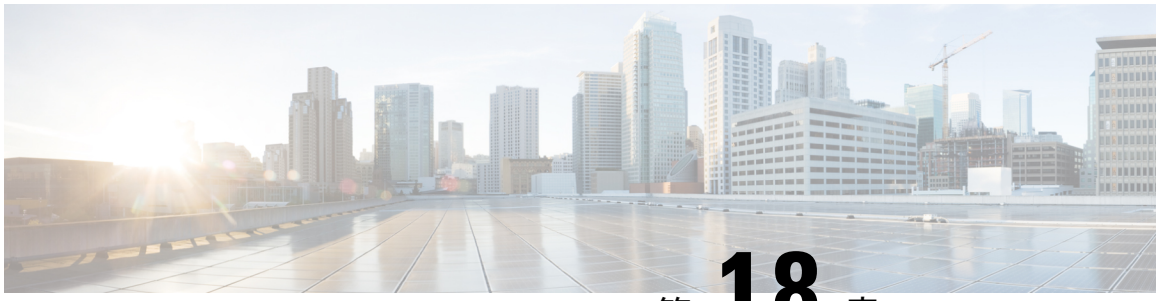
バルク統計	説明
udp-total-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-unmanaged-large-flow カウントの数値を示します。
udp-total-io-bytes	Cisco Ultra Traffic Optimization の UDP total-IO のバイト数を示します。
udp-total-large-flow-bytes	Cisco Ultra Traffic Optimization の UDP total-large-flow のバイト数を示します。
udp-total-recovered-capacity-bytes	Cisco Ultra Traffic Optimization の UDP total-recovered キャパシティのバイト数を示します。
udp-total-recovered-capacity-ms	Cisco Ultra Traffic Optimization の UDP total-recovered キャパシティをミリ秒単位で示します。
tcp-uplink-drop	Cisco Ultra Traffic Optimization の TCP uplink-drop の数を示します。
tcp-uplink-hold	Cisco Ultra Traffic Optimization の TCP uplink-hold の数を示します。
tcp-uplink-forward	Cisco Ultra Traffic Optimization の TCP uplink-forward の数を示します。
tcp-uplink-forward-and-hold	Cisco Ultra Traffic Optimization の TCP uplink-forward および hold の数を示します。
tcp-uplink-hold-failed	Cisco Ultra Traffic Optimization の TCP uplink-hold-failed の数を示します。
tcp-uplink-bw-limit-flow-sent	Cisco Ultra Traffic Optimization に関して送信された TCP uplink-bw limit-flow の数を示します。
tcp-dnlink-drop	Cisco Ultra Traffic Optimization の TCP downlink-drop の数を示します。
tcp-dnlink-hold	Cisco Ultra Traffic Optimization の TCP downlink-hold の数を示します。
tcp-dnlink-forward	Cisco Ultra Traffic Optimization の TCP downlink-forward の数を示します。
tcp-dnlink-forward-and-hold	Cisco Ultra Traffic Optimization の TCP downlink-forward および hold の数を示します。

バルク統計	説明
tcp-dnlink-hold-failed	Cisco Ultra Traffic Optimization の TCP downlink-hold-failed の数を示します。
tcp-dnlink-bw-limit-flow-sent	Cisco Ultra Traffic Optimization に関して送信された TCP downlink-bw limit-flow の数を示します。
tcp-dnlink-async-drop	Cisco Ultra Traffic Optimization の downlink-async-drop の数を示します。
tcp-dnlink-async-hold	Cisco Ultra Traffic Optimization の TCP downlink-async-hold の数を示します。
tcp-dnlink-async-forward	Cisco Ultra Traffic Optimization の TCP downlink-async-forward の数を示します。
tcp-dnlink-async-forward-and-hold	Cisco Ultra Traffic Optimization の TCP downlink-async-forward および hold の数を示します。
tcp-dnlink-async-hold-failed	Cisco Ultra Traffic Optimization の TCP downlink-async-hold-failed の数を示します。
tcp-process-packet-drop	Cisco Ultra Traffic Optimization の TCP process-packet-drop の数を示します。
tcp-process-packet-hold	Cisco Ultra Traffic Optimization の TCP process-packet-hold の数を示します。
tcp-process-packet-forward	Cisco Ultra Traffic Optimization の TCP process-packet-forward の数を示します。
tcp-process-packet-forward-failed	Cisco Ultra Traffic Optimization の TCP process-packet-forward-failed の数を示します。
tcp-process-packet-forward-and-hold	Cisco Ultra Traffic Optimization の TCP process-packet-forward および hold の数を示します。
tcp-process-packet-forward-and-hold-failed	Cisco Ultra Traffic Optimization の TCP process-packet-forward-failed および hold-failed の数を示します。
tcp-pkt-copy	Cisco Ultra Traffic Optimization の TCP packet-copy の数を示します。

バルク統計	説明
tcp-pkt-Copy-failed	Cisco Ultra Traffic Optimization の TCP packet-copy-failed の数を示します。
tcp-process-pkt-copy	Cisco Ultra Traffic Optimization の TCP process-packet-copy の数を示します。
tcp-process-pkt-copy-failed	Cisco Ultra Traffic Optimization の TCP process-packet-copy-failed の数を示します。
tcp-process-pkt-no-packet-found-action-forward	Cisco Ultra Traffic Optimization の TCP プロセスパケット、パケットが見つからない、アクション転送の数を示します。
tcp-process-pkt-no-packet-found-forward-and-hold	Cisco Ultra Traffic Optimization の TCP プロセスパケット、パケットが見つからない、アクション転送および保留の数を示します。
tcp-process-pkt-no-packet-found-action-drop	Cisco Ultra Traffic Optimization の TCP プロセスパケット、パケットが見つからない、アクションドロップの数を示します。
tcp-todrs-generated	Cisco Ultra Traffic Optimization の生成済み TCP TODR の数を示します。
udp-uplink-drop	Cisco Ultra Traffic Optimization の UDP uplink-drop の数を示します。
udp-uplink-hold	Cisco Ultra Traffic Optimization の UDP uplink-hold の数を示します。
udp-uplink-forward	Cisco Ultra Traffic Optimization の UDP uplink-forward の数を示します。
udp-uplink-forward-and-hold	Cisco Ultra Traffic Optimization の UDP uplink-forward および hold の数を示します。
udp-uplink-hold-failed	Cisco Ultra Traffic Optimization の失敗した UDP uplink-hold の数を示します。
udp-uplink-bw-limit-flow-sent	Cisco Ultra Traffic Optimization に関して送信された UDP uplink-bw limit-flow の数を示します。
udp-dnlink-drop	Cisco Ultra Traffic Optimization の UDP downlink-drop の数を示します。
udp-dnlink-hold	Cisco Ultra Traffic Optimization の UDP downlink-hold の数を示します。

バルク統計	説明
udp-dnlink-forward	Cisco Ultra Traffic Optimization の UDP downlink-forward の数を示します。
udp-dnlink-forward-and-hold	Cisco Ultra Traffic Optimization の UDP downlink-forward および hold の数を示します。
udp-dnlink-hold-failed	Cisco Ultra Traffic Optimization の失敗した UDP downlink-hold の数を示します。
udp-dnlink-bw-limit-flow-sent	Cisco Ultra Traffic Optimization に関して送信された UDP downlink-bw limit-flow の数を示します。
udp-dnlink-async-drop	Cisco Ultra Traffic Optimization の UDP downlink-async-drop の数を示します。
udp-dnlink-async-hold	Cisco Ultra Traffic Optimization の UDP downlink-async-hold の数を示します。
udp-dnlink-async-forward	Cisco Ultra Traffic Optimization の UDP downlink-async-forward の数を示します。
udp-dnlink-async-forward-and-hold	Cisco Ultra Traffic Optimization の UDP downlink-async-forward および hold の数を示します。
udp-dnlink-async-hold-failed	Cisco Ultra Traffic Optimization の失敗した UDP downlink-async-hold の数を示します。
udp-process-packet-drop	Cisco Ultra Traffic Optimization の UDP process-packet-drop の数を示します。
udp-process-packet-hold	Cisco Ultra Traffic Optimization の UDP process-packet-hold の数を示します。
udp-process-packet-forward	Cisco Ultra Traffic Optimization の UDP process-packet-forward の数を示します。
udp-process-packet-forward-failed	Cisco Ultra Traffic Optimization の失敗した UDP process-packet-forward の数を示します。
udp-process-packet-forward-and-hold	Cisco Ultra Traffic Optimization の UDP process-packet-forward および hold の数を示します。

バルク統計	説明
udp-process-packet-forward-and-hold-failed	Cisco Ultra Traffic Optimization の失敗した UDP process-packet-forward および hold の数を示します。
udp-pkt-copy	Cisco Ultra Traffic Optimization の UDP packet-copy の数を示します。
udp-pkt-Copy-failed	Cisco Ultra Traffic Optimization の UDP packet-copy-failed の数を示します。
udp-process-pkt-copy	Cisco Ultra Traffic Optimization の UDP process-packet-copy の数を示します。
udp-process-pkt-copy-failed	Cisco Ultra Traffic Optimization の失敗した UDP process-packet-copy の数を示します。
udp-process-pkt-no-packet-found-action-forward	Cisco Ultra Traffic Optimization の UDP プロセスパケット、パケットが見つからない、アクション転送の数を示します。
udp-process-pkt-no-packet-found-forward-and-hold	Cisco Ultra Traffic Optimization の UDP プロセスパケット、パケットが見つからない、アクション転送および保留の数を示します。
udp-process-pkt-no-packet-found-action-drop	Cisco Ultra Traffic Optimization の UDP プロセスパケット、パケットが見つからない、アクションドロップの数を示します。
udp-todrs-generated	Cisco Ultra Traffic Optimization の生成済み UDP TODR の数を示します。



第 18 章

複数の VNF への Cinder ボリュームのマルチアタッチの有効化

- 機能の概要と変更履歴 （395 ページ）
- 機能説明 （396 ページ）
- マルチアタッチ Cinder ボリュームの設定 （397 ページ）
- モニタリングおよびトラブルシューティング （398 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	• VPC-DI
機能のデフォルト	無効：有効にするには設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
P-GW および SAEGW では、Cinder ボリュームマルチアタッチ機能が次のように拡張されています。 • **monitor system volume** CLI コマンドを使用して、システム ボリューム ステータスをモニターします。 • マルチアタッチ cinder ボリューム機能のデタッチ中にスイッチオーバーの理由を変更します。 • SNMP トラップ通知を発生させます。	2024.02.0
最初の導入。	21.25

機能説明

Cinder は、VNF にボリュームを割り当てるための OpenStack ブロックストレージサービスです。ボリュームは、永続的なストレージを可能にするためにインスタンスにアタッチされるブロックストレージデバイスです。

OSP 16.0 より前の P-GW では、仮想顧客宅内機器（VCPE）と RedHat を使用するときに、運用上の問題が発生していました。VM の回復機能は QvPC-DI の VM 制御機能（CF）を停止させ、コンピューティングホストの障害により別のコンピューティングホスト上で復旧を試みます。新しい CF インスタンスが起動し、冗長ディスクアレイ（RAID1）が形成されると、アクティブな CF インスタンスは internet Small Computer System Interface（iSCSI）チャネルを介してディスクの同期を実行します。このプロセスはブロック単位で実行され、ディスク全体で反復されます。ディスクの同期は DI-LAN を介して行われます。ディスクサイズが 250GB を超えると、ストレージ構成、DI-LAN ネットワーク帯域幅、トラフィックによっては時間がかかります。

この問題を克服するために、OSP16.1 を使用して Cinder ボリュームのマルチアタッチをサポートします。この Cinder マルチアタッチ機能を使用すると、ボリュームを複数の VNF インスタンスに同時にアタッチできます。

- QvPC-DI の CF1（アクティブ）と CF2（スタンバイ）は、オーケストレータの起動時に同じマルチアタッチボリュームに接続します。
- StarOS は、CF1 と CF2 が iSCSI チャネルを介して同じディスクボリュームに接続されているかどうかを検出します。

- Cinderボリュームのマルチアタッチケースが検出されると、HD-RAIDはHDローカルディスクのみ（アクティブなCFに接続されたディスク）を使用して形成されます。このプロセスは、動作上の問題を解決するためにHD-RAIDミラーリングを回避します。

マルチアタッチでのディスク障害

マルチアタッチでのディスク障害の場合、両方のCFが同じボリュームを指しているため、CFをスイッチオーバーできません。Cinderボリュームマルチアタッチでディスク障害が検出されると、自動ICSRスイッチオーバーが開始されます。Cinderボリュームマルチアタッチのディスク障害シナリオを処理するために、シャーシ間セッションリカバリ（ICSR）設定が使用されます。

システム ボリューム ステータスのモニター

vPGWのアクティブなCFカードのマルチアタッチCinderボリュームに障害が発生した場合、サービス冗長性プロトコル（SRP）グローバル コンフィギュレーション モードのシステムボリュームモニター 機能によって、以下のことを実行できます。

- CLIコマンドを使用してボリュームのアタッチやデタッチ中のシステムボリュームをモニタリングする。
- マルチアタッチCinderボリュームがアクティブなCFカードから切断され、SRPスイッチオーバーが発生した場合に、スイッチオーバー理由を変更する。
- アクティブなVNFのスタンバイCFカードがボリュームのデタッチを検出したときに、SNMPトラップを通知する。

マルチアタッチ Cinder ボリュームの設定

システムがアクティブなCFからマルチアタッチCinderボリュームのステータスをモニターできるようにするには、次のCLIコマンドを使用します。

```
configure
  context context_name
    service-redundancy-protocol
    [ no ] monitor system volume
  end
```

注：

- **monitor system volume**：サービス冗長性プロトコル（SRP）を有効にしてボリュームをモニターします。
- **no**：ボリュームモニタリングを無効にします。

モニタリングおよびトラブルシューティング

この項では、show コマンドを使用してこの機能を監視およびトラブルシューティングする方法について説明します。

コマンドと出力の表示

ここでは、この機能の show コマンドとそれらの出力に関する情報を示します。

show hd raid verbose

このコマンドの出力に、次の新しいフィールドが追加されました。

- HD Raid
  - Degraded—No (Multiattach)

出力例を以下に示します。

```
HD RAID:
  State                : Available (clean)
  Degraded             : No(Multiattach)
  UUID                 : 643094ff:2cb03262:6e34e7e0:eddbca63
  Size                 : 214GB (214000000000 bytes)
  Action               : Idle
  Disk                 : hd-local1
  State                : In-sync component
  Created              : Tue Apr  9 09:00:17 2024
  Updated              : Wed Apr 24 02:21:18 2024
  Events               : 113252
  Model                : QEMU QEMU HARDDISK 2.5+
  Serial Number        : d6ae9d7e-12b1-4b62-93c3-1946ae882113
  Location             : CFC1 A7E5A7CF-561C-48A9-8784-F9580A3A7DAD
  Size                 : 214.7GB (214748364800 bytes)
  Disk                 : hd-remote1
  State                : Valid image of 643094ff:2cb03262:6e34e7e0:eddbca63
  Created              : Tue Apr  9 09:00:17 2024
  Updated              : Wed Apr 24 02:21:18 2024
  Events               : 113252
  Model                : QEMU QEMU HARDDISK 2.5+
  Serial Number        : d6ae9d7e-12b1-4b62-93c3-1946ae882113
  Location             : CFC2 59AE2254-E3C6-4E8C-8A94-03556C1B2EEB
  Size                 : 214.7GB (214748364800 bytes)
```

show srp monitor

show srp monitor コマンドが拡張され、マルチアタッチ シリンダ ボリュームの使用量モニターステータスが表示されるようになりました。

```
Auth. probe monitor state: Success
Auth. probe monitors up:   0
……
…….
VPP monitor state:          Success
SX monitor state:           Success
Volume monitor state:       Success
```

show srp monitor volume コマンドが拡張され、マルチアタッチ シリンダ ボリュームのステータスが表示されるようになりました。

```
[local]laas-setup# show srp monitor volume
+----- Type:  (A) - Auth. probe  (B) - BGP  (D) - Diameter  (F) - BFD  (E) - EGQC
|                     (C) - Card (V) - VPP  (S) - Sx  (M) - Multiattach Cinder Volume
|
|+---- State: (I) - Initializing (U) - Up   (D) - Down
||
||+--- GroupId
|||
vvv IP Addr         Port  Context(VRF Name)                      Last Update
-------------------------------------------------------------------------------
MI-   -                 -          -                 Tue Feb 06 06:04:50 2024
-------------------------------------------------------------------------------
```

show srp call-loss statistics

show srp call-loss statistics show コマンドは、アクティブ CF のボリュームデタッチに関するスイッチオーバーの理由を **Cinder Volume failure** と表示します。

```
[local]CXTMVPGWVNC-Primary-11# show srp call-loss statistics
Thursday December 21 16:23:28 UTC 2023
Switchover-4  started at : Thu Dec 21 16:20:44 2023,  took 1 seconds to finish.
    Switchover reason : Cinder Volume failure
```

（注） マルチアタッチボリュームがスタンバイ VNF からデタッチされると、次の 2 つの状況が発生する可能性があります。

- アクティブな VNF でマルチアタッチボリュームのデタッチが発生すると、サービスに影響が及ぶ可能性があります。両方の VNF にボリュームがアタッチされていないため、このサービスへの影響は、自動 SRP スイッチオーバーが制限されている場合でも発生します。
- 強制の有無にかかわらず、SRP スイッチオーバーコマンドを手動で実行すると、スイッチオーバーが発生する可能性があります。このようにサービスに影響が及ぶのは、ピア VNF にもマルチアタッチボリュームがアタッチされていないためです。

  そのため、ピアの HD RAID ステータスを速やかに修正することを推奨します。また、手動 SRP スイッチオーバーを実行する前に、ピアの HD RAID ステータスが適切であることを確認してください。

SNMP トラップ通知による SRP スイッチオーバー理由の確認

スタンバイ CF カードは次の SNMP トラップを生成します。

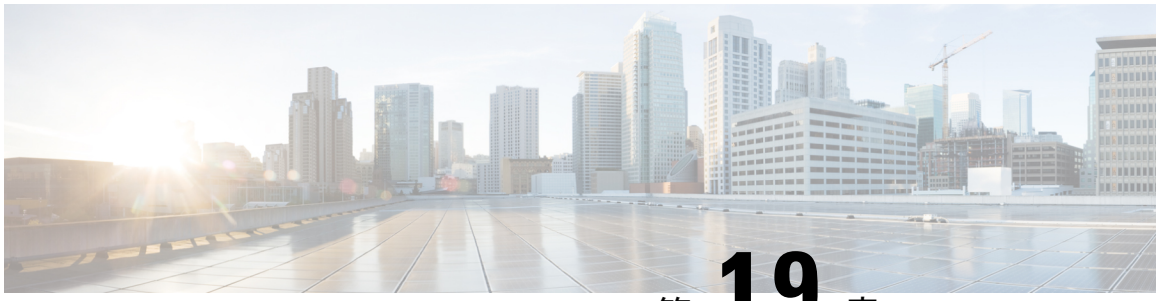
- **StorageNotFound**：ボリュームのデタッチ
- **StorageFound**：ボリュームのアタッチ

アクティブな CF カードからマルチアタッチボリュームがデタッチされたことが原因でスイッチオーバーが発生した場合、SRRPSwitchoverOccurred トラップは理由を **Cinder Volume Failure** と表示します。

```
Internal trap notification 1278
 (SRPSwitchoverOccured)  vpn SRP ipaddr 2002:4888:34:13:386:200:0:11 rtmod
 18 Switchover Reason: (18) Cinder Volume Failure
```



（注） Cinder ボリュームがアクティブカードに再接続されても、ソフトリロードが実行されない限り、システムで自動的に検出されません。



第 19 章

リリース状態へ移行することによるホールド IP のクリア

- 機能の概要と変更履歴 （401 ページ）
- 機能説明 （402 ページ）
- 単一の IP または IP の範囲で IPv4 アドレスの状態を保留から保留解除に変更する （404 ページ）
- 単一の IP または IP プレフィックスの範囲で IPv6 アドレスの状態を保留から保留解除に変更する （405 ページ）
- アドレスホールドタイマーの経過時間に基づく IPv4 状態のクリア （406 ページ）
- アドレスホールドタイマーの経過時間に基づく IPv6 状態のクリア （408 ページ）
- ポーリング間隔の設定 （410 ページ）
- コンテキストレベルでの事前および最終しきい値の設定 （410 ページ）
- IPv4 プールレベルでの事前および最終しきい値の設定 （413 ページ）
- IPv6 プールレベルでの事前および最終しきい値の設定 （414 ページ）
- デフォルトしきい値の設定 （415 ページ）
- デフォルトのポーリング間隔の設定 （416 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	• 無効：しきい値の設定が必要

	• EXEC モードのクリア CLI には適用されません。
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide* • *Command Line Interface Reference* • *Thresholding Configuration*

マニュアルの変更履歴

改訂の詳細	リリース
P-GW は、IPv4 プールと IPv6 プールの両方のアドレスホールドリストからの IP のクリアをサポートします。	2024.03.0

機能説明

P-GW では、IP アドレスを HOLD 状態から RELEASE 状態に移行する EXEC レベルコマンドのサポートが導入されました。

IPv4/IPv6 プールに含まれる膨大な数のアドレスが HOLD 状態になっている場合は、この CLI を使用してアドレスを HOLD から RELEASE に移行できます。

次の目的で、アドレスホールドタイマー（AHT）クリアの操作を実行できます。

- HOLD 状態にある IPv4 または IPv6 プール名に属する特定の IP または IP の範囲に関して、IPv4 または IPv6 の状態を HOLD から RELEASE に手動で変更します。
- 保留持続時間が指定された経過時間以上である IPv4 または IPv6 プールに指定された経過時間に基づいて、選択された最も古い IP の IPv4 または IPv6 の状態を HOLD から RELEASE に手動で変更します。

アドレスホールドタイマーのクリアに関するガイドライン、制限事項、および制約事項

ガイドライン

アドレスホールドタイマーをクリアするには、次のガイドラインに従ってください。

- アドレスホールドタイマーが IP プールに対して有効になっているかどうかを確認します。詳細については、「アドレスホールドタイマーのサポート」の章を参照してください。

- アップグレードの場合、 **ip-pool-usable** しきい値 CLI を有効にして再プロビジョニングする必要があります。

（注） デフォルトでは、コンテキストレベルとプールレベルの両方の CLI 設定で IP プールの使用可能なしきい値は無効になっています。

- ダウングレードの場合は、コンテキストレベルとプールレベルの両方の CLI 設定で **ip-pool-usable** しきい値を削除します。削除しない場合は、IP プールの設定が失敗します。

  削除を実行するには、必要なプールレベルの CLI パラメータを再設定するか、すでに保存されているダウングレードバージョンの構成ファイルをロードします。

- SNMP トラップのしきい値設定が、その場で適用されます。

制限事項

シャーシ間セッションリカバリ（ICSR）チェックポインティングは、**Clear HoldToRelease** CLI 設定ではサポートされていません。この制限による推奨事項は次のとおりです。

- 両方のシャーシで同時に **Clear HoldToRelease** CLI を実行します。
- すべてのクリア範囲、経過時間、および特定 IP の CLI は、ICSR ピアで同時に実行する必要があります。

  経過時間に基づくクリアは、1 つの ICSR セットアップでアクティブシャーシとスタンバイシャーシの両方で同時に実行する必要があります。アクティブシャーシとスタンバイシャーシ間でこのコマンドを実行する際の時間差により、ホールド IP とリリース IP に不一致が生じ、コマンドが後で実行されたシャーシでさらに多くのホールド IP がクリアされる可能性があります。したがって、「clear by range」コマンドを使用する方が、「clear by age」コマンドよりも優先されます。

（注） clear コマンドを実行しても、使用された IP アドレスが変更されることはありません。

制約事項

AHT のクリアに関する IP プールしきい値には、次の制限が適用されます。

- **ip-pool-usable** しきい値は、そのクリアしきい値より小さい値にする必要があります。
- **ip-pool-usable-final** しきい値は、そのクリアしきい値より小さい値にする必要があります。
- **ip-pool-usable-final** しきい値は ip-pool-usable しきい値よりも小さくする必要があります。

- **ip-pool-usable-final** クリアしきい値は、ip-pool-usable clear しきい値よりも小さくする必要があります。

単一の IP または IP の範囲で IPv4 アドレスの状態を保留から保留解除に変更する

IP プールに属する単一の IP または IP の範囲で、IPv4 IP の状態を HOLD から RELEASE に手動で変更できます。

始める前に

「リリース状態へ移行することによるホールド IP のクリア （401 ページ）」の「ガイドライン」、「制限事項」、および「制約事項」のセクションを確認します。

手順

ステップ 1 EXEC モードで特定のコンテキストを入力します。

context *context_name*

例：

```
 [local]qvpc-si#context egress
 [egress]qvpc-si# clear ip hold-to-releasestate { pool-name <ipv4-pool-name>}  { <ipv4_address >|
{ range <start_ip_address> <end_ip_address> count <1-5000>}}
```

ステップ 2 EXEC モードで次のコマンドを使用して、**clear ip hold-to-releasestate** パラメータを入力します。

clear ip hold-to-releasestate{ pool-name *ipv4_pool_name }{ ipv4_address* **| range** *start_ip_address end_ip_address* **count** *value* **} }**

- **clear ip hold-to-releasestate** パラメータは、アドレスを HOLD 状態から RELEASE 状態に移行します。
- IPv4 プール名は、言及された IP/範囲が AHT 保留リストから削除された場所を示します。サイズ 1 ～ 31 のプール名を設定でき、プール名では大文字と小文字が区別されます。
- AHT リストから IP アドレスが削除される開始 IP アドレス範囲を指定します。最大 5000 の 保留 IP のみがクリアされます。
- count パラメータは、HOLD 状態から RELEASE 状態に移行する IP の最大数を指定します。 クリアする IP アドレスの数を 1 ～ 5000 の整数で指定します。

例：

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ip hold-to-releasestate { pool-name <ipv4-pool-name>}  { <ipv4_address >|
{range <start_ip_address> <end_ip_address> count <1-5000>}}
 ---------------------------------------------------------------------
```

```
[egress]qvpc-si# clear ip hold-to-releasestate pool-name ?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA  ?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA 11.0.2.3
-------------------------------------------------------------------
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range 11.0.2.3?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range 11.0.2.3 11.0.2.20
 -------------------------------------------------------------------
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range 11.0.2.3 11.0.2.20 coun?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range 11.0.2.3 11.0.2.20 count ?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA range 11.0.2.3 11.0.2.20 count 60
<cr>                - newline
```

単一の IP または IP プレフィックスの範囲で IPv6 アドレスの状態を保留から保留解除に変更する

IPv6 プールに属する単一の IP プレフィックスまたは IP プレフィックスの範囲で、IPv6 IP の状態を HOLD から RELEASE に手動で変更できます。

始める前に

「リリース状態へ移行することによるホールド IP のクリア （401 ページ）」の「ガイドライン」、「制限事項」、および「制約事項」のセクションを確認します。

手順

ステップ 1 EXEC モードで特定のコンテキストを入力します。

context*context_name*

例：

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ipv6  hold-to-releasestate { pool-name <ipv6-pool-name>}  {{ prefix
<ipv6_address>} | {range <startIPv6prefix> <endIPv6prefix> count <1-5000>}}
```

ステップ 2 EXEC モードで次のコマンドを使用して、clear ipv6 hold-to-release パラメータを入力します。

clear ipv6 hold-to-releasestate{ pool-name *ipv6_pool_name* **} { { prefix** *ipv6_address* **} | { range** *startIPv6prefix endIPv6prefix* **count** *value* **} }**

- **clear ipv6 hold-to-releasestate** パラメータは、アドレスを HOLD 状態から RELEASE 状態に移行します。
- IPv6 pool name は、どの IP プールの指定された *IPv6* のプレフィックス範囲が、AHT ホールドリストからクリアされるかを示します。設定可能なプール名の文字数は 1 ～ 31 です。プール名では大文字と小文字が区別されます。

- AHT リストから IP アドレスをクリアする最初と最後の IPv6 プレフィックスを指定します。を参照してください。
- count パラメータは、HOLD 状態から RELEASE 状態に移行する IP の最大数を指定します。 クリアする IP アドレスの数を 1 ～ 5000 の整数で指定します。

単一 IP プレフィックスのクリアの設定出力例を示します。

例：

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ipv6  hold-to-releasestate { pool-name <ipv6-pool-name>}  {{ prefix
<ipv6_address>} | {range <startIPv6prefix> <endIPv6prefix> count <1-5000>}}
 ----------------------------------------
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA prefix 2068::323
  <cr>                 - newline
 ----------------------------------------------------------------------------------
```

範囲 IP プレフィックスのクリアの設定出力例を示します。

例：

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ipv6  hold-to-releasestate { pool-name <ipv6-pool-name>}  {{ prefix
<ipv6_address>} | {range <startIPv6prefix> <endIPv6prefix> count <1-5000>}}
 ----------------------------------------
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA range?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA range 3001::?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA range 3001::  3001:0:0:5:: ?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA range 3001::  3001:0:0:5:: count

[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA range 3001::  3001:0:0:5:: count
60
 <cr>                 - newline
 ----------------------------------------------------------------------------------
```

アドレスホールドタイマーの経過時間に基づく IPv4 状態のクリア

IP プールに指定されている経過時間に基づいて、選択された IP の IPv4 の状態を保留から保留解除に手動で変更できます。

手順

ステップ 1 EXEC モードで特定のコンテキストを入力します。

context *context_name*

例：

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ip hold-to-releasestate { pool-name <ipv4-pool-name>} {age <hold-age-in-seconds
> count <1-5000>}
```

ステップ 2 EXEC モードで次のコマンドを使用して、age パラメータを入力します。

clear ip hold-to-releasestate { pool-name *ipv4_pool_name }* **{ age** *hold-age-in-seconds* **count** *value* **}**

その他の情報：

- **hold-to-releasestate** パラメータは、アドレスを HOLD 状態から RELEASE 状態に移行します。
- IPv4 プール名は、どの IPv4 プールの指定された IP または範囲が AHT 保留リストからクリアされるかを示します。設定可能なプール名の文字数は 1 ～ 31 です。プール名は大文字と小文字が区別されます。
- hold-age は、60 ～ 31556926 の秒数で指定する必要があります。
- count パラメータは、HOLD 状態から RELEASE 状態に移行する IP の最大数を指定します。クリアする IP アドレスの数を 1 ～ 5000 の整数で指定します。

例：

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ip hold-to-releasestate { pool-name <ipv4-pool-name>} {age  <
hold-age-in-seconds > count <1-5000>}
  -----------------------------------------------------------
[egress]qvpc-si# clear ip hold-to-releasestate pool-name?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age 120
-----------------------------------------------------
[egress]qvpc-si# clear ip hold-to-releasestate pool-name?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA?
---------------------------------------
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age 300 ?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age 300 count ?
[egress]qvpc-si# clear ip hold-to-releasestate pool-name poolA age 300 count 60
<cr>                - newline
```

ステップ 3 **show ip pool address** show コマンドを使用して、IPv4 アドレスに設定された経過時間を確認します。

例：

```
[egress]qvpc-si# show ip pool address pool-name ipv4-public
+-------- (B) Busyout
|
|+------- (F)-FREE (U)-USED (H)-HOLD (Q)-QUARANTINE (R)-RELEASE
||+------ Quarantine
||| Address         NAI/MSID Hash   Hold/Qrntn Timer/ Session Start/Disconnect  Hold Age
||                                   Session ID
vv ==============  ================ ================      ========================= =========

Pool: ipv4-public
 U 10.0.0.12       9cd3cb187bcbd63c         1          Wed Jul 03 06:14:54 2024   -
 F 10.0.0.13       0000000000000000         -                           -          -
```

```
F 10.0.0.14       0000000000000000        -                          -          -
H 10.0.0.10       4a97ad2930ffc700 230               Wed Jul 03 06:18:19 2024   70
H 10.0.0.11       0c645044e6b388b9 249               Wed Jul 03 06:18:38 2024   51
```

アドレスホールドタイマーの経過時間に基づく IPv6 状態のクリア

IP プールに対して指定された経過時間に基づいて、選択した IP の IPv6 状態をホールドからリリースに手動で変更できます。CLI で特定の IP 情報をクリアし、経過時間を指定して、指定された値以上の保持期間を持つ IP を選択して、状態を HOLD から RELEASE に移行します。

手順

ステップ 1 EXEC モードで特定のコンテキストを入力します。

context *context_name*

例：

```
 [local]qvpc-si#context egress
 [egress]qvpc-si# clear ipv6 hold-to-releasestate { pool-name <ipv6-pool-name>} {age
<hold-age-in-seconds > count <1-5000>}
```

ステップ 2 EXEC モードで次のコマンドを使用して、経過時間パラメータを入力します。

clear ipv6 hold-to-releasestate { pool-name *ipv6_pool_name }* { **age** *hold-age-in-seconds* **count** *value***}**

その他の情報：

- **hold-to-releasestate** パラメータは、アドレスを HOLD 状態から RELEASE 状態に移行します。
- IPv6 pool name は、どの IP プールの指定された IPv6 のプレフィックス範囲が、AHT ホールドリストからクリアされるかを示します。設定可能なプール名の文字数は 1 ～ 31 です。プール名は大文字と小文字が区別されます。
- hold-age は秒単位で指定し、60 ～ 31556926 である必要があります。
- count パラメータは、HOLD 状態から RELEASE 状態に移行する IP の最大数を指定します。クリアする IP アドレスの数を 1 ～ 5000 の整数で指定します。

例：

```
[local]qvpc-si#context egress
[egress]qvpc-si# clear ipv6 hold-to-releasestate { pool-name <ipv6-pool-name>} {age
<hold-age-in-seconds > count <1-5000>}
----------------------------------------
```

```
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name ?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA age?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA age 90 ?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA age 90 count ?
[egress]qvpc-si# clear ipv6 hold-to-releasestate pool-name poolA age 64 count 60   <cr>
      - newline
```

ステップ 3 **show ipv6 pool pool-name** show コマンドを使用して、IPv6 アドレスの設定された経過時間を確認します。

例：

```
[egress]qvpc-si# show ipv6 pool pool-name ipv6-public
    Pool Name:     ipv6-public
    Group Name:
    Pool Type:     Public        Priority: 0
    Pool Id:       2001          Vrf: n/a
    Pool Status:   Good
    Start Prefix:  5001::/64
    End Prefix:    5001:0:0:4::/64
    Addr-Hold-Timer: 300
   Total Prefix:  5       Used Prefix: 1      Free Prefix: 1       On-Hold Prefix: 2       Released
 Prefix: 1
    Pool Address Type: Normal
    Configured Prefix: N/A
    User-Plane  ID   : N/A
    Virtual-FE  ID   : N/A
                 Nexthop Forwarding Address: Disabled
      Network Reachability Detection Server: Disabled
                  Suppress-Switchover-ADVS: Disabled
                   Allow-Static-Allocation: Disabled
                  Duplicate-Addr-Detection: Disabled
                         Send-Pilot-Packet: Enabled
                         Advertise-if-used: Disabled
                 Group Available Threshold: Disabled    Clear: Disabled
                       Pool-Free Threshold: Disabled    Clear: Disabled
                       Pool-Used Threshold: Disabled    Clear: Disabled
              cip-local-pool-used Threshold: Disabled    Clear: Disabled
       cip-local-pool-in-use-addr Threshold: Disabled    Clear: Disabled
                     Pool-Usable Threshold: Disabled    Clear: Disabled
               Pool-Usable-Final Threshold: Disabled    Clear: Disabled    age: Disabled

+-------- (B) Busyout
|
|+------- (F)-FREE (U)-USED (H)-HOLD (R)-RELEASE
||
|| Address                  NAI/MSID Hash    Hold Timer/           Session Start/Disconnect  Hold
Age
||                                            Session ID

vv ======================= ================ ================      ========================= =========

Pool Name: ipv6-public
 U 5001:0:0:1::/64          4a97ad2930ffc700 2                      Wed Jul 03 06:29:02 2024
-

 F 5001:0:0:4::/64          0000000000000000         -                          -
-

 R 5001::/64                c9600956165ae917         -              Wed Jul 03 05:13:02 2024
-
```

```
H 5001:0:0:2::/64          0c645044e6b388b9 276                    Wed Jul 03 06:30:16 2024  24

H 5001:0:0:3::/64          9cd3cb187bcbd63c 292                    Wed Jul 03 06:30:32 2024  8
```

ポーリング間隔の設定

このタスクを使用して、**ip-pool-usable** および **ip-pool-usable-final** しきい値のポーリング間隔を定義します。この設定は、事前しきい値設定と最終しきい値設定の両方に適用できます。

手順

グローバル コンフィギュレーション モードでポーリング間隔を設定します。

threshold poll { available-ip-pool-group | ip-pool-free | ip-pool-hold | ip-pool-release | ip-pool-used | **ip-pool-usable** } interval time

例：

```
[local]qvpc-si# configure
[local]qvpc-si# threshold poll { available-ip-pool-group | ip-pool-free | ip-pool-hold |
ip-pool-release | ip-pool-used | ip-pool-usable } interval <time>
```

コンテキストレベルでの事前および最終しきい値の設定

解放状態に移行して保留 IP をクリアする機能では、コンテキストレベルで 2 つのしきい値がサポートされています。

フリーまたは解放状態の IP で使用可能な IP プールの **ip-pool-usable** および **ip-pool-usable-final** しきい値を有効にするには、以下の作業を実行します。

設定されたしきい値に基づいて生成される事前および最終しきい値 SNMP アラームには次のタイプがあります。

- 条件に入った場合の PreThreshIPPoolUsable アラーム
- 条件をクリアした場合の PreThreshClearIPPoolUsable アラーム
- 条件に入った場合の FinalThreshIPPoolUsable アラーム
- 条件をクリアした場合の FinalThreshClearIPPoolUsable アラーム

始める前に

ip-pool-usable-final を設定するために、**ip-pool-usable** が設定済みであるかどうかを確認します。

プールレベルおよびコンテキストレベルで IP プールしきい値のモニタリングを有効にするには、『Thresholding Configuration Guide』の「IP プールしきい値」の章を参照してください。

手順

ステップ 1 IP プールの使用可能な事前しきい値状態をフリーまたは解放のいずれかに設定します。

例：

```
[local]qvpc-si# configure
[local]qvpc-si# threshold poll { available-ip-pool-group | ip-pool-free | ip-pool-hold |
ip-pool-release | ip-pool-used | ip-pool-usable } interval <time>
[local]qvpc-si#context egress
[egress]qvpc-si# threshold ip-pool-usable <low_thresh> [ clear <high_thresh> ] [ip-pool-usable-final
 <low_thresh> [ clear <high_thresh> ]]
[egress]qvpc-si# threshold ip-pool-usable 40 clear 50 ip-pool-usable-final 35 clear 36
```

PreThreshIPPoolUsable トラップは、利用可能な IP プールが、設定された **ip-pool-usable** の下限しきい値以下になると発生します。

PreThreshClearIPPoolUsable トラップは、プールの使用可能な値がクリア上限しきい値を超えるとトリガーされます。

ステップ 2 IP プールの使用可能な最終しきい値状態をフリーまたは解放のいずれかの状態に設定します。

threshold ip-pool-usable *low_thresh* [clear *high_thresh*] **[ip-pool-usable-final** *low_thresh* **[clear** *high_thresh* **]]]**

FinalThreshIPPoolUsable アラームは、測定されたプールの使用可能な値が ip-pool-usable-final 値以下の場合に発生します。**FinalThreshClearIPPoolUsable** トラップは、**ip-pool-usable-final** クリア値がクリアしきい値より大きい場合にクリアされます。

例：

```
[local]qvpc-si# configure
[local]qvpc-si# threshold poll { available-ip-pool-group | ip-pool-free | ip-pool-hold |
ip-pool-release | ip-pool-used | ip-pool-usable } interval <time>
[local]qvpc-si#context egress
[egress]qvpc-si# threshold ip-pool-usable <low_thresh> [ clear <high_thresh> ] [ip-pool-usable-final
 <low_thresh> [ clear <high_thresh> ]]
[egress]qvpc-si# threshold ip-pool-usable 40 clear 50 ip-pool-usable-final 35 clear 36
```

ステップ 3 **show threshold** CLI コマンドを使用して、**ip-pool-usable** および **ip-pool-usable-final** の設定値を確認します。

例：

```
 [egress]qvpc-si# show threshold

Threshold operation model: ALARM
```

```
No non-default threshold configured

Active thresholds:

Name:              ip-pool-used
Config Scope:      Context[egress]
Threshold:         0%
Clear Threshold:   0%
                         Poll Interval:    60Seconds
Next Poll Time:    2024-Mar-28+13:08:00

Name:              ip-pool-hold
Config Scope:      Context[egress]
Threshold:         0%
Clear Threshold:   0%
Poll Interval:     300Seconds
Next Poll Time:    2024-Mar-28+13:10:00

Name:              ip-pool-release
Config Scope:      Context[egress]
Threshold:         0%
Clear Threshold:   0%
Poll Interval:     300Seconds
Next Poll Time:    2024-Mar-28+13:10:00

Name:              ip-pool-free
Config Scope:      Context[egress]
Threshold:         0%
Clear Threshold:   0%
Poll Interval:     300Seconds
Next Poll Time:    2024-Mar-28+13:10:00

Name:              ip-pool-usable
Config Scope:      Context[egress]
Threshold:         0%
Clear Threshold:   0%
Poll Interval:     60Seconds
Next Poll Time:    2024-Mar-28+13:10:00

Name:              ip-pool-usable-final
Config Scope:      Context[egress]
Threshold:         0%
Clear Threshold:   0%
Poll Interval:     60Seconds
Next Poll Time:    2024-Mar-28+13:10:00


Name:              available-ip-pool-group
Config Scope:      Context[egress]
Threshold:         10%
Clear Threshold:   10%
Poll Interval:     300Seconds
Next Poll Time:    2024-Mar-28+13:10:00

Name:              cip-local-pool-used
Config Scope:      Context[egress]
Threshold:         0%
Clear Threshold:   0%
Poll Interval:     300Seconds
Next Poll Time:    2024-Mar-28+13:10:00

Name:              cip-local-pool-in-use-addr
Config Scope:      Context[egress]
```

```
Threshold:        0
Clear Threshold:  0
Poll Interval:    300Seconds
Next Poll Time:   2024-Mar-28+13:10:00


NOTE: IP pool threshold values can be overridden
      by IP pool configurations.

Enabled threshold groups: (name, scope)
available-ip-pool-group        Context[egress]

Non-default poll intervals:
ip-pool-used                              60Sec
place-holder                               0Sec
ip-pool-usable                            60Sec
```

IPv4 プールレベルでの事前および最終しきい値の設定

解放状態に移行して保留 IP をクリアする機能では、IPv4 プールレベルで 2 つのしきい値がサポートされています。

フリーまたは解放状態の IP で使用可能な IP プールの **pool-usable** および **pool-usable final** しきい値を有効にするには、以下の作業を実行します。

設定されたしきい値に基づいて生成される事前および最終しきい値 SNMP アラームには次のタイプがあります。

- 条件に入った場合の PreThreshIPPoolUsable アラーム
- 条件をクリアした場合の PreThreshClearIPPoolUsable アラーム
- 条件に入った場合の FinalThreshIPPoolUsable アラーム
- 条件をクリアした場合の FinalThreshClearIPPoolUsable アラーム

始める前に

pool-usable-final を設定するために、**pool-usable** が設定済みであるかどうかを確認します。

プールレベルおよびコンテキストレベルで IP プールしきい値のモニタリングを有効にするには、『*Thresholding Configuration Guide*』の「IP Pool Thresholds」の章を参照してください。

手順

ステップ 1 IP プールの使用可能な事前しきい値状態をフリーまたは解放のいずれかに設定します。

ip pool *name* **alert-threshold [pool-usable** *low_thresh* **[clear** *high_thresh* **]]**

例：

```
 [local]qvpc-si# context egress
 [egress]qvpc-si[egress]qvpc-si #ip pool name alert-threshold pool-usable < low_thresh > [ clear <
 high_thresh > ] [pool-usable-final < low_thresh > [ clear < high_thresh > ]]
[egress]qvpc-si# ip pool name alert-threshold pool-usable 50 clear 60 pool-usable-final 30 [clear
50
```

PreThreshIPPoolUsable トラップは、利用可能な IP プールが、設定された **ip-pool-usable** の下限しきい値以下になると発生します。

PreThreshClearIPPoolUsable トラップは、プールの使用可能な値がクリア上限しきい値を超えるとトリガーされます。

ステップ 2 IP プールの使用可能な最終しきい値状態をフリーまたは解放のいずれかに設定します。

ip pool name alert threshold [pool-usable low_thresh [clear high_thresh] **[pool-usable-final** *low_thresh* **[clear** *high_thresh* **]]]**

FinalThreshIPPoolUsable アラームは、測定されたプールの使用可能な値が **pool-usable** 値以下の場合に発生します。**FinalThreshClearIPPoolUsable** トラップは、**pool-usable-final** クリア値がクリアしきい値より大きい場合にクリアされます。

例：

```
 [local]qvpc-si# context egress
 [egress]qvpc-si[egress]qvpc-si #ip pool name alert-threshold pool-usable < low_thresh > [ clear <
 high_thresh > ] [pool-usable-final < low_thresh > [ clear < high_thresh > ]]
[egress]qvpc-si# ip pool name alert-threshold pool-usable 50 clear 60 pool-usable-final 30 [clear
50
```

IPv6 プールレベルでの事前および最終しきい値の設定

解放状態に移行して保留 IP をクリアする機能では、IPv6 プールレベルで 2 つのしきい値がサポートされています。

フリーまたは解放状態の IP で使用可能な IP プールの **pool-usable** および **pool-usable-final** しきい値を有効にするには、以下の作業を実行します。

設定されたしきい値に基づいて生成される事前および最終しきい値 SNMP アラームには次のタイプがあります。

- 条件に入った場合の PreThreshIPPoolUsable アラーム
- 条件をクリアした場合の PreThreshClearIPPoolUsable アラーム
- 条件に入った場合の FinalThreshIPPoolUsable アラーム
- 条件をクリアした場合の FinalThreshClearIPPoolUsable アラーム

始める前に

pool-usable-final を設定するために、**pool-usable** が設定済みであるかどうかを確認します。

プールレベルおよびコンテキストレベルで IP プールしきい値のモニタリングを有効にするには、『Thresholding Configuration Guide』の「IP Pool Thresholds」の章を参照してください。

手順

ステップ 1 IP プールの使用可能な事前しきい値状態をフリーまたは解放のいずれかに設定します。

ipv6 pool name alert-threshold [pool-usable *low_thresh* **[clear** *high_thresh* **]]**

例：

```
 [local]qvpc-si# context egress
[egress]qvpc-si# ipv6 pool testv6 alert-threshold pool-usable <low_thresh> [ clear <high_thresh> ]
 [ pool-usable-final <low_thresh> [ clear <high_thresh> ]]
[egress]qvpc-si#  ipv6 pool testv6 alert-threshold pool-usable 40 clear 50 pool-usable-final 35
clear 36
```

PreThreshIPPoolUsable トラップは、利用可能な IP プールが、設定された **pool-usable** の下限しきい値以下になると発生します。

PreThreshClearIPPoolUsable トラップは、プールの使用可能な値がクリア上限しきい値を超えるとトリガーされます。

ステップ 2 IP プールの使用可能な最終しきい値状態にフリーまたは解放のいずれかを入力します。

ipv6 pool *alert_name* **alert-threshold pool-usable** *low_thresh* [clear *high_thresh* **[pool-usable-final** *low_thresh* **[clear** *high_thresh* **]]**

例：

```
[local]qvpc-si# context egress
[egress]qvpc-si# ipv6 pool testv6 alert-threshold pool-usable <low_thresh> [ clear <high_thresh> ]
 [ pool-usable-final <low_thresh> [ clear <high_thresh> ]]
[egress]qvpc-si#  ipv6 pool testv6 alert-threshold pool-usable 40 clear 50 pool-usable-final 35
clear 36
```

FinalThreshIPPoolUsable アラームは、測定されたプールの使用可能な値が **pool-usable-final** の下限しきい値以下になると発生します。**FinalThreshClearIPPoolUsable** トラップは、**プールの使用可能な**値がクリア上限しきい値より大きい場合にクリアされます。

デフォルトしきい値の設定

コンテキストレベル **ip-pool-usable** および **ip-pool-usable-final** しきい値のデフォルト値を設定するには、次のタスクを使用します。

始める前に

手順

コンテキストレベルの **ip-pool-usable** および **ip-pool-usable-final threshold** のデフォルト値を設定するには、次のように設定します。

default threshold ip-pool-usable

例：

```
[egress]qvpc-si(config-ctx)# default threshold ip-pool-usable
[egress]qvpc-si(config-ctx)# default threshold ?
available-ip-pool-group cip-local-pool-in-use-addr cip-local-pool-used ip-pool-free ip-pool-hold
ip-pool-release ip-pool-used ip-pool-usable monitoring
```

デフォルトのポーリング間隔の設定

このタスクを使用して、**ip-pool-usable** および **ip-pool-usable-final** しきい値のデフォルトのポーリング間隔を設定します

手順

ステップ 1 **ip-pool-usable** および **ip-pool-usable-final** しきい値にデフォルトのポーリング間隔を設定します。

default threshold poll ip-pool-usable interval

例：

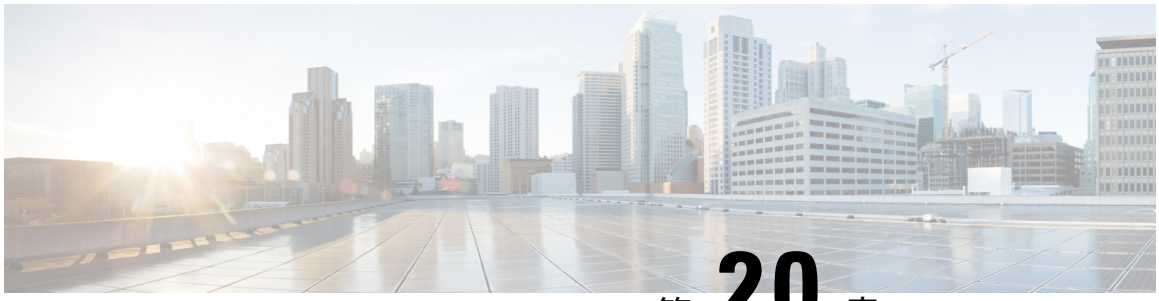
```
[egress]qvpc-si(config)# default threshold poll ?
ip-pool-free ip-pool-hold ip-pool-release ip-pool-used ip-pool-usable
[egress]qvpc-si(config)# default threshold poll ip-pool-usable ?
[egress]qvpc-si(config)# default threshold poll ip-pool-usable interval
```

ステップ 2 しきい値のデフォルト値を確認します。

例：

```
[local]qvpc-si# show threshold default | grep -i pool
(context)ip-pool-used 5Min Notify Above 0%
(context)ip-pool-hold 5Min Notify Above 0%
(context)ip-pool-release 5Min Notify Above 0%
(context)ip-pool-free 5Min Notify Below 0%
(context)ip-pool-usable 5Min Notify Below 0%
(context)ip-pool-usable-final 5Min Notify Below 0%
(context)available-ip-pool-group 5Min Notify Below 10%
```

```
(context)cip-local-pool-used 5Min Notify Above 0%
(context)cip-local-pool-in-use-addr 5Min Notify Above 0
(disc-rsn)Pool-IP-address-not-valid 15Min Notify Above 0
(disc-rsn)lpool-ip-validation-failed 15Min Notify Above 0
(disc-rsn)lpool-static-ip-addr-not-allowed 15Min Notify Above 0
(disc-rsn)mipha-ip-pool-busyout 15Min Notify Above 0
(disc-rsn)All-dynamic-pool-addr-occupied 15Min Notify Above 0
(disc-rsn)NAT-Pool-BusyOut-Or-Pend-Delete 15Min Notify Above 0
```



第 20 章

Elastic Services Controller のクラウド初期化サポート

- 機能の概要と変更履歴 （419 ページ）
- 機能説明 （419 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	StarOS
該当プラットフォーム	VPC-SI
機能のデフォルト	有効、常時オン
このリリースでの関連する変更点	Openstack 16 以降
関連資料	*ASR 5500 System Administration Guide*

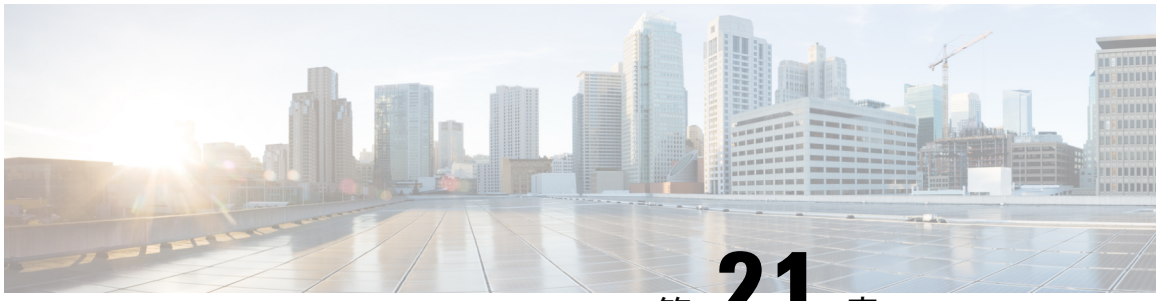
マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.27

機能説明

Elastic Services Controller（ESC）が QvPC-DI の制御機能（CF）にアクティブおよびスタンバイで Cinder マルチアタッチボリュームを使用する場合、仮想マシン（VM）オーケストレーション用に呼び出される Openstack API バージョンは 2.60 以上です。この API バージョンでは、ESC はセキュリティ上の理由から、構成ファイルをエンコードして VM に挿入します。VM は

エンコードされた構成ファイルを読み取ることができないため、ESC は **user_data** 圧縮ファイルを使用します。この **user_data** ファイルには、VM の起動に必要な構成ファイルが含まれています。



第 21 章

CoA、RADIUS DM、セッションのリダイレクト（ホットライン）

この章では、システムでの認可変更（CoA）、接続解除メッセージ（DM）、およびセッションリダイレクト（ホットライン）のサポートについて説明します。これらの機能を実装するために使用されるRADIUS属性、アクセス制御リスト（ACL）、フィルタ処理について取り上げます。製品アドミニストレーションガイドには、システム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、本アドミニストレーションガイドの説明に従って、ご使用のサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

重要 すべての機能、コマンド、キーワード/変数が、すべてのネットワーク機能やサービスで使用可能またはサポートされているわけではありません。これは、プラットフォームのタイプとインストールされているライセンスによって異なります。

- RADIUS の認可変更メッセージと切断メッセージ （421 ページ）
- セッションのリダイレクト（ホットライン） （427 ページ）

RADIUS の認可変更メッセージと切断メッセージ

このセクションでは、システムにCoAおよびDMRADIUSメッセージを導入する方法と、CoAおよびDMメッセージを使用して応答するようにシステムを設定する方法について説明します。

CoA の概要

システムは、AAA サーバーからの CoA メッセージをサポートして、サブスクライバセッションに関連付けられているデータフィルタを変更します。AAA サーバーからの CoA 要求メッセージには、NAS とサブスクライバセッションを識別する属性と、サブスクライバセッションに適用するデータフィルタのデータフィルタ ID が含まれている必要があります。filter-id 属性（属性 ID 11）には、アクセス制御リスト（ACL）の名前が含まれます。ACL の設定の詳細に

ついては、『*System Administration Guide*』の「*IP Access Control Lists*」の章を参照してください。

システムでCoA要求が正常に実行されると、CoA-ACKメッセージがRADIUSサーバーに返送され、データフィルタがサブスクライバセッションに適用されます。それ以外の場合は、サブスクライバセッションに変更を加えずに、error-cause属性付きのCoA-NAKメッセージが送信されます。



重要 単一のCoAでACLとルールベースを同時に変更することはサポートされていません。この場合、要求ごとに1つの属性変更を要求するAAAサーバーを介して2つの個別のCoA要求を送信できます。

DM の概要

DMメッセージは、RADIUSサーバーからのサブスクライバセッションをシステム内で切断するために使用されます。DM要求メッセージには、サブスクライバセッションを識別するために必要な属性が含まれている必要があります。システムがサブスクライバセッションを正常に切断すると、DM-ACKメッセージがRADIUSサーバーに返送されます。切断に失敗した場合は、適切なエラー理由とともにDM-NAKメッセージが送信されます。

ライセンス要件

RADIUS認可変更（CoA）と接続解除メッセージ（DM）は、ライセンスが必要なシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

CoA および DM の有効化

RADIUSの認可変更メッセージと切断メッセージを有効にするには、次の手順を実行します。

手順

ステップ 1 CoA および DM の有効化 （423 ページ） の説明に従って、システムがRADIUSサーバーからのCoAメッセージとDMメッセージを受信して応答できるようにします。

ステップ 2 EXECモードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

ステップ 3 CoA および DM 統計の表示 （425 ページ） の説明に従って、CoAメッセージおよびDMメッセージの統計を表示します。

重要
この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンド、および/またはキーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。すべてのコマンド、キーワード、変数を使用できるわけではありません。これは、プラットフォームのタイプとインストールされているライセンスによって異なります。

CoA および DM の有効化

次の例に示すコマンドを使用して、システムがRADIUSサーバーからのCoAメッセージとDMメッセージを受信して応答できるようにします。

```
configure
   context <context_name>
      radius change-authorize-nas-ip <ipv4/ipv6_address>
      end
```

注：

- <*context_name*> は、CoA と DM を有効にする AAA コンテキストの名前です。

  詳細については、『*AAA Interface Administration and Reference*』[英語] を参照してください。

- **radius change-authorize-nas-ip** コマンドでは、オプションのキーワードと変数をいくつか使用できます。このコマンドに関する詳細については、『*Command Line Interface Reference*』を参照してください。

CoA と DM の属性

CoAおよびDMメッセージを受け入れて対応するには、対象のシステムとサブスクライバセッションを正しく識別する必要があります。

システムを識別するには、次の属性のいずれかを使用します。

- NAS-IP-Address：CoA/DM 要求に NAS IP アドレスが存在する場合は、NAS IP アドレスと一致する必要があります。
- NAS-Identifier：この属性が存在する場合、属性値がサブスクライバセッションで生成された nas-identifier と一致する必要があります。

サブスクライバセッションを識別するには、次の属性のいずれかを使用します。

- 3GPP2 サービスが設定されている場合、相関識別子に次の属性が使用されます。
  - 3GPP2-Correlation-ID：この値は、サブスクライバセッションの 3GPP2-correlation-id と完全に一致する必要があります。これは、サブスクライバセッション識別で推奨される方法の 1 つです。

- 3GPP サービスが設定されている場合、次の属性が各種識別子に使用されます。
  - 3GPP-IMSI：International Mobile Subscriber Identification（IMSI）番号を検証し、特定の PDP コンテキストで指定された IMSI と一致する必要があります。
  - 3GPP-NSAPI：Network Service Access Point Identifier（NSAPI）は、特定の PDP コンテキストで指定された NSAPI と一致する必要があります。
- User-Name：この値は、セッションのサブスクライバ名と完全に一致する必要があります。これは、サブスクライバセッション識別で推奨される方法の 1 つです。
- Framed-IP-Address：この値は、セッションのフレーム IP アドレスと完全に一致する必要があります。
- Calling-station-id：この値はモバイルステーション ID と一致する必要があります。

サブスクライバセッションに適用する ACL を指定するには、次の属性を使用します。

- Filter-ID：CoA のみ。これは、既存のアクセス制御リストの名前にする必要があります。CoA 要求に Filter-ID が存在する場合、指定された ACL は指定されたサブスクライバセッションにすぐに適用されます。コンテキスト コンフィギュレーション モードのコマンド **radius attribute filter-id direction** は、フィルタを適用する方向を制御します。

次の属性もサポートされています。

- Event-Timestamp：この属性は、ログに記録されているイベントが発生したときのタイムスタンプです。
- 3GPP2 サービスが設定されている場合、次の追加属性がサポートされます。
  - 3GPP2-Disconnect-Reason：この属性は、ユーザーの接続を切断する理由を示します。この属性は、ホーム RADIUS サーバーから PDSN への RADIUS 接続解除要求メッセージ内に存在する場合があります。
  - 3GPP2-Session-Termination-Capability：radius change-authorize-nas-ip コマンドを発行して CoA および DM を有効にすると、この属性はホーム RADIUS サーバーへの RADIUS Access-Request メッセージに含まれます。この値が 3 の場合は、システムが RADIUS による動的な許可とモバイル IPv4 の登録失効の両方をサポートしていることを示します。この属性は RADIUS Access-Accept メッセージにも含まれており、ホームネットワークによって優先されるリソース管理メカニズムを搭載します。これはセッションで使用され、値は 1 ～ 3 になります。

CoA および DM Error-Cause 属性

Error-Cause 属性は、システムに要求の結果を伝えるために使用されます。RADIUS サーバーに返送される CoA、DM NAK、ACK メッセージ内にこの属性が存在します。

エラー原因の値クラスは次のとおりです。

- 0 ～ 199、300 ～ 399 を予約済み

- 200-299：正常終了
- 400 ～ 499：RADIUS サーバーのエラー
- 500-599：NAS/プロキシのエラー

CoA 要求または DM 要求が正常に完了すると、次のエラー原因が ACK メッセージで送信されます。

- 201：削除された残留セッションコンテキスト

CoA 要求または DM 要求が失敗した場合、次のエラー原因が NAK メッセージで送信されます。

- 401：Uサポートされていない属性
- 402：属性が見つからない
- 403：NAS 識別情報のミスマッチ
- 404：無効な要求
- 405：サポートされていないサービス
- 406：サポートされていない拡張子
- 501：管理上の禁止
- 503：セッションコンテキストが検出されない
- 504：セッションコンテキストが削除できない
- 506：リソースが使用不可能

CoA および DM 統計の表示

次のコマンドを入力して、CoA および DM メッセージの統計を表示します。

show session subsystem facility aaamgr

次に、このコマンドの出力例を示します。

```
1 AAA Managers
807 Total aaa requests                                    0 Current aaa requests
379 Total aaa auth requests                               0 Current aaa auth requests
    0 Total aaa auth probes                               0 Current aaa auth probes
    0 Total aaa auth keepalive                          0 Current aaa auth keepalive
426 Total aaa acct requests                               0 Current aaa acct requests
    0 Total aaa acct keepalive                          0 Current aaa acct keepalive
379 Total aaa auth success                                0 Total aaa auth failure
    0 Total aaa auth purged                               0 Total aaa auth cancelled
    0 Total auth keepalive success                    0 Total auth keepalive failure

    0 Total auth keepalive purged
    0 Total aaa auth DMU challenged
367 Total radius auth requests                        0 Current radius auth requests

    2 Total radius auth requests retried
```

```
    0 Total radius auth responses dropped
    0 Total local auth requests                          0 Current local auth requests

   12 Total pseudo auth requests                         0 Current pseudo auth requests

    0 Total null-username auth requests (rejected)
    0 Total aaa acct completed                            0 Total aaa acct purged
    0 Total acct keepalive success                       0 Total acct keepalive timeout

    0 Total acct keepalive purged
    0 Total aaa acct cancelled
  426 Total radius acct requests                         0 Current radius acct requests

    0 Total radius acct requests retried
    0 Total radius acct responses dropped
    0 Total gtpp acct requests                           0 Current gtpp acct requests

    0 Total gtpp acct cancelled                           0 Total gtpp acct purged
    0 Total null acct requests                           0 Current null acct requests

   54 Total aaa acct sessions                             5 Current aaa acct sessions
    3 Total aaa acct archived                             0 Current aaa acct archived
    0 Current recovery archives                           0 Current valid recovery
records
    2 Total aaa sockets opened                            2 Current aaa sockets open
    0 Total aaa requests pend socket open
    0 Current aaa requests pend socket open
    0 Total radius requests pend server max-outstanding
    0 Current radius requests pend server max-outstanding
    0 Total aaa radius coa requests                      0 Total aaa radius dm requests

    0 Total aaa radius coa acks                           0 Total aaa radius dm acks
    0 Total aaa radius coa naks                           0 Total aaa radius dm naks
    2 Total radius charg auth                             0 Current radius charg auth
    0 Total radius charg auth succ                        0 Total radius charg auth
fail
    0 Total radius charg auth purg                        0 Total radius charg auth
cancel
    0 Total radius charg acct                             0 Current radius charg acct
    0 Total radius charg acct succ                        0 Total radius charg acct
purg
    0 Total radius charg acct cancel
  357 Total gtpp charg                                    0 Current gtpp charg
  357 Total gtpp charg success                            0 Total gtpp charg failure
    0 Total gtpp charg cancel                             0 Total gtpp charg purg
    0 Total prepaid online requests                       0 Current prepaid online
requests
    0 Total prepaid online success                        0 Current prepaid online
failure
    0 Total prepaid online retried                        0 Total prepaid online
cancelled
    0 Current prepaid online purged
    0 Total aaamgr purged requests
    0 SGSN: Total db records
    0 SGSN: Total sub db records
    0 SGSN: Total mm records
    0 SGSN: Total pdp records
    0 SGSN: Total auth records
```

セッションのリダイレクト（ホットライン）

重要 このセグメントでこの機能に関して説明されている機能性は、HNB-GW セッションには適用されません。

概要

セッションリダイレクトは、既存または新しいサブスクライバセッションのトラフィックにACLルールを適用することにより、サブスクライバのトラフィックを外部サーバーにリダイレクトする手段を提供します。サブスクライバからのTCP/IPまたはUDP/IPパケットの宛先アドレスと宛先ポート（オプション）が書き換えられ、パケットが指定のリダイレクトアドレスに転送されます。サブスクライバに戻るトラフィックでは、送信元アドレスとポートが元の値に書き換えられます。リダイレクト ACL は、RADIUS 認可変更（CoA）機能によって動的に適用できます。

セッションのリダイレクト機能は、サブスクライバのごくわずかなサブセットを常にリダイレクトすることを目的としていることに注意してください。セッションマネージャでの大きなメモリオーバーヘッドを避けるために、この機能に割り当てられるデータ構造は最小限に抑えられます。

ライセンス要件

セッションのリダイレクション（ホットライン）は、ライセンス供与されたシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

動作

ACL ルール

「**readdress server**」という名前の ACL ルールは、サブスクライバセッションのリダイレクトをサポートしています。このルールを含む ACL は、ユーザーの接続先コンテキストで設定する必要があります。TCP および UDP プロトコルパケットのみがサポートされています。ACL ルールでは、リダイレクトされるアドレスとオプションのポートを指定できます。送信元および宛先のアドレスとポート（サブスクライバから発信されるトラフィックに関する）には、ワイルドカードを使用できます。リダイレクトされるポートが指定されていない場合、トラフィックは、データグラム内の元の宛先ポートと同じポートにリダイレクトされます。ACLの設定の詳細については、『*System Administration Guide*』の「*IP Access Control Lists*」の章を参照してく

ださい。**readdress server** の詳細については、『*Command Line Interface Reference*』の「*ACL Configuration Mode Commands*」の章を参照してください。

サブスクライバセッションのリダイレクト

readdress server ルールを含む ACL は、RADIUS サーバーからの CoA メッセージを介して既存の加入者セッションに適用されます。CoA メッセージには、サブスクライバセッションを識別する 3GPP2-Correlation-ID、User-Name、Acct-Session-ID、または Framed-IP-Address 属性が含まれています。CoA メッセージには、**readdress server** ルールを含む ACL の名前を指定する Filter-Id 属性も含まれます。これにより、既存のサブスクライバセッションに ACL を動的に適用できます。デフォルトでは、CoA メッセージ内の Filter-Id にプレフィックス **in:** または **out:** が含まれていない限り、ACL は一致するサブスクライバの入力フィルタと出力フィルタの両方として適用されます。

CoA メッセージについて、およびシステムでの CoA メッセージの実装方法については、RADIUS の認可変更メッセージと切断メッセージ （421 ページ）を参照してください。



重要 単一の CoA で ACL とルールベースを同時に変更することはサポートされていません。この場合、要求ごとに 1 つの属性変更を要求する AAA サーバーを介して 2 つの個別の CoA 要求を送信できます。

リダイレクトでのセッション制限

セッションマネージャが消費するメモリ量を制限するために、セッションマネージャごとに 2000 のリダイレクト対象セッションエントリ数の制限が割り当てられます。この制限は、現在リダイレクトされている一連のサブスクライバで均等に共有されます。使用可能なセッションエントリ数が不足して、リダイレクトされたセッションエントリがサブスクライバで無効になる場合、常に使用された日付が最も古いエントリが無効になります。

リダイレクトの停止

サブスクライバのリダイレクトされたセッションエントリは、RADIUS サーバーから発行された CoA メッセージで再アドレス付けサーバーの ACL ルールを含まないフィルタが指定されるまで、アクティブ状態が維持されます。これが発生すると、サブスクライバのリダイレクトされたセッションエントリは削除されます。

リダイレクトされたすべてのセッションエントリは、サブスクライバがセッションを切断した場合も削除されます。

IP フラグメントの処理

TCP/UDP ポート番号はリダイレクトメカニズムの一部であるため、フラグメント化された IP データグラムは、リダイレクトされる前にリアセンブルする必要があります。フラグメントが正しくない順序で送信される場合、特にリアセンブリが必要です。セッションマネージャがデータグラムのリアセンブルを実行します。リアセンブルが試行されるのは、データグラムがリダイレクトサーバーの ACL ルールに一致する場合に限られます。メモリ使用量を制限する

ため、1つのサブスクライバに対して同時にリアセンブルできるデータグラムは、最大10個までです。追加の要求が発生すると、リアセンブル中の最も古いデータグラムが破棄されます。リアセンブリのタイムアウトは2秒に設定されています。また、セッションマネージャがリアセンブルするフラグメントの合計数の上限は1000に設定されています。この上限に達すると、セッションマネージャでリアセンブル中の最も古いデータグラムとそのフラグメントリストが破棄されます。ユーザーがこれらの制限値を設定することはできません。

リカバリ

セッションマネージャが停止すると、ACLルールが回復されます。MNがセッションの新しいトラフィックを開始する場合、セッション リダイレクト エントリが再作成される必要があります。そのため、クラッシュが発生した場合、インターネット側からのトラフィックはMNにリダイレクトされません。

AAA アカウンティング

宛先ベースのアカウンティングが実装されている場合、サブスクライバからのトラフィックは、リダイレクトされたアドレスではなく、元の宛先アドレスを使用するようにアカウンティングされます。

サブスクライバのリダイレクトされたセッションエントリの表示

次のコマンドを入力して、サブスクライバのリダイレクトされたセッションエントリを表示します。

show subscribers debug-info { callid *<id>* **| msid** *<id>* **| username** *<name>* **}**

次のコマンドは、MSIDが0000012345のサブスクライバのデバッグ情報を表示します。

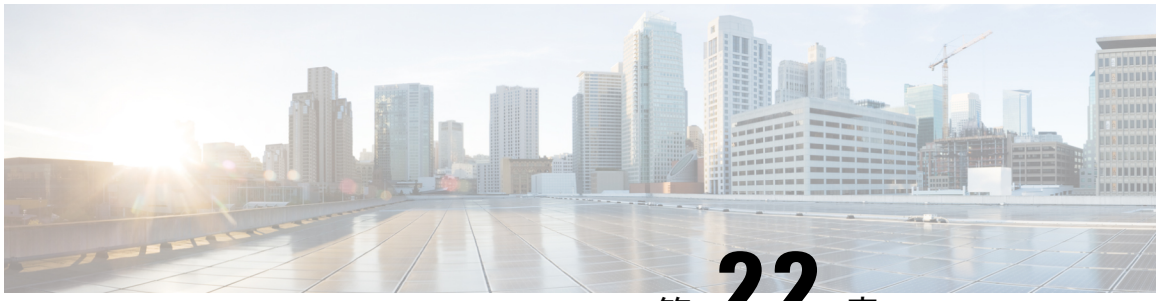
show subscribers debug-info msid 0000012345

次に、このコマンドの出力例を示します。

```
username: user1 callid: 01ca11b1    msid: 0000100003
  Card/Cpu: 4/2
  Sessmgr Instance: 7
  Primary callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:            27         26         15700ms        15700ms
     Micro:           76         76          4200ms         4200ms
    Current state: SMGR_STATE_CONNECTED
    FSM Event trace:
            State                           Event
            SMGR_STATE_OPEN                 SMGR_EVT_NEWCALL
            SMGR_STATE_NEWCALL_ARRIVED      SMGR_EVT_ANSWER_CALL
            SMGR_STATE_NEWCALL_ANSWERED     SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LINK_CONTROL_UP
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_AUTH_REQ
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_IPADDR_ALLOC_SUCCESS
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_UPDATE_SESS_CONFIG
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LOWER_LAYER_UP
Data Reorder statistics
         Total timer expiry:       0         Total flush (tmr expiry):  0
```

```
        Total no buffers:         0         Total flush (no buffers):  0
        Total flush (queue full): 0         Total flush (out of range):0
        Total flush (svc change): 0         Total out-of-seq pkt drop: 0
                Total out-of-seq arrived: 0
IPv4 Reassembly Statistics:
        Success:                  0         In Progress:               0
        Failure (timeout):        0         Failure (no buffers):      0
        Failure (other reasons):  0
Redirected Session Entries:
        Allowed:                  2000      Current:                   0
        Added:                    0         Deleted:                   0
        Revoked for use by different subscriber: 0
  Peer callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:             0          0             0ms            0ms
     Micro:            0          0             0ms            0ms
    Current state: SMGR_STATE_CONNECTED
    FSM Event trace:
            State                           Event
            SMGR_STATE_OPEN                 SMGR_EVT_MAKECALL
            SMGR_STATE_MAKECALL_PENDING     SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LOWER_LAYER_UP
            SMGR_STATE_CONNECTED            SMGR_EVT_AUTH_REQ
            SMGR_STATE_CONNECTED            SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_CONNECTED            SMGR_EVT_REQ_SUB_SESSION
            SMGR_STATE_CONNECTED            SMGR_EVT_RSP_SUB_SESSION
username: user1 callid: 01ca11b1    msid: 0000100003
  Card/Cpu: 4/2
  Sessmgr Instance: 7
  Primary callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
     Full:            27         26         15700ms        15700ms
     Micro:           76         76          4200ms         4200ms
    Current state: SMGR_STATE_CONNECTED
    FSM Event trace:
            State                           Event
            SMGR_STATE_OPEN                 SMGR_EVT_NEWCALL
            SMGR_STATE_NEWCALL_ARRIVED      SMGR_EVT_ANSWER_CALL
            SMGR_STATE_NEWCALL_ANSWERED     SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LINK_CONTROL_UP
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_AUTH_REQ
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_IPADDR_ALLOC_SUCCESS
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_UPDATE_SESS_CONFIG
            SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LOWER_LAYER_UP
Data Reorder statistics
        Total timer expiry:       0         Total flush (tmr expiry):  0
        Total no buffers:         0         Total flush (no buffers):  0
        Total flush (queue full): 0         Total flush (out of range):0
        Total flush (svc change): 0         Total out-of-seq pkt drop: 0
                Total out-of-seq arrived: 0
IPv4 Reassembly Statistics:
        Success:                  0         In Progress:               0
        Failure (timeout):        0         Failure (no buffers):      0
        Failure (other reasons):  0
Redirected Session Entries:
        Allowed:                  2000      Current:                   0
        Added:                    0         Deleted:                   0
        Revoked for use by different subscriber: 0
Peer callline:
  Redundancy Status: Original Session
  Checkpoints   Attempts    Success    Last-Attempt   Last-Success
```

```
   Full:             0          0             0ms            0ms
   Micro:            0          0             0ms            0ms
  Current state: SMGR_STATE_CONNECTED
  FSM Event trace:
          State                           Event
          SMGR_STATE_OPEN                 SMGR_EVT_MAKECALL
          SMGR_STATE_MAKECALL_PENDING     SMGR_EVT_LINE_CONNECTED
          SMGR_STATE_LINE_CONNECTED       SMGR_EVT_LOWER_LAYER_UP
          SMGR_STATE_CONNECTED            SMGR_EVT_AUTH_REQ
          SMGR_STATE_CONNECTED            SMGR_EVT_AUTH_SUCCESS
          SMGR_STATE_CONNECTED            SMGR_EVT_REQ_SUB_SESSION
          SMGR_STATE_CONNECTED            SMGR_EVT_RSP_SUB_SESSION
          SMGR_STATE_CONNECTED            SMGR_EVT_ADD_SUB_SESSION
          SMGR_STATE_CONNECTED            SMGR_EVT_AUTH_REQ
          SMGR_STATE_CONNECTED            SMGR_EVT_AUTH_SUCCESS
Data Reorder statistics
       Total timer expiry:       0        Total flush (tmr expiry):  0
       Total no buffers:         0        Total flush (no buffers):  0
       Total flush (queue full): 0        Total flush (out of range):0
       Total flush (svc change): 0        Total out-of-seq pkt drop: 0
       Total out-of-seq arrived: 0
IPv4 Reassembly Statistics:
       Success:                  0        In Progress:               0
       Failure (timeout):        0        Failure (no buffers):      0
       Failure (other reasons):  0
Redirected Session Entries:
       Allowed:                  2000     Current:                   0
       Added:                    0        Deleted:                   0
       Revoked for use by different subscriber: 0
```



第 22 章

P-GW/SAEGW/S-GW でのコリジョン処理

- 機能説明 （433 ページ）
- 機能の仕組み （434 ページ）
- コリジョン処理の設定 （437 ページ）
- コリジョン処理機能のモニタリング （438 ページ）

機能説明

ノードが、ピアノードからの特定のプロシージャメッセージを予期しているにもかかわらず、代わりにピアから異なるプロシージャメッセージを受信すると、ネットワークで GTPv2 メッセージのコリジョンが発生します。GTP プロシージャのコリジョンはネットワーク内で非常に一般的です。特に、ダイナミックポリシーおよび課金制御の場合、ネットワーク内でコリジョンが発生する可能性が非常に高くなります。

これらのコリジョンは、統計によって追跡され、各メッセージコリジョンタイプに対して事前定義されたアクションに基づいて処理されます。これらの統計は、通信事業者がネットワークの問題をデバッグするために役立ちます。

重要 SAEGW が Pure P-GW または Pure S-GW として設定されている場合、通信事業者は、それぞれのコリジョン統計を確認できます（発生した場合）。

他の機能との関係

- この機能は、P-GW、SAEGW、S-GW の基本ソフトウェアライセンスの一部です。追加のライセンスは必要ありません。
- P-GW、S-GW、または SAEGW サービスは、GTPv2 コリジョンの統計を表示するように設定する必要があります。

機能の仕組み

コリジョン処理

GTPv2 メッセージのコリジョンが発生すると、P-GW、SAEGW、および S-GW によって処理されます。これらはまた、コリジョンの処理内容に関する情報を使用して統計機能により追跡されます。

特に、**show egtpc statistics** verbose コマンドの出力が拡張され、S-GW および P-GW の入力インターフェイスでの GTPv2 メッセージのコリジョンの追跡と処理に関する情報が提供されるようになりました。利用可能な情報は次のとおりです。

- **Interface**：コリジョンが発生したインターフェイス：SGW（S4/S11）、SGW（S5）、および P-GW（S8）。
- **Old Proc (Msg Type)**：コリジョンの原因となったインターフェイスに新しいメッセージが到着したときに eGTP-C で実行されていたプロシージャを示します。カッコ内の Msg Type は、この進行中のプロシージャをトリガーしたメッセージを示します。古いプロシージャは 3GPP TS 23.401 に準拠していることに注意してください。
- **New Proc (Msg Type)**：新しいプロシージャとメッセージタイプ。新しいプロシージャは 3GPP TS 23.401 に準拠していることに注意してください。
- **Action**：コリジョンを処理するために実行される事前定義されたアクション。アクションは次のいずれかになります。
  - **No Collision Detected**
  - **Suspend Old**：元の（古い）メッセージの処理を一時停止し、新しいメッセージを処理してから古いメッセージの処理を再開します。
  - **Abort Old**：元のメッセージの処理を中止し、新しいメッセージを処理します。
  - **Reject New**：新しいメッセージを拒否し、元の（古い）メッセージを処理します。
  - **Silent Drop New**：到着した新しいメッセージをドロップし、古いメッセージを処理します。
  - **Parallel Hndl**：元の（古い）メッセージと新しいメッセージの両方を並行して処理します。
  - **Buffer New**：新しいメッセージをバッファリングし、元の（古い）メッセージを処理した後に処理します。
  - **Counter**：各コリジョンタイプが発生した回数。



重要 コマンド出力の *Message Collision Statistics* セクションは、コリジョン統計のいずれかのカウンタ合計がゼロより大きい場合にのみ表示されます。

サンプル出力：

```
Message Collision Statistics
   Interface      Old Proc (Msg Type)       New Proc (Msg Type)    Action    Counter
    SGW(S5)   NW Init Bearer Create (95)  NW Init PDN Delete (99)  Abort Old    1
```

この例では、出力は、P-GW からのベアラー作成要求（95）メッセージにより、S-GW 出力インターフェイス（S5）でベアラーの作成プロシージャが進行中であることを示しています。その応答が MME から S-GW に届く前に、P-GW からのベアラー削除要求（99）メッセージにより、新しいプロシージャとして PDN 削除がトリガーされています。

このコリジョンが原因で eGTP-C レイヤで実行されるアクションは、ベアラーの作成プロシージャを中止（Abort Old）し、PDN 削除の開始プロシージャを通常どおり続行することです。Counter の合計数が 1 の場合、このコリジョンが 1 回発生したことを示します。

コリジョン処理のシナリオ例

ここでは、S-GW と P-GW に関するいくつかのコリジョン処理シナリオについて説明します。

S-GW は、次の場合に、S-GW 入力インターフェイスで追加のコリジョンを処理します。

1. ベアラー作成要求メッセージまたはベアラー更新要求メッセージと、MME 間または RAT 間のベアラー変更要求メッセージ（ULI の変更がありおよびなし）。
2. ダウンリンクデータ通知（DDN）メッセージと、ベアラー作成要求またはベアラー更新要求。

これらのコリジョンシナリオを処理するための S-GW の動作は次のとおりです。

1. S-GW 入力インターフェイスで CBReq および MBReq（MME 間または RAT 間（ULI の変更がありまたはなし））のコリジョンが発生すると、メッセージは並行して処理されます。CBReq は、ピアからのベアラー作成要求（CBRsp）を待ちます。また、MBReq が P-GW と並行して送信されます。
2. SGW 入力インターフェイスでの UBReq と MBReq（MME 間または RAT 間（ULI の変更がありまたはなし））のコリジョンは、一時停止と再開の手順で処理されます。UBReq は一時停止され、MBReq が処理されます。MBRsp が SGW 入力インターフェイスからピアに送信されると、UBReq 手順が再開されます。
3. ベアラー作成要求（CBR）またはベアラー更新要求（UBR）とダウンリンクデータ通知（DDN）メッセージは、並行して処理されます。

その結果、S-GW によって発生した原因コードメッセージ 110（ハンドオーバー手順が進行中のため一時的に拒否）は、そのようなコリジョンの一部とは見なされません。コリジョンは並行して処理されます。

次の GTP-C コリジョン処理シナリオの例は、P-GW でも発生します。

DBCmd または MBreq コリジョンの処理

P-GW では、通信事業者は、デフォルトベアラーに対するベアラー変更要求（MBreq）メッセージが P-GW で保留中の場合に、ベアラー削除コマンド（DBcmd）メッセージのコリジョンを P-GW がどう処理するかを設定できます。

DBCmd メッセージと MBReq メッセージのコリジョンを処理するために CLI で制御するオプションは 3 つあります。

- MBreq メッセージが保留中の場合、DBcmd メッセージをキューに入れます。このオプションの利点は、ほとんどのコリジョンで DBCmd メッセージが失われないことです。MBRsp が送信されるまで、P-GW で保持されます。
- MBreq メッセージが保留中の場合、DBCmd メッセージをドロップします。このオプションでは、S-GW が DBCmd を再試行する必要があることに注意してください。
- StarOS 19.0 より前の動作を使用します。MBreq メッセージを中止し、DBcmd メッセージを処理します。このオプションの利点は、通信事業者が StarOS 19.0 より前の機能を維持する場合に下位互換性が提供されることです。

CLI コマンド **collision handling** を使用すると、DBCmd メッセージと MBReq メッセージでのコリジョンシナリオの処理をより柔軟に設定できます。また、このコリジョン処理シナリオの動作を設定する手順については、このドキュメントの DBcmd メッセージ動作の設定 （437 ページ） を参照してください。

MBReq と CBreq での並行処理。CBRsp の処理

P-GW と S-GW は、次のコリジョンシナリオの例を処理します。

ノードは CBRsp メッセージをキューに入れ、MBRsp が送信されると P-GW または S-GW セッションマネージャに CBRsp メッセージを渡します。その結果として、通信事業者は MME からの CBRsp メッセージの再送信を確認できません。

トランザクションが一時停止された場合の UBrsp の処理

P-GW と S-GW は、次のコリジョンシナリオの例を処理します。

P-GW または S-GW が UBRsp メッセージを受信すると、P-GW または S-GW は、一時停止されたトランザクションの UBRsp メッセージを処理します。その結果、UBRsp メッセージは、MBRsp メッセージが送信されるまでバッファに格納されます。

ドロップおよび再試行のための MBR を介した MBR のコリジョン処理

mbreq を介したベアラー変更要求（mbreq）でのコリジョンを回避するため、MME は、egtp-service での `mbreq-over-mbreq drop` CLI 設定により、MBR を介した MBR のコリジョンでのドロップおよび再試行機能をサポートします。次の機能が動作します。

- サービス要求のベアラー変更要求が保留状態の場合、MME はベアラー変更要求を送信します
- S-GW は E-RAB 手順でのベアラー変更要求メッセージをドロップします
- MME は、最初の MBR 応答まで、ドロップされた MBR を再試行します。

制限事項

P-GW、SAEGW、S-GW のコリジョン処理機能に既知の制限はありません。

標準準拠

仕様および標準規格では、コリジョン処理のケースに関する厳格なルールは指定されていません。

コリジョン処理の設定

オペレータはコマンド ライン インターフェイス（CLI）を使用して、次の GTPv2 メッセージ コリジョンを処理するように P-GW の動作を設定できます。

- デフォルトベアラーの MBreq メッセージが P-GW で保留中の場合の DBcmd メッセージ



重要 CLI による設定は、他のすべての P-GW および S-GW コリジョン処理シナリオに必要では**ありません。**

DBcmd メッセージ動作の設定

次の例を使用して、デフォルトベアラーの修正ベアラー要求メッセージが P-GW で保留中である場合のベアラー削除コマンドメッセージのコリジョン処理の動作を設定します。

```
configure
   context  context_name
      egtp-service  egtp_service_name
         collision-handling dbcmd-over-mbreq  { drop | queue }
         { default | no } collision-handling dbcmd-over-mbreq
         end
```

注：

- **collision-handling dbcmd-over-mbreq** ：MBreq が保留中の場合、DBcmd のコリジョン処理を設定します。
- **drop**：MBreq メッセージが保留中の場合、DBcmd メッセージをドロップします。
- **queue**：MBreq メッセージが保留中の場合、DBcmd メッセージをキューに入れます。

  デフォルトの動作では、MBReq メッセージは中止され、DBcmd メッセージが処理されます。

設定の確認

デフォルトベアラーの MBreq メッセージが P-GW 設定で保留の場合に DBcmd メッセージを確認するには、Exec モードで次のコマンドを使用します。

```
show egtpc service all
      Collision handling: DBcmd when MBreq pending: <Queue DBcmd>, <Drop DBcmd>, or
<Abort MBreq and handle Dbcmd>
```

コリジョン処理機能のモニタリング

ここでは、コリジョン処理機能をモニターする方法について説明します。

コリジョン処理の show コマンドと出力

ここでは、P-GW、SAEGW、および S-GW でのコリジョン処理機能をサポートする show コマンドとその出力について説明します。

show configuration

このコマンドの出力は、MBreq メッセージが保留中の DBcmd メッセージのコリジョン処理、または MBreq メッセージがドロップ中の MBreq メッセージのコリジョン処理が有効か無効かを示します。

- collision-handling dbcmd-over-mbreq queue
- no collision-handling dbcmd-over-mbreq queue
- collision-handling mbreq-over-mbreq drop

show egtp-service all | name

このコマンドの出力は、デフォルトベアラーの MBreq メッセージが Drop MBreq または Abort MBreq によって保留状態になっている場合に、P-GW が DBcmd メッセージをどのように処理して、MBreq シナリオに対処するよう設定されているかを表示します。

- コリジョン処理
  - MBreq 保留中の MBreq

show egtp statistics verbose

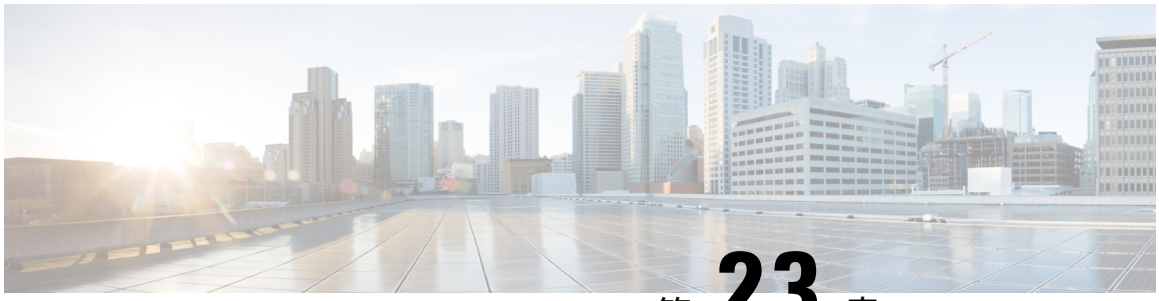
このコマンドの出力が拡張され、P-GW/S-GW 入力インターフェイスでサポートされているすべての GTPv2 メッセージのコリジョンに関する詳細情報が提供されるようになりました。これには次の情報が含まれます。

- コリジョンが発生したインターフェイス。
- コリジョンの原因となったインターフェイスに新しいメッセージが到着したときにeGTP-Cで実行されていたプロシージャ。カッコ内の Msg Type は、この進行中のプロシージャをトリガーしたメッセージを示します。
- 新しいプロシージャとメッセージタイプ。
- コリジョンを処理するために実行される事前定義されたアクション。

- 各コリジョンタイプが発生した回数。



重要　コマンド出力の *Message Collision Statistics* セクションは、コリジョン統計のいずれかのカウンタ合計がゼロより大きい場合にのみ表示されます。



第 23 章

P-GW と GGSN における Closed Subscriber Group のモビリティイベントのサポート

- 機能の概要と変更履歴 （441 ページ）
- 機能説明 （442 ページ）
- アクセス コントロール （442 ページ）
- 機能の仕組み （445 ページ）
- 動作マトリックス （447 ページ）
- モニタリングおよびトラブルシューティング （448 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • GGSN
該当プラットフォーム	• ASR 5500 • VPC-DI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Statistics and Counters Reference* • *P-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、P-GW と GGSN の Closed Subscriber Groups モビリティイベントのサポートが追加されています。	21.23

機能説明

Closed Subscriber Group（CSG）は、CSG のメンバーとしてパブリック ランド モバイル ネットワーク（PLMN）の 1 つ以上の CSG セルにアクセスできるサブスクライバグループを識別します。CSG ID は PLMN の範囲内にある一意の識別子であり、CSG セルまたは CSG セルのグループに関連付けられた PLMN の CSG を識別します。GGSN によって要求されたサブスクライバ セッションの CSG 情報変更レポートについては、MS が CSG セルまたはハイブリッドセル内にある場合、Serving GPRS Support Node（SGSN）にユーザー CSG 情報が含まれます。

ユーザーが CSG セルまたはハイブリッドセルに出入りしたときにイベント通知が P-GW およびゲートウェイ GPRS サポート（GGS）に送り返されない場合、ユーザーに異なるポリシーと課金特性を提供する機能は制限されます。この StarOS 21.23 およびこれ以降のリリースでは、CSG モビリティイベントのサポートが複数のネットワーク要素（eNodeB、MME、SGW、PGW、PCRF、SGSN、GGSN、HSS など）で使用できます。この CSG モビリティイベント機能は、3GPP 標準に基づく P-GW と GGSN の CSG 機能を完全にサポートします。この CSG モビリティイベント機能には、次の機能が含まれています。

- CSG 通知イベントを有効にしてトリガーします。
- 適切なポリシーと課金ルールを適用します。

アクセス コントロール

CSG モビリティイベント機能は、S5/S8、Gn/Gp、Gx、および Rf インターフェイスで機能します。

S5 および S8 インターフェイス

CSG 情報を処理するメッセージタイプには、MME から開始されたメッセージと PGW から開始されたメッセージが表示されます。S-GW は、MME 間、および P-GW 間で情報を渡します。

- **セッション作成要求**：S-GW および P-GW への CSG 情報変更レポートをサポートするように MME が設定されている場合、セッション作成要求（CSR）メッセージには CSG Change Reporting Support Indication（CCRSI）フラグが含まれます。UE が CSG またはハイブリッドセルを介して接続されている場合は、ユーザー CSG 情報（UCI）IE が CSR に含まれます。ユーザー CSG 情報 IE には、CSG またはハイブリッドセルの PLMN と CSG ID、アク

セスモード（クローズドまたはハイブリッド）、およびアクセスモードがハイブリッドの場合は CSG 内の UE のメンバーシップステータスが含まれます。

- **セッション作成応答**：CSG情報レポートが開始または停止された場合、P-GWまたはS-GWは、セッション作成応答でCSG情報レポートアクション（CIRA）IEを送信します。このIEには、CSG（非ハイブリッド）セル、サブスクライブされているハイブリッドセル、またはサブスクライブされていないハイブリッドセルに UE が出入りしたときに、MME がレポートする必要があるかどうかを示す 3 ビットが含まれます。3 ビットすべてがゼロに設定されている場合、S-GW と P-GW への CSG 情報のレポートはすべて停止されます。MME は、CSG レポート情報を PDN コンテキストの一部として保存します。
- **ベアラー作成要求**：MME からの CSG レポートが変更された場合、P-GW と S-GW からのベアラー作成要求メッセージには CIRA IE が含まれます。MME は、CSG レポート情報を PDN コンテキストの一部として保存します。
- **ベアラー変更要求**：S-GW と P-GW への CSG 情報変更レポートをサポートするように MME が設定されている場合、ベアラー変更要求の Indication IE の CCRSI フラグがセットされます。P-GW や S-GW が CSG 情報レポートを要求して、TAU、ハンドオーバー、または UE 開始のサービス要求が行われている場合、MME はベアラー変更要求メッセージに UCI IE を含めます。
- **ベアラー更新要求**：MME からの CSG レポートが変更された場合、P-GW と S-GW からのベアラー作成要求メッセージには CIRA IE が含まれます。MME は、CSG レポート情報を PDN コンテキストの一部として保存します。
- **変更通知要求**：ベアラー作成要求またはベアラー変更要求なしに CSG 接続情報に変更がある場合、MME は、要求された各 PDN の S-GW と P-GW に変更通知要求を送信します。変更通知要求には UCI IE が含まれます。ロケーションレポートも変更通知要求メッセージを使用するため、MME は可能な限り、ロケーション変更のレポートと CSG 変更を同じメッセージにバンドルして、送信される変更通知要求メッセージの数を最小限に抑えます。
- **変更通知応答**：MME からの CSG レポートが変更された場合、P-GW と S-GW からの変更通知応答メッセージには CIRA IE が含まれます。MME は、CSG レポート情報を PDN コンテキストの一部として保存します。

Gn インターフェイスと Gp インターフェイス

CSG情報を処理するメッセージタイプには、SGSNから開始されたメッセージとGGSNから開始されたメッセージが表示されます。

- **PDP コンテキスト作成要求（CPC 要求）**：GGSN への CSG 情報変更レポートをサポートするように SGSN が設定されている場合、CPC 要求メッセージには CSG Change Reporting Support Indication（CCRSI）フラグが含まれます。UE が CSG またはハイブリッドセルを介して接続されている場合は、ユーザー CSG 情報（UCI）IE が CPC に含まれます。ユーザー CSG 情報 IE には、CSG またはハイブリッドセルの PLMN と CSG ID、アクセスモー

ド（クローズドまたはハイブリッド）、およびアクセスモードがハイブリッドの場合は CSG 内の UE のメンバーシップステータスが含まれます。

（注） アクセスモード値が予約されている場合（2 または 3）、GGSN/P-GW の UCI 値は無視されます。

- **PDP コンテキスト作成応答（CPC 応答）**：CSG 情報レポートが開始または停止された場合、GGSN は、CPC 応答で CSG 情報レポートアクション（CIRA）IE を送信します。この IE には、CSG（非ハイブリッド）セル、サブスクライブされているハイブリッドセル、またはサブスクライブされていないハイブリッドセルに UE が出入りしたときに、SGSN が報告する必要があるかどうかを示す 3 ビットが含まれます。3 ビットすべてがゼロに設定されている場合、GGSN への CSG 情報のレポートはすべて停止されます。
- **PDP コンテキスト更新要求（UPC 要求）**：SGSN が CSG 情報変更レポートをサポートしており、CSG 情報レポートアクションを介して GGSN によって CSG 変更レポートが要求された場合、拡張共通フラグ IE の CCRSI フラグが UPC 要求で設定されます。UE が CSG セルまたはハイブリッドセルを介してアクセスされている場合は、ユーザー CSG 情報 IE が SGSN に含まれます。
- .**ネットワークで要求された PDP コンテキスト更新要求（NRUPC 要求）**：SGSN からの CSG レポートが変更された場合、GGSN からの NRUPC 要求メッセージには CIRA IE が含まれます。SGSN は、CSG レポート情報を PDN コンテキストの一部として保存します。
- **MS 情報変更通知要求**：MS 情報変更通知要求には、拡張共通フラグ IE の UCI IE および CCRSI フラグが含まれます。ロケーションレポートも MS 情報変更通知要求メッセージを使用するため、SGSN は可能な限り、ロケーション変更のレポートと CSG 変更を同じメッセージにバンドルして、送信される MS 情報変更通知要求メッセージの数を最小限に抑えます。
- **MS 情報変更通知応答**：SGSN からの CSG レポートが変更された場合、GGSN からの変更通知応答メッセージには CIRA IE が含まれます。SGSN は、CSG レポート情報を PDN コンテキストの一部として保存します。

Gx インターフェイス

CSG が Gx インターフェイスを介して関連するメッセージを処理しているときに、次の機能が実行されます。

- **[Internet Protocol]**：IP 接続アクセスネットワーク（IP-CAN）セッション中に、PCRF は IP-CAN セッションに CSG セルまたはハイブリッドセルの変更に関するレポートが必要かどうかを判断します。
- UE が CSG セルやハイブリッドセルに出入りすると、ポリシーおよび課金適用機能（PCEF）が USER_CSG_INFORMATION_CHANGE、USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE、

USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE イベントのいずれかを報告します。PCEF は User-CSG-Information AVP 内の CSG の変更も報告します。

- 後続の CCA-U メッセージで CSG-Information-Reporting AVP が受信されない場合は、既存の CSG-Information-Reporting の値が再利用されます。
- PCRF は CSG-Information-Reporting AVP を使用して、RF インターフェイスを介して課金データ機能（CDF）やオフライン課金サーバー（OFCS）にユーザーの CSG 情報の変更を報告するよう PCEF に伝えます。この AVP を IPCAN セッション中に受信しなかった場合、PCEF はユーザーの CSG 情報の変更を CDF や OFCS に報告しません。

Rf インターフェイス

CSG 情報の処理での ACR メッセージには次があります。

- ACR 開始メッセージの間のみに情報を送信する PS レベル（Ps-Information AVP）でのユーザー CSG 情報（UCI）。後続のメッセージで UCI 情報の SDC レベル（Service-Data-Container AVP）を送信します



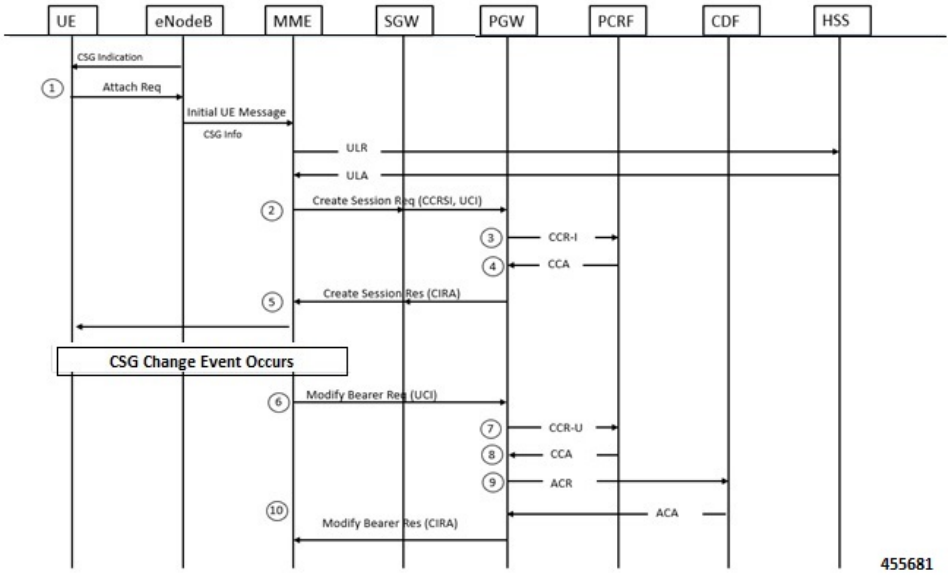
重要 Rf プロファイルの設定 **attribute csg** により、ACR 開始メッセージでの送信時に PS レベルの UCI 情報が有効になります。

- ユーザー CSG 情報（UCI）の変更値は、ユーザー CSG 情報の変更をアクセス側から受信し、CSG 情報の OFCS に対する CSG 変更レポートが PCRF からの Reporting AVP で有効になるたびに、SDC レベルで Change-Condition AVP に追加されます。
- IP-CAN セッション中に CSG 情報レポートを受信しない場合、P-GW は Rf インターフェイスを介して OFCS に User CSG Information AVP を送信しません。

機能の仕組み

次の図は、Closed Subscriber Group を実装した場合の EPC 要素間のメッセージフローを示しています。

図 *16 :* 非公開サブスクライバ グループ メッセージのコールフロー



次のステップでワークフローについて説明します。

1. eNodeB は CSG 情報を UE にブロードキャストします。接続要求イベントが発生すると、eNodeB は初期 UE メッセージで独自の CSG 関連情報を MME に送信します。MME はサブスクライバのプロファイルを取得するために、HSS にロケーション更新要求（ULR）を送信します。HSS はサブスクリプションデータを含むロケーション更新応答で応答します。これには CSG サブスクリプションデータが含まれます。
2. MME は、HSS からのユーザープロファイルに従ってコールを処理します。MME は CSG メンバーシップインジケーションを設定し、アクセスモードと CSG-ID を追加して S-GW に渡します。S-GW は、P-GW に透過的に情報を渡します。
3. P-GW は、PCRF に対してポリシーと課金ルールを要求します。
4. PCRF はユーザー サブスクリプション プロファイルに基づいて、Event-Trigger:=USER_CSG_INFORMATION_CHANGE、USER_CSG_HYBRID_SUBSCRIBED_INFORMATION_CHANGE、USER_CSG_HYBRID_UNSUBSCRIBED_INFORMATION_CHANGE、CSG-Information-Reporting AVP を送信します。
5. P-GW は Event-Trigger:=USER_CSG_INFO_CHG を受信すると、セッション作成応答に CSG-Information-Reporting-Action を設定します。
6. MME は CSG-Membership-Status を eNodeB に送信します。これは、アクセスモードがハイブリッドに設定されている場合にのみ発生します。
7. CSG 変更イベントが発生すると、eNodeB/MME はイベントを報告します。MME は通知変更要求またはベアラー変更要求を使用して CSG 変更イベントを更新します。

8. P-GW は Event-Reporting-Indication AVP を使用して CSG 変更イベントを PCRF に報告します。
9. PCRF は Charging-Rule-Base-Name でポリシーと課金ルールを更新するか、新しい Charging-Rule-Base-Name をインストールします。
10. PCRF が CHANGE_CSG_CELL フラグを付けて CSG-Information-Reporting AVP を報告すると、P-GW は Rf インターフェイスを介して CDF に課金レコードを報告し、User-CSG-Information AVP を含めます。
11. ポリシーと課金ルールの変更によってベアラーの変更または作成が発生した場合、P-GW はベアラー変更応答や通知変更応答の一部として CSG 情報レポートアクション IE を送信するか、ベアラー変更要求を介して変更を開始できます。

動作マトリックス

次のメッセージタイプと CSG AVP は、Gx および Rf インターフェイスで使用できます。

表 *39 :* メッセージタイプの動作（*E-UTRAN/UTRAN*）

メッセージ タイプ	User-CSG-Information AVP（Gx）	User-CSG-Information AVP（Rx）
セッション作成要求/PDP コンテキスト作成要求	CCR - I	ACR-Start
ベアラー変更要求/PDP コンテキスト更新要求	CCR-U	ACR-Interim
変更通知要求/MS 情報変更通知要求	CCR-U	ACR-Interim
セッション削除要求/PDP コンテキスト削除要求	-	ACR-Stop
ベアラー削除要求	-	ACR-Interim/Stop

（注） Gx および Rf インターフェイスの CSG 情報では、3G および E-UTRAN RAT タイプのみがサポートされます。

ハンドオフが予想される動作：E-UTRAN または 3G から他の RAT タイプ（Wi-Fi など）への UE ハンドオーバーがある場合、User-CSG-Information AVP は Gx および Rf インターフェイスで送信されません。

モニタリングおよびトラブルシューティング

ここでは、Closed Subscriber Group のモビリティイベント機能に使用可能な show コマンドの出力について説明します。

コマンドと出力の表示

show subscribers pgw-only full all

show subscribers pgw-only full all コマンドの出力が拡張され、P-GW および GGSN での Closed Subscriber Groups モバイルイベント機能をサポートする次の出力フィールドが追加されました。

同様に、**show subscribers ggsn-only full all** および **show subscribers saegw-only full** CLI コマンドの出力が拡張され、次の出力フィールドが追加されました。

フィールド	説明
UCI	
MCC	ユーザー CSG 情報のモバイル国コード（MCC）を表示します。
MNC	ユーザー CSG 情報のモバイル ネットワーク コード（MNC）を表示します。
CSG-ID	Closed Subscriber Group の ID を表示します。
[Access Mode]	一致するアクセスモードを表示します。
LCSG	Leave Closed Subscribers Group（LCSG）の値を表示します。デフォルト値は 0 です
CMI	CSG メンバーシップ情報（CMI）を表示します。表示される CMI は、ハイブリッドセルのメンバーまたは非メンバーのいずれかです。

show ims-authorization sessions full all

このコマンドの出力が拡張され、P-GW および GGSN でのクローズド サブスクライバ グループ モバイル イベント機能をサポートする次の出力フィールドが追加されました。

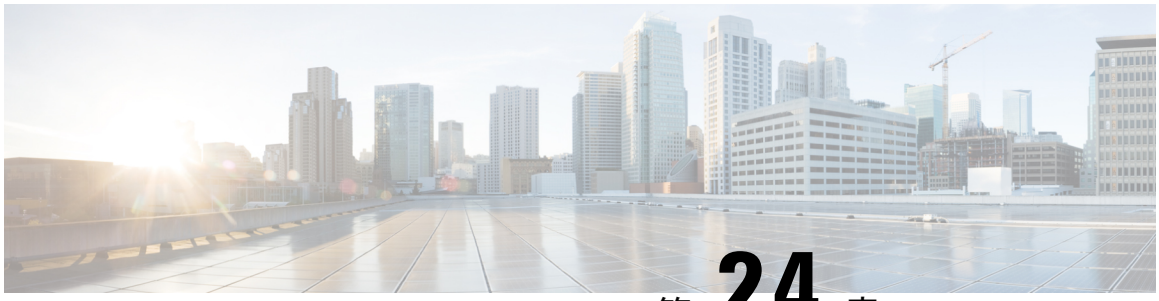
フィールド	説明
認証決定：	
イベントトリガー：	

フィールド	説明
ユーザー CSG 情報変更	ユーザー CSG 情報変更要求イベントトリガーの総数を表示します。
ユーザー CSG ハイブリッドサブスクライブ情報変更	ユーザー CSG ハイブリッドサブスクライブ情報変更要求イベントトリガーの合計数を表示します。
ユーザー CSG ハイブリッドサブスクライブ解除情報変更	ユーザー CSG ハイブリッドサブスクライブ解除情報変更要求イベントトリガーの合計数を表示します。

show ims-authorization service statistics

このコマンドの出力には、CSG 機能の統計が表示されます。

フィールド	説明
再承認トリガー	
ユーザー CSG 情報変更	ユーザー CSG 情報変更カウンタの合計数を表示します。
ユーザー CSG ハイブリッド登録情報変更	ユーザー CSG ハイブリッド登録情報変更カウンタの合計数を表示します。
ユーザー CSG ハイブリッド登録解除情報変更	ユーザー CSG ハイブリッド登録解除情報変更カウンタの合計数を表示します。



第 24 章

クラウドソーシングの最適化

- 機能の概要と変更履歴 （451 ページ）
- 機能説明 （452 ページ）
- 機能の仕組み （452 ページ）
- **エレファント検出メカニズムの検出モードの設定** （454 ページ）
- トライアルモードでのクラウドソース最適化の設定 （455 ページ）
- モニタリングおよびトラブルシューティング （455 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：ライセンスが必要
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide* • *Command Line Interface Reference* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.23

機能説明

クラウドソーシング最適化機能は、履歴データセッションを使用して、アクティブなエレファントフローからの回復キャパシティを増やします。このとき、プロファイルをシーティングして、セルの状態や機能を迅速に学習します。

クラウドソーシングの最適化機能により、以下のことが可能です

- トラフィックフローのパフォーマンスをキャプチャするリアルタイムセルと履歴セルの特性を報告する。
- 同じセッションマネージャによる同じサブスクライバからのトラフィックを処理する。
- 場所の更新を有効にする。
- ULI の変更ではなく ECGI の変更に基づいて Cisco Ultra Traffic Optimization ライブラリに報告する。
- 各 VPP インスタンスに情報をクラウドソーシングする。

（注） クラウドソーシング最適化機能は、P-GW がユーザーの場所について（たとえば MME から）学習する場合にのみ機能します。そのため、ユーザーロケーション情報の更新を有効にする必要があります。

他の機能との関係性

クラウドソーシング最適化機能は、Cisco Ultra Traffic Optimization 機能に関連しています。詳細については、『*P-GW Administration GuideP*』の「*Cisco Ultra Traffic Optimation*」の章 [英語] を参照してください。

ライセンス

クラウドソーシング最適化機能には、機能パック 1 のライセンスが必要です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

機能の仕組み

クラウドソーシングの最適化手順では、次のことが記述されます。

- ECGI 情報の処理

- 強化されたエレファント検出メカニズム
- トライアルモードメカニズム

ECGI 情報の処理

以下は、ECGI データを処理するためのワークフローです。

- P-GW は、ULI 情報を記録するときにセッション作成要求を受信します。
- P-GW ではトラフィックが発生し、記録された ULI 情報がフローの作成中に CUTO に報告されます。
- ロケーションの更新中に、フロー途中のベアラー変更要求で新しい ULI 情報が受信されます。各サブスクライバのすべてのフローがオンロードされ、新しい ULI 情報が CUTO ストリーム変更で報告され、ルールが一致するとストリームが再度オフロードされます。

  「CUTO アップグレードパック 1」ライセンスで以下が実行されます。

  - CUTO アルゴリズムに基づいて、ULI 情報のレポートが生成されます。
  - ULI タイプと ECGI 情報は、複数のフェーズでのフローの終了後に TODR でキャプチャされます。スケールシナリオでのフローの分析に役立ちます。

強化されたエレファント検出メカニズム

バイト単位、時間単位、またはバイトと時間の両単位のしきい値に基づくエレファントロジックの検出が追加されました。これは、設定 CLI で次のように使用します。

- 検出メカニズムは、次の 2 つのモードにグループ分けされます。
  - **基本モード**：基本モードでは、しきい値バイトパラメータ値が考慮されます。
  - **拡張モード**：拡張モードでは、しきい値バイト値とシード時間値の組み合わせが考慮されます。

  これらのいずれかの値を初めて通過したときに、フローがエレファントになります。

（注） シード時間は、拡張モードでの検出に適用できます。CLI のすべてのパラメータを表示するために、CUTO アップグレードパック 1 ライセンスでシード時間と検出モードの CLI オプションを必ずアクティブにしてください。

- エレファントフローの検出は、CUTO ベースポリシーの設定パラメータ（シード時間、検出モード）に基づいており、検出アルゴリズムの拡張ベースのポリシーパラメータは考慮しません。CLI により次のような主旨の警告が表示されます。

設定されたシード時間は検出には反映されません。設定する場合は、ヘビーセッション下で設定してください。

- 検出原因（時間またはバイト）と cuto モード（アクティブまたはパッシブ）が TODR に記録されます。これは規模の大きいフローの分析に役立ちます。検出原因は「CUTO アップグレードパック 1」ライセンスで記録され、cuto モードはライセンスなしで記録されます。これは、基本 CUTO ライセンスでも同様です。

トライアルモード

トライアルモードでは、アクティブモードとパッシブモードを定期的に切り替えて CUTO のネットワークの有効性を示す A/B テストキャンペーンを P-GW 内からスケジュール設定する機能が使用できます。トライアルモードは、traffic-optimization ライセンスまたは Cisco Ultra Traffic Optimization 抑制ライセンスで動作します。ただし、これをオンにするために「CUTO 機能パック 1」ライセンスは必要ありません。トライアルモードはアクティブなシャーシにのみ適用されるため、サービスリクエスト（SR）はサポートされていますが、ICSR はサポートされていません。

重要 トライアルモード中に **cuto-profile** を変更することはできないため、**cuto-profile** に変更を加える前に必ずトライアルモードを無効にしてください。

エレファント検出メカニズムの検出モードの設定

バイト単位、時間単位、またはバイトと時間の両単位のしきい値に基づくエレファントロジックの検出は、次のようにして設定 CLI に追加します。

```
configure
   active-charging service service_name
      [ no ] traffic-optimization-policy policy_name[extended]
         default detection-mode
         detection-mode
         [ no ] heavy-session { standard-flow-timeout
standard_flow-timeout_value  threshold threshold_value  seed-time seed_time_value
}
         end
```

注：

- **default**：検出モードのデフォルト設定。
- **detection-mode**：ヘビーセッション検出モードを設定します。検出モードのデフォルト値は「enhanced」です。
- **heavy-session**：ヘビーセッション検出関連のパラメータを設定します。

- **seed-time**：エレファントフローの検出時間をミリ秒単位で設定します。このパラメータは enhanced 検出モードで使用します。

トライアルモードでのクラウドソース最適化の設定

次の CLI コマンドを使用して、トライアルモードでクラウドソーシング最適化機能を有効にします。

```
configure
   require active-charging
   active-charging service service_name
      traffic-optimization-profile
        trial-mode  start-time YYYYMMDDHHMM end-time YYYYMMDDHHMM
mode-toggle-interval mode_toggle_interval initial-mode initial_active |
initial_passive
        end
```

注：

- **trial-mode**：トライアルモードでクラウドソーシング最適化機能を有効にします。
- **start-time** ：トライアルを開始する現地時刻（YYYY:MM:DD:HH:MM）。
- **end-time** ：トライアルを終了する現地時刻（YYYY:MM:DD:HH:MM）。
- **toggle-mode-interval** ：CUTO モードを周期的にアクティブとパッシブで切り替える間隔を分単位で指定します。間隔には 15、30、60 分を指定できます。開始間隔は 15 分です。
- **initial-mode** ：トライアルが開始されたときの初期モードを、アクティブまたはパッシブに設定します。
  - active：CUTO モードをアクティブにしてトライアルモードを開始します。
  - passive：CUTO モードをパッシブにしてトライアルモードを開始します。

モニタリングおよびトラブルシューティング

ここでは、P-GW 上のクラウドソーシング最適化ソリューションのモニタリングとトラブルシューティングに使用できるコマンドについて説明します。

コマンドと出力の表示

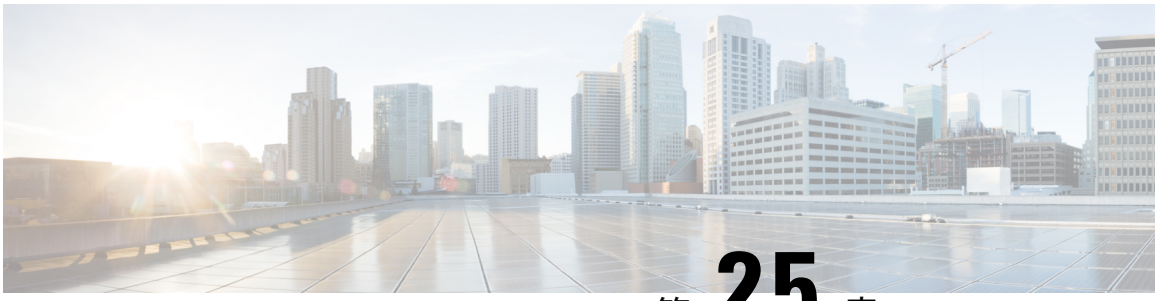
このセクションでは、Crowd Sourcing Optimization をサポートするために導入された show コマンドとフィールドについて説明します。

show active-charging traffic-optimization policy all

アクティブな課金サービスレベルでのヘビーセッション、拡張ヘビーセッション、およびトラフィック最適化ポリシーの設定値を表示します。

表 *40*：

フィールド	説明
Heavy-Session：ヘビーセッション検出関連のパラメータを表示します。	
Seed-Time	エレファントフローの検出時間をミリ秒単位で表示します。
Detection-Mode：ヘビーセッション検出モードを示します（デフォルト：enhanced）。	
Extended Heavy-Session：拡張ポリシーのヘビーセッション検出関連のパラメータを表示します。	
Seed-Time	エレファントフローの検出時間をミリ秒単位で表示します。



第 25 章

アクセスリンク IP フラグメンテーションのカスタマイズ

- 機能の概要と変更履歴 （457 ページ）
- 機能説明 （458 ページ）
- アクセスリンク IP フラグメンテーションの設定 （458 ページ）
- モニタリングおよびトラブルシューティング （460 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• GGSN • P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	有効、常時オン
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
IPv4 トラフィックに APN MTU を適用するための access-link fastpath のサポートが追加されました。	21.27
最初の導入。	21.26

機能説明

P-GW APN レベルの設定は、MTU より大きい IP パケットの転送またはドロップロジックが、GTPU カプセル化のオーバーヘッドのために高くなる場合に、IP フラグメント化を制御します。複数の設定を APN レベルで上書きするために、グローバルレベルの CLI では、展開時間が短縮され、設定サイズが削減され、エラーが最小限に抑えられます。

（注） CLI が APN レベルで設定されていない場合、デフォルトではグローバルレベルの設定が適用されます。CLI がグローバルレベルで設定されていない場合は、デフォルト値が適用されます。

アクセスリンク IP フラグメンテーションの設定

アクセスリンク IP フラグメンテーションの設定は、次のステップから構成されます。

- グローバルレベルのアクセスリンク IP フラグメンテーションの設定
- APN レベルのアクセスリンク IP フラグメンテーションの設定
- IPv4 トラフィックに APN MTU を適用するためのアクセスリンク Fastpath の設定

グローバルレベルのアクセスリンク IP フラグメンテーションの設定

次の設定を使用して、グローバル コンフィギュレーション モードでアクセスリンクの IP フラグメンテーションを設定します。

```
configure
  [ default ] access-link ip-fragmentation { df-fragment-and-icmp-notify
 | df-ignore | normal }
  end
```

注：

- **access-link ip-fragmentation**：リンク MTU がパケット長よりも小さい場合での、モバイルノードに対するアクセスリンク IP フラグメンテーションを設定します。
- **df-fragment-and-icmp-notify**：パケットがフラグメント化されている場合に DF ビット設定を部分的に無視します。また、パケットに対して DF ビットが設定されている場合でも、送信元に ICMP 到達不能エラーを送信します。
- **df-ignore**：パケットがフラグメント化されている場合に DF ビット設定を無視します。これはデフォルト値です。
- **normal**：通常のフラグメンテーションプロセスを設定します。
- **default**：デフォルト値は **df-ignore** に設定されます。

APN レベルのアクセスリンク IP フラグメンテーションの設定

APN コンフィギュレーション モードでアクセスリンクの IP フラグメンテーションを設定するには、次の設定コマンドを使用します。

```
configure
  context context_name
    apn apn_name
      [ no ] access-link ip-fragmentation { df-fragment-and-icmp-notify
 | df-ignore | normal }
      end
```

（注） **no** オプションが APN 設定に導入され、**default** オプションは廃止されました。

注：

- **access-link ip-fragmentation**：リンク MTU がパケット長よりも小さい場合での、モバイルノードに対するアクセスリンク IP フラグメンテーションを設定します。
- **df-fragment-and-icmp-notify**：パケットがフラグメント化されている場合に DF ビット設定を部分的に無視します。また、パケットに対して DF ビットが設定されている場合でも、送信元に ICMP 到達不能エラーを送信します。
- **df-ignore**：パケットがフラグメント化されている場合に DF ビット設定を無視します。
- **normal**：通常のフラグメンテーションプロセスを設定します。

APN MTU を適用するためのアクセスリンク Fastpath の設定

ダウンリンク SGi IP パケットは、GTP トンネルを介して送信される前にフラグメント化される場合があります。パケットサイズと GTP トンネルカプセル化が APN MTU サイズ以下の場合、パケットはフラグメント化されません。パケットサイズおよび GTP トンネルカプセル化が APN MTU サイズよりも大きい場合、パケットはフラグメント化されて GTP トンネルを介

して送信されます。パケットは、内部パケットまたは外部パケットのいずれかでフラグメント化されます。グローバルレベルの設定では、フラグメントされていないパケットを受信すると、VPP 対応プラットフォームは強制的に外部パケットのフラグメンテーションを実行します。

fastpath にアクセスリンクして IPv4 トラフィックで APN MTU を適用するには、次の設定コマンドを使用します。

```
configure
   [ no ] access-link fastpath apn-ppp-mtu-enforce
   end
```

注：

- **access-link fastpath apn-ppp-mtu-enforce**：VPP ベースの fastpath IPv4 データストリームに APN MTU を適用します。



（注） 設定後、新たに作成されたベアラーは新しく設定された値に設定されます。ただし、この設定が原因で進行中のベアラートラフィックが影響を受けることはありません。**access-link fastpath apn-ppp-mtu-enforce** はデフォルトで無効になっており、VPC-DI プラットフォームではサポートされていません。

モニタリングおよびトラブルシューティング

ここでは、各種 show コマンドとそれらの出力に関する情報を示します。

show コマンドと出力

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show configuration access-link

このコマンドの出力には、次のフィールドが表示されます。

フィールド	説明
access-link ip-fragmentation normal	グローバルレベルで設定されている場合、それぞれの値を表示します。設定が **default** または **df-ignore** に設定されている場合、出力は表示されません。

show configuration access-link verbose

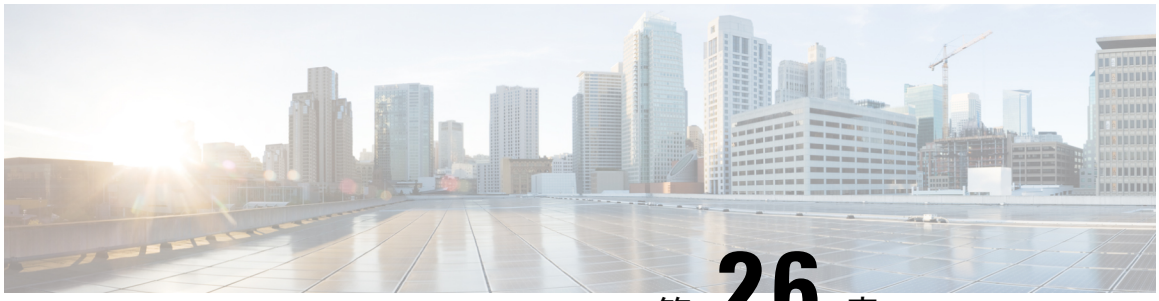
このコマンドの出力には、次のフィールドが表示されます。

フィールド	説明
access-link ip-fragmentation df-ignore	グローバルレベルで設定されている場合、それぞれの値を表示します。設定が **default** または **df-ignore** に設定されている場合、df-ignore が表示されます。

show config apn <apn_name>

このコマンドの出力には、次のフィールドが表示されます。

フィールド	説明
access-link ip-frag: df-ignore (APN-Configured: False)	APN に適用されるアプリケーションロジックを表示します。APN-Configured では、アプリケーションロジックが APN（True）とグローバルレベル（False）のどちらに由来するかを確認します。



第 26 章

Diamproxy ピア接続ステータス監査

- 機能の概要と変更履歴 （463 ページ）
- 機能説明 （463 ページ）
- 機能の仕組み （464 ページ）
- Diamproxy ピア接続ステータス監査の設定 （465 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	ASR 5500
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.3

機能説明

Diameterプロキシ（Diamproxy）とさまざまなエンドポイント用に設定されたピアとの間のTCP接続の状態は、オープンまたはクローズのいずれかです。すべてのピア（またはエンドポイン

ト）のこれらの TCP 接続の状態は、Diamproxy およびクライアント（sessmgrs/aaamgrs）で維持され、Diamproxy を介してこれらのピアとの通信を可能にします。Sessmgrs/aaamgrs の接続ステータスがアイドルで、Diamproxy がオープン状態の場合、Diameter メッセージングは失敗し、コールが失敗することが確認されます。これが、監査メカニズムと自動修正が必要であり、有用である主な理由です。

ネットワークの状態によっては、接続状態がランダムに変化することがあります。この変更が適切に伝達されない場合、クライアントで接続状態に関する不一致が発生する可能性があります。同様に、新しいピアが設定されると、クライアントは、Diamproxy への PIN ピアメッセージを開始して、新しいピアの設定を通知します。Diamproxy で行われるスロットリングにより、一部の PIN ピアメッセージがドロップされます。これによっても、クライアントで接続状態の不一致が発生する可能性があります。

この機能は、Diamproxy と Diabase クライアント間のピア接続ステータス監査メカニズムによって、これらの不一致を自動検出および自動修正するのに役立ちます。Diamproxy は、すべてのエンドポイントにわたる Diameter ピアの現在の接続ステータスを、登録済みの Diabase クライアントに定期的に公開します（sessmgr/aaamgr タスク）。Diabaseクライアントは、現在の接続ステータスを監査し、接続ステータスに不一致がある場合は修正措置を講じます。

機能の仕組み

この機能の動作の概要を以下に示します。

1. Diamproxy は、sessmgr および aaamgr を使用してエンドポイントピアの接続ステータスの監査プロセスを開始します。
2. ピアの接続ステータスに不一致がある場合、sessmgr と aaamgr は自動修正アクションを開始します。
3. Diamproxy と sessmgr/aaamgr 間でピア接続ステータスの不一致がある場合、事前に定義された時間間隔内に修正されます。
4. 任意のタイプのリカバリイベントやピア接続ステータス監査プロセスの後、起動中にピア接続ステータスの調整で競合状態は発生しません。

以下のいずれかのイベントが発生すると、接続を安定させるために監査が 3 分遅延します。

1. Diamproxy タスクの開始。
2. Diamproxy タスクの再起動。
3. ICSR スイッチオーバー -> シャーシの状態がスタンバイからアクティブに移行。
4. 計画されているカードの移行 -> 移行終了時刻から 3 分後に監査を開始。
5. 計画外のカードの移行 -> Diamproxy タスクの再起動と同じ。

Diamproxy ピア接続ステータス監査の設定

ここでは、この機能をサポートするために使用可能な CLI コマンドについて説明します。

接続ステータスの監査間隔の有効化

接続ステータスの監査間隔を有効にするには、グローバル コンフィギュレーション モードで次の CLI コマンドを使用します。

```
configure
  diameter-proxy conn-audit interval audit_interval
  exit
```

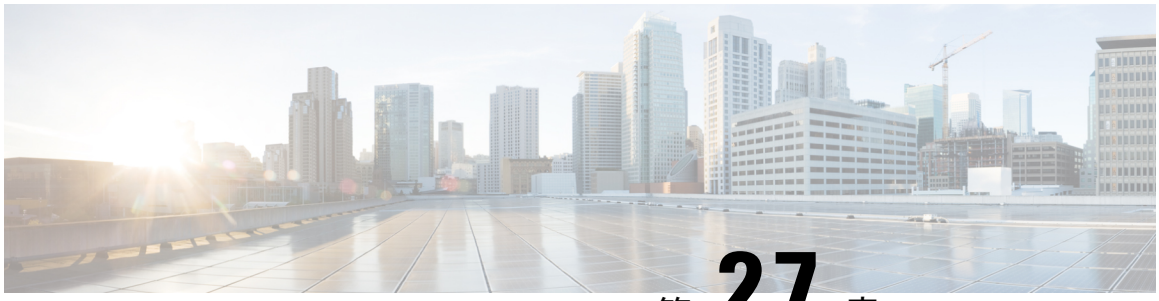
注：

- **diameter-proxy**：Diamproxy 関連の設定を指定します。
- **conn-audit**：定期的な接続ステータスの監査プロセスを指定します。デフォルトでは、無効です。
- **interval** *audit_interval*：接続ステータスの監査間隔を 1 ～ 10 の範囲で分単位で指定します。推奨値は 2 分です。
- すでに設定されている場合は、**default diameter-proxy conn-audit** CLI コマンドを使用すると、Diabase クライアントで Diamproxy ピア接続ステータス監査を無効にできます。
- Diabase クライアントで Diamproxy ピア接続ステータス監査を有効にすると、Diameterインターフェイスを使用するサービスのパフォーマンスに影響する可能性があります。

Diamproxy ピア接続ステータス監査の確認

次の CLI コマンドを使用して、すべての Diameter ピアで接続のステータスが 同期中であるかどうかを確認します。

- **show diameter peers full debug**



第 27 章

4G（LTE）ネットワークのダイレクトトンネル

この章では、パケット データ トラフィックを最適化するための 4G（LTE）ネットワークの S12 インターフェイスを介したダイレクトトンネル（DT）機能のサポートについて手短に説明します。

ダイレクトトンネルをサポートする Cisco LTE デバイス（3GPP TS 23.401 v8.3.0 準拠）には、以下が含まれます。

- サービング GPRS サポートノード（S4-SGSN）
- サービングゲートウェイ（S-GW）
- PDN ゲートウェイ（P-GW）

重要 ダイレクトトンネルは、ライセンスが必要なシスコの機能です。設定するには、個別の機能ライセンスが必要です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

この章で説明する内容は、次のとおりです。

- 4G ネットワークのダイレクトトンネル：機能説明 （467 ページ）
- 機能の仕組み （470 ページ）
- ダイレクトトンネルのサポートの設定 （496 ページ）
- ダイレクトトンネルのモニタリングと障害対応 （500 ページ）

4G ネットワークのダイレクトトンネル：機能説明

高速パケットアクセス（HSPA）および IP マルチメディア サブシステム テクノロジーにより、今後数年間でユーザープレーンデータの量が大幅に増加します。RNC と S-GW 間のユーザー

プレーンデータのダイレクトトンネリングを使用して、UMTS システムアーキテクチャを拡張することにより、より高いトラフィックレートをサポートできます。

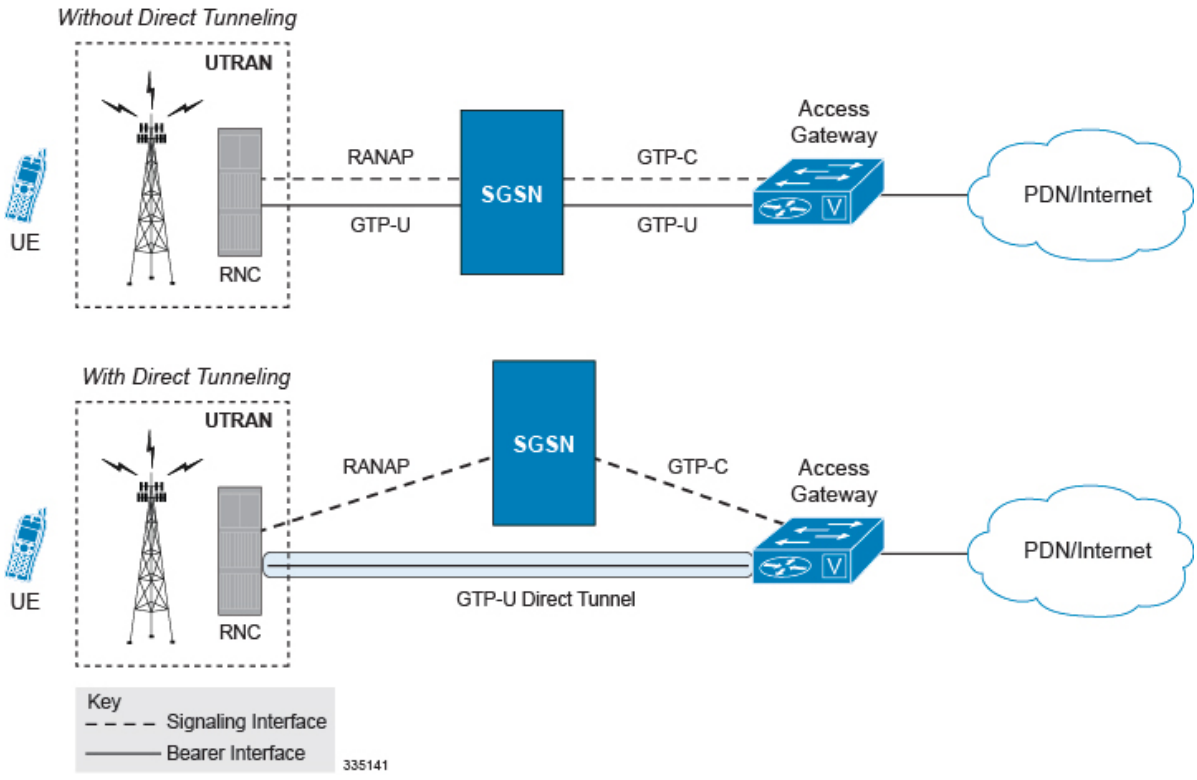
ダイレクトトンネル（DT）は、UE に影響を与えずにコアアーキテクチャを最適化し、LTE/SAE アーキテクチャとは別個に導入できるソリューションを実現します。

重要 ダイレクトトンネルは、ライセンスが必要なシスコの機能です。設定するには、個別の機能ライセンスが必要です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

重要 ダイレクトトンネルの確立は SGSN によって制御されます。4G ネットワークの場合、確立には、S4 ライセンス対応 SGSN セットアップと、S4-SGSN としての設定が必要です。

ダイレクトトンネルが確立されると、S4-SGSN/S-GW は、コントロールプレーン（RANAP/GTP-C）シグナリングを引き続き処理し、PDP コンテキストのアクティブ化でダイレクトトンネルを確立する決定をその後も処理します。

図 17 : GTP-U ダイレクトトンネリング

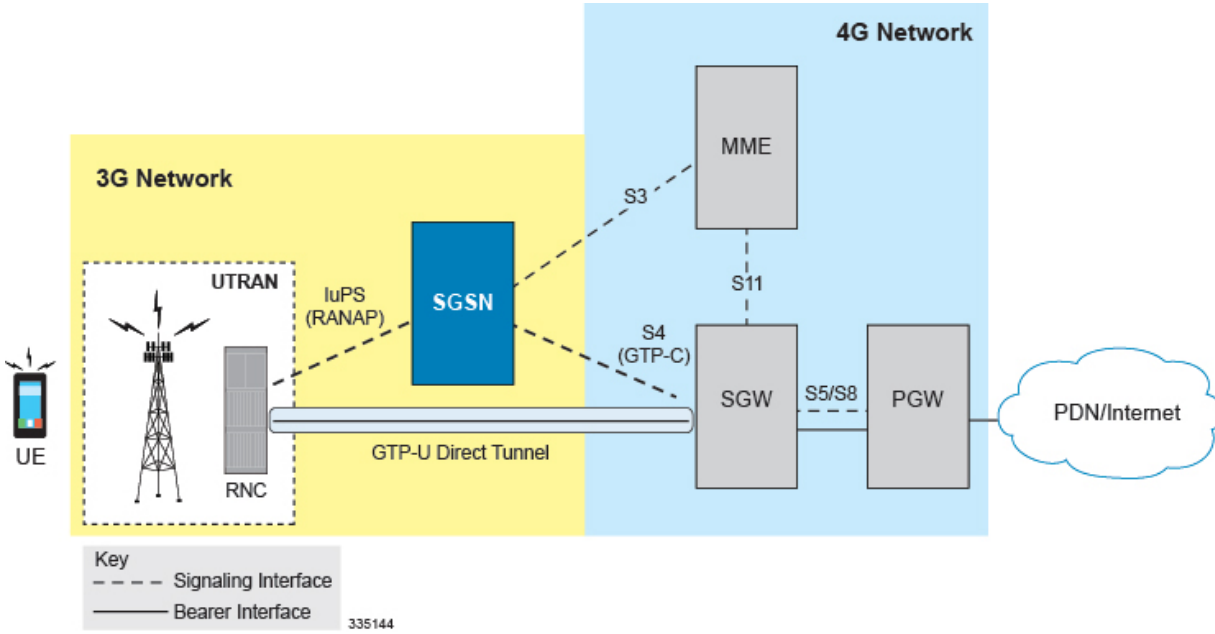


ダイレクトトンネルでは、ユーザープレーンからのスイッチング遅延を排除することで、ユーザーエクスペリエンスが向上します（たとえば、Web ページの迅速な配信、会話型サービスの

ラウンドトリップ遅延の短縮など）。他の利点として、ダイレクトトンネル機能では、S4-SGSN/S-GW からユーザープレーン処理を処理するための要件を削除することにより、ユーザープレーンリソース（およびハードウェア）の使用率を向上させる最適化機能が導入されています。

ダイレクトトンネルは、S-GW へのベアラー作成応答またはベアラー変更要求を使用して、S4-SGSN が S12 インターフェイス経由で RNC と S-GW 間のユーザープレーントンネル（GTP-U トンネル）を直接確立する際に、PDP コンテキストのアクティブ化で実現されます。

図 *18*：ダイレクトトンネリング：*LTE* ネットワーク、*S12* インターフェイス



ダイレクトトンネルを展開した場合の主な結果として、パケットコアの SGSN/S-GW コンポーネントと GGSN/P-GW コンポーネントの両方で、コントロールプレーンの負荷が大幅に増加します。その結果、GGSN/P-GW への PDP コンテキスト更新メッセージの量と頻度が大幅に増加するため、展開には拡張性の高い GGSN/P-GW が必要です。SGSN/S-GW プラットフォームの機能により、コントロールプレーンのキャパシティがダイレクトトンネル展開の制限要因にならないことが保証されます。

S4-SGSN は、以下に示すシナリオで、RNC と S-GW 間の GTP-U ダイレクトトンネルの確立をサポートします。

- プライマリ PDP のアクティブ化
- セカンダリ PDP のアクティブ化
- サービス要求の手順
- S-GW の変更を伴わない内部 SGSN ルーティングエリア更新
- S-GW の変更を伴う内部 SGSN ルーティングエリア更新
- S-GW の変更を伴わない内部 SGSN SRNS 再配置
- S-GW の変更を伴う内部 SGSN SRNS 再配置
- S-GW の変更を伴う新規 SGSN SRNS 再配置

- S-GW 再配置なしの新規 SGSN SRNS 再配置
- 間接データ転送トンネル用 S12U FTEID のアプリケーションも使用した E-UTRAN 発 UTRAN 着 Iu モード IRAT ハンドオーバー
- 間接データ転送トンネル用 S12U FTEID のアプリケーションも使用した UTRAN 発 E-UTRAN 着 Iu モード IRAT ハンドオーバー
- ネットワーク開始 PDP のアクティブ化

Gn インターフェイスを使用する 2G または 3G SGSN のダイレクトトンネリングと比較して、DT が有効な場合の S4-SGSN では下記のシナリオの相違が生じます。

- RAB リリース
- Iu リリース
- RNC からのエラー通知
- S-GW からのダウンリンクデータ通知
- S-GW からのダウンリンクデータエラーの通知
- MS 開始 PDP の変更
- UE が IDLE の場合の P-GW 開始 PDP の変更
- HLR/HSS 開始 PDP の変更
- ダイレクトトンネルによるセッションリカバリ

上記のシナリオは、ダイレクトトンネルが確立された場合の S4-SGSN での手順の相違を示しています。

機能の仕組み

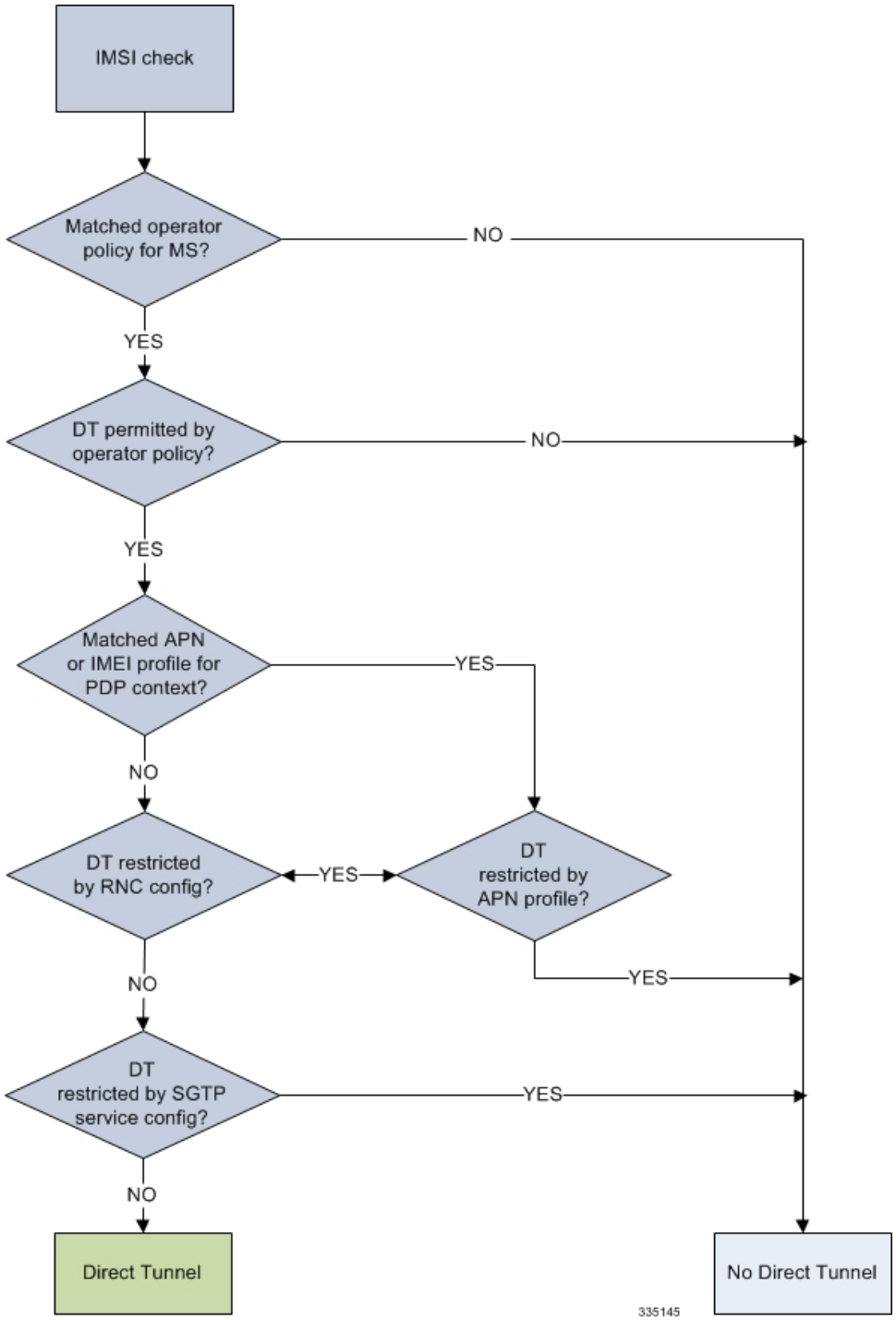
DT 機能により、PS ドメイン内の RNC と SGW 間のダイレクト ユーザー プレーン トンネルが有効になります。ダイレクトトンネリングを使用して、S4-SGSN は RNC に S-GW の TEID とユーザープレーンアドレスを提供し、また S-GW に RNC の TEID とユーザープレーンアドレスを提供します。

SGSN はコントロール プレーン シグナリングを処理し、RNC と S-GW の間にダイレクトトンネルをいつ確立するのかを決定します。または、この目的のために（設定に基づいて）2 つのトンネルをいつ使用するのかを決定します。

ダイレクトトンネル確立ロジック

次の図は、ダイレクトトンネルがセットアップされるかどうかを決定するために S4-SGSN/S-GW 内で使用されるロジックを示しています。

図 *19 :* ダイレクトトンネリング：確立ロジック



ダイレクトトンネルの確立

S4-SGSN は、DT に S12 インターフェイスを使用します。

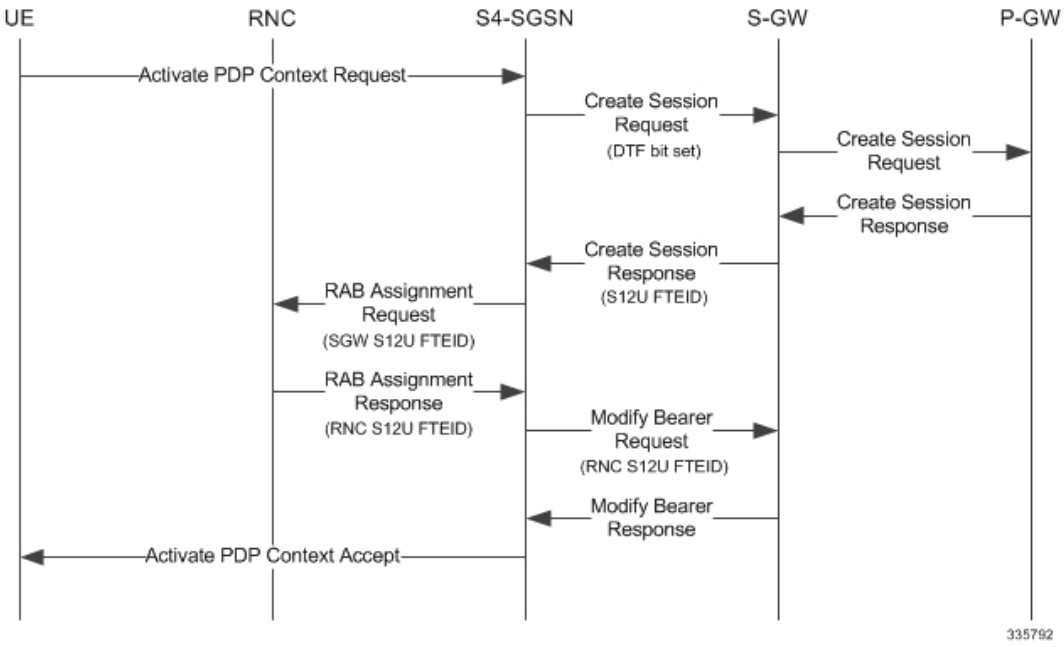
プライマリ PDP コンテキストのダイレクトトンネルアクティブ化

PDP コンテキストのアクティブ化手順で、このソリューションは、TS 29.274 で定義されている GPRS トンネリングプロトコル v2（GTPv2）の新しい情報要素（IE）を使用します。SGSN は、次の図に示すように、RNC および S-GW のユーザープレーンアドレスを S12U FTEID として提供します。

PDP のアクティブ化中に、RNC と S-GW 間にダイレクトトンネルを確立するための手順は次のとおりです。

- SGSN は、指示フラグ DTF（ダイレクトトンネルフラグ）ビットが設定されたセッション作成要求を S-GW に送信します。
- セッション作成応答で、S-GW は、SGSN に S12U FTEID（完全修飾トンネル エンドポイント識別子）を送信します。
- SGSN は、RAB 割り当て要求中に S-GW S12U を RNC に転送します。
- RAB 割り当て応答で、RNC は、トランスポートアドレスとトンネルエンドポイント ID（TEID）を SGSN に送信します。
- SGSN は、ベアラー変更要求で RNC S12 U FTEID を S-GW に転送します。

図 *20 :* ダイレクトトンネルを使用したプライマリ *PDP* のアクティブ化



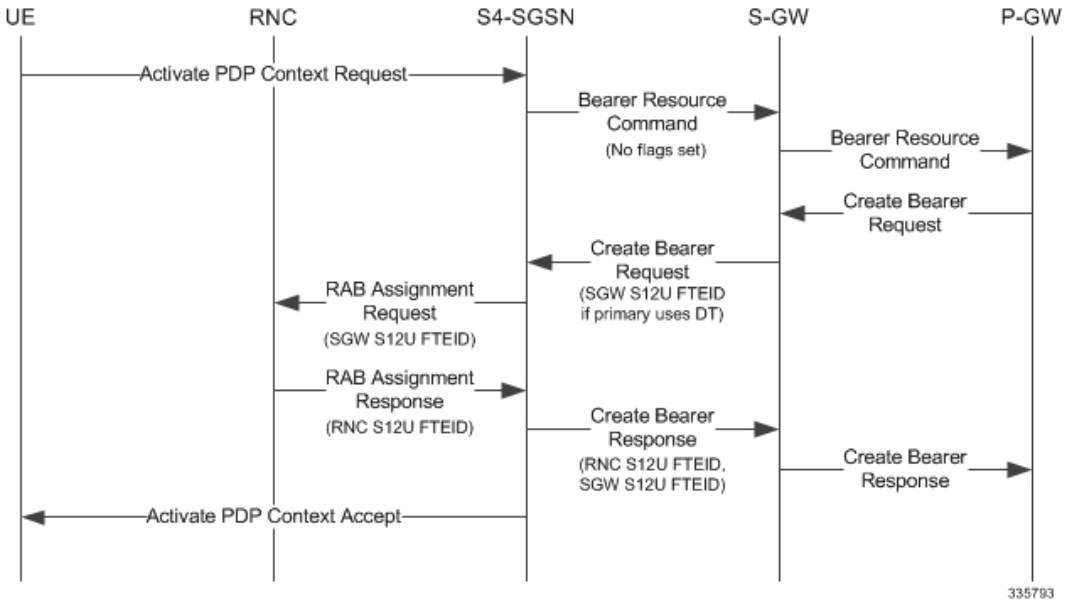
UE によって開始されたセカンダリ PDP コンテキストのダイレクトトンネル有効化

次に、セカンダリ PDP コンテキストアクティブ化のためのダイレクトトンネルを確立する一般的なシーケンスを示します。

- SGSN は、フラグが設定されていない S-GW にベアラーリソースコマンドを送信します。（S-GW は、ダイレクトトンネルがプライマリに対して有効になっていることをすでに認識しています）。

- S-GW は、S12U FTEID を含むベアラー作成応答を SGSN に送信します。
- SGSN は、RAB 割り当て要求を介して S-GW S12U を RNC に転送します。
- RAB 割り当て応答で、RNC は、そのトランスポートアドレスと TEID を SGSN に送信します。
- SGSN は、RNC から受信した S12U TEID を、ベアラー作成応答を介して S-GW に転送します。

図 *21* : ダイレクトトンネルを使用したセカンダリ *PDP* のアクティブ化



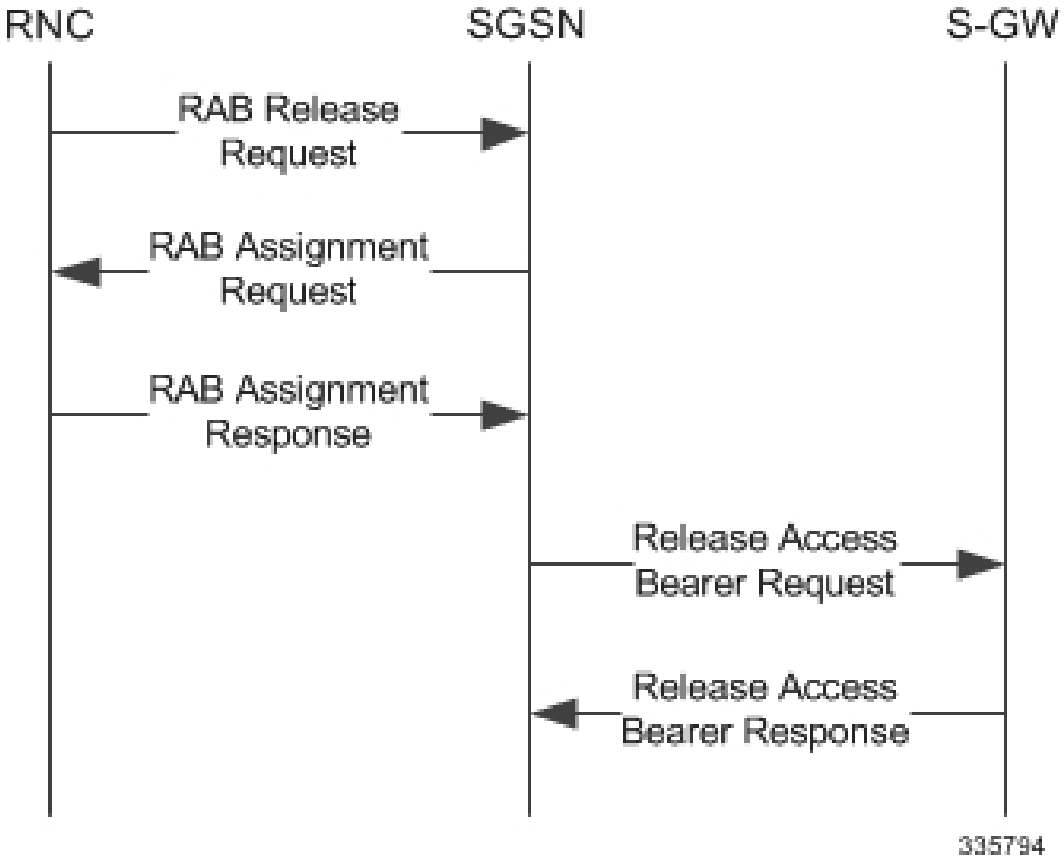
ダイレクトトンネルによる RAB リリース

SGSN は、ダイレクトトンネルでアクティブ化されたベアラーコンテキストの RNC から RAB リリース要求を受信すると、ベアラーアクセスリリース要求を S-GW に送信します。

S-GW は、ベアラーアクセスリリース要求を受信すると S12 U RNC FTEID を削除します。ダウンリンクデータが検出された場合、S-GW はデータを転送するためのユーザープレーン FTEID がないため、ダウンリンクデータ通知を送信します。

ストリーミングクラスまたは会話クラスのベアラーは、非アクティブにする必要があるため、ベアラーアクセスリリース要求に含まれません。ただし、S4-SGSN は現在、RAB リリース時のストリーミング/会話ベアラーの非アクティブ化をサポートしていません。

図 *22:* ダイレクトトンネルを使用した *RAB* のリリース手順



重要 通信事業者は、S4-SGSN で会話クラスまたはストリーミングクラスのベアラーを使用しないでください。

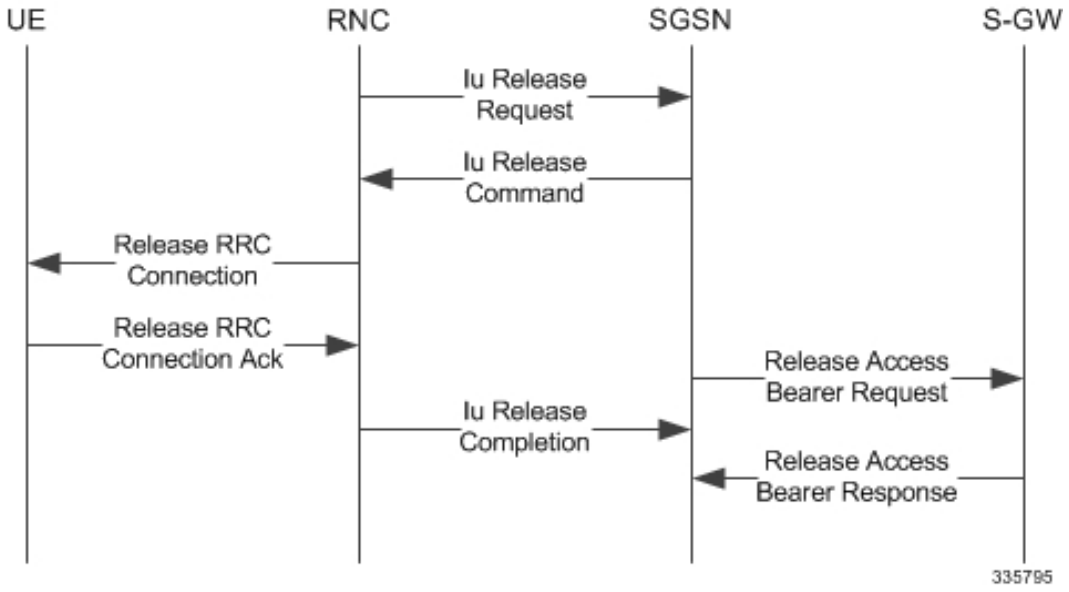
ダイレクトトンネルによる IU リリース

SGSN は、Iu リリースを受信し、ベアラーがダイレクトトンネリングでアクティブ化されると、ベアラーアクセスリリース要求を S-GW に送信します。

ストリーミングクラスまたは会話クラスのベアラーは、非アクティブにする必要があるため、ベアラーアクセスリリース要求に含まれません。ただし、S4-SGSN は現在、Iu リリース時のストリーミングまたは会話ベアラーの非アクティブ化をサポートしていません。

重要 通信事業者は、S4-SGSN で会話クラスまたはストリーミングクラスのベアラーを使用しないでください。

図 *23 :* ダイレクトトンネルを使用した *Iu* のリリース手順

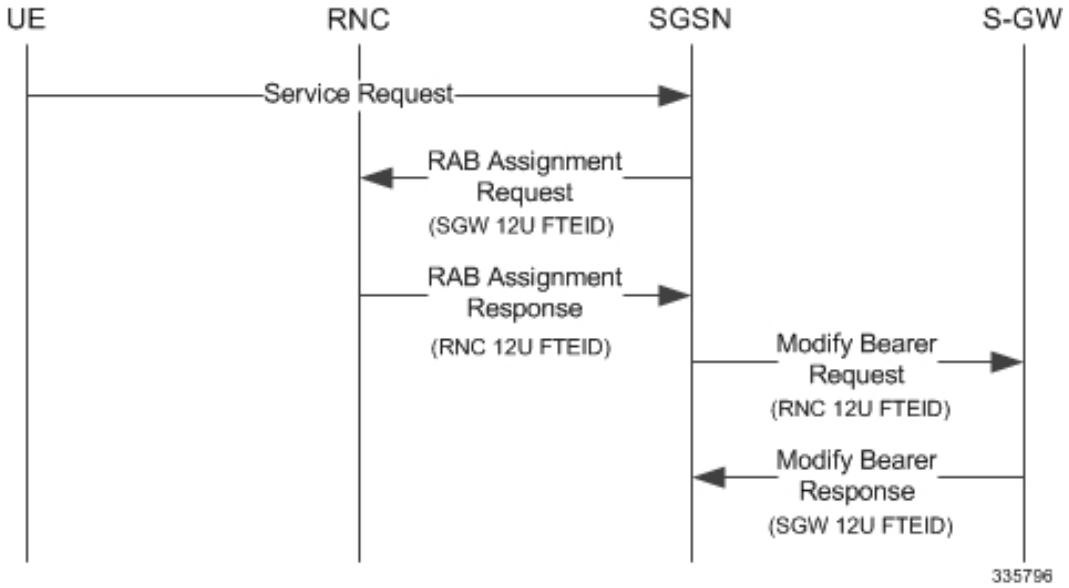


ダイレクトトンネルによるサービス要求

UEがアイドル状態で、データまたはシグナリング接続を確立する必要がある場合、UEはデータのサービス要求を送信します。また、UE は、SGSN からページングされたときに、サービス要求を SGSN に送信することもできます。

SGSNは、データのサービス要求を受信すると、RABを確立し、RNCから受信した12U FTEIDを使用して、S-GW にベアラー変更要求を送信します。

図 *24 :* ダイレクトトンネルを使用したサービス要求手順



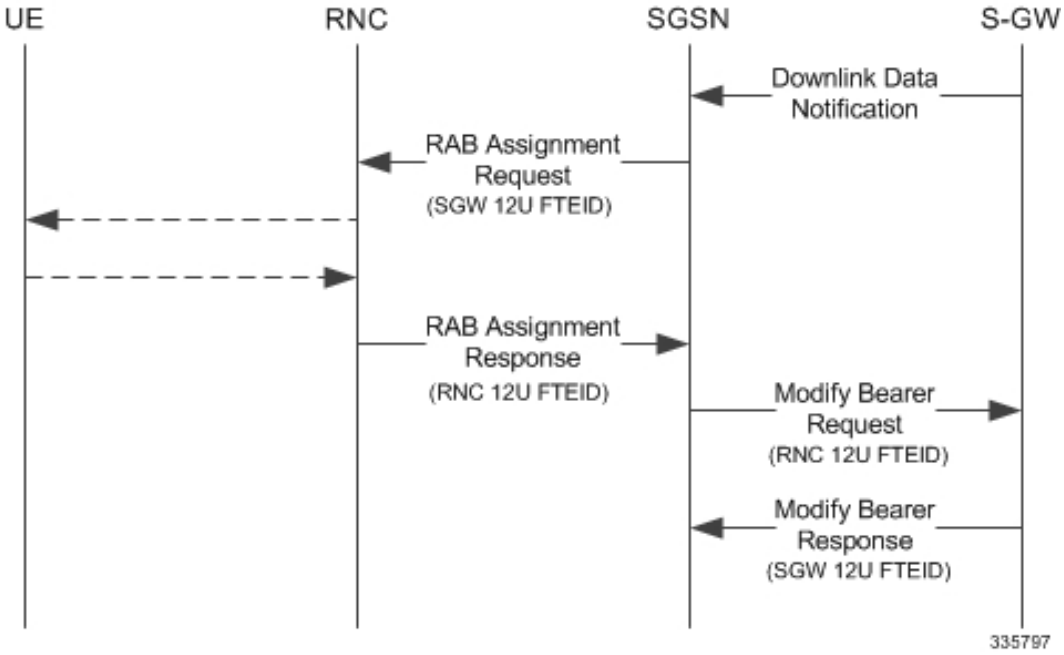
UE が接続状態のときのダイレクトトンネルによるダウンリンクデータ通知

RAB がリリースされると（ただし UE は SGSN との Iu 接続を維持します）、SGSN は S-GW に、アクセスベアラーリリース要求を介して RNC 側 TEID をリリースするように通知します。

S-GW は、アクセスベアラーリリース要求の受信後にダウンリンク GTPU データを P-GW から受信した場合、そのデータの転送先である RNC TEID も SGSN ユーザープレーン TEID も認識していません。そのため、RAB を確立するように SGSN に信号を送信します。このシグナリングメッセージは、S-GW からのダウンリンクデータ通知メッセージです。

S-GW からのダウンリンクデータ通知が受信されると、欠落しているすべての RAB が確立され、ベアラー変更要求が RNC S12U FTEID で S-GW に送信されます。

図 *25 :* ダイレクトトンネルを使用したダウンリンクデータ通知

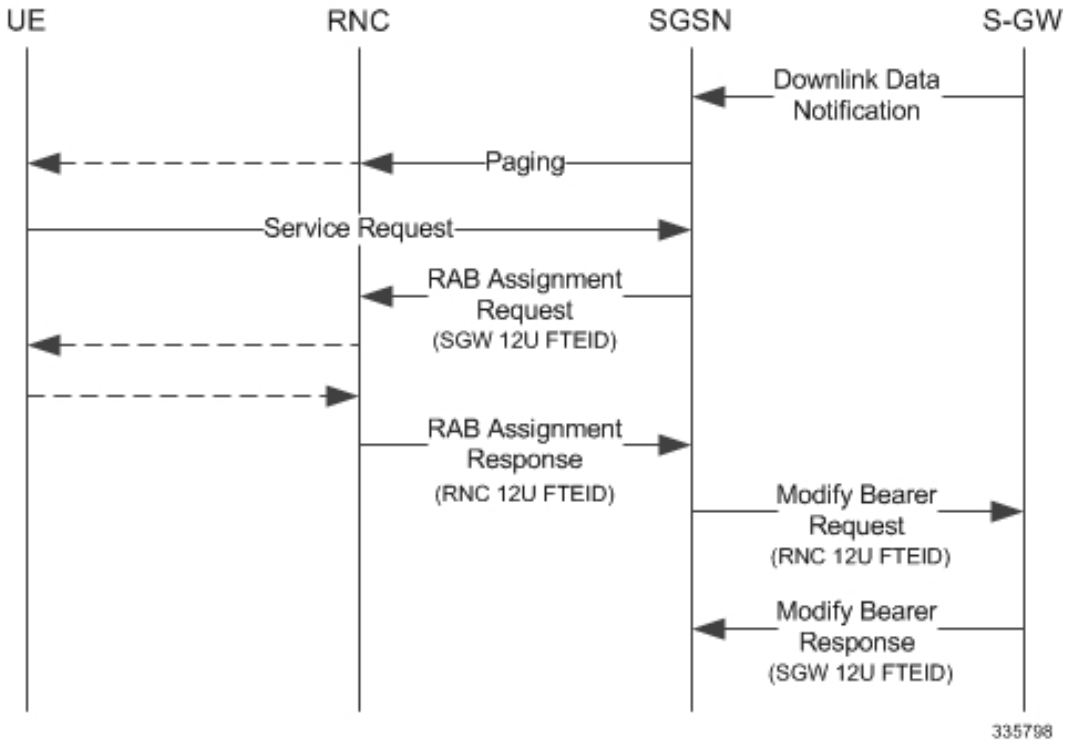


UE がアイドル状態のときのダイレクトトンネルによるダウンリンクデータ通知

IU が解放されると、UE は IDLE になります。SGSN は、アクセスベアラー解放要求を送信して、RNC 側 TEID を解放するように S-GW に通知します。この時点以降に S-GW が P-GW からダウンリンク GTPU データを受信しても、S-GW では、そのデータの転送先である RNC TEID や SGSN ユーザープレーン TEID が分かりません。

S-GW がアクセスベアラー解放要求の受信後にダウンリンク GTPU データを受信しても、S-GW では、そのデータの転送先である RNC TEID や SGSN ユーザープレーン TEID が分かりません。そのため、RAB を確立するように SGSN に信号を送信します。このシグナリングメッセージは、S-GW からのダウンリンクデータ通知です。UE がアイドル状態のときに S-GW からダウンリンクデータ通知を受信した場合、SGSN は RAB を確立する前に UE をページングします。SGSN は、RNC S12U FTEID で S-GW にベアラー変更要求を送信します。

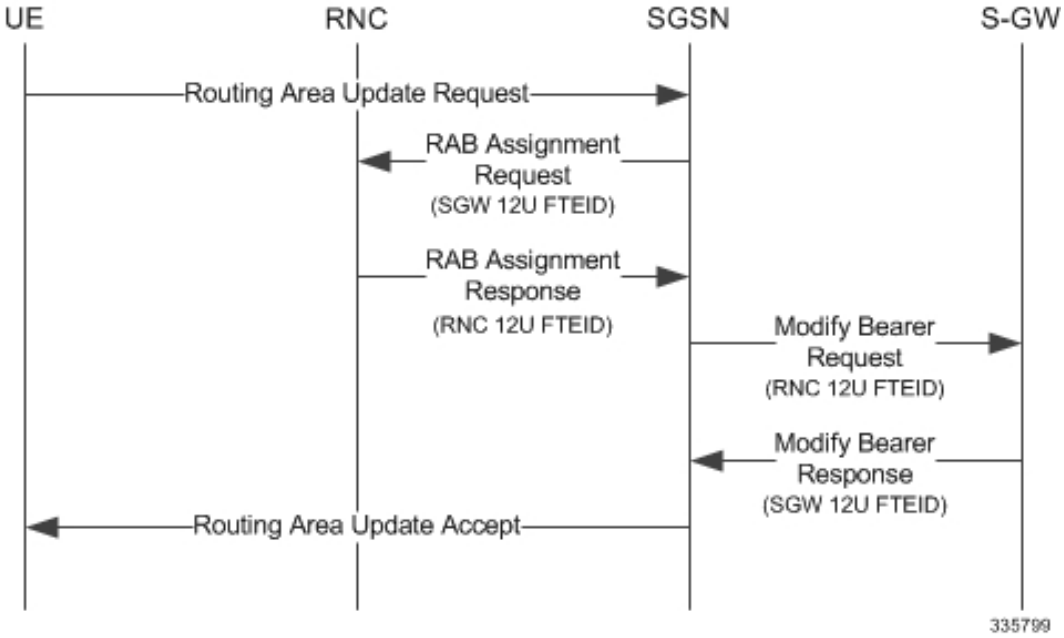
図 *26 : UE* がアイドル状態の場合のダウンリンクデータ通知



S-GW の変更を伴わない内部 SGSN ルーティングエリアの更新

ダイレクトトンネルを使用したS-GWの変更を伴わないルーティングエリアの更新では、SGSN が RNC FTEID を使用して S-GW にベアラー変更要求を送信します。SGSN は、送信元 RNC に RAB が存在していた場合にのみ、宛先 RNC との RAB を確立します。

図 *27 : S-GW* の変更を伴わないルーティングエリア更新の手順



S-GW の変更を伴わないルーティングエリア更新の詳細な動作を次の表に示します。

表 *41 : S-GW* の変更を伴わないルーティングエリア更新の動作表

シナリオ	以前の RNC ステータス	以前の RNC RAB	以前の RNC DT ステータス	PLMN の変更	新しい RNC DT ステータス	S-GW の変更	SGSN アクション
内部 RAU	なし	RAB なし	サポート対象	なし	サポート対象	なし	新しい RNC との RAB は確立されません。S-GW へのベアラー変更要求はありません
内部 RAU	あり	RAB なし	サポート対象	なし	サポート対象	なし	新しい RNC との RAB は確立されません。S-GW へのベアラー変更要求はありません

シナリオ	以前の RNC ステータス	以前の RNC RAB	以前の RNC DT ステータス	PLMN の変更	新しい RNC DT ステータス	S-GW の変更	SGSN アクション
内部 RAU	あり	一部の RAB	サポート対象	いずれも可	サポート対象	なし	現在の RAB のみ確立されます。変される RAB のあベアラーを使用MBR が S-GW に信され、残りは無されます。RAB のいベアラーは、R後に非アクティブなります。PLMN変更された場合、MBR は新しい PLMN ID を伝送す。
内部 RAU	なし	RAB なし	サポート対象	あり	サポート対象	なし	新しい RNC との RAB は確立されん。MBR は PLMのみが変更されて信されます。ベラーコンテキスト TEID を伝送しません。
内部 RAU	あり	RAB なし	サポート対象	あり	サポート対象	なし	同上。
内部 RAU	なし	RAB なし	未サポート	なし	サポート対象	なし	新しい RNC との RAB は確立されん。DTF が設定れ、ユーザー FT のないベアラー変要求が S-GW に送されます。
内部 RAU	あり	RAB なし	未サポート	なし	サポート対象	なし	同上。

シナリオ	以前の RNC ステータス	以前の RNC RAB	以前の RNC DT ステータス	PLMN の変更	新しい RNC DT ステータス	S-GW の変更	SGSN アクション
内部 RAU	あり	一部の RAB	未サポート	いずれも可	サポート対象	なし	現在の RAB のみが確立されます。変更される RAB のあるベアラーを使用して MBR が S-GW に送信され、残りは解放されます。RAB のないベアラーは、RAU 後に非アクティブになります。PLMN が変更された場合、MBR は新しい PLMN ID を伝送し、ベアラーを変更します。
内部 RAU	なし	RAB なし	未サポート	あり	サポート対象	なし	新しい RNC との RAB は確立されません。MBR は PLMN のみが変更されて送信されます。ダウンリンクデータ通知を受信すると、SGSN はページング/サービス要求/RAB の確立を行います。
内部 RAU	あり	RAB なし	未サポート	あり	サポート対象	なし	同上。
内部 RAU：**新しい RNC はダイレクトトンネルをサポートしていません。S-GW の再配置はありません**							
内部 RAU	なし	RAB なし	サポート対象	いずれも可	未サポート	なし	新しい RNC との RAB は確立されません。SGSN は、S4U TEID を付けて S-GW にベアラー変更要求を送信します。PLMN ID に変更がある場合は、新しい PLMN ID が伝送されます。

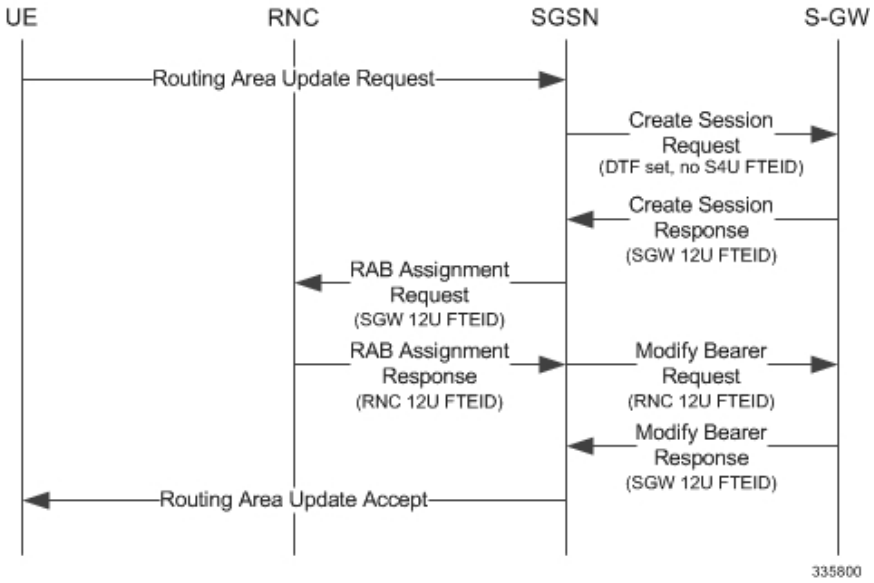
シナリオ	以前の RNC ステータス	以前の RNC RAB	以前の RNC DT ステータス	PLMN の変更	新しい RNC DT ステータス	S-GW の変更	SGSN アクション
内部 RAU	あり	RAB なし	サポート対象	いずれも可	サポート対象外	なし	同上。
内部 RAU	あり	一部の RAB	サポート対象	いずれも可	サポート対象外	なし	現在の RAB のみ確立されます。S TEID を持つすべのベアラーで M がS-GW に送信ます。PLMN ID 更がある場合は、しい PLMN ID が送されます。

S-GW の変更を伴うルーティングエリア更新

S-GW の変更を伴うルーティングエリア更新では、SGSN は、DTF フラグが設定され、ユーザープレーン FTEID がないセッション作成要求を送信します。そのセッション作成応答で、S-GW は S12U FTEID を送信し、それが RAB 割り当て要求を介して RNC に転送されます。

SGSN は、RAB Assignment Response で受信した RNC FTEID を、ベアラー変更要求で S-GW に送信します。内部 SGSN RAU では、考慮すべき多くのシナリオがあります。

図 *28 : SGW* の変更を伴うルーティングエリア更新の手順



次の表に、S-GW の変更を伴うルーティングエリア更新の詳細な動作を示します。

表 *42 : S-GW* の変更を伴うルーティングエリア更新の動作表

シナリオ	以前の RNC ステータス	以前の RNC RAB	以前の RNC DT ステータス	PLMN の変更	新しい RNC DT ステータス	S-GW の変更	SGSN アクション
内部 RAU：両方の **RNC** がダイレクトトンネルをサポートする。**SGW** の再配置							
内部 RAU	Not Present	RAB なし	サポート対象	いずれも可	サポート対象	[はい（Yes）]	DTF フラグ付き、S4U/S12U FTEID なしで CSR 要求を新しい S-GW に送信します。S-GW は、自身の S12U TEID を送信します。これは、SGSN が DP のリモート TEID の一部として格納します。新しい RNC との間で RAB が確立されないため、SGSN は S-GW への MBR 要求を開始しません。その後、S-GW がダウンリンクデータを取得すると、SGSN は DDN を取得して RAB を確立し、MBR を送信します。
内部 RAU	あり	RAB なし	サポート対象	いずれも可	サポート対象	[はい（Yes）]	同上。

シナリオ	以前の RNC ステータス	以前の RNC RAB	以前の RNC DT ステータス	PLMN の変更	新しい RNC DT ステータス	S-GW の変更	SGSN アクション
内部 RAU	あり	一部の RAB	サポート対象	いずれも可	サポート対象	[はい（Yes）]	DTF フラグ付き S4U/S12U FTEID しで CSR 要求を しい S-GW に送信 ます。S-GW は自 の S12U TEID を通 します。現在の E が、新しい RNC の間で確立されて す。MBR は、こ らの現在の RAB のみ開始され、残 のベアラーが削除 れます。
内部 RAU：古い RNC がダイレクトトンネルをサポートしない。SGW の再配置							
内部 RAU	Not Present	RAB なし	未サポート	いずれも可	サポート対象	[はい（Yes）]	DTF フラグ付き S4U/S12U FTEID しで CSR 要求を しい S-GW に送信 ます。S-GW は、 身の S12U TEID を 信します。これに SGSN が DP のリ モート TEID の一 として格納しま 新しい RNC との で RAB が確立さ ないため、SGSN S-GW への MBR 求を開始しませ その後、S-GW が ウンリンクデータ 取得すると、SG は DDN を取得し RAB を確立して MBR を送信しま す。
内部 RAU	present	RAB なし	未サポート	いずれも可	サポート対象	[はい（Yes）]	同上。

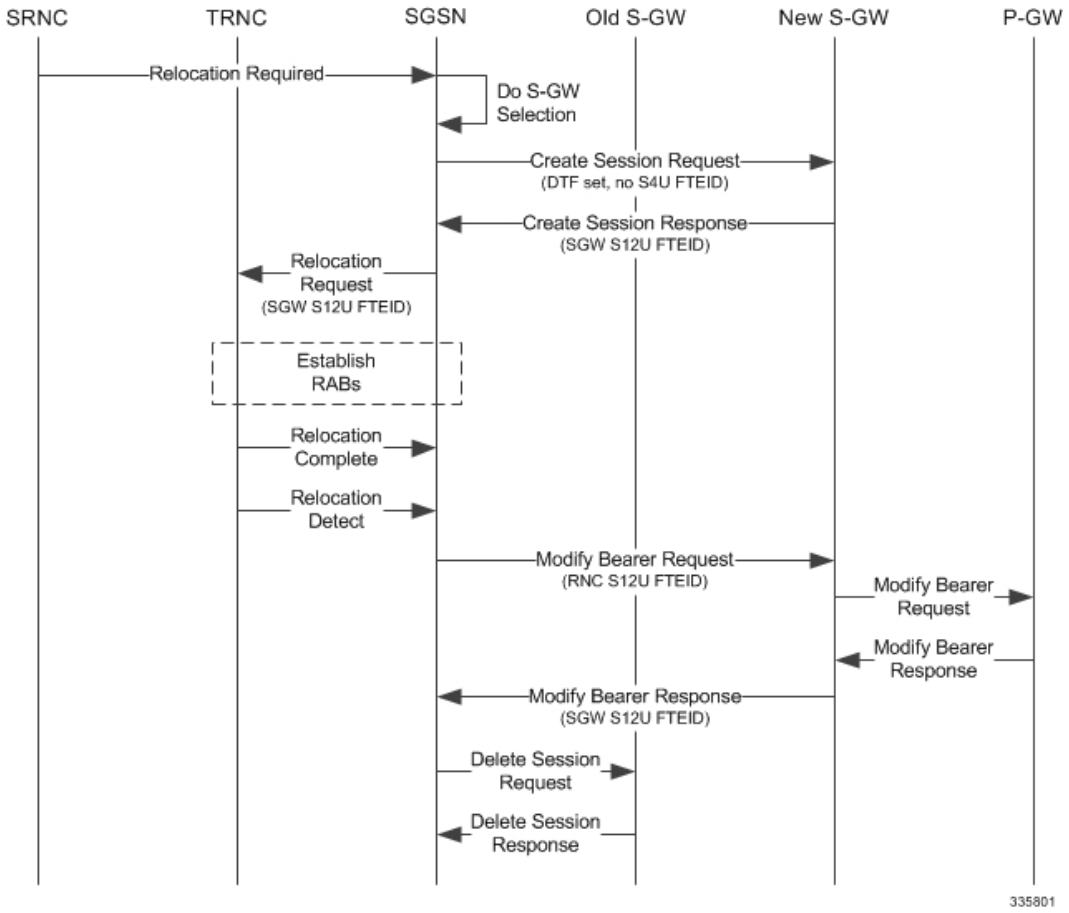
シナリオ	以前の RNC ステータス	以前の RNC RAB	以前の RNC DT ステータス	PLMN の変更	新しい RNC DT ステータス	S-GW の変更	SGSN アクション
内部 RAU	あり	一部の RAB	サポート対象外	いずれも可	サポート対象	[はい（Yes）]	DTF フラグ付き、S4U/S12U FTEID なしで CSR 要求を新しい S-GW に送信します。S-GW は自身の S12U TEID を送信します。現在の RAB が新しい RNC との間で確立され、MBR は現在のこれらの RAB のみで開始されます。残りは削除されるベアラーとなります。
内部 RAU：**新しい RNC はダイレクトトンネルをサポートしていません。SGW の再配置**							
内部 RAU	Not Present	RAB なし	サポート対象	いずれも可	未サポート	はい	DTF フラグなし、S4U FTEID ありの CSR 要求。
内部 RAU	あり	RAB なし	サポート対象	いずれも可	未サポート	はい	DTF フラグなし、S4U FTEID ありの CSR 要求。
内部 RAU	あり	一部の RAB	サポート対象	いずれも可	未サポート	はい	DTF フラグなし、S4U FTEID ありの CSR 要求。PDP の非アクティブ化なし。

S-GW の変更を伴う内部 SRNS

S-GW の変更を伴う内部 SRNS（サービング無線ネットワークサブシステム）では、SGSN は、DTF フラグが設定され、ユーザープレーン FTEID がないセッション作成要求を送信します。新しい S-GW からのセッション作成応答には、SGSN が再配置要求でターゲット RNC に転送する SGW S12U FTEID が含まれます。

SGSN は、ベアラー変更要求で RNC S12U FTEID を新しい S-GW に送信します。

図 *29 : S-GW* の変更を伴う内部 *SRNS*

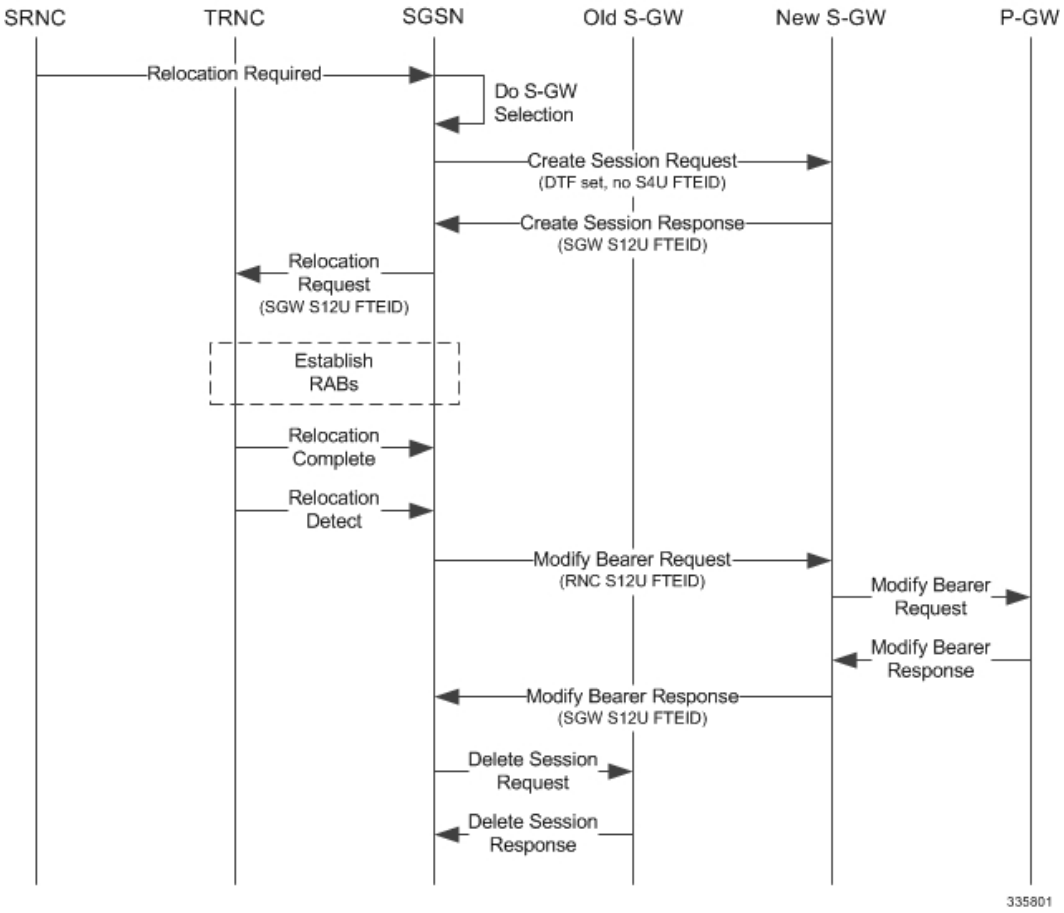


次の表には、内部 SRNS シナリオの詳細な動作が含まれています。

S-GW の変更を伴わない内部 SRNS

S-GW の変更を伴わない内部 SRNS では、再配置要求が SGW S12U FTEID とともに送信されます。受信された RNC S12U FTEID は、ベアラー変更要求で S-GW に転送されます。

図 *30 : S-GW* の変更を伴わない内部 *SRNS*



次の表には、内部 SRNS シナリオの詳細な動作が含まれています。

表 *43 :* 内部 *SRNS* の動作

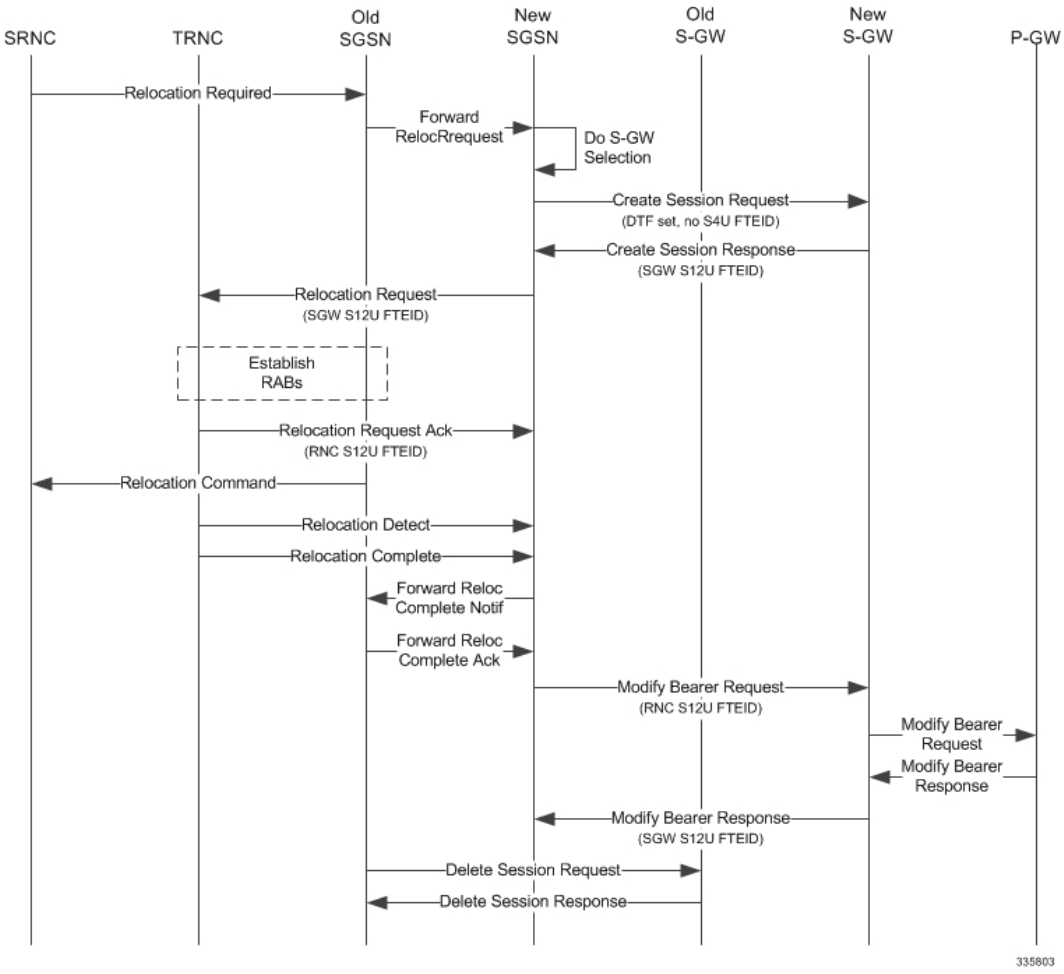
以前の RNC DT ステータス	新しい RNC DT ステータス	S-GW の再配置	動作
サポート対象	サポート対象	非対応	ターゲット RNC への再配置要求が S-GW S12 U FTEID とともに送信されます。S-GW へのベアラー変更要求が RNC S12 U FTEID とともに送信されます。
サポート対象	未サポート	非対応	ターゲット RNC への再配置要求が SGSN S4 U FTEID とともに送信されます。S-GW へのベアラー変更要求が SGSN S4 U FTEID とともに送信されます。
未サポート	サポート対象	非対応	ターゲット RNC への再配置要求が S-GW S12U FTEID とともに送信されます。S-GW へのベアラー変更要求が RNC S12 U FTEID とともに送信されます。

以前の RNC DT ステータス	新しい RNC DT ステータス	S-GW の再配置	動作
未サポート	サポート対象	[はい（Yes）]	新しい S-GW へのセッション作成要求が、DTF フラグが設定され、ユーザープレーン FTEID がない状で送信されます。S-GW が CSR 応答で S4U FTEID 送信した場合でも、SGSN は、それを S12U FTEID して内部的に処理し、再配置を続行します。ターゲット RNC への再配置要求が、セッション作成応答で信した S12 U FTEID とともに送信されます。新しい S-GW へのベアラー変更要求が RNC S12U FTEID もに送信されます。
サポート対象	未サポート	はい	新しい SGW へのセッション作成要求が S4 U FTEI とともに送信されます。ターゲット RNC への再配 要求が SGSN U FTEID とともに送信されます。ベ ラー変更要求が SGSN S4U FTEID とともに送信さ ます。
サポート対象	サポート対象	[はい（Yes）]	SGSN が、新しい SGW に、DTF フラグが設定され ユーザープレーン FTEID がないセッション作成要 を送信します。S-GW が CSR 応答で S4U FTEID を 信した場合でも、SGSN は、それを S12U FTEID て内部的に処理し、再配置を続行します。ターゲッ RNC への再配置要求が、セッション作成応答で受 した S12 U FTEID とともに送信されます。新しい S-GW へのベアラー変更要求が RNC U FTEID とと に送信されます。

S-GW の変更と直接データ転送を伴う新しい SRNS

新しい SGSN は、DTF フラグが設定され、ユーザープレーン FTEID のないセッション作成要求を新しい S-GW に送信します。新しい SGSN は、セッション作成応答で受信した SGW S12U FTEID を再配置要求でターゲット RNC に送信します。新しい SGSN は、再配置要求の確認応答で受信した RNC S12U FTEID をベアラー変更要求で新しい に送信します。

図 *31 : S-GW* の変更とデータ転送を伴う新しい *SRNS*

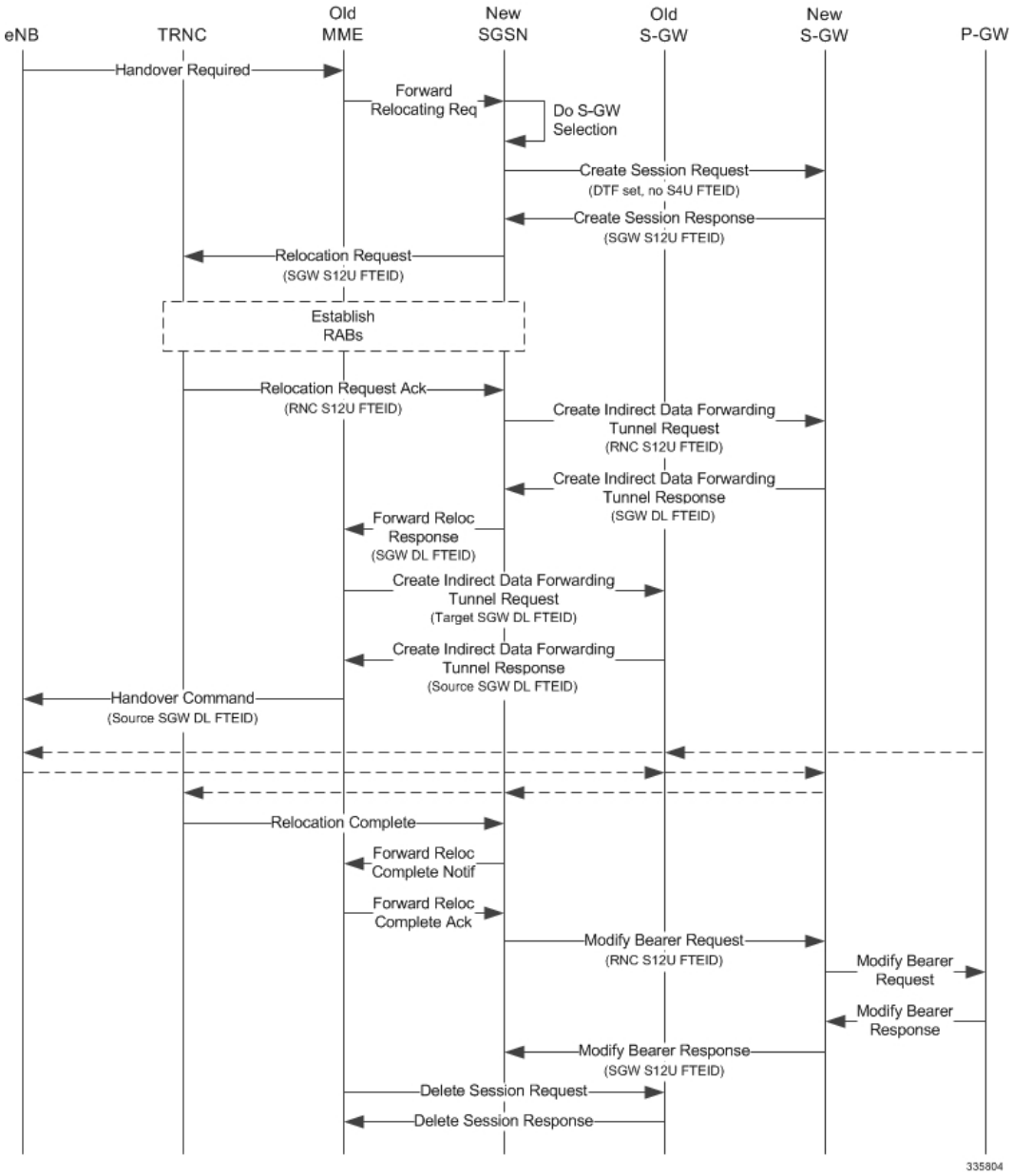


新しい SRNS シナリオの詳細な動作を以下の表に示します。

S-GW の変更と間接データ転送を伴う新しい SRNS

新しい SGSN SRNS 中の間接データ転送（IDFT）は、E-UTRAN から UTRAN への接続モードの IRAT ハンドオーバー中に発生します。コールフローの詳細については、次の図を参照してください。

図 *32 : S-GW* の変更と間接データ転送を伴う新しい *SRNS*



新しい SRNS シナリオの詳細な動作を以下の表に示します。

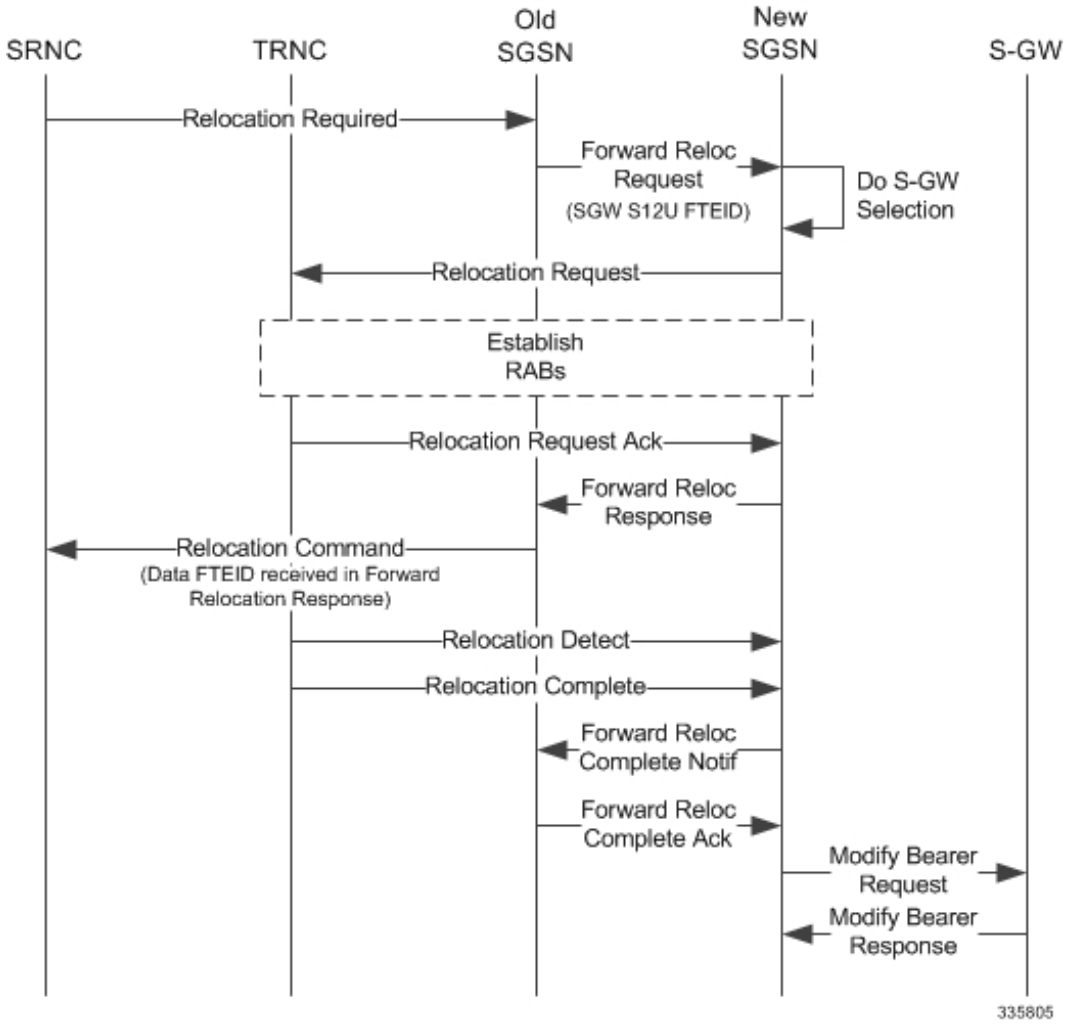
表 *44 :* 新しい *SRNS* の動作

ターゲット RNC DT ステータス	直接転送	S-GW の再配置	動作
サポート対象	非対応	非対応	転送再配置要求で、SGW S12U FTEID を含む再割り当て要求を受信します。SGSN は、転送再配置応答に RNC U FTEID を含めます。RNC U FTEID は、DTF フラグが設定されたベアラー変更要求でも送信されます。
サポート対象	対応	非対応	転送再配置要求で、SGW S12U FTEID を含む再割り当て要求を受信します。転送再配置応答に RNC U FTEID が含まれます。また、ベアラー変更要求で RNC U FTEID が送信され、DTF フラグが設定されます。
サポート対象	非対応	対応	セッション作成要求が、DTF フラグが設定され、ユーザープレーン FTEID がない状態で送信されます。再配置要求が、セッション作成応答で受信した SGW S12U FTEID とともに送信されます。SGW が CSR 応答で S4U FTEID を送信した場合でも、それを S12U FTEID として内部的に処理し、再配置を続行します。間接データ転送トンネル作成要求が、再配置要求確認応答で受信した RNC FTEID とともに送信されます。IDFT 作成応答で受信した SGW DL U FTEID が、転送再配置応答で送信されます。DTF が設定されたベアラー変更要求が、RNC U FTEID とともに送信されます。
サポート対象	対応	対応	セッション作成要求が、DTF フラグが設定され、ユーザープレーン FTEID がない状態で送信されます。再配置要求が、セッション作成応答で受信した SGW S12U FTEID とともに送信されます。SGW が CSR 応答で S4U FTEID を送信した場合でも、それを S12U FTEID として内部的に処理し、再配置を続行します。RNC FTEID が転送再配置応答で送信され、DTF フラグが設定されたベアラー変更要求が RNC U FTEID とともに送信されます。

直接データ転送を伴う古い SRNS

このシナリオには、2 つの SGSN 間の SRNS 再配置が含まれているため、IDFT は適用されません。データは、送信元とターゲット RNC の間で直接転送されます。転送再配置要求が S12U FTEID とともに送信されます。

図 *33 :* 直接データ転送を伴う古い *SRNS*



以下の表には、旧 SRNS の詳細な動作が含まれています。

間接データ転送を伴う古い SRNS

古い SGSN SRNS 中の間接データ転送（IDFT）は、UTRAN から E-UTRAN への接続モードの IRAT ハンドオーバー中に発生します。転送再配置要求が SGW S12U FTEID とともに送信されます。

図 *34 :* 間接データ転送 *4* を伴う古い *SRNS*

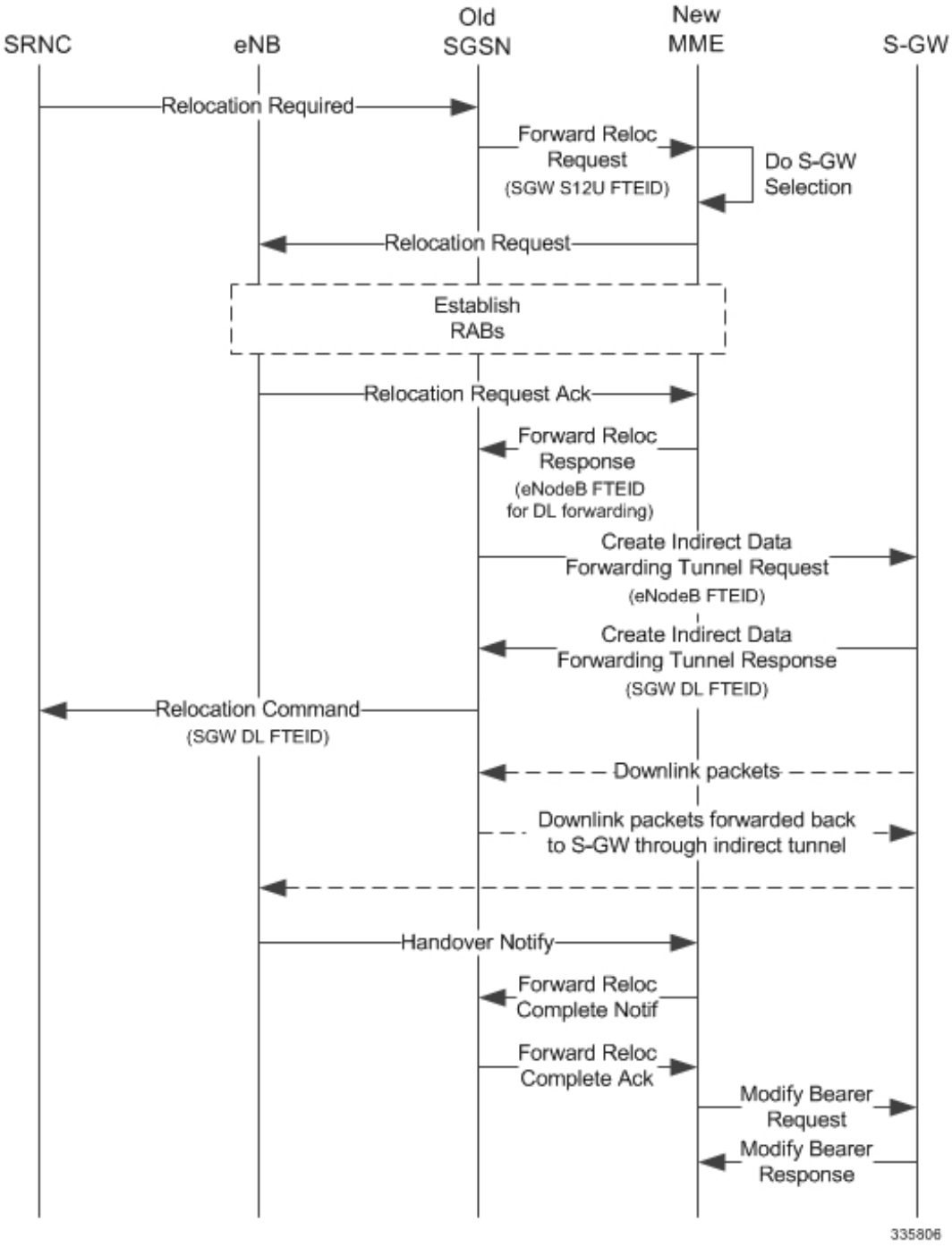


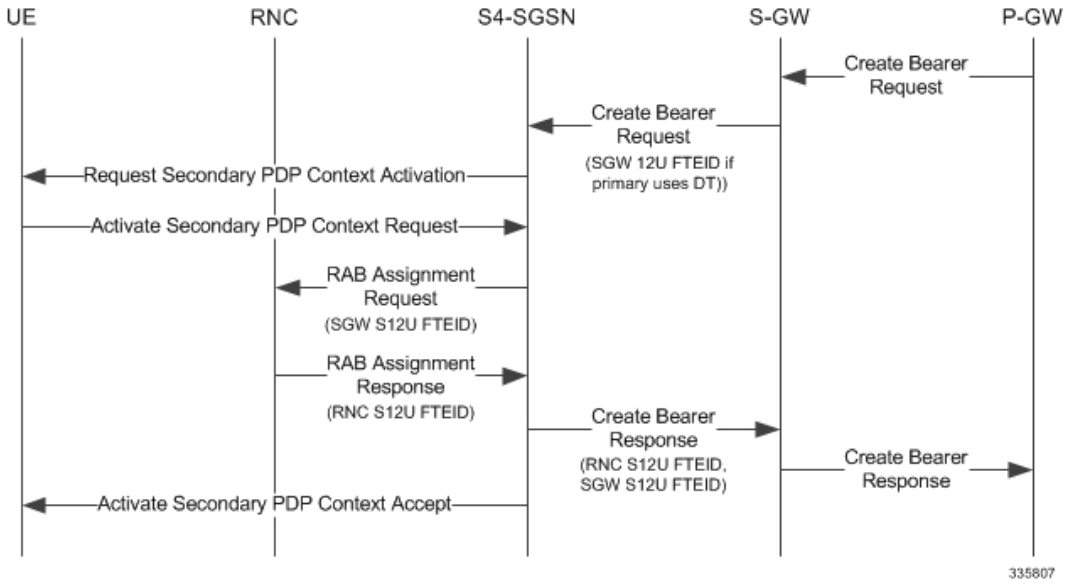
表 *45 :* 以前の *SRNS* の動作

送信元 RNC DT ステータス	直接転送	S-GW の再配置	動作
サポート対象	非対応	非対応	転送再配置要求が SGW S12 U FTEID とともに送信されます。ピアが MME の場合、IDFT が適用されます。次に、転送再配置応答で受信されたユーザープレーン FTEID を使用して、間接データ転送トンネル要求が送信されます。これは eNB ユーザープレーンの FT になります。間接データ転送トンネル応答の作成で受信された SGW DL 転送ユーザープレーン FTEID は、再配置コマンドで送信されます。
サポート対象	対応	非対応	転送再配置要求が SGW S12 U FTEID とともに送信されます。転送再配置応答で受信された eNB/RNC ユーザープレーン FTEID は、再配置コマンドで送信されます。
サポート対象	非対応	対応	転送再配置要求が SGW S12 U FTEID とともに送信されます。ピアが MME の場合、IDFT が適用されます。次に、転送再配置応答で受信された eNB ユーザープレーン FTEID を使用して、間接データ転送トンネル要求が送信されます。間接データ転送トンネル応答の作成で受信された SGW DL 転送ユーザープレーン FTEID は、再配置コマンドで送信されます。
サポート対象	対応	対応	転送再配置要求が SGW S12 U FTEID とともに送信されます。転送再配置応答で受信された eNB/RNC ユーザープレーン FTEID は、再配置コマンドで送信されます。

ネットワークによって開始されたセカンダリ PDP コンテキストのアクティブ化

S-GW は、SGW S12U FTEID を使用して、ネットワークによって開始されたセカンダリ PDP コンテキストのアクティブ化に関するベアラー作成要求を送信します。この FTEID は、RAB 割り当て要求で RNC に送信されます。RAB 割り当て応答で受信した RNC S12U FTEID は、ベアラー作成応答で S-GW に送信されます。

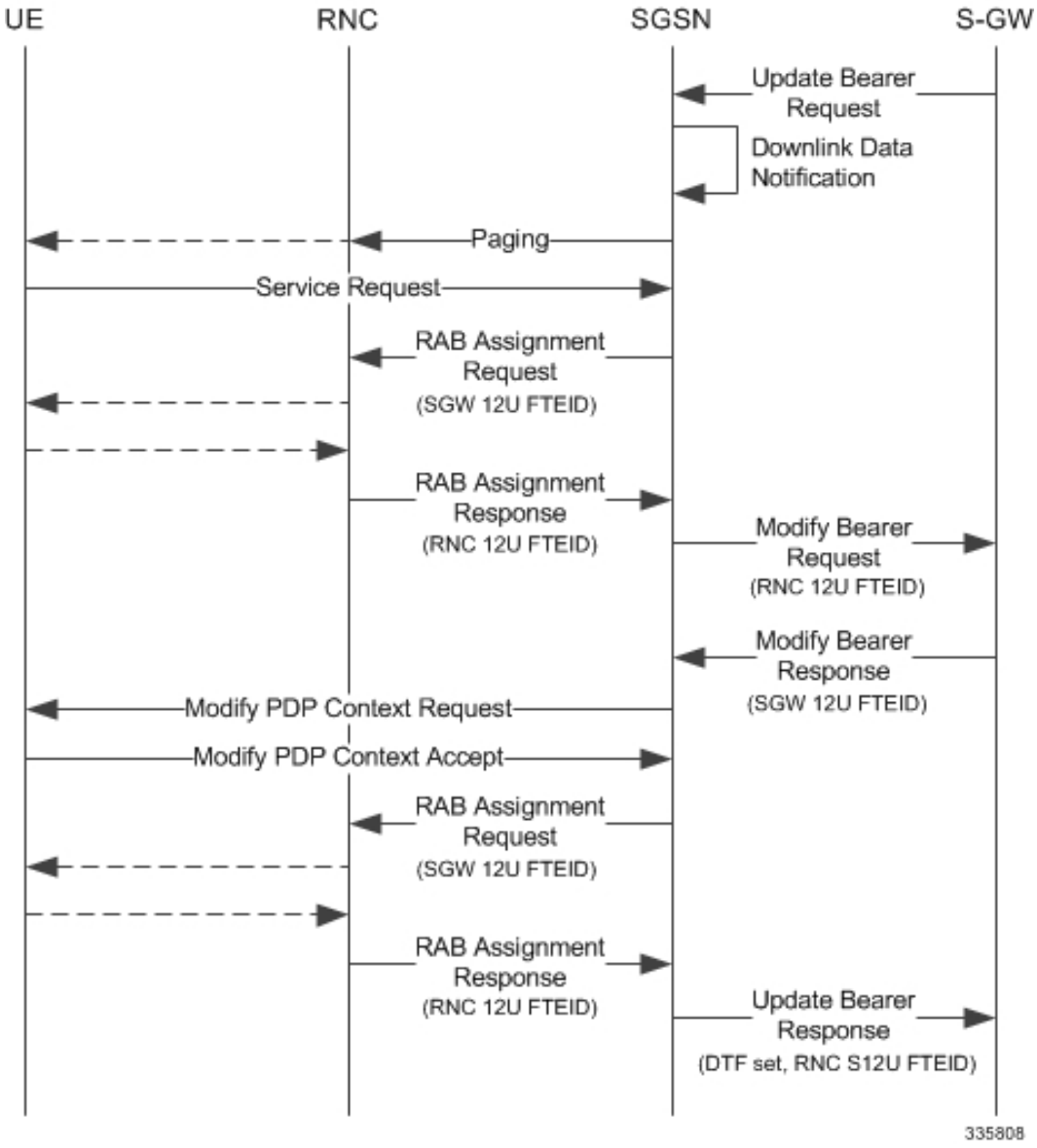
図 *35 :* ネットワークによって開始されたセカンダリ *PDP* コンテキストのアクティブ化 *5*



UE がアイドル状態のときの PGW 初期化変更

UE がアイドル状態にあり、PGW 初期化変更を受信した場合、SGSN は最初の MBR を送信します。PGW 初期化変更がアイドル状態になると、SGSN は PGW 初期化変更をキューに入れ、内部でダウンリンクデータ通知をフィードします。これにより、すべての RAB がセットアップされ（古い QoS を使用）、ベアラー変更要求が送信されます。ダウンリンクデータ手順が完了すると、キューに入れられた PGW 初期化変更が処理されます。

図 *36 : UE* がアイドル状態のときの *PGW* 初期化変更



制限事項

RAB の確立によってトリガーされた内部 RAU、内部 SRNS、またはサービス要求中に、いくつかの RAB がベアラー変更要求に失敗した場合、SGSN は、それらの RAB を削除対象のベアラーとしてマークします。現在の仕様では、S12U U-FTEID を持つ少数のベアラーと U-FTEID を持たない少数のベアラーを使用して、ベアラー変更要求を送信することはできません。

そのようなベアラー変更要求を可能にするための 3GPP で進行中の CR があり、S-GW は、U-FTEID を持っていなかったベアラーのダウンリンクデータを取得したときに DDN を送信する必要があります。この CR が承認されると、SGSN は、S12U FTEID を持つベアラーの部分的

なセットと、U-FTEIDを持たない一部のベアラーの送信を（将来のリリースで）サポートします。

標準準拠

直接トンネルは、次の標準規格に準拠しています。

- 3GPP TS 23.060 version 10 sec 9.2.2 General Packet Radio Service (GPRS) Service description
- 3GPP TS 29.274 v10.5.0 3GPP Evolved Packet System (EPS) Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)

ダイレクトトンネルのサポートの設定

SGSNは、ダイレクトトンネルのセットアップが許可されるか禁止されるかを決定します。現在、この機能の設定コマンドを提供している製品は、SGSNおよびS-GWのみです。ダイレクトトンネルをサポートしている他の製品はすべて、デフォルトでサポートします。

デフォルトでは、ダイレクトトンネルサポートは次のとおりです。

- SGSN/S-GWでは「禁止」
- GGSN/P-GWでは「許可」

SGSN/S-GWダイレクトトンネル機能は、オペレータポリシー設定内で有効になります。オペレータポリシーの1つの側面は、ダイレクトGTP-Uトンネルのセットアップを許可または禁止することです。オペレータポリシーが設定されていない場合、システムは、「default」という名前のオペレータポリシーの設定を調べます。「default」オペレータポリシーでダイレクトトンネルが許可されている場合、適用されるオペレータポリシーが設定されていない着信コールには、ダイレクトトンネルが許可されます。オペレータポリシーの目的と使用方法の詳細については、「オペレータポリシー」のセクションを参照してください。

S4-SGSNでのダイレクトトンネルの設定

GTP-Uダイレクトトンネル（DT）を設定するには、コール制御プロファイルとRNCの両方でDTを有効にする必要があります。



重要 MS/UEでダイレクトトンネリングを許可するには、両方のエンドポイントでダイレクトトンネリングを有効にする必要があります。

GTP-Uダイレクトトンネルのセットアップの有効化

SGSNは、ダイレクトトンネルをセットアップできるかどうかを判断します。デフォルトでは、SGSNはダイレクトトンネルをサポートしません。次の設定では、コール制御プロファイルでGTP-U DTを有効にします。

```
config
  call-control-profile policy_name
    direct-tunnel attempt-when-permitted [ to-ggsn | to-sgw ]
    end
```

注：

- コール制御プロファイルは事前に作成、構成して、事前に作成、構成した有効な通信事業者ポリシーに関連付けられている必要があります。通信事業者ポリシーの作成/設定については、このガイドの「通信事業者ポリシー」の章を参照してください。
- **direct-tunnel** コマンドに **to-ggsn** オプションと **to-sgw** オプションが追加され、通信事業者はSGSNがダイレクトトンネルに使用するインターフェイスを選択できるようになりました。Gn/GP-SGSN と S4-SGSN が併置されている場合、
  - キーワード **attempt-when-permitted** をフィルタなしで使用して、両方のインターフェイスタイプ（GGSN に対する GTP-U および SGW に対する S12）を有効にします。
  - RNC と GGSN 間の GTP-U インターフェイスのみを有効にするには、キーワード **attempt-when-permitted** と **to-ggsn** キーワードフィルタを使用します。
  - RNC と SGW の間で S4 の S12 インターフェイスのみを有効にするには、キーワード **attempt-when-permitted** と **to-sgw** キーワードフィルタを使用します。
- 構成からダイレクトトンネル設定を削除するには、**direct-tunnel attempt-when-permitted [to-ggsn | to-sgw]** コマンドを使用します。
- ダイレクトトンネルは SGSN では許可されますが、宛先ノードと RNC の両方で許可されている場合にのみセットアップされます。

RNC へのダイレクトトンネルの有効化

無線アクセスコントローラ（RNC）への SGSN アクセスは、IuPS サービスで設定されます。各 IuPS サービスには、RNC に応じて通信と機能を決定する複数の RNC 設定を含めることができます。デフォルトでは、DT 機能はすべての RNC に対して有効になっています。

次の設定シーケンスで、以前はダイレクトトンネリングが無効になっていた特定の RNC に対する DT が有効になります。

```
config
  context ctxt_name
    iups-service service_name
      rnc id rnc_id
        default direct-tunnel
        end
```

注：

- IuPS サービスは事前に作成され、設定されている必要があります。
- RNC 設定は、IuPS サービス設定内で事前に作成されている必要があります。
- 設定用のコマンドの詳細については、『*Command Line Interface Reference*』[英語] を参照してください。

ダイレクトトンネルの制限

次の設定シナリオでは、S4-SGSN が SGSN 間 RAU 中に S12 インターフェイスを介してダイレクトトンネリングをセットアップすることが禁止されます。

```
config
  call-control-profile profile_name
    rau-inter avoid-s12-direct-tunnel
    end
```

特定の RNC によるダイレクトトンネリングを制限する：次の設定シナリオでは、コールが特定の RNC から発信された場合に、SGSN がダイレクトトンネルのセットアップを試行することを制限します。

```
config
  context context_name
    iups-service service_name
      rnc id rnc_id
        direct-tunnel not-permitted-by-rnc
        end
```

コール制御プロファイル設定の確認

コール制御プロファイルのダイレクトトンネル設定を表示して確認するには、次のコマンドを使用します。

show call-control-profile full name *<profile_name>*

このコマンドの出力には、指定したコール制御プロファイルのダイレクトトンネルを含むすべての設定が表示されます。

```
Call Control Profile Name = ccprofile1
.
.
.
Re-Authentication
            : Disabled
Direct Tunnel
                : Not Restricted
GTPU Fast Path
               : Disabled
.
.
```

RNC 設定の確認

RNC 設定のダイレクトトンネル設定を表示して確認するには、次のコマンドを使用します。

show iups-service name *<service_name>*

このコマンドの出力には、指定した IuPS サービスのダイレクトトンネルを含むすべての設定が表示されます。

```
IService name                                                  : iups1
.
.
.
Available RNC:
    Rnc-Id                                                          : 1
    Direct Tunnel                                              : Not Restricted
```

S-GW での S12 ダイレクトトンネルのサポートの設定

このセクションの例では、RAT 間ハンドオーバーで S4 SGSN のダイレクトトンネルバイパスをサポートする S12 インターフェイスを設定します。

S-GW でのダイレクトトンネル機能は、S12 インターフェイスを設定することで有効になります。その後、S4 SGSN が、S11 インターフェイスを介して制御メッセージ内の FTEID を S-GW に送信することで、ダイレクトトンネルを作成します。S-GW は、S12 インターフェイスを介したダイレクトトンネルを設定するために必要な識別情報を SGSN に提供する、独自の U-FTEID で応答します。



重要 **interface-type** コマンドを変更すると、親サービス（eGTP または GTP-U サービスが設定されているサービス）が自動的に再起動します。サービスを再起動すると、親サービスに関連付けられているアクティブコールがドロップされます。

この機能を構成するには、次の例を使用します。

```
configure
   context egress_context_name -noconfirm
      interface s12_interface_name
         ip address s12_ipv4_address_primary
         ip address s12_ipv4_address_secondary
         exit
      exit
   port ethernet slot_number/port_number
      no shutdown
      bind interface s12_interface_name egress_context_name
      exit
   context egress_context_name -noconfirm
      gtpu-service s12_gtpu_egress_service_name
         bind ipv4-address s12_interface_ip_address
         exit
      egtp-service s12_egtp_egress_service_name
         interface-type interface-sgw-egress
         validation-mode default
         associate gtpu-service s12_gtpu_egress_service_name
         gtpc bind address s12_interface_ip_address
         exit
      sgw-service sgw_service_name -noconfirm
         associate egress-proto gtp egress-context egress_context_name
egtp-service s12_egtp_egress_service_name
         end
```

注：

- S12 インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。

ダイレクトトンネルのモニタリングと障害対応

show subscribers sgsn-only

このコマンドの出力は、ダイレクトトンネルが確立されたかどうかを示します。

show subscribers sgsn-only full all

```
Username: 123456789012345
 Access Type: sgsn-pdp-type-ipv4        Network Type: IP
 Access Tech: WCDMA UTRAN
  |
  |
 NSAPI: 05                               Context Type: Primary
 Context initiated by: MS
 Direct Tunnel : Established
```

show gmm-sm statistics sm-only

このコマンドの出力には、ダイレクトトンネルを持つアクティブ PDP コンテキストの合計数が表示されます。

show gmm-sm statistics sm-only

```
Activate PDP Contexts:
 Total Actv PDP Ctx:
  3G-Actv Pdp Ctx:             1  2G-Avtv Pdp Ctx:       0
  Gn Interface:                1  Gn Interface:          0
  S4 Interface:                1  S4 Interface:          0
 Total Actv Pdp Ctx:
  with Direct Tunnel:          1
```

ダイレクトトンネルのバルク統計

現在、ダイレクトトンネルでの PDP コンテキストの数のモニターに使用可能なバルク統計はありません。

EGTPC スキーマでのバルク統計は、ダイレクトトンネルとアイドルモードシグナリングリダクション（ISR）の両方（3G および 2G）に適用できます。次の統計は、ダイレクトトンネルと ISR のいずれかがアクティブな場合に、Iu または RAB のリリース時に SGSN によって S-GW に送信されるアクセスベアラーリリース要求および応答メッセージを追跡します。

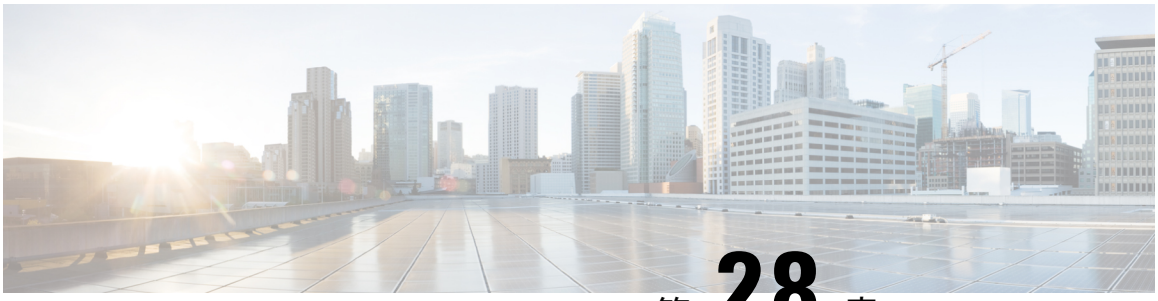
- tun-sent-relaccbearreq
- tun-sent-retransrelaccbearreq
- tun-recv-relaccbearresp
- tun-recv-relaccbearrespDiscard
- tun-recv-relaccbearrespaccept

- tun-recv-relaccbearrespdenied

EGTPC スキーマの次のバルク統計は、ダイレクトトンネルと ISR のいずれかがアクティブな場合、S-GW と SGSN 間のダウンリンクデータ通知（DDN）確認応答および障害メッセージを追跡します。

- tun-recv-dlinknotif
- tun-recv-dlinknotifDiscard
- tun-recv-dlinknotifNorsp
- tun-recv-retransdlinknotif
- tun-sent-dlinknotifackaccept
- tun-sent-dlinknotifackdenied
- tun-sent-dlinkdatafail

これらの変数の詳細な説明については、『*Statistics and Counters Reference*』の EGTPC スキーマ統計の章を参照してください。



第 28 章

動的保証ビットレート

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （503 ページ）
- 機能説明 （504 ページ）
- 機能の仕組み （504 ページ）
- 制限事項と制約事項 （506 ページ）
- 専用 GBR ベアラーの設定 （506 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.4

機能説明

保証ビットレート（GBR）専用ベアラーが使用されている場合は、リソースの帯域幅がネットワーク上で予約されます。サブスクライバデータフローが、割り当てられた値よりも低帯域幅である場合、余分な GBR はネットワーク上で無駄になります。

この機能により、ゲートウェイがベアラーでの GBR の使用状況を定期的にモニターし、その使用状況に対応する柔軟性が追加されます。ゲートウェイは、それに応じて、割り当てられた GBR をステップアップまたはステップダウンします。

機能の仕組み

この項では、ダイナミック GBR 機能の動作について説明します。

- 専用 GBR ベアラーは、セッションセットアップ時または特定のコールイベント時にローカルポリシーの設定を使用して作成されます。
- SAEGW は、ベアラーの作成後に GBR を 30 秒間隔でモニターします。
- 各間隔の後、SAEGW は設定されたしきい値で平均データレートを検証します。
- しきい値違反があると、GBR は設定値に従ってステップアップまたはステップダウンします。
- SAEGW では、GBR の上限と下限のしきい値の設定、および上限と下限のしきい値に対応するステップアップまたはステップダウンの値の設定が可能です。

上限しきい値違反

最初のしきい値違反

- サブスクライバは、QCI=qci1、GBR を 1000 kbps、上限しきい値を 80%（800 kbps）に設定して専用ベアラーを作成します。
- 30 秒ごとにデータレートが評価されます。しきい値制限に違反すると、SAEGW はベアラー更新要求を開始して GBR 値をアップグレードし、設定されたパーセンテージの値でステップアップます。
- 30 秒後、評価されたデータレートが 800 kbps を超えている場合、ベアラー更新要求が開始され GBR をアップグレードします。GBR は、初期設定された GBR とステップアップで設定されたパーセンテージの集約値でアップグレードされます。たとえば、ステップ

アップ増分が 20%（200 kbps）に設定されている場合、ベアラー更新要求は 1200 kbps でトリガーされます。

2 回目のしきい値違反：

- GBR が 1200 kbps に増加すると、モニタリングされる新しい上限しきい値は 1200 の 80%、つまり 960 kbps になります。
- 次のモニタリング間隔で、データレートの使用が 960 kbps を超えると、SAEGW は再びベアラー更新要求を開始して、GBR 値をアップグレードします。これらの GBR 値がアップグレードされ、設定されたパーセンテージ値（20%）でステップアップします。ただし、この 20% はベース値が 1000 であり、1200 kbps ではありません。したがって、増分は再び 200 kbps であり、ベアラー更新要求は新しい GBR として 1400 kbps となります。



重要 ステップ増分のパーセンテージは、ベアラーのベース（初期）値のものであり、現在ネゴシエートされている値ではありません。GBR をステップアップできる最大値は、設定された MBR 値です。

下限しきい値違反

最初のしきい値違反

- サブスクライバは、QCI=qci1、GBR を 1000 kbps、下限しきい値を 50% に設定して、専用ベアラーを作成します。
- 上限しきい値違反により、SAEGW は GBR を 1400 kbps にアップグレードしました。
- ベアラーの使用が 700 kbps（現在の GBR の 50%）を下回ると、SAEGW はベアラー更新要求を開始して GBR をダウングレードします。これらの GBR 値はダウングレードされ、設定値（例：20%）分ステップダウンします。すなわち、1400 - 200 = 1200 kbps となります。



重要 ステップ減分のパーセンテージは、ベアラーのベース（初期）値のものであり、現在ネゴシエートされている値ではありません。GBR 値が、初期ネゴシエート値未満にステップダウンすることはありません。

2 回目のしきい値違反：

- GBR が 1200 kbps に低下すると、データはさらに減少して新しい 50% 下限しきい値に違反します。つまり、1200 の 50% = 600 kbps です。
- SAEGW はベアラー更新要求を開始して GBR 値をダウングレードし、設定値（20%）でステップダウンします。つまり、1200 - 200 = 1000 kbps となります。

制限事項と制約事項

ここでは、この機能の制限事項と制約事項について説明します。

- SAEGW は、30 秒間隔でベアラー帯域幅をモニターします。
- GBR の使用量が設定されたしきい値の設定可能なパーセンテージを超えると、SAEGW はベアラー変更手順を開始します。SAEGW は上限設定値を使用して、ベアラー QoS 更新でこの手順を開始します。これに応じて、eNB と UER は GBR を調整します。
- GBR の使用量が設定されたしきい値の設定可能なパーセンテージより下になると、SAEGW はベアラー変更手順を開始します。このベアラー変更手順は下限設定値を使用して、ベアラー QoS 更新で開始されます。これに応じて、eNB と UER は GBR を調整します。
- 複数のルールが同じベアラーに設定されている場合、現在ネゴシエートされているベアラー値から QoS が適用されます。この機能がベアラーで有効になっている場合、ruledef に対応する課金アクションの個々の値は無視されます。
- モニター対象のベアラーについては、ビットレートが変更されるか、ルールが削除されると、GBR の基本値が変更されます。この GBR の基本値の変更により、ステップアップまたはステップダウンの値が変更されます。
- セッションリカバリと ICSR がサポートされています。
- ステップアップとステップダウンの値は、ベアラーに適用されている現在の GBR ではなく、ベアラーの GBR の基本値に基づいて計算されます。

専用 GBR ベアラーの設定

ここでは、この機能のために追加された設定コマンドについて説明します。

この設定後、以下の新しい設定を有効にする必要があります。

1. ステップダウンする GBR 値を決定するための GBR の下限（%）。
2. ステップアップする GBR 値を決定するための GBR の上限（%）。
3. しきい値のステップアップ（%）。
4. しきい値のステップダウン（%）。この値は、ステップアップしきい値よりも小さくする必要があります。

trigger

この CLI コマンドに、新しい CLI キーワード **Bearer-creation** と **monitor-bearer-bandwidth** が追加されました。キーワード **bearer-creation** は、作成されたすべての新しいベアラーでトリ

ガーします。キーワード**monitor-bearer-bandwidth**は、ベアラー帯域幅が評価されるたびにトリガーします。

```
configure
    active-charging service <service_name>
       service scheme <service_scheme_name>
          [ no ] trigger {  bearer-creation | flow-create | loc-update
 | monitor-bearer-bandwidth |  sess-setup }
          end
```

注：

デフォルトでは、この CLI は無効になっています。

- **no**：あらかじめ設定されている場合は、指定した設定を削除します。
- **Bearer-creation**：すべての新しいベアラーでトリガーします。
- **flow-create**：すべての新しいフローでトリガーします。
- **loc-update**：サブスクライバのロケーションが変更されるたびにトリガーします。
- **sess-setup**：セッションのセットアップでトリガーします。
- **monitor-bearer-bandwidth**：ベアラー帯域幅が評価されるたびにトリガーします。

committed-data-rate

この CLI コマンドが ACS トリガー アクション コンフィギュレーション モードに追加され、現在のネゴシエートされている値の認定データレートを設定できるようになりました。

```
configure
    active-charging service <service_name>
       trigger-condition <trigger_condn_name>
         [ no ] committed-data-rate { lower_threshold <value_in_percentage>
 | upper_threshold <value_in_percentage> }
          end
```

注：

- **no**：現在ネゴシエートされている値の認定データレートを無効にします。
- **commited-data-rate**：現在ネゴシエートされている値の認定データレートを指定します。
- **Lower threshold**：現在のネゴシエートされている値のしきい値をパーセンテージで設定します。
- **upper threshold**：現在のネゴシエートされている値のしきい値をパーセンテージで設定します。
- *value_in_percentage*：初期設定される committed-data-rate 値のパーセンテージを指定します。これは、0 ～ 100 の整数値です。

step-up

この新しい CLI コマンドが ACS トリガー アクション コンフィギュレーション モードに追加され、認定データレートの値をステップアップできるようになりました。

```
configure
    active-charging service <service_name>
      trigger-action <trigger_action_name>
         [ no ] step-up committed-data-rate <negotiated_value>
         end
```

注：

- **no**：あらかじめ設定されている場合は、指定した設定を削除します。
- **step-up**： *negotiated_value*で定義されたパーセンテージで認定データレートの値をステップアップします。
- **commited-data-rate**：認定データレートを定義します。

  negotiated_value：初期設定される committed-data-rate 値のパーセンテージを指定します。これは、0 ～ 100 の整数値です。

step-down

この新しい CLI コマンドが ACS トリガー アクション コンフィギュレーション モードに追加され、認定データレートの値をステップダウンできるようになりました。

```
configure
    active-charging service <service_name>
      trigger-action <trigger_action_name>
         [ no ] step-down committed-data-rate <negotiated_value>
         end
```

注：

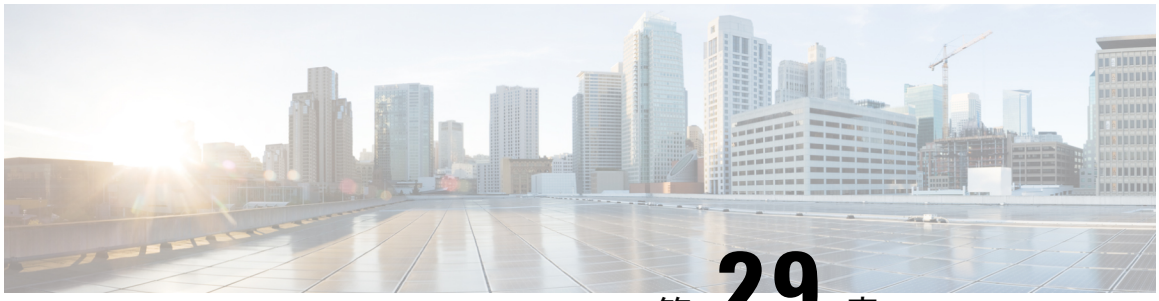
- **no**：あらかじめ設定されている場合は、指定した設定を削除します。
- **step-down**： *negotiated_value*で定義されたパーセンテージで認定データレートの値をステップダウンします。
- **commited-data-rate**：認定データレートを定義します。

  negotiated_value：初期設定される committed-data-rate 値のパーセンテージを指定します。これは、0 ～ 100 の整数値です。

設定例

ここでは、この機能で使用する CLI コマンドの設定例を示します。

```
config
  active-charging service ACS
  trigger-action ta1
      step-up  committed-data-rate  20
    exit
  trigger-action ta2
     step-down committed-data-rate  30
    exit
    trigger-condition tc1
      qci = 1
      committed-data-rate upper-threshold 80
    exit
    trigger-condition tc2
      qci = 1
      committed-data-rate lower-threshold 50
    exit
    service-scheme scheme1
      trigger monitor-bandwidth
        priority 1 trigger-condition tc1 trigger-action ta1
        priority 2 trigger-condition tc2 trigger-action ta2
      exit
    subs-class class1
      any-match = TRUE
    exit
    subscriber-base base1
      priority 1 subs-class class1 bind service-scheme scheme1
    exit
exit
```



第 29 章

トランザクションまたは発信元ホストに基づく動的なトランスポートの選択

- 機能の概要と変更履歴 （511 ページ）
- 機能説明 （512 ページ）
- Diameter ベースインターフェイスの低および高優先順位チャネルの特性 （513 ページ）
- S11、S5、またはS8インターフェイスの低優先順位チャネルと高優先順位チャネルの特性 （514 ページ）
- 機能の仕組み （514 ページ）
- トランザクションまたは発信元ホストに基づく動的なトランスポート選択の設定 （519ページ）
- モニタリングおよびトラブルシューティング （522 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効 - 設定が必要
このリリースでの関連する変更点	N/A
関連資料	N/A

マニュアルの変更履歴

改訂の詳細	リリース
初版 **重要** この機能は、すべてのお客様の展開シナリオでは検証されていません。サポートについては、セールスアカウントチームにお問い合わせください。	21.22

機能説明

国家安全保障上のインシデントや緊急事態に備え、システムの効果的な管理を実現するには、信頼性と安全性に優れた通信システムが必要です。National Security and Emergency Preparedness（NS/EP）は一連の音声、ビデオ、およびデータのサービスです。パブリックパケット交換サービスプロバイダーから利用できるサービスに属し、NS/EP通信をサポートするための優先サービスを提供します。NS/EP 通信システムには、固定回線、ワイヤレス、ブロードキャスト、ケーブルテレビ、無線、公共安全システム、衛星通信、およびインターネットが含まれます。

Wireless Priority Services（WPS）は、全世界および複数の地域の携帯電話ネットワークで職員の優先アクセスや優先処理を提供し、コール完了の可能性を高めるNS/EP通信プログラムの1つです。

ファーストレスポンダとも呼ばれるWPSユーザーは、国家安全保障と緊急事態への対応の管理に不可欠なコマンドアンドコントロール機能を担当します。ネットワークでWPSユーザーのトラフィックを伝送する場合、すべてのネットワーク要素は個別および集合的に次の条件に従う必要があります。

- **コントロール プレーン トラフィックの優先順位付け**：WPSユーザーのコントロール プレーン トラフィックは、LTEコアのさまざまなネットワーク機能間で他のサブスクライバよりも優先されます。
- P1、P2、P3は、WPSユーザーが使用できる3つの優先順位レベルです。
  - P1とP2のユーザーはHSS/PCRFで識別され、GWはデフォルトおよび専用のベアラーの作成、変更、更新、削除時にそれぞれの優先順位（ARP）を使用します。
  - P1およびP2のWPSユーザーは、高い優先順位で扱われます。
  - 優先順位付けされたユーザーのコントロールプレーンIPパケットのDSCPマーキングはDSCP = 47でマークされ、他のすべてのユーザー制御パケットIPパケットはDSCP = 32でマークされます。
- **Diameter インターフェイス**：
  - P-GW、Policy Change Rule Function (PCRF)、およびDiameterルーティングエージェント(DRA)は、Gxインターフェイスや Rxインターフェイスなどの Diameterインター

フェイスの設定を使用して、サブスクライバのポリシー制御や課金制御をサポートします。

- P-GWおよびS-GWは、それぞれのピアとの間でS5、S8、S11、S1Uなどの非Diameterインターフェイスを使用します。

Diameter ベースインターフェイスの低および高優先順位チャネルの特性

Differentiated Services Code Point（DSCP）のマーキング中は、低優先順位チャネルは通常優先順位のユーザーを示し、高優先順位チャネルはWPSユーザーを示します。PGW（Gx）のDRAへのピア接続を図に示します。

図 *37 : Gx* インターフェイスを介した低優先順位チャネルおよび高優先順位チャネルの概要

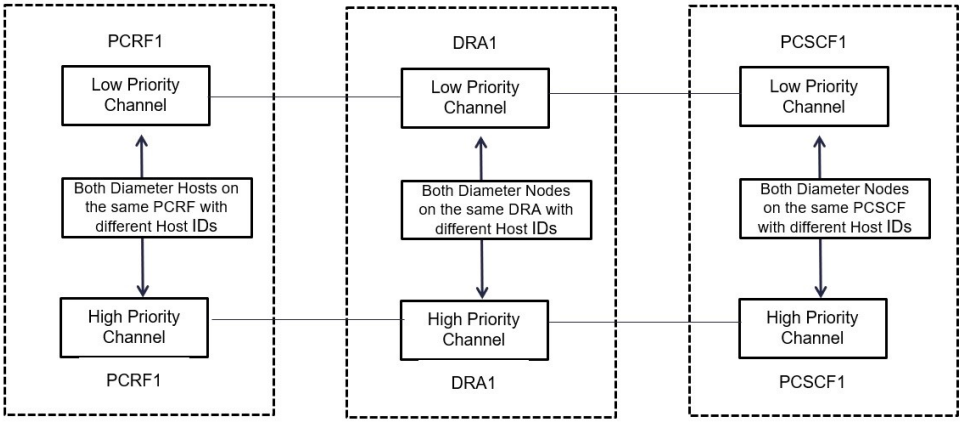


表 *46 : Gx* インターフェイスの低優先順位チャネルと高優先順位チャネル

優先順位チャネル	Diameterインターフェイス	IP レイヤ DSCP	IP レイヤを介したTCP接続	Diameter ホスト FQDN
低優先順位	Gx	32 と等しい	32 （注） このチャネルは非 WPS Diameter メッセージ用ですが、すべてのレッドピアがダウンしている場合などのエラーシナリオで WPS Diameter メッセージを伝送する可能性があります。	未変更 例：0 0 0 1-diamproxy. PGW-Gx', 'dra1', 'pcrf1

優先順位チャネル	Diameter インターフェイス	IP レイヤ DSCP	IP レイヤを介した TCP 接続	Diameter ホスト FQDN
高優先順位	Gx	47 と等しい	47	高い優先順位に固有 例： 0001-diamproxy. PGW-Gx-wps', ' dra1-wps', 'pcrf1-wps'.

S11、S5、または S8 インターフェイスの低優先順位チャネルと高優先順位チャネルの特性

S5 インターフェイスと S11 インターフェイスは GTPv2 ベース（トランスポートプロトコルとして UDP を使用）で、低優先順位チャネルと高優先順位チャネルに次の特性があります。

表 *47 :* 他のインターフェイスの低優先順位チャネルと高優先順位チャネル

優先順位チャネル	Diameter インターフェイス	IP レイヤ DSCP	IP レイヤを介した TCP 接続	Diameter ホスト FQDN
低優先順位	S11 または S5 または S8	32	—	—
高優先順位	S11 または S5 または S8	47	—	—

機能の仕組み

この機能の動作の概要を以下で説明します。PGW は **wps profile** に基づいて、高い優先順位または低い優先順位のいずれかのチャネルを選択します。APN 名、QCI、および ARP が表に示されているとおりに一致すると、セッションは IMSA での WPS セッションとして検出されます。

表 *48 : APN*、*QCI*、および *ARP* の優先順位レベルに基づく *WPS* メッセージの優先順位付け

APN 名	QCI	ARP	DSCP
IMS	66,69	*	47
IMS	*	1、2	47
IMS	8	3	47

APN 名	QCI	ARP	DSCP
IMS	9	5	47
IMS	2	4	47

次の表では、トランザクションまたは発信元ホストに基づく動的なトランスポート選択のプロセスについて説明します。

表 *49 :* 手順

プロセス	説明
WPS ユーザーと非 WPS ユーザーの識別	• WPS ユーザーを有効または無効にするには、Diameter のエンドポイントで CLI コマンド **priority-select** を使用します。この CLI コマンドは、IMS 承認サービスのポリシー制御設定にあります。 • PGW は、割り当ておよび保持プライオリティ（ARP）値がタグ付けされたすべての eMPS セッションを含むセッション作成要求を受信します。 • PGW は、その ARP 値が WPS と一致しているかどうかを確認します。 • セッションマネージャは、受信した ARP 値が eMPS セッションと一致しているかどうかを確認します。 • eMPS セッションの一致と有効な優先順位選択という上記の基準が満たされている場合、ユーザーは WPS ユーザーと呼ばれます。それ以外の場合、ユーザーは通常ユーザーと呼ばれます。

プロセス	説明
セッションの優先順位付け	ポリシー変更ルール機能（PCRF）では、非 WPS ユーザー向けの低い優先順位のセッションと WPS ユーザー向けの高い優先順位のセッションといった 2 つの優先順位レベルを定義できます。 • **WPS セッション時に常時**：WPS ユーザーに属する GTPv2-S5、GTPv2-S11、GTPv2-S8、および Gx セッションは、常に高い優先順位として扱われます。 • **オンデマンド WPS セッション**：非 WPS ユーザーに属する GTPv2-S5、GTPv2-S11、GTPv2-S8、および Gx セッションを、より高い優先順位（より低い ARP PL 値）に動的に昇格できます。この最も一般的な例は、WPS ユーザーが非 WPS ユーザーに WPS コール（*272 で始まるコールをダイヤルすることにより開始）を発信する場合です。このようなタイプのセッションは、オンデマンド eMPS セッションと呼ばれます。 • 高い優先順位のセッションに属するコントロールプレーン Gx メッセージは、高い優先順位のチャネルを使用します。 • 高くない優先順位のセッションに属するコントロールプレーン Gx メッセージは、高い優先順位のチャネルを使用します。

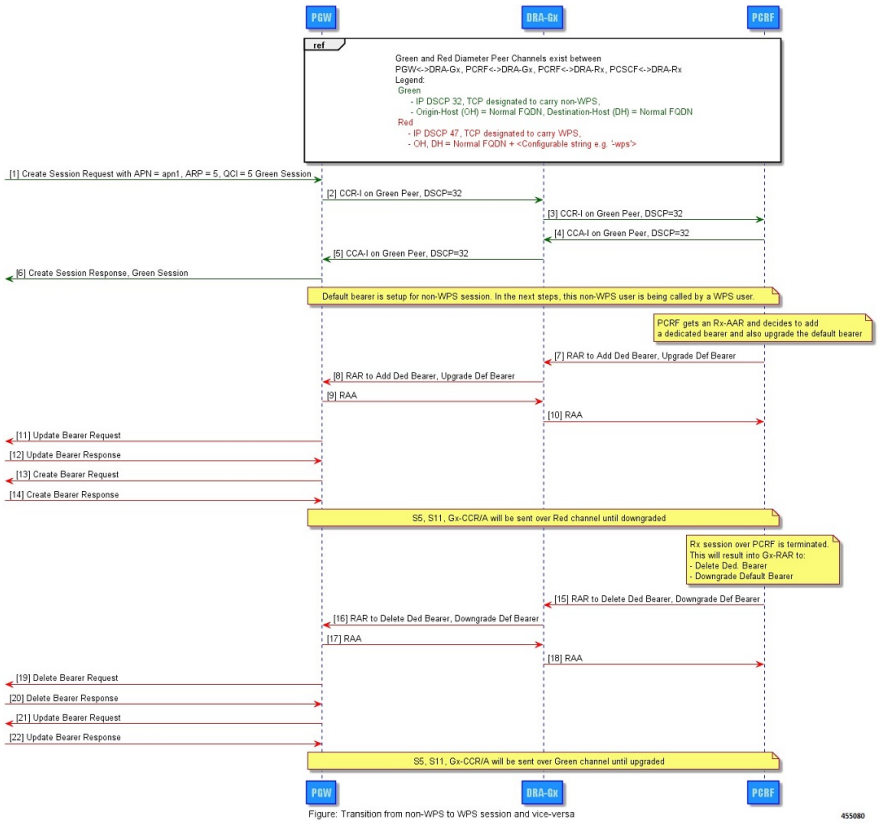
プロセス	説明
通常ユーザーと WPS ユーザー間のパスの差別化	Gx インターフェイスでは、CLI レベルで 2 番目のパスを形成するためにさまざまな接続が行われます。 • P-GW は 2 セットの DRA ピア接続を作成します。1 つは高い優先順位に設定され、もう 1 つは通常の優先順位のメッセージに設定されます。 • P-GW は、セッションのタイプ（WPS セッションまたは非 WPS セッション）に応じて、特定の接続ペアで CCR-Initial および CCR-Update Gx メッセージを送信します。 • ピアに **priority-select** フラグを設定すると、WPS セッションのすべての CCR メッセージが高い優先順位のピアで開始されます。P-GW がユーザーを WPS ユーザーとして識別すると、DSCP を 47 にマーキングして優先順位の高いピアにバインドします。ただし、非 WPS サブスクライバの Diameter メッセージは低い優先順位のピアで開始され、DSCP は 32 に設定されます。 （注） ピアの DSCP 設定が指定されていない場合は、Diameter エンドポイントに設定されたグローバル DSCP 値が使用されます。Diameter エンドポイントにグローバル DSCP 値が設定されていない場合は、DSCP 値「0」が使用されます。 WPS ユーザーに関しては、CCR-I メッセージをトリガーする前次のアクションが実行されます。 • 高い優先順位のピアの選択。 • 既存の AVP 文字列がピア設定で設定されている場合、発信元ホスト ID に文字列が追加されます。文字列が設定されていない場合、デフォルトの **-wps** 文字列が発信元ホスト ID に追加されます。 • DRA または PCRF は、CCR-I の受信時に高い優先順位のチャネルを介して CCA-I で応答します。その後のメッセージは、高い優先順位のチャネルに従います。

この機能の主なコールフローには、非 WPS セッションから WPS セッションへの移行と、PCRF によって開始されたベアラー削除が含まれます。

CSR（セッション作成要求）に 1 つのベアラーがあり、ARP が eMPS プロファイルで定義された ARP と一致しない場合、セッションは低い優先順位のセッションとして扱われます。すべての Gx メッセージは、PCRF への低い優先順位のチャネルに従います。ただし、モバイルによってトリガーされた専用ベアラーの ARP が、eMPS プロファイルで定義された ARP と一致する場合、低い優先順位のセッションは WPS セッションに移行されます。

（注） このドキュメントでは、低い優先順位のチャネルと緑色のチャネルが同じ意味で使用されています。赤色のチャネルと高い優先順位のチャネルについても同様です。

図 *38 :* 非 *WPS* セッションと *WPS* セッション相互の移行



（注） StarOS 21.22 リリースでは、WPS セッションは eMPS セッションと同じであり、eMPS プロファイルに基づいています。

表 *50 :* 手順

ステップ	説明
1 ～ 6	低い優先順位のチャネルは、非 WPS セッションに使用されます。

ステップ	説明
7 ～ 14	P-GW が eMPS プロファイルで定義された ARP を含む RAR を受信すると、次の操作が実行されます。 • 内部で、セッションが eMPS セッションに更新されます。 • P-GW は高い優先順位のピアを識別し、発信メッセージの発信元ホスト AVP に文字列「-wps」（または設定された origin-host-suffix 文字列）を追加します。 Gx、S5、およびS11 での後続の発信メッセージは、セッションが再度ダウングレードされるまで、高い優先順位のチャネルに従います。
15 ～ 22	P-GW が eMPS プロファイルで定義されていない ARP を含む RAR を受信すると、セッションが eMPS（WPS）セッションから非 WPS にダウングレードされます。
（注） セッションが eMPS 状態にあり、高い優先順位の Gx ピアが使用できない場合、低い優先順位のピアが Gx トラフィックに使用されます。使用可能なピアが存在しない場合、コールはドロップされます。	

トランザクションまたは発信元ホストに基づく動的なトランスポート選択の設定

ここでは、トランザクションまた発信元ホストに基づいて動的トランスポート選択を設定する方法について説明します。

1. eMPS プロファイルの設定
2. eMPS プロファイルの P-GW サービスへの関連付け
3. eMPS セッションの Gx 優先順位付けの有効化
4. APN サービスの WPS 機能およびプライオリティサービスの有効化

eMPS プロファイルの設定

このセクションでは、eMPS プロファイルの設定方法を説明します。次のコマンドを使用して eMPS プロファイルを設定します。この eMPS プロファイルは、eMPS ベアラーまたはセッションとしてベアラーまたはセッションを識別およびマークするために使用されます。

```
configure
   [ no ] emps-profile emps_profile_name -noconfirm
```

```
[ no ] earp { [string value] }
[ no ] dscp-marking { dscp-value }
end
```

注：

- **emps-profile emps_profile_name**：eMPS セッションの属性を定義するための eMPS プロファイルを設定します。*emps_profile_name* は、1 ～ 63 文字の文字列です。
- **-noconfirm**：確認のプロンプトなしで新しい eMPS プロファイルを作成します。
- **earp**：最大 8 つの eARP 優先順位レベル（PL）値を設定して、設定された eARP 優先順位値を持つセッションを eMPS セッションとしてマークできるようにします。eMPS プロファイルでは、最大 8 つの eARP 値を設定できます。
- **dscp-marking**：eMPS セッションに適用される DSCP 値を指定します。dscp_value は、0x0 ～ 0x3F の 16 進数である必要があります。

（注） eMPS プロファイルの設定（eMPS ベアラーまたはセッションとしてベアラーまたはセッションを識別するために使用される eMPS ARP の設定）、および eMPS 統計に関連する補足情報については、『*P-GW Administration Guide*』または『*SAEGW Administration Guide*』の「*VoLTE/*緊急コールの拡張優先順位付け」の章を参照してください。

P-GW や S-GW サービスへの eMPS プロファイルの関連付け

ここでは、eMPS プロファイルを P-GW や S-GW サービスに関連付ける方法について説明します。

```
configure
  context context_name
    pgw-service service_name
      associate emps-profile emps_profile_name
      end
```

```
configure
  context context_name
    Sgw-service service_name
      associate emps-profile emps_profile_name
      end
```

注：

- **no**：P-GW または S-GW サービスと eMPS プロファイの関連付けを無効にします。
- **associate emps-profile***emps_profile_name*：eMPS プロファイルを P-GW または S-GW サービスに関連付けます。

eMPSセッションのGx優先順位付けとワイヤレスプライオリティサービスの有効化

ここでは、eMPS セッションの Gx 優先順位付けレベルを有効にする方法について説明します

```
configure
  context context_name
    [ no ]ims-auth-service service_name
      [ no ] policy control
         [ no ] diameter origin endpoint  endpoint_name  priority-select

          [ no ] diameter session-prioritization
      end
```

注：

- **priority-select**：選択したIMS認証サービスのワイヤレスプライオリティサービス（WPS）を有効にします。



（注） WPS 機能では、**priority-select** キーワードは必須です。

- **[no] diameter session-prioritization**：eMPS セッションの Gx シグナリングの優先順位付けを有効または無効にします。
  - デフォルトでは、**diameter session-prioritization** CLI コマンドは無効になっており、Gx メッセージは WPS 値に基づいて優先順位付けされません。
  - 以前に設定されている場合は、**no diameter session-prioritization** CLI コマンドを使用してデフォルトの動作を設定します。
  - **diameter session-prioritization** CLI は、eMPS プロファイルとともに、Gx が設定で有効になっている場合に有効になります。
  - **diameter session-prioritization** 設定コマンドは、高優先順位チャネルを通過する Diameter メッセージに DRMP-0 AVP をアタッチします。DRA/PCRF は、P-GW から DRA または DRA から PCRF Gx のリンクで高優先順位チャネルから低優先順位チャネルへのフォールバックが発生した場合、DRMP-0 に基づいて適切なアクションを実行します。



（注） diameter session-prioritization は既存の CLI であり、WPS 機能の必須設定ではありません。

低優先度ピアと高優先度ピアの区別

ここでは、低優先度ピアと高優先度ピアを区別する方法について説明します。ポリシー制御の下の優先度エンドポイントの設定により、WPS 機能は、ポリシー制御領域の IMS 承認サービスにのみ適用されるようになります。Gx インターフェイスに適用されます。

```
configure
  context context_name
    [ no] diameter endpoint pgw-gx
      peer PGW-Gx-green-1  realm_address ipv4 address | ipv6 address
portport_number
      peer PGW-Gx-wps-1  realm_address ipv4 address | ipv6 address port
port_number priority-select origin-host-suffix value dscp value
    end
```

注：

- **priority-select**：ピアを高優先度の WPS ピアとして定義します。両方のパラメータを設定することはオプションです。ピアを設定するときは、次の条件が適用されます。
  - **priority-select** が設定されていない場合、ピアは高優先度の **WPS** ピアとして扱われません。
  - **origin-host-suffix**：**priority-select** がピアに設定されている場合、そのピアは **WPS** ピアとして扱われます。**wps** ピアに **Origin-host-suffix** が設定されている場合、設定された文字列が発信元ホスト ID に追加されます。そうでない場合は、デフォルトの **-wps** 文字列が発信ホスト ID に追加されます（pgw-gx-wps など）。
  - **dscp**：DSCP が高優先度ピアに設定されていない場合、エンドポイントレベルの DSCP が DRA/PCRF への IP パケットに書き込まれます。それ以外の場合は、設定された DSCP が IP パケットに書き込まれます。

モニタリングおよびトラブルシューティング

この項では、障害対応情報、show コマンドと出力、IMSA レベルの統計情報、Diameter 統計情報、およびバルク統計について説明します。

コマンドと出力の表示

この CLI コマンドを使用して、ルールインストールの失敗の統計、優先順位付けされた DRMP メッセージの数、WPS および非 WPS セッションの統計の各出力フィールドの詳細を表示します。

show ims-authorization policy-control statistics

この CLI コマンドを使用して、`Rule Installation Failure` 統計、優先順位付けされた DRMP メッセージの数、WPS および非 WPS セッションの統計の詳細に関する出力フィールドを表示します。

フィールド	説明
DPCA WPS Session Stats	
Total Current Sessions	このシステムで現在実行されている DPCA WPS セッションの総数
Switched from Priority Chnl	ワイヤレスプライオリティから通常に移動されたサブスクライバの合計を示します
Switched to Priority Chnl	通常からワイヤレスプライオリティに移動したサブスクライバの合計を示します
DPCA WPS Message Stats	
Priority Channel 高優先度チャネルで送受信された WPS セッションのメッセージの統計を示します。	
Total messages Received	IMS 承認ポリシー制御のために受信したポリシー制御メッセージの合計。
Total Messages Sent	IMS承認ポリシー制御サーバーに送信されたメッセージの合計。
Total CCR	受信したクレジット制御リクエスト（CCR）メッセージの合計。
Total CCA	CCRへの応答として送信されたクレジット制御応答（CCA）メッセージの合計。
CCR-Initial	受信した初期 CCR メッセージの総数。
CCA-Initial	初期 CCR メッセージへの応答として送信された初期 CCA メッセージの合計数。
CCA-Initial Accept	初期CCRメッセージへの応答として受信した初期CCAメッセージの合計数。
CCA-Initial Reject	初期の CCR メッセージに対する応答として拒否された初期 CCA メッセージの合計数。
CCA-Initial Dropped	S-GW復元、DPCAがオフであるか存在しない、またはIMSAセッションが保持モードであるためにドロップされたCCA-Iメッセージの合計数。
CCA-Initial Timeouts	初期CCRメッセージへの応答がタイムアウトした初期CCAメッセージの合計数。
CCR-Update	更新のための初期 CCR 後に受信したクレジット制御要求（CCR）メッセージの総数。

フィールド	説明
CCA-Update	CCR を更新するために応答として送信されたクレジット制御応答（CCA）メッセージの合計。
CCA-Update Timeouts	CCR を更新するために応答として送信されたがタイムアウトしたクレジット制御応答（CCA）メッセージの合計。
CCA-Update Errors	CCA-Updateメッセージの解析中に発生したエラーの合計数。
CCA-Update Dropped	S-GW復元、DPCAがオフであるか存在しない、またはIMSAセッションが保持モードであるためにドロップされたCCA-Uメッセージの合計数。
CCR-Final	アプリケーションを終了するために受信した最終 CCR メッセージの合計数。
CCA-Final	セッションを終了するための最終 CCR メッセージへの応答として送信された最終 CCA メッセージの合計数。
CCA-Final Timeouts	セッションを終了するための最終 CCR メッセージへの応答として送信されたがタイムアウトした最終 CCA メッセージの合計数。
CCA-Final Errors	CCA-Terminate メッセージの解析中に発生したエラーの合計数。
CCA-Final Dropped	S-GW復元、DPCAがオフであるか存在しない、またはIMSAセッションが保持モードであるためにドロップされたCCA-Tメッセージの合計数。
ASR	受信したセッション中止要求（ASR）の合計数。
ASA	セッション中止要求（ASR）への応答として送信されたセッション中止承諾（ASA）メッセージの合計数。
RAR	再承認のために受信した Re-Auth-Requests（RAR）の合計数。
RAA	再承認応答（RAA）メッセージ応答がある再承認要求（RAR）の合計数。
RAR-CCR collision	未処理のクレジット制御要求（CCR）メッセージがある場合に、PCRFから受信した再承認要求（RAR）メッセージの合計数。
Non-Priority Channel	**プライオリティチャネルで送受信されることが想定されるが、非プライオリティチャネルで送受信された WPS セッションのメッセージの統計を示します。**

フィールド	説明
Total messages Received	IMS 承認ポリシー制御のために受信したポリシー制御メッセージの合計。
Total Messages Sent	IMS承認ポリシー制御サーバーに送信されたメッセージの合計。
Total CCR	受信したクレジット制御リクエスト（CCR）メッセージの合計。
CCR-Initial	受信した初期 CCR メッセージの総数。
CCA-Initial	初期 CCR メッセージへの応答として送信された初期 CCA メッセージの合計数。
CCA-Initial Accept	初期CCRメッセージへの応答として受信した初期CCAメッセージの合計数。
CCA-Initial Reject	初期の CCR メッセージに対する応答として拒否された初期 CCA メッセージの合計数。
CCA-Initial Dropped	S-GW復元、DPCAがオフであるか存在しない、またはIMSAセッションが保持モードであるためにドロップされたCCA-Iメッセージの合計数。
CCA-Initial Timeouts	初期CCRメッセージへの応答がタイムアウトした初期CCAメッセージの合計数。
CCR-Update	更新のための初期 CCR 後に受信したクレジット制御要求（CCR）メッセージの総数。
CCA-Update	CCR を更新するために応答として送信されたクレジット制御応答（CCA）メッセージの合計。
CCA-Update Timeouts	CCR を更新するために応答として送信されたがタイムアウトしたクレジット制御応答（CCA）メッセージの合計。
CCA-Update Errors	CCA-Updateメッセージの解析中に発生したエラーの合計数。
CCA-Update Dropped	S-GW復元、DPCAがオフであるか存在しない、またはIMSAセッションが保持モードであるためにドロップされたCCA-Uメッセージの合計数。
CCR-Final	アプリケーションを終了するために受信した最終 CCR メッセージの合計数。
CCA-Final	最終 CCR メッセージに応答してセッションを終了するために送信された最終 CCA メッセージの合計数。

フィールド	説明
CCA-Final Timeouts	セッションを終了するための最終 CCR メッセージへの応答として送信されたがタイムアウトした最終 CCA メッセージの合計数。
CCA-Final Errors	CCA-Terminate メッセージの解析中に発生したエラーの合計数。
CCA-Final Dropped	S-GW 復元、DPCA がオフであるか存在しない、または IMSA セッションが保持モードであるために ドロップされた CCA-T メッセージの合計数。
ASR	受信したセッション中止要求（ASR）の合計数。
ASA	セッション中止要求（ASR）への応答として送信されたセッション中止承諾（ASA）メッセージの合計数。
RAR	再承認のために受信した Re-Auth-Requests（RAR）の合計数。
RAA	再承認応答（RAA）メッセージ応答がある再承認要求（RAR）の合計数。
RAR-CCR collision	未処理のクレジット制御要求（CCR）メッセージがある場合に、PCRF から受信した再承認要求（RAR）メッセージの合計数。

show diameter peers full all

この CLI コマンドを使用して、ピアの詳細を表示します。

フィールド	説明
優先順位チャネル	ピアの優先順位が高いかどうかを示します。次のオプションがあります。 • **Yes**：ピアが WPS であることを示します。 • **No**：ピアが非 WPS であることを示します。
設定済み DSCP	Gx IP パケットで使用される DSCP 値を示します。 • 設定されている場合、ピア固有の DSCP を表示します。 • 設定されていない場合、エンドポイントで設定された DSCP が表示されます。

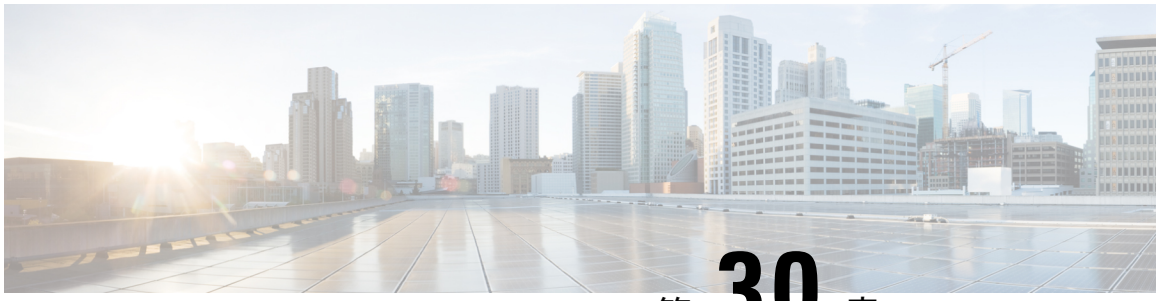
バルク統計

ここでは、P-GW のトランザクションまたは発信元ホスト機能に基づく動的トランスポート選択のバルク統計について説明します。

IMSA スキーマ

WPS と非 WPS のユーザーの高優先順位および低優先順位カテゴリを追跡するために、IMSA スキーマには次のバルク統計が含まれています。

カウンタ	説明
dpca-imsa-total-session-priority-channel	ワイヤレス優先サブスクライバの累積数を表示します。
dpca - imsa - total - sessions-switched -from - priority - channel	ワイヤレス優先から通常に移行したサブスクライバの累積数を示します。
dpca - imsa- total- sessions-switched - to- priority- channel	通常からワイヤレス優先に移行したサブスクライバの累積数を示します。



第 30 章

PCO を使用した ePDG の選択

- 機能説明 （529 ページ）
- 機能の仕組み （529 ページ）
- 制限事項 （530 ページ）
- PCO を使用した ePDG 選択の設定 （530 ページ）
- PCO を使用した ePDG 選択機能のモニタリングと障害対応 （531 ページ）

機能説明

この機能の目的は、PGW が通信事業者の PCO で ePDG の IP アドレスを送信できるようにして、Wi-Fi ネットワークへの接続時に UE が地理的に最も近い ePDG に接続されるようにすることです。これにより、最も近い ePDG への IPSEC トンネルのセットアップが容易になり、VoWIFI やその他の機能の遅延が減少します。

ネットワーク内の PCO オプションをカスタマイズするために、新しい CLI が導入されました。

重要 これはライセンスで制御される機能です。ライセンスの詳細については、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

重要 ePDG PCO は、S5-S8 インターフェイスで受信される CS 要求に対してのみサポートされます。この機能は、GGSN コールには適用されません。

機能の仕組み

- APN には 1 つの ePDG FQDN を設定できます。
- オペレータ固有の PCO は、S5/S8 インターフェイスの CSReq/Res および PMIP S2a インターフェイスの PBU/PBA でサポートされます。

- P-GW は FQDN 解決に DNS サーバーを使用します。
- 最大 2 つの IPv4 アドレスと 2 つの IPv6 ePDG アドレスを PCO で送信できます。

制限事項

この機能は、GGSN コールには適用されません。

PCO を使用した ePDG 選択の設定

epdg fqdn の設定

ネットワークでPCO（プロトコル設定オプション）オプションをカスタマイズするには、次の例を使用します。

```
configure
     apn apn_name
       pco-options epdg fqdn domain_name
       no pco-options
       end
```

注：

- **no:** カスタマイズされた PCO オプションをどの UE にも送信しません。
- **pco-options:** ネットワークでのカスタマイズされた PCO（プロトコル設定オプション）オプションの送信を制御します。
- **epdg:** PCO で通信事業者固有の epdg の選択を有効にします。デフォルト設定は無効です。
- **fqdn:** 完全修飾ドメイン名を指定します。これに基づいて、IP アドレスは DNS からクエリされます。

設定の確認

この機能の設定は、EXEC モードで次のコマンドを使用して確認できます。

- **show configuration**
- **show configuration verbose**

コマンド出力については、「モニタリングとトラブルシューティング」の項を参照してください。

PCO を使用した ePDG 選択機能のモニタリングと障害対応

次の項では、PCO機能を使用したePDG選択をモニターするために使用できるコマンドについて説明します。

PCO を使用した ePDG 選択機能の show コマンド

show apn *apn_name*

このコマンドを実行すると、次の出力が表示されます。

```
show apn name intershat
PCO Options:
    custom1      Mode: enabled
    Link MTU:    1500
    ePDG Selection FQDN: <epdg.com> / N.A.

APN QCI Stats: Disabled
Bearer duration stats config: Disabled
Event Reporting: Disabled

HSGW Static PGW-FQDN:
    Primary  FQDN: N/A   Secondary  FQDN: N/A
```

show config

このコマンドは変更され、ePDG が設定されている場合に次の出力が表示されるようになりました。

```
   pco-options epdg fqdn epdg.com
```

ユーザーが[supportrecord]セクションを指定していない場合は、showconfigurationverbose

このコマンドは、**epdg fqdn** が設定されている場合、次の出力を表示します。

```
 no pco-options epdg
```

show pgw-service statistics name

このコマンドを実行すると、次の出力が表示されます。

```
ePDG selection PCO statistics:

IPv6 PCO:
Request received: 20
Response sent: 18
Response not sent as configuration not present: 1
Response not sent as DNS query fails/ expires: 1
```

```
IPv4 PCO:
Request received: 20
Response sent: 18
Response not sent as configuration not present: 1
Response not sent as DNS query fails/ expires: 1
```

show saegw-service statistics name function pgw

このコマンドを実行すると、次の出力が表示されます。

```
ePDG selection PCO statistics:

IPv6 PCO:
Request received: 20
Response sent: 18
Response not sent as configuration not present: 1
Response not sent as DNS query fails/ expires: 1

IPv4 PCO:
Request received: 20
Response sent: 18
Response not sent as configuration not present: 1
Response not sent as DNS query fails/ expires: 1
```



第 31 章

IMSI をセッション ID に組み込む

- 機能の概要と変更履歴 （533 ページ）
- 機能説明 （534 ページ）
- 機能の仕組み （534 ページ）
- 制限事項 （535 ページ）
- Diameter 中間アカウンティング インターバルの設定 （536 ページ）
- モニタリングおよびトラブルシューティング （536 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• GGSN • P-GW • SAEGW • S-GW
該当プラットフォーム	• ASR 5500 • VPC - DI • VPC - Si
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A

関連資料	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *S-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.3

機能説明

Diameterインターフェイスに関連したネットワークの問題のトラブルシューティングと調査を行うには、サブスクライバまたはUE固有のDiameterトラフィックをフィルタリングすることが重要です。特定の IMSI に関連付けられたトラフィックは、IMSI 情報が Diameter Session ID AVP に組み込まれている場合は、Diameter セッション ID がなくても、簡単にフィルタリングできます。この機能により、オペレータはサブスクライバまたはUE固有のDiameterトラフィックをフィルタリングできます。

この機能では、Gx、Gy、および Gz（Rf）インターフェイスを介して Diameter Session ID AVP に IMSI を組み込むために、**diameter endpoint configuration** モードでの新しい CLI コマンド **session-id include imsi** が導入されています。

重要 この機能はライセンスで制御されています。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

機能の仕組み

新しい CLI コマンド **session-id include imsi** が **diameter endpoint configuration** モードに追加され、その Diameter エンドポイントに関連付けられているすべての Diameter セッションの Session-Id AVP への IMSI の包含を有効化または無効化できるようになりました。オペレータは、必要な Diameter エンドポイントのみを有効にし、Session-ID AVP への IMSI の包含を制御できます。**session-id include imsi** が各 Diameter エンドポイントで有効になっている場合、IMSI 情報は、Gx、Gy、および Gz（Rf）インターフェイスを介して Diameter Session-ID AVP に含められます。

「IMEI のみ」の緊急コールの場合、その緊急 PDN の IMSI 情報は利用できません。したがって、**session-id include imsi** が有効になっている場合、この IMSI 情報は、Gx、Gy、および Gz インターフェイスの Diameter Session-ID に含められません。**session-id include imsi** の設定は、新しい PDN 接続にのみ影響し、既存の PDN 接続動作（Gx、Gy、および Gz（Rf））インターフェイスには影響しません。たとえば、PDN 作成後の Gy Diameter エンドポイントに IMSI を含める CLI コマンドが有効になっていることがあります。この設定の変更後に新しい専用ベアラーが作成された場合、新しい専用ベアラーに対して確立された Gy セッションは、Gy Diameter セッション ID の IMSI に含められません。

セッション マネージャ リカバリ/ICSR の Session-ID AVP への影響はありません。Gx、Gy、および Gz（Rf）セッションに関連付けられたセッション ID は、（最新のエンドポイント設定に関係なく）透過的に回復されます。新しいセッションは、新しくアクティブになったシャーシの設定に従って、セッション ID を使用して起動します。

制限事項

この機能には次の既知の制限事項があります。

- IMSI 情報を機密情報とみなすと、通信事業者はこの CLI オプションを有効にする前にセキュリティ面を考慮する必要があります。
- 「IMEI のみ」の緊急コールの場合、IMSI 情報は緊急 PDN には使用できないため、Gx、Gy、および Gz（Rf）インターフェイスの Diameter Session-ID には含まれません。
- ICSR アップグレードシナリオでは、アップグレードされたシャーシが安定した状態で、ICSR ダウングレードの可能性がない場合にのみ、この新しい CLI オプションを有効にする必要があると想定されています。
- 新しいバージョンのシャーシで新しい CLI が有効になっている場合、ICSR ダウングレードは推奨されません。
- 新しい CLI オプションは古いソフトウェアバージョンでは使用できないため、ICSR ダウングレードは推奨されません。ICSR ダウングレードを実行すると、Session-ID の一部として IMSI が含まれる Diameter セッションに次の影響が発生します。
  - Gx および Gy：既存の Diameter セッション（Gx、Gy）は、古い形式の Session-ID でダウングレードされます。その場合、P-GW と PCRF の両方が同期していないため、P-GW または PCRF（またはその両方）でセッションがハングアップします。PCRF（RAR）/P-GW（CCR-U）からの通信は、古いセッションの削除につながる可能性があります。
  - Gz（Rf）：ただし、Rf セッションは適切に回復する必要があり、Rf シグナリングはすべて Rf サーバーに適切に送信されますが、応答を処理できません。これは、diamproxy が新しい形式のセッション ID を解析できず、Rf セッションは消去されるまで再び古い状態になるためです。

Diameter 中間アカウンティング インターバルの設定

次の CLI コマンドが **diameter endpoint** コンフィギュレーション モードに追加され、Gx、Gy、および Gz（Rf）の Diameter エンドポイントごとに IMSI が Diameter session-ID に含まれるようになりました。設定の変更は、Gx、Gy、および Rf の新しいセッションにのみ適用されます。設定の変更は、Gx、Gy、および Rf での既存のセッションの動作には影響しません。Gy の場合、サブスクライバごとに複数の Diameter セッションを開始でき、セッション ID 形式の設定はサブスクライバにバインドされます。この設定は、最初の Diameter セッションが確立されたときに有効になり、後続の Gy サブセッションでは最初のセッションで使用されたセッション ID 形式が引き続き使用されます。

```
configure
    context context_name
      diameter endpoint endpoint_name
         [no] session-id include imsi
         end
```

注：

- **session-id**：Diameter Session-ID 形式を示します。
- **include**：設定された情報を Diameter Session-ID に含めます。
- **imsi**：Diameter Session-ID に International Mobile Subscriber Identification（IMSI）を含めます。
- **no**：この機能を無効にします。つまり、IMSI は Diameter Session-ID に含まれません。これはデフォルトの動作です。
- デフォルトでは、CLI は無効になっているため、IMSI は Diameter Session-ID に入力されません。

モニタリングおよびトラブルシューティング

以下では、機能をモニターするために使用できるコマンドを説明します。

コマンドと出力の表示

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show configuration

上記のコマンドの出力が変更され、CLI が有効か無効かに応じて、次の新しいフィールドが表示されるようになりました。

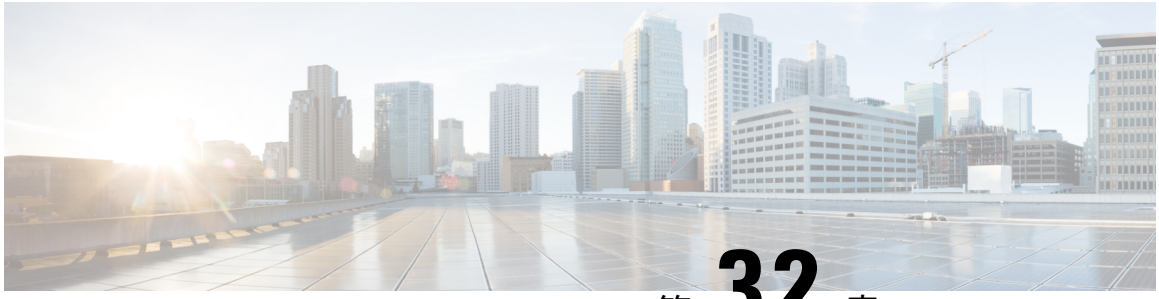
- session-id include imsi
- no session-id include imsi

show configuration [verbose]

上記のコマンドの出力が変更され、CLI が有効か無効かに応じて、次の新しいフィールドが表示されるようになりました。

- session-id include imsi
- no session-id include imsi

show configuration [verbose]



第 32 章

IMS APN の S6b の有効化

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （539 ページ）
- 変更された機能 （540 ページ）
- IMS APN の S6b を有効にするためのコマンドの設定 （541 ページ）
- 信頼できる Wi-Fi の S6b 認証の有効化 （541 ページ）
- コマンドと出力の表示 （542 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• GGSN • P-GW • SAEGW
該当プラットフォーム	すべて（All）
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

重要　リリース 21.2 および N5.1 よりも前に導入された機能の改訂履歴の詳細は示していません。

改訂の詳細	リリース
このリリースでは、S2a 承認が有効になっており、authorize-with-hss eGTP 設定を使用して、LTE インターフェイスと Wi-Fi インターフェイスの認証要求を分離しています。この機能により、S2aインターフェイスのみに対して、APN と P-GW サービスの両方で S6b 認証が有効になります。	21.21
この機能により、APN レベルで 3G アクセスに対する S6b 認証が有効になり、P-GW が新しい P-GW ID を HSS に対して更新できるようになります。	21.6
最初の導入。	21.2 よりも前

変更された機能

現在、P-GW は、GGSN サービスレベル設定での 3G アクセス用の S6b 認証の有効化をサポートしています。

LTE または Wi-Fi アクセスの場合、S6b 認証は、P-GW サービスレベルの設定と APN レベルの設定の両方でサポートされます。特定の APN に対して S6b 認証が有効になっている場合、LTE で参加したサブスクライバが Wi-Fi、次に 3G に転送すると、UE は 3G で IMS セッションの再登録を実行します。別の P-GW が選択されます。ただし、SGSN では新しい P-GW が更新されません。HSS には古い P-GW の履歴があります。サブスクライバが再び LTE に転送した後に Wi-Fi に転送する場合、元の P-GW に引き継ぎます。とはいえ、古い P-GW には新しい IMS セッションがないため、引き継ぎに失敗します。この機能により、APN レベルで 3G アクセスに対する S6b 承認が有効になり、P-GW が新しい P-GW ID を HSS に更新できるようになります。この方法で不整合に対処します。次の 2 つの **authorize-with-hss** CLI キーワードが APN レベルで追加され、3G アクセスおよび GnGp ハンドオーバーのための S6b 認証が有効になります。

- **gn-gp-enabled**：コール接続時および gn-gp ハンドオーバー時に、3G アクセス用の S6b 認証を有効にします。
- **gn-gp-disabled**：サブスクライバが 3G アクセスに移行すると、S6b 接続を終了します。これは、設定に関係なくセッションが続行された従来のハンドオーバー動作をオーバーライドするために使用されます。

（注） **authorize-with-hss** または **authorize-with-hss egtp** が設定されている場合、これらの新しいキーワードはデフォルトでは設定されません。この機能のために導入されたCLIコマンドを設定して、カスタマイズされたこの動作を明示的に有効にする必要があります。

S6b 認証の機能拡張：StarOS 21.21 以降のリリースでは、S2a 認証が有効になっており、**authorize-with-hss egtp** 設定を使用して、LTE インターフェイスと Wi-Fi インターフェイスの認証要求を分離しています。この機能により、S2aインターフェイスのみに対して、APN と P-GW サービスの両方で S6b 認証が有効になります。

IMS APN の S6b を有効にするためのコマンドの設定

S6b 認証は APN レベルで有効にできます。**authorize-with-hss** CLI コマンドに 2 つの新しいキーワードが追加されました。

S6b を有効または無効にするには、次のコマンドを実行します。

```
configure
   context context_name
      apn apn_name
       authorize-with-hss [ egtp [ gn-gp-enabled ] [ s2b [ gn-gp-enabled
 [ report-ipv6-addr ] ] ] [ s5-s8 [ gn-gp-disabled | gn-gp-enabled ] ]
 [ report-ipv6-addr ] | lma [ s6b-aaa-group aaa-group-name |
report-ipv6-addr ] | report-ipv6-addr ]
        [ default | no ] authorize-with-hss
        exit
```

注：

- **gn-gp-disabled**：3G 初期接続および GNGP ハンドオーバーの S6b 承認を無効にします。
- **gn-gp-enabled**：3G 初期接続および GNGP ハンドオーバーの S6b 承認を有効にします。
- **s2b**：egtp-S2b の S6b 承認を有効にします。
- **s5-s8**：egtp-S5S8 の S6b 承認を有効にします。
- **report-ipv6-addr**：S6b インターフェイスへの AAR を介した IPv6 レポートを有効にします。

信頼できる Wi-Fi の S6b 認証の有効化

信頼できる Wi-Fi の S6b 認証の有効化

S6b 認証は、HSS 認証プロセスを使用するすべての LTE および Wi-Fi インターフェイスで有効になっています。LTE インターフェイスと Wi-Fi インターフェイスで認証要求を分離するため

に、新しい設定が導入されました。**authorize-with-hss egtp** の設定部分に、信頼できる Wi-Fi インターフェイスを表すパラメータ S2a が追加されました。これにより、S2A インターフェイスのみに対して S6b 認証が有効になります。これは、APN と P-GW の両方のサービス設定で実行されます。

次の S2a 設定コマンドを使用して、信頼できる Wi-Fi を authorize-with-hss egtp で指定します。

```
configure
  context context_name
    apn apn_name| pgw-service service_name
     authorize-with-hss [ egtp [s2a [gn-gp-enabled [report-ipv6-addr]
] ] ]
       [ default | no ] authorize-with-hss
       exit
```



（注） S2a と S2b、S2a と S5-S8、または S2b と S5-S8 の組み合わせで S6b 認証を有効にできます。

APN および P-GW サービスで S2a インターフェイスのみの S6b 認証を有効にする例を以下に示します。

APN サービスの例

```
apn intershat
     pdp-type ipv4 ipv6
     bearer-control-mode mixed
     selection-mode subscribed sent-by-ms chosen-by-sgsn
     authorize-with-hss egtp s2a
     ims-auth-service ims-ggsn-auth
     ip access-group acl4-1 in
     ip access-group acl4-1 out
     ip context-name egress
     ipv6 access-group acl6-1 in
     ipv6 access-group acl6-1 out
     active-charging rulebase prepaid
   exit
```

P-GW サービスの例

```
 pgw-service pgw_service
     authorize-with-hss egtp s2a
     associate ggsn-service ggsn-service
     associate egtp-service egtp_service
     associate peer-map map_pgw
     egtp create-session-rsp apn-ambr-always-include
   exit
```

コマンドと出力の表示

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show apn name

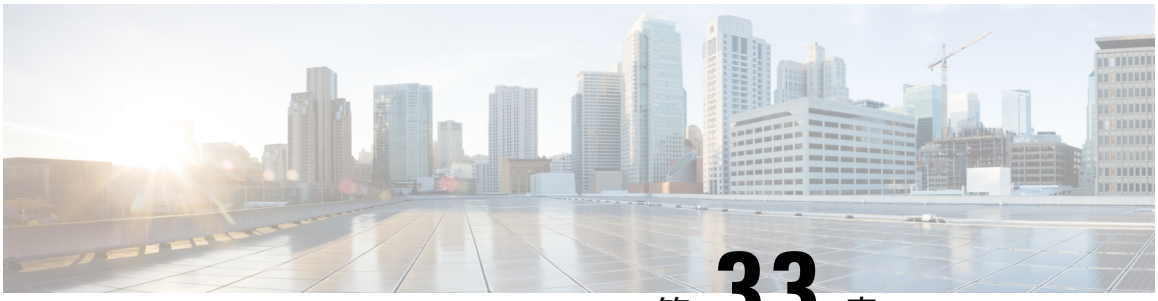
この CLI コマンドが変更され、gn-gp の有効または無効ステータスが追加されました。

- S6b での認証：HSS-EGTP-S5S8 GN-GP-Disabled
- S6b での認証：HSS-EGTP-S5S8 GN-GP-Enabled

show config apn intershat

gn-gp の有効または無効ステータスを示すために、次の新しいフィールドが show コマンドに追加されました。

- authorize-with-hss egtp s5-s8 gn-gp-enabled
- authorize-with-hss egtp s5-s8 gn-gp-disabled



第 33 章

ePDGおよびP-GWでの緊急コールのサポート

この機能により、ePDG および P-GW での緊急コールのサポートが可能になります。

- 機能の概要と変更履歴 （545 ページ）
- 機能説明 （546 ページ）
- 機能の仕組み （547 ページ）
- S2b 緊急通話の AAA 障害処理の設定 （555 ページ）
- APN および S6b 承認の設定 （557 ページ）
- モニタリングおよびトラブルシューティング （558 ページ）

機能の概要と変更履歴

該当製品または機能エリア	P-GW SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、S2b インターフェイスからの新しい緊急コールがサポートされています。 **重要** この機能は、このリリースでは完全には機能しておらず、テスト目的でのみ使用できます。詳細については、シスコのアカウント担当者にお問い合わせください。	21.20
初版	21.1

機能説明

ePDG と P-GW により、3GPP リリース 13 に従って、P-GW の信頼できない Wi-Fi を介した緊急通話の確立がサポートされます。IMS 緊急セッションをサポートするために緊急ベアラーサービスが提供されます。緊急ベアラーサービスとは、緊急サービスをサポートするようにネットワークが設定されている場合に、サービスを提供しているネットワークによって提供される機能を指します。緊急ベアラーサービスは、通常どおりにアタッチされた UE のほかに、現地の規制に応じてサービスが制限されている UE に提供されます。限定的なサービス状態での緊急サービスの受信には、サブスクリプションは不要です。

Diameter への認証承認要求（AAA）が、信頼できない Wi-Fi 緊急通話用の新しい Emergency-Indication AVP を伝送するようになりました。緊急サービス用の PDN 接続に関連する Diameter 要求が最も優先されます。地域/国の要件やネットワーク通信事業者のポリシーに応じて、これらの Diameter 要求は、3GPP AAA サーバーでトラフィックの削減を適用する必要がある場合に最後にスロットルされます。

サポートされる機能

ePDG および P-GW の 3GPP リリース 13 の緊急通話のサポート対象には、次の機能が含まれます。

- P-GW の信頼できない Wi-Fi を介した緊急通話の確立。P-GW には、緊急 PDN 接続の確立時にのみ、AAA S6b インターフェイスを介した新しい **Emergency-Indication** AVP が含まれます。
- 合法的傍受が、S2b インターフェイスを介した緊急 PDN でサポートされます。
- さまざまなセッション作成要求メッセージ IE が変更され、緊急ベアラーの確立の 4 種類の動作すべてをサポートするようになりました。
- シャーシ内およびシャーシ間リカバリが、S2b インターフェイスを介した緊急通話でサポートされます。

- ネットワークで開始される専用ベアラーの作成が、S2b インターフェイスを介した緊急通話でサポートされます。
- 緊急 APN では、最大 APN 制限は無視されます。
- 複数の PDN が、S2b インターフェイスを介した緊急通話でサポートされます。
- 同じ IMEI で IMSI を使用せずに S2b インターフェイスを介して緊急通話のコンテキストを置換することが可能です。
- P-GW の緊急関連の統計とバルク統計を利用できます。
- S2b 緊急通話のグレースフルシャットダウンがサポートされています。

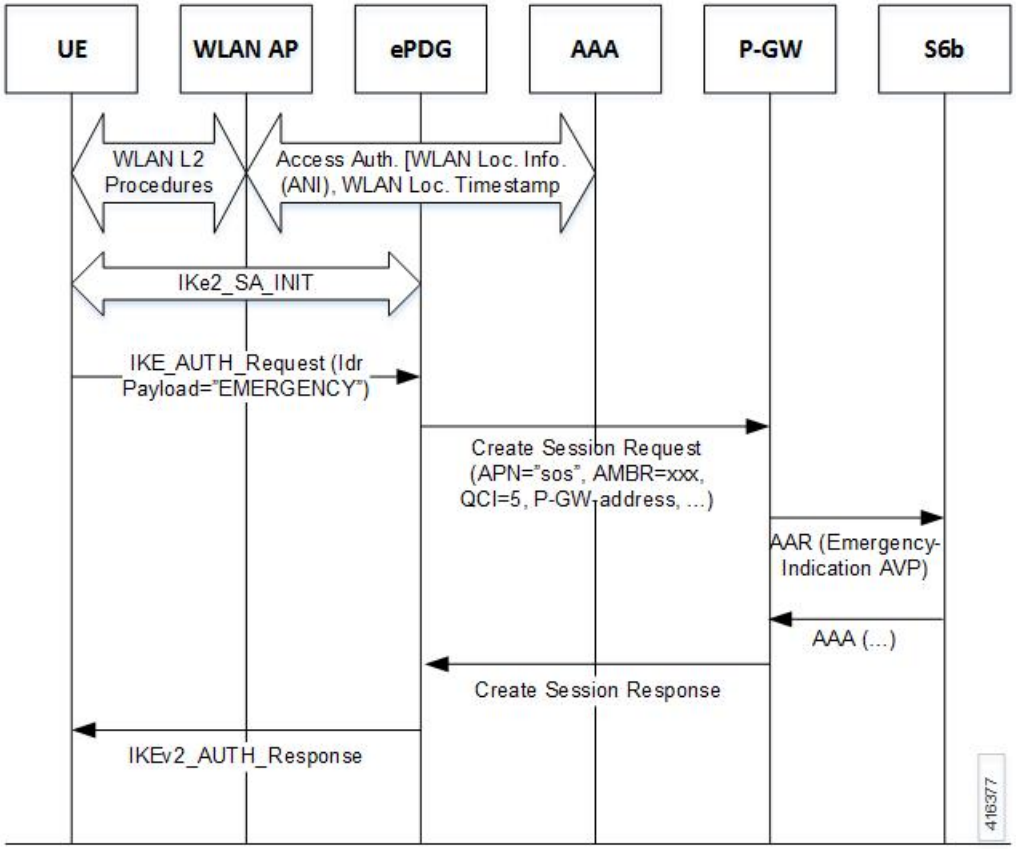
以前の動作：緊急通話はS2bインターフェイスではサポートされていませんでした。また、s2b インターフェイスと LTE 間のハンドオフは、緊急通報ではサポートされていませんでした。

新しい動作：緊急通話が S2b インターフェイスでサポートされるようになり、S2b インターフェイスからLTEへの緊急通話のハンドオーバーとその逆も「認証されたIMSI」でのみサポートされます。

機能の仕組み

ePDGは、セッション作成要求（CSReq）メッセージをP-GWに送信します。P-GWは、CSReq メッセージで受信したアクセスポイント名（APN）から、適用する緊急関連ポリシーを推測します。緊急にアタッチされたユーザー機器（UE）では、国際モバイルステーション識別子（IMSI）を認証できない場合、またはUEがそれを提供していない場合、国際モバイル機器識別子（IMEI）が UE 識別子として使用されます。

図 *39 :* コールフロー：*ePDG* および *P-GW* での *3GPP R13* 緊急コールのサポート



P-GW は、3GPP AAA サーバーが緊急サービスに特定のポリシーのみを適用するように、S6b インターフェイスを介して **Emergency-Indication** AVP を送信します。未認証の UE の場合、3GPP AAA サーバーは、ホームサブスクライバサーバー（HSS）を P-GW のアイデンティティで更新しません。認証済みの UE の場合、この通知は「PDN GW currently in use for emergency services」というメッセージとともに送信されます。このメッセージには、PDN GW アドレスと、PDN 接続が HSS への緊急サービス向けであること示す通知が含まれており、HSS はこの情報を緊急サービス用の UE コンテキストの一部として保存します。

緊急ベアラー確立に関する 4 つの異なる動作すべてがサポートされます。

- 有効な UE のみ。
- 認証済みの UE のみを許可。
- IMSI は必須、認証はオプション。
- すべての UE を許可。

このセクションでは、新しい属性値ペア（AVP）と、この機能をサポートする変更された情報要素について説明します。

Emergency-Indication AVP

新しい **Emergency-Indication** AVP は、認証および承認要求で、緊急サービス用の PDN 接続を確立する要求をシグナリングするよう定義されています。

情報要素

このセクションでは、機能と適切に連動するように変更されたセッション作成要求に含まれるその他の重要な要素について説明します。

表 *51 :* セッション作成要求の情報要素

情報要素	P	条件/コメント	IE タイプ	Ins.
IMSI	C	IMSI は、S4/S11 インターフェイスのメッセージに含まれており、MME/SGSN によって提供されている場合は S5/S8 インターフェイスのメッセージにも含まれます。ただし、次の場合を除きます。 UE が緊急でアタッチされ、UE が UICCless の場合。 IMSI は、S4/S11 インターフェイスのメッセージに含まれており、MME/SGSN によって提供されている場合は S5/S8 インターフェイスのメッセージにも含まれます。ただし、識別子としては使用されません。 - UE が緊急アタッチされているものの、IMSI が認証されていない場合。 IMSI は、S2a/S2b インターフェイスのメッセージに含まれています。	IMSI	0

情報要素	P	条件/コメント	IE タイプ	Ins.
[MSISDN]	C	E-UTRAN 初期アタッチ、および信頼できるまたは信頼できない非 3GPP IP アクセスから E-UTRAN へのハンドオーバーでは、S11 インターフェイスで使用される場合は IE が含まれます（HSS からのサブスクリプションデータで提供される場合）。PDP コンテキストのアクティブ化手順、および信頼できるまたは信頼できない非 3GPP IP アクセスから UTRAN/GERAN へのハンドオーバーでは、S4 インターフェイスで使用される場合は IE が含まれます（HSS からのサブスクリプションデータで提供される場合）。 IE は、UE 要求 PDN 接続の際、MME がその UE 用に IE を保存している場合に含まれます。MME/SGSN によって提供されているなら、S5/S8 インターフェイスで使用される場合に含まれます。 ePDG は、S2b 上の GTP を使用したアタッチ、S2b 上の GTP を使用した追加の PDN に対する UE 開始の接続、および S2b 上の GTP を使用した信頼できない非 3GPP IP アクセスに対するハンドオーバー、緊急セッションのための初期アタッチ（S2b 上の GTP）で、HSS/AAA によって提供されている場合、S2b インターフェイスにこの IE を含めます。 TWAN は、GTP S2a 上の WLAN での初期アタッチ、S2a 上の GTP を使用した追加の PDN に対する UE 開始の接続、S2a 上の GTP を使用した TWAN へのハンドオーバーで、HSS/AAA によって提供されている場合、S2a インターフェイスにこの IE を含めます。	[MSISDN]	0

情報要素	P	条件/コメント	IE タイプ	Ins.
ME アイデンティティ（MEI）	C	MME/SGSN には、S11/S4 インターフェイス上の ME アイデンティティ（MEI）IE が含まれています。 - UE が緊急でアタッチされ、UE が UICCless の場合。 - UE が緊急アタッチされているときに、IMSI が認証されていない場合。 それ以外のすべての場合、MME/SGSN には S11/S4 インターフェイス上の ME アイデンティティ（MEI）IE が含まれています（使用可能な場合）。	MEI	0
	CO	TWAN/ePDG には S2a/S2b インターフェイス上の ME Identity（MEI）IE が含まれます（可能な場合）。		
サービス提供ネットワーク	C	この IE は、E-UTRAN 初期アタッチ、信頼できるまたは信頼できない非 3GPP IP アクセスから E-UTRAN へのハンドオーバー、PDP コンテキストのアクティブ化、信頼できるまたは信頼できない非 3GPP IP アクセスから UTRAN/GERAN へのハンドオーバー、UE の要求した PDN 接続、S2b 上の GTP を使用したアタッチ、S2b 上の GTP を使用した追加の PDN への UE 開始の接続、S2b 上の GTP を使用した信頼できない非 3GPP IP アクセスへのハンドオーバー、および緊急セッションのための初期アタッチ（S2b 上の GTP）で、S4/S11、S5/S8 および S2b インターフェイスに含まれます。	サービス提供ネットワーク	0
通知フラグ	C	この IE は、該当するフラグのいずれかが 1 に設定されている場合に含まれます。 該当するフラグは次のとおりです。 - 未認証 IMSI：メッセージ内に存在する IMSI が認証されておらず、緊急アタッチ UE 用である場合、S4/S11 および S5/S8 インターフェイスでこのフラグが 1 に設定されます。	説明	0

情報要素	P	条件/コメント	IE タイプ	Ins.
選択モード	C	この IE は、この IE は、E-UTRAN 初期アタッチ、信頼できるまたは信頼できない非 3GPP IP アクセスから E-UTRAN へのハンドオーバー、PDP コンテキストのアクティブ化、信頼できるまたは信頼できない非 3GPP IP アクセスから UTRAN/GERAN へのハンドオーバー、および UE の要求した PDN 接続で、S4/S11 および S5/S8 インターフェイスに含まれます。 この IE は、S2b 上の GTP を使用した初期アタッチ、S2b 上の GTP を使用した信頼できない非 3GPP IP アクセスへのハンドオーバー、S2b 上の GTP を使用した追加の PDN への UE 開始の接続、および緊急セッションのための初期アタッチで、S2b インターフェイスに含まれます（S2b 上の GTP）。 IE は、UE/MME/SGSN/ePDG/TWAN によって登録済み APN と未登録 APN のどちらが選択されたかを示します。 この IE は、GTP S2a 上の WLAN での初期アタッチ、S2a 上の GTP を使用した TWAN へのハンドオーバー、および S2a 上の GTP を使用した追加の PDN への UE 開始の接続で、S2a インターフェイスに含まれます。値は「MS or network provided APN, subscription verified」に設定されます。	選択モード	0
	CO	使用可能な場合、この IE は、S-GW の再配置による TAU/RAU/HO 時に、S11/S4 インターフェイス上の MME/SGSN によって送信されます。		
UE ローカル IP アドレス	CO	ePDG は、緊急セッションのための初期アタッチ（S2b 上の GTP）中、S2b インターフェイスにこの IE を含めます。それ以外の場合、ePDG は、ローカルポリシーに基づいて S2b インターフェイスにこの IE を含める必要があります。	IP Address	0
UE PDP ポート	CO	NAT が検出されており、UE ローカル IP アドレスが存在する場合、ePDG は S2b インターフェイスにこの IE を含めます。	ポート番号（Port Number）	0
WLAN ロケーション情報	CO	この IE は、WLAN ロケーション情報が使用可能な場合、S2b インターフェイスに含まれます。	TWAN 識別子	1

情報要素	P	条件/コメント	IE タイプ	Ins.
WLAN ロケーションタイムスタンプ	CO	この IE は、WLAN ロケーションタイムスタンプが使用可能な場合、S2b インターフェイスに含まれます。	TWAN 識別子タイムスタンプ	0

緊急ハンドオーバーのサポート

サブスクライバが WLAN 経由で緊急コールを発信すると、ユーザー機器（UE）は *NAI* に *sos* を追加して、これが ePDG への緊急アタッチであることを示します。 ePDG は、セッション作成要求でこの緊急アタッチについて P ゲートウェイに通知します。発信者が WLAN から LTE のカバレッジに移動した場合、またはその逆に移動した場合、コールはドロップされることなく引き渡されます。

P-GW は、次の緊急コールのハンドオーバーをサポートしています。

- **LTE から Wi-Fi（S2b）への緊急コールのハンドオーバー**：認証済み UE での LTE から Wi-Fi（S2b）への緊急コールのハンドオーバーがサポートされます。UE が LTE から信頼できない Wi-Fi に移行する際、LTE は、S6b サーバーへの認証承認要求（AAR）をトリガーし、その認証承認要求（AAR）で送信された *Emergency-Indication* AVP を使用します。また、Wi-Fi（S2b）コールのクリア時に STR が送信されます。

  1. ePDG が、セッション作成要求を P-GW に送信します。
  2. UE が IKE 設定要求で P-CSCF を要求した場合は、P-CSCF が要求されます。
  3. ダウンリンクパケットが LTE アクセスで送信されます。ePDG には、GTPv2 セッション作成要求の PAA（PDN アドレス割り当て）で UE からの IKE メッセージ内で受信した IP アドレスが含まれます。
  4. P-GW が、3GPP AAA に AAR を送信して、サブスクライバの APN を承認し、APN の HSS 上の P-GW アドレスを更新します。
  5. P-GW が、クレジット制御要求（CCR）を使用して IP-CAN 変更の指示を PCRF に送信します。
  6. 3GPP AAA が、AAA を P-GW に送信します。
  7. ポリシーおよび課金ルール機能（PCRF）は、クレジット制御応答（CCA）で IP-CAN セッション変更を承認します。
  8. P-GW が、S5 セッションを識別し、要求された IP アドレスセッションを再割り当てして、セッション作成応答メッセージで ePDG に応答します。
  9. ePDG が、ベアラー作成応答メッセージを送信します。
  10. P-GW が、ベアラー削除要求メッセージを送信します。
  11. S-GW が、P-GW にベアラー削除応答メッセージを送信します。

- **Wi-Fi（S2b）から LTE への緊急コールのハンドオーバー**：認証済み UE での Wi-Fi（s2b）から LTE への緊急コールのハンドオーバーがサポートされます。LTE の緊急コールでは S6b インターフェイス承認が有効になっていないため、信頼できない Wi-Fi から LTE への緊急コールのハンドオーバーは、S6b サーバーへのセッション終了要求（STR）をトリガーします。

  1. MME が、MME 緊急設定データから P-GW を選択し、セッション作成要求を送信します。
  2. S-GW が、セッション作成要求を送信します。
  3. P-GW は、Gx 認証が有効になっているか、または P-GW がローカルポリシーを適用しており、ローカルポリシーが設定されているかどうかを問い合わせない場合、クレジット制御要求（CCR）で IP-CAN 変更の通知を PCRF に送信します。P-GW が、S6b サーバーにセッション終了要求を送信し、PAA で IPv6 プレフィックスや IPv4 アドレスを提供します。

（注） MME がピギーバックのサポートを表明している場合、P-GW は、ベアラー要求メッセージをセッション作成応答メッセージにピギーバックします。

  4. MME が、S-GW にベアラー変更要求を送信します。
  5. S-GW が、各メッセージを個別に処理します。S-GW が、ベアラー作成応答を P-GW に転送します（ピギーバックなし）。

- **HO = 0 での緊急 PDN ハンドオーバー**：LTE から Wi-Fi へのハンドオーバーがサポートされます。

  1. ePDG が、セッション作成要求を P-GW に送信します。UE が IKE Config 要求で P-CSCF を要求した場合は、P-CSCF が要求されます。

（注） セッションが WLAN にハンドオーバーされている間は、P-GW でダウンリンクパケットがドロップされます。

  2. P-GW は LTE セッションをチェックします。
  3. LTE セッションがある場合、P-GW は、3GPP AAA に AAR を送信して、サブスクライバの APN を承認し、APN の HSS 上の P-GW アドレスを更新します。
  4. 3GPP AAA が、AAA を P-GW に送信します。
  5. P-GW が、クレジット制御要求（CCR）を使用して IP-CAN 変更の指示を PCRF に送信します。

6. PCRF が、クレジット制御応答（CCA）メッセージで IP-CAN セッション変更を確認応答します。このメッセージには、ポリシールールと課金ルールが含まれます。P-GW が、P-GW で報告する必要があるイベントを適用およびトリガーします。
7. オンラインフラグが有効になっていて、P-GW に WLAN 料金設定グループのクォータがない場合、またはオンライン課金サーバー (OCS) が以前に WLAN 料金設定グループの 4011 を送信していない場合、P-GW は、使用状況をレポートする OCS に CCR-u を送信します。
8. P-GW が、S5 セッションを識別し、要求された IP アドレスセッションを再割り当てして、セッション作成応答メッセージで ePDG に応答します。
9. P-GW が、セッション作成応答を送信した後、中間アカウンティング要求（ACR）を OFCS に送信します。
10. OFCS が、P-GW に ACA で応答します。
11. P-GW が、S-GW にベアラー削除要求を送信します。
12. S-GW が、P-GW にベアラー削除応答を送信します。

S2b 緊急通話の AAA 障害処理の設定

S6b サーバーからの障害によって S2b インターフェイス経由の緊急通話が拒否されないようにする必要があります。それには、緊急通報に使用される APN での障害処理を設定する必要があります。

処理は、結果コードで示される障害とは無関係に緊急通話が続行されるよう、**aaa group** で設定します。

S2b 緊急通話の AAA 障害処理を設定するには、次のようにします。

```
configure
  context ingress_context_name
    aaa group default
      diameter authentication failure-handling authorization-request
result-code 3000 to 5999 action continue
       diameter authentication failure-handling authorization-request
request-timeout action continue
           end
```

以下の前提条件があることに注意してください。

- PCRF によってトリガーされた IP CAN セッション変更要求により、デフォルトのベアラー QCI と IMS シグナリングに使用される QCI 以外の QCI を持つすべての PCC ルールが削除されると、PCEF は設定可能な緊急非アクティブタイマーを起動します。設定された期間が過ぎると、P-GW は、IMS 緊急セッションにサービスを提供する IP CAN セッションの IP CAN セッション終了要求を開始します。

- Gx または S6b インターフェイスが緊急 APN として設定されていない仮想 APN を返した場合、通話は原因コード「APN_DENIED_NO_SUBSCRIPTION」で拒否されます。

Gx 障害（PCRF がダウン）の障害処理テンプレートを設定するには、次のようにします。

```
configure
  failure-handling-template gx_template
    msg-type any failure-type diabase-error action continue
local-fallback
       end
```

次の例は、Gx 障害（PCRF が ErrorCode を返した）の障害処理テンプレート設定を示しています。

```
configure
  failure-handling-template gx_template
     msg-type credit-control-initial failure-type diameter result-code
 3000 to 5999 action continue local-fallback
         msg-type credit-control-update failure-type diameter
result-code 3000 to 5999 action continue local-fallback
            end
```

次の例は、Gx 遅延応答での障害処理テンプレート設定を示しています。

```
configure
  failure-handling-template gx_template
    msg-type credit-control-initial failure-type resp-timeout action
continue
       msg-type credit-control-update failure-type resp-timeout action
 continue
         end
```

Gx 障害（PCRF がダウン、または PCRF が ErrorCode を返した）でのローカルポリシーを設定するには、次のようにします。

```
configure
        local-policy-service service_name
          ruledef  ruledef_name
             condition priority  priority  { variable { eq | ge | gt | le
 | lt | match | ne | nomatch } regex | string_value | int_value | set
}
            end
```

```
configure
  local-policy-service service_name
    actiondef   actiondef_name
      action priority  priorityaction_name arguments
        end
```

```
configure
  local-policy-service service_name
    eventbase   eventbase_name
      rule priority  priority   [ event list_of_events ] ruledef
```

```
ruledef_name actiondef actiondef_name [ continue ]
        end
configure
   contextcontect_name
      ims-auth-service   service_name
         [ no ] policy-control
            associate failure-handling-template gx_template
               associate local-policy-service  service_name
                  end
```

APN および S6b 承認の設定

LTE で緊急 PDN をアタッチするための APN の設定

S6b Gx を使用した緊急 PDN ハンドオーバーの場合、LTE で緊急 PDN をアタッチするように APN モードを設定します。

```
configure
   context context_name
      apn apn_name
         emergency-apn
         end
```

S6b 承認の有効化

次に、S6b 承認を有効にする設定例を示します。

```
configure
   context context_name
      pgw-service  service_name
         apn apn_name
          authorize-with-hss  [ egtp[gn-gp-enabled] [ s2b [gn-gp-enabled]
 [ s5-s8 [gn-gp-enabled | gn-gp-enabled]] [ report-ipv6-addr ]| lma [
s6b-aaa-group aaa-group-name  | report-ipv6-addr ] | report-ipv6-addr
] [ default | no ] authorize-with-hss
            end
```

S2b インターフェイス eGTP サービスの有効化

S2b インターフェイス eGTP サービスを有効にするには、次の設定を使用します。

```
configure
   context context_name
      egtp-service service_name
```

```
        interface-type { interface-cgw-egress | interface-epdg-egress
| interface-mme | interface-pgw-ingress [ s2a ] [ s2b ] | interface-sgsn
 | interface-sgw-egress | interface-sgw-ingress }

        end
```

設定例に従って、S2b インターフェイス eGTP サービスを有効にします。

```
configure
         context EPC2
           egtp-service PGW21EGTP
            interface-type  | interface-pgw-ingress [ s2b ] [ s2a ]
                              end
```

モニタリングおよびトラブルシューティング

以下の項では、機能をモニターするために使用できるコマンドについて説明します。

show コマンドと出力

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

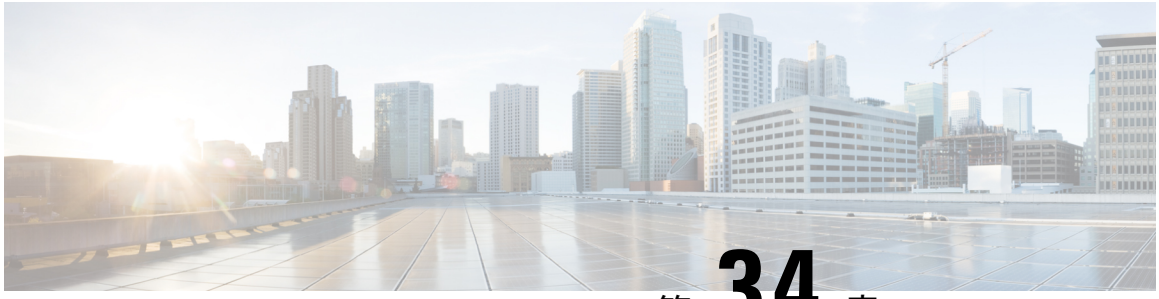
show apn

```
pdp type:  ipv4 and ipv6
apn type:  emergency
ehrpd access: N/A
absolute timeout :  0            idle timeout :  0
emergency inactivity timeout :  1000
idle-timeout-activity ignore-downlink:   Disabled
…..
```

show pgw- service-statistics-all

```
pgw# show pgw-service statistics all
PGW Node Level Statistics:
VPN Name: local
Total bearers active:
  Default bearers:    5                                   Dedicated bearers:  5
    Normal bearers:   2                                   UE-initiated:  0
    Emergency bearers (Auth-IMSI): 1                      Network-initiated: 5
    Emergency bearers (Unauth-IMSI):1                     Normal bearers:   2
    Emergency bearers (Only IMEI): 1                      Emergency bearers (Auth-IMSI):
  1
    Emergency bearers (Unauth-IMSI):1

    Emergency bearers (Only IMEI): 1
```



第 34 章

VoLTE/緊急コールの拡張優先順位付け

この章では、P-GW、SAE-GW、および S-GW での VoLTE/緊急コールの拡張優先順位付け機能に対する StarOS のサポートについて説明します。

- 機能説明 （559 ページ）
- 機能の仕組み （561 ページ）
- VoLTE/緊急コールの拡張優先順位付けの設定 （562 ページ）
- VoLTE/緊急コールの拡張優先順位付けのモニタリングと障害対応 （565 ページ）

機能説明

National Security/Emergency Preparedness（NS/EP）Next Generation Network（NGN）Priority Services（NGN-PS）（旧称 NGN Government Emergency Telecommunications Service（GETS））とは、パブリックパケット交換サービスプロバイダーから利用可能なサービスに基づく一連の音声、動画、およびデータのサービスです。NS/EP NGN-PS は、サービスユーザーの NS/EP 通信に関する優先処理を提供するものであり、サービスプロバイダーのネットワークで、輻輳を原因とする障害が発生したり、自然災害（洪水、地震、ハリケーンなど）による損傷が発生したり、人為的な災害（物理攻撃、サイバー攻撃、または他の形態のテロ攻撃など）が発生したりした場合に特に必要です。

P-GW および S-GW からの制御メッセージの DSCP マーキングは、関連付けられている egtpc-service 設定に基づいていました。

eMPS セッションに属する制御メッセージ、または eMPS プロファイルに関連付けられている割り当ておよび保持プライオリティ（ARP）を含む制御メッセージの場合、DSCP マーキングは eMPS プロファイルで設定された DSCP 値に基づいています。

この機能拡張の一部として、Government Industry Requirements（GIR）NS/EP NGN で定義されている優先処理のために、P-GW および S-GW で特定の GTP-C メッセージをマーキングするためのサポートも追加されています。

他の機能との関係

ARP 値別の GTP-C メッセージのバルク統計：S-GW/P-GW は、NS/EP NGN-PS の使用に割り当てられた値のセットから選択された ARP を含む、受信した GTP-C メッセージの総数のペグカウントを指定された間隔（分単位）で生成します。このペグカウントは、S-GW/P-GW レベルで管理されます。

eMPS PDN に対応する GTP-C メッセージ、または NS/EP NGN 優先サービス用に予約された設定済み ARP（PL）のセットからの ARP を含むメッセージのスロットリングを防ぐために、次の設定が考慮されます。

1. **負荷の過負荷制御**

   過負荷制御プロファイルでは、eMPS サービス用に NS/EP NGN-PS の使用のために予約されている ARP のセットも **throttling-behavior exclude** および **self-protection-behavior exclude** CLI コマンドで定義する必要があります。これにより、eMPS PDN の着信 GTP-C メッセージや、eMPS の使用のために予約された ARP のセットからの ARP を含む着信 GTP-C メッセージがスロットリングされなくなります。負荷の過負荷構成の設定例：

   ```
   configure
     gtpc-overload-control-profile profile_name
       throttling-behavior { earp { 1...15 } * } { exclude }
       self-protection-behavior { earp { 1...15 } * }  { exclude }
       end
   ```

2. **輻輳状態でのコールの優先処理の場合**

   eMPS サービス用に NS/EP NGN-PS で予約された ARP を、次の輻輳制御 CLI コマンドで設定することをお勧めします。これにより、コンテキストレベルで **congestion-control** CLI コマンドによって定義された輻輳状態の間に、新しいコール要求がスロットリングされなくなります。

   ```
   configure
     context context_name
       egtp-service service_name
         gtpc allow-on-congestion arp arp_value
         end
   ```

3. **GTP-C RLF スロットリング**

   - GTP-C RLF スロットリング機能が有効になっている場合は、**gtpc overload-protection egress throttling-override-policy** CLI コマンドを、NS/EP NGN-PS 用に予約されている ARP（PL）で設定する必要があります。これにより、eMPS サービスが RLF スロットリングをバイパスするようなります。
   - 着信メッセージの GTP-C RLF スロットリングが **gtpc overload-protection ingress msg-rate** *message_rate* CLI コマンドを使用して設定されている場合、eMPS 関連メッセージをスロットリングできます。現在、着信 RLF スロットリングに対するバイパスポリシーはありません。



重要 ARP（PL）の設定で動作する既存の機能は、設定された ARP 値が eMPS サービスの NS/EP NGN-PS で予約されている値と同じかどうかに関係なく、以前と同様に機能し続けます。既存の機能が eMPS 要件で動作する必要がある場合は、eMPS サービス用に予約された NS/EP NGN-PS と同じ ARP（PL）値を設定する必要があります。

ライセンス

DSCP マーキング機能を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

機能の仕組み

GIR 参照ドキュメント

次の表では、GIR ドキュメントに基づき、この機能の要件について説明します。

要件番号	説明
R-127	[202] S-GW は、優先順位を付けて GTP-C の「ダウンリンクデータ通知」メッセージ、GTP-C の「ベアラー作成要求」メッセージ、GTP-C の「ベアラー更新要求」メッセージを送信するものとします。いずれのメッセージにも NS/EP NGN-PS で使用するために サービスプロバイダーによって割り当てられたセットから選択された ARP が含まれます。
R-130	[204] S-GW は、S-GW から MME に送られる S11「セッション作成応答」メッセージに優先処理マークを付けるものとします。このメッセージでは、NS/EP NGN-PS コール/セッションに対応する ARP を使用してベアラーを確立するよう要求されます。
R-132	[205] S-GW は、S-GW から MME に送られる S11 「ベアラー作成要求」および S11「ベアラー更新要求」メッセージに優先処理マークを付けるものとします。これらのメッセージでは、UE には現在 NS/EP NGN-PS サービス用に確立または更新されているベアラーがあることが示されます。
R-134	[206] S5/S8 インターフェイスが GTP ベースの場合、S-GW は S-GW から PDN-GW に送られる S5/S8「セッション作成要求」メッセージに優先処理マークを付けるものとします。このメッセージでは、UE によって NS/EP NGN-PS 用にベアラーが確立されることが示されます。

要件番号	説明
R-137	[207] S5/S8 インターフェイスが GTP ベースの場合、S-GW は S-GW から PDN-GW に送られる S5/S8 の「ベアラー作成応答」および「ベアラー更新応答」メッセージに優先処理マークを付けるものとします。これらのメッセージでは、UE には現在 NS/EP NGN-PS 用に確立または更新されたベアラーがあることが示されます。
R-143	[213] S5/S8 インターフェイスが GTP ベースの場合、PDN-GW は PDN-GW から S-GW に送られる S5/S8「セッション作成応答」メッセージに優先処理マークを付けるものとします。 このメッセージでは、NS/EP NGN-PS コール/セッションに対応する ARP を使用してベアラーを確立するよう要求されます。
R-146	[216] S5/S8 インターフェイスが GTP ベースの場合、PDN-GW は PDN-GW から S-GW に送られる S5/S8 の「ベアラー作成要求」および「ベアラー更新要求」メッセージに優先処理マークを付けるものとします。これらのメッセージでは、 UE には現在、NS/EP NGN-PS 用に確立または更新されたベアラーがあることが示されます。

VoLTE/緊急コールの拡張優先順位付けの設定

次の項では、この機能を有効にするための設定コマンドについて説明します。

eMPS プロファイルとその関連属性の設定

コンフィギュレーションモードレベルで、eMPS プロファイルとその関連属性を定義するための CLI コマンドオプションが導入されました。

- **eARP 設定**：この設定は、ベアラー/PDN を eMPS としてマーキングするために使用されます。
- **DSCP 設定**：この設定は、S-GW/P-GW で、設定済み DSCP マーキングによって eMPS PDN に関連付けられたさまざまな発信 GTP-C メッセージをマーキングするために使用されます。

```
configure
  [ no ] emps-profile emps_profile_name -noconfirm
  [ no ] earp { [ 1...15 ] { [ 1...15 ] { [ 1...15 ] } } }
  [ no ] dscp-marking dscp_value
  end
```

注：

- **emps-profile** *emps_profile_name*：eMPS セッションの属性を定義するための eMPS プロファイルを設定します。*emps_profile_name* は、1 ～ 63 文字の文字列です。
- **earp**：最大 3 つの eARP 優先順位レベル（PL）値を設定して、設定された eARP 優先順位値を持つセッションを eMPS セッションとしてマークできるようにします。
- **-noconfirm**：確認のプロンプトなしで新しい eMPS プロファイルを作成します。
- **dscp-marking** *dscp_value*：eMPS セッションに適用される DSCP 値を指定します。*dscp_value* は、0x0 ～ 0x3F の 16 進数である必要があります。
- eMPS プロファイルでは、最大 3 つの eARP 値を設定できます。上記の CLI 構文では、1 つのコマンドで 1 つ以上（最大 3 つ）の eARP 値を柔軟に設定できます。次に例を示します。

  earp 1 2 3

  または

  earp 4
- 最後に設定された一連の eARP 値により、前の設定が上書きされます。たとえば、次の 2 つのコマンドを順番に呼び出すと、eARP 値 4 のみが設定されます。

  earp 1 2 3

  earp 4
- eMPS プロファイル名は一意である必要があり、コンテキスト全体で大文字と小文字が区別されません。
- **no earp** コマンドを使用すると、設定されているすべての eARP 値を無効にできます。ただし、これにより、対応する eMPS プロファイルが削除されることはありません。**no emps-profile** *emps_profile_name* CLI コマンドにより、プロファイルが削除します。
- 警告メッセージ：存在しない eMPS プロファイルの **no** が実行されると、警告メッセージが表示されます。次に例を示します。

  ```
  no emps-profile xyz
  eMPS Profile : xyz does not exist
  ```

  未設定の eARP の **no** が実行された場合、警告メッセージは表示されません。
- 既存のプロファイルが削除されると、警告および確認メッセージが表示されます。

  ```
  This operation will result in deletion of this eMPS Profile.
  Are you sure? [Yes|No]:
  ```
- 最大 64 個の異なる eMPS プロファイルを設定できます。

eMPS プロファイルの P-GW サービスへの関連付け

次に示すコマンドは、eMPS プロファイルを P-GW サービスに関連付けます。

```
configure
  context context_name
    pgw-service service_name
      associate emps-profile emps_profile_name
      end
```

注：

- **no associate emps-profile**：機能を無効にします。
- **emps-profile** *emps_profile_name*：eMPS プロファイルを P-GW サービスに関連付けます。*emps_profile_name* は、1 ～ 63 文字の文字列です。
- 入力する eMPS プロファイル名は、大文字と小文字が区別されません。
- デフォルトでは、pgw-service に関連付けられている eMPS プロファイルはありません。
- SAE-GW が関連付けられている P-GW サービスの場合、eMPS プロファイルは、関連付けられている S-GW サービスに設定されているものと同じである必要があります。同じではない場合、**show configuration error** CLI コマンドの出力で報告されます。

eMPS プロファイルの S-GW サービスへの関連付け

次に示すコマンドは、eMPS プロファイルを S-GW サービスに関連付けます。

```
configure
  context context_name
    sgw-service service_name
      associate emps-profile emps_profile_name
      end
```

注：

- **no associate emps-profile**：機能を無効にします。
- **emps-profile** *emps_profile_name*：eMPS プロファイルを S-GW サービスに関連付けます。*emps_profile_name* は、1 ～ 63 文字の文字列です。
- 入力する eMPS プロファイル名は、大文字と小文字が区別されません。
- デフォルトでは、sgw-service に関連付けられている eMPS プロファイルはありません。
- SAE-GW が関連付けられている S-GW サービスの場合、eMPS プロファイルは、関連付けられている P-GW サービスに設定されているものと同じである必要があります。同じではない場合、**show configuration error** CLI コマンドの出力で報告されます。

VoLTE/緊急コールの拡張優先順位付けのモニタリングと障害対応

ここでは、この機能拡張に対応した show コマンドや出力について説明します。

コマンドや出力の表示

show emps-profile { all | name <emps_profile_name> }

上記の CLI コマンドは、関連する属性で設定された特定の、またはすべての eMPS プロファイルを表示するために導入されました。また、既存の **show config [verbose]** CLI コマンドの出力は、eMPS の設定を反映するように変更されています。

- **earp configured**: <earp_value>
- **dscp-marking configured**: <dscp-value>

これらの CLI コマンドを使用して、設定が適切かどうかを確認できます。

show pgw-service { name <name> | all }

このコマンドの出力が変更され、P-GW サービスに関連付けられた eMPS プロファイルが反映されるようになりました。

- **eMPS Profile Name** : <emps_profile_name>



重要　一度に最大 1 つの eMPS プロファイルを P-GW サービスに関連付けることができます。最新の設定により、以前に関連付けられた設定が上書きされます。

show sgw-service { name <name> | all }

このコマンドの出力が変更され、S-GW サービスに関連付けられた eMPS プロファイルが反映されるようになりました。

- **eMPS Profile Name** : <emps_profile_name>



重要　一度に最大 1 つの eMPS プロファイルを S-GW サービスに関連付けることができます。最新の設定により、以前に関連付けられた設定が上書きされます。

show subscribers pgw-only full all

このコマンドの出力が変更され、セッションが eMPS かどうかが反映されるようになりました。次に例を示します。

```
Username: 0123456789@username
 Subscriber Type   : Visitor
 Status            : Online/Active
 State             : Connected
 Connect Time      : Wed Sep  7 07:02:49 2016
 Auto Delete       : No
 Idle time         : 00h00m08s
 MS TimeZone       : n/a                    Daylight Saving Time: n/a
 Access Type: gtp-pdn-type-ipv4             Network Type: IP
 Access Tech: eUTRAN                        pgw-service-name: pgw_service
 Callid: 00004e21                           IMSI: 123456789012341
 MSISDN: 0123456789
 Interface Type: S5S8GTP                    Low Access Priority: N/A
 TWAN Mode: N/A
 eMPS Bearer: Yes
 Emergency Bearer Type: N/A
 IMS-media Bearer: No
```

show subscribers saegw-only full all

このコマンドの出力が変更され、セッションが eMPS かどうかが反映されるようになりました。次に例を示します。

```
Username: 0123456789@username
 SAEGW Call mode   : Co-located
 Subscriber Type   : Home
 .
 .
 .
 MSISDN: 0123456789
 TWAN Mode: N/A
 eMPS Bearer: Yes
 MS TimeZone       :                      Daylight Saving Time: n/a
 MEI               : 1122334455667788     Accounting mode      : GTPP
```

show pgw-service statistics

このコマンドの出力が変更され、eMPS PDN 統計情報が表示されるようになりました。次に例を示します。

```
PDNs By Emergency-Type:
 Emergency PDNs:
  Active:               0    Setup:            0
   Authentic IMSI:      0    Authentic IMSI:   0
 .
 .
 .
eMPS PDNs:
  Current Active:                    1      Cumulative Activated:   1
  Cumulative De-activated:           1
IPv4v6 PDN-Type Received with DAF False :         0
```

それぞれの説明は次のとおりです。

- **Current Active**：いずれかの PDN が eMPS PDN としてセットアップされている場合、またはeMPS PDN にアップグレードされている場合に増分されます。eMPS PDN がリリースされている場合、または非 eMPS PDN にデグレードされている場合に減分されます。
- **Cumulative Activated**：いずれかの PDN が eMPS PDN としてセットアップされたとき、または eMPS PDN にアップグレードされたときに増分されます。
- **Cumulative De-activate**：eMPS PDN がリリースされたとき、または非 eMPS PDN にデグレードされたときに増分されます。

show saegw-service statistics all function pgw

このコマンドの出力が変更され、eMPS PDN 統計情報が表示されるようになりました。次に例を示します。

```
PDNs By Emergency-Type:
 Emergency PDNs:
  Active:               0    Setup:            0
   Authentic IMSI:      0    Authentic IMSI:   0
 .
 .
 .
eMPS PDNs:
  Current Active:                   1       Cumulative Activated:   1
  Cumulative De-activated:          1
IPv4v6 PDN-Type Received with DAF False :         0
```

それぞれの説明は次のとおりです。

- **Current Active**：いずれかの PDN が eMPS PDN としてセットアップされている場合、またはeMPS PDN にアップグレードされている場合に増分されます。eMPS PDN がリリースされている場合、または非 eMPS PDN にデグレードされている場合に減分されます。
- **Cumulative Activated**：いずれかの PDN が eMPS PDN としてセットアップされたとき、または eMPS PDN にアップグレードされたときに増分されます。
- **Cumulative De-activate**：eMPS PDN がリリースされたとき、または非 eMPS PDN にデグレードされたときに増分されます。

show saegw-service statistics

このコマンドの出力が変更され、saegw-service に関連付けられた PGW アンカー/SGW アンカー PDN の eMPS 統計情報が表示されるようになりました。次に例を示します。

```
PDNs By Emergency-Type:
 Emergency PDNs:
  Active:               0    Setup:            0
  Released:      0
 .
 .
 .
eMPS PDNs:
 Colocated PDNs:
  Current Active:                   1       Cumulative Activated:   1
  Cumulative De-activated:          0
```

```
PGW-Anchor PDNs:
 Current Active:                  1       Cumulative Activated:   1
 Cumulative De-activated:         0
SGW-Anchor PDNs:
 Current Active:                  1       Cumulative Activated:   1
 Cumulative De-activated:         0
```

上記の統計情報は、SAE-GW コールタイプに基づいてさらに分類されます。

- **Colocated eMPS PDNs**：Collapsed PDN の eMPS PDN 統計情報を反映します。
- **PGW-Anchor eMPS PDNs**：PGW アンカー PDN の eMPS PDN 統計情報が反映されます。
- **SGW-Anchor eMPS PDNs**：SGW アンカー PDN の eMPS PDN 統計情報が反映されます。

それぞれの説明は次のとおりです。

- **Current Active**：いずれかの PDN が eMPS PDN としてセットアップされている場合、または eMPS PDN にアップグレードされている場合に増分されます。eMPS PDN がリリースされている場合、または非 eMPS PDN にデグレードされている場合に減分されます。
- **Cumulative Activated**：いずれかの PDN が eMPS PDN としてセットアップされたとき、または eMPS PDN にアップグレードされたときに増分されます。
- **Cumulative De-activate**：eMPS PDN がリリースされたとき、または非 eMPS PDN にデグレードされたときに増分されます。

show sgw-service statistics all

このコマンドの出力が変更され、セッションが eMPS かどうかが反映されるようになりました。次に例を示します。

```
Subscribers Total:
  Active:               0    Setup:            2
  Released:             1
 .
 .
 .
eMPS PDN Statistics:
  Current Active:                  1       Cumulative Activated:   1
  Cumulative De-activated:         0
```

show saegw-service statistics all function sgw

このコマンドの出力が変更され、eMPS PDN 統計情報が表示されるようになりました。次に例を示します。

```
Subscribers Total:
  Active:               0    Setup:            0
  Released:             0
 .
 .
 .
eMPS PDN Statistics:
```

```
Current Active:                  1       Cumulative Activated:    1
Cumulative De-activated:         0
```

show configuration error

次のシナリオで、設定エラーが表示されます。

- 同じ sae-gw サービスに関連付けられた pgw-service と sgw-service で異なる eMPS プロファイルが設定されている場合。次に例を示します。

```
##############################################################
    Displaying SAEGW-Service system errors
##############################################################
Error   : eMPS profile of SGW <sgw-service> and PGW service <pgw_service>
is not same for SAEGW service <saegw-service> in the context <context_name>.
Total 1 error(s) in this section !
```

- 存在しない emps-profile が pgw-service に関連付けられている場合。次に例を示します。

```
##############################################################
    Displaying PGW-Service system errors
##############################################################
Error   : eMPS Profile <emps_profile_pgw> configured for PGW service <pgw_service>
is not present in the system
Total 1 error(s) in this section !
```

- 存在しない emps-profile が sgw-service に関連付けられている場合。次に例を示します。

```
##############################################################
    Displaying SGW-Service system errors
##############################################################
Error   : eMPS Profile <emps_profile_sgw> configured for SGW service <sgw_service>
is not present in the system
Total 1 error(s) in this section !
```

VoLTE/緊急コールの拡張優先順位付けのバルク統計

PGW スキーマ

この機能の一部として、次のバルク統計が P-GW スキーマに追加されました。

- sessstat-pdn-emps-current-active：現在アクティブな P-GW eMPS PDN の総数。
- sessstat-pdn-emps-cumulative-activated：eMPS PDN としてセットアップされているか、eMPS PDN にアップグレードされている P-GW PDN の総数。
- sessstat-pdn-emps-cumulative-deactivated：リリースされた、または非 eMPS PDN にデグレードされた P-GW PDN の総数。

SGW スキーマ

この機能の一部として、次のバルク統計が S-GW スキーマに追加されました。

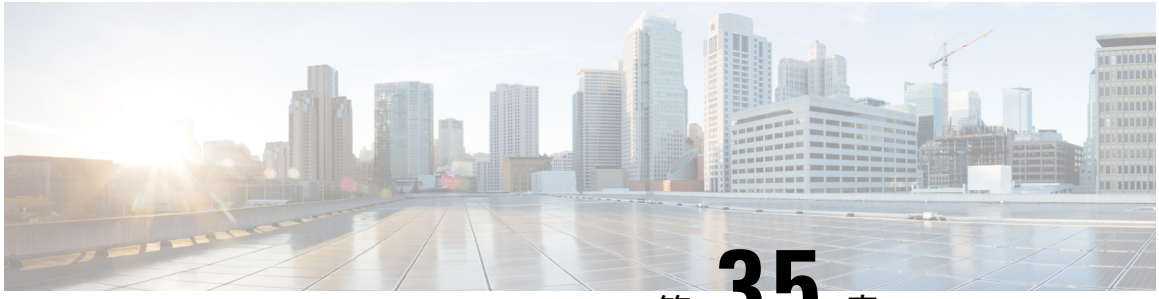
- sessstat-pdn-emps-current-active：現在アクティブな S-GW eMPS PDN の総数。

- sessstat-pdn-emps-cumulative-activated：eMPS PDN としてセットアップされているか、eMPS PDN にアップグレードされている S-GW PDN の総数。
- sessstat-pdn-emps-cumulative-deactivated：リリースされた、または非 eMPS PDN にデグレードされた S-GW PDN の総数。

SAEGW スキーマ

この機能の一部として、次のバルク統計が SAE-GW スキーマに追加されました。

- pgw-anchor-pdns-emps-current-active：現在アクティブな P-GW アンカー eMPS PDN の総数。
- pgw-anchor-pdns-emps-cumulative-activated：eMPS PDN としてセットアップされているか、eMPS PDN にアップグレードされている P-GW アンカー PDN の総数。
- pgw-anchor-pdns-emps-cumulative-deactivated：リリースされた、または非 eMPS PDN にデグレードされた P-GW アンカー PDN の総数。
- saegw-colocated-pdns-emps-current-active：現在アクティブな P-GW Collapsed eMPS の総数。
- saegw-colocated-pdns-emps-cumulative-activated：eMPS PDN としてセットアップされているか、eMPS PDN にアップグレードされている SAEGW Collapsed PDN の総数。
- saegw-colocated-pdns-emps-cumulative-deactivated：リリースされた、または非 eMPS PDN にデグレードされた SAE-GW Collapsed PDN の総数。
- sgw-anchor-pdns-emps-current-active：現在アクティブな S-GW アンカー eMPS PDN の総数。
- sgw-anchor-pdns-emps-cumulative-activated：eMPS PDN としてセットアップされているか、eMPS PDN にアップグレードされている S-GW アンカー PDN の総数。
- sgw-anchor-pdns-emps-cumulative-deactivated：リリースされた、または非 eMPS PDN にデグレードされた S-GW アンカー PDN の総数。



第 35 章

拡張 QCI のオプション

この章では、拡張 QCI 機能について説明します。

- QCI ごとのパケットドロップカウンタと QCI レベルカウンタの ARP 精度 （571 ページ）
- QCI 値と ARP 値の両方に基づく DSCP マーキング （585 ページ）
- 新しい標準 QCI のサポート （589 ページ）
- 非標準 QCI のサポート （627 ページ）

QCI ごとのパケットドロップカウンタと QCI レベルカウンタの ARP 精度

このセクションでは、QCI ごとのパケットドロップカウンタと QCI レベルカウンタの ARP 精度機能について説明します。

機能説明

このセクションでは、QCI ごとのパケットドロップカウンタと QCI レベルカウンタの ARP 精度機能について説明します。

QCI および ARP の可視性のサポート

StarOS リリース 20.2 では、ソフトウェアの機能が強化されており、Quality of Service Class Index（QCI）および Allocation and Retention Priority（ARP）ベースの QoS 統計の表示がサポートされています。

ARP は、ネットワークが輻輳した状況で優先順位の低いベアラーをドロップまたはダウングレードするための 3GPP メカニズムです。ネットワークは ARP を確認し、新しい専用ベアラーを無線ベースステーションを介して確立できるかどうかを判断します。QCI は通信事業者のプロビジョニング値であり、ベアラーレベルのパケット転送処理を制御します。

この機能が拡張されたため、通信御者は、同じ QCI 値で実行されている複数のサービスを識別する QoS 統計情報をモニターできるようになりました。さらに、Enhanced Charging Service（ECS）がパケットをドロップした具体的な理由を提供するためのパケットドロップカウンタ

が導入されました。パケットドロップカウンタは、ARP ごとに出力されます。これにより、通信事業者はサービスに影響を与える可能性のあるネットワーク問題の特定とトラブルシュートを行う際に使用できる追加情報を得ることができます。

重要 ARP 値については、Allocation/Retention Priority（ARP）情報要素（IE）の優先度レベル値のみが考慮されます。ARP IE のプリエンプション脆弱性（PVI）およびプリエンプション機能（PCI）フラグは考慮されません。

既存の **show apn statistics name** *apn-name* および **show apn statistics** *Exec Mode* CLI コマンドが強化されました。これらのコマンドの出力で、QCI/ARP ベースの QoS 統計情報が可視化されるようになりました。

ライセンス

重要 QCI レベルカウンタの ARP 精度はライセンス制御機能です。QCI ごとのパケットドロップカウンタ機能にはライセンスは必要ありません。ライセンスの詳細については、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

QCI レベルカウンタの ARP 精度の設定

ここでは、QCI レベルカウンタの ARP 精度機能を設定する方法について説明します。

重要 QCI レベルカウンタの ARP 精度はライセンス制御機能です。QCI ごとのパケットドロップカウンタ機能にはライセンスは必要ありません。ライセンスの詳細については、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

この機能の設定は、次のタスクで構成されています。

1. 統計プロファイルを作成します。
2. QCI ごとのパケットドロップカウンタの収集を有効にします。
3. QCI/ARP レベルの統計の収集を有効にします。
4. 統計プロファイルを APN に関連付けます。
5. 設定を確認します。

統計プロファイルの作成

「グローバル コンフィギュレーション モード」にアクセスし、統計プロファイルを作成するには、次の例を使用します。

```
configure
   stats-profile stats_profile_name
   end
```

注：

- *stats_profile_name* は、1 ～ 63 文字の英数字文字列である必要があります。

パケットドロップ統計の収集の有効化

「統計プロファイル コンフィギュレーション モード」にアクセスし、統計プロファイルを作成して、パケットドロップ統計の収集を有効にするには、次の例を使用します。

```
configure
   stats-profile stats_profile_name
      packet-drop
      end
```

パケットドロップ統計の収集の無効化

```
configure
   stats-profile stats_profile_name
      no packet-drop
      end
```

注：

- *stats_profile_name*は、既存の統計プロファイルの名前である必要があります。この名前は、1 ～ 63 文字の英数字文字列である必要があります。
- **packet-drop**：指定された統計プロファイルのパケットドロップ統計の収集を有効にします。
- **no packet-drop**：指定された統計プロファイルのパケットドロップ統計の収集を無効にします。

QCI/ARP レベル統計の収集の有効化

「統計プロファイル コンフィギュレーション モード」にアクセスし、統計プロファイルに関する QCI/ARP レベルの統計の収集を有効にするには、次の例を使用します。

```
configure
   stats-profile stats_profile_name
     qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | [ non-std { non-gbr
 | gbr } ] } { arp { all | [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
11 |12 | 13 | 14 | 15 ] + } }
     end
```

QCI/ARP 統計の収集を無効にするには、次の手順を実行します。

```
configure
   stats-profile stats_profile_name
  no qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | [ non-std { non-gbr
 | gbr } ] } { arp { all | [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
```

```
11 |12 | 13 | 14 | 15 ] + } }
  end
```

注：

- *stats_proflle_name* は、既存の統計プロファイルの名前である必要があります。この名前は、1 ～ 64 文字の英数字文字列である必要があります。
- **qci**：指定された QCI に関する ARP 優先順位レベルの統計の収集を設定します。
- **non-std**：非標準 QCI に関する ARP 優先順位レベルの統計の収集を設定します。
- **non-gbr**：非標準非保証ビットレート（GBR）QCI に関する ARP 優先順位レベルの統計の収集を設定します。
- **gbr**：非標準 GBR QCI に関する ARP 優先順位レベルの統計の収集を設定します。
- **arp**：指定された ARP 値に関する ARP 優先順位レベルの統計の収集を設定します。
- **no**：指定された **qci** 設定および **arp** 設定に関する ARP 優先順位レベルの統計の収集を無効にします。

統計プロファイルと APN の関連付け

「APN コンフィギュレーション モード」にアクセスし、統計プロファイルを APN に関連付けるには、次の例を使用します。

```
configure
  apn apn_name
    stats-profile stats_profile_name
    end
```

統計プロファイルと指定した APN の関連付けを解除するには、次の手順を実行します。

```
configure
  apn apn_name
    no stats-profile
    end
```

注：

- *stats_profile_name*：既存の統計プロファイルの名前である必要があります。この名前は、1 ～ 63 文字の英数字文字列である必要があります。
- P-GW/SAEGW/GGSN サービスごとに最大 64 の統計プロファイルを設定できます。
- **no stats-profile**：統計プロファイルと APN の関連付けを解除します。



重要 統計プロファイルが、12 を超える APN に関連付けられている場合は、メモリとパフォーマンスへの影響に関する次の警告が表示されます。

```
[WARNING] Configuring QCI/ ARP level statistics for more then 12 APNs will have
memory and performance impact. Do you want to continue [Y/N]
```

設定の確認

次の手順で設定を確認します。

最初に、統計プロファイルが正しいAPNに関連付けられていることを確認します。*EXEC*モードで、次のコマンドを入力します。

show apn name *apn_name*

注：

- コマンド出力で、**stats profile** フィールドを探します。この APN に関連付けられている統計プロファイルの名前が含まれている必要があります。

次に、統計プロファイルの設定が正しいことを確認します。*EXEC* モードで、次のコマンドを入力します。

show stats-profile name *stats_profile_name*

注：

- *stats_profile_name* は、設定を表示する統計プロファイルの名前です。
- このコマンドの出力には、次の情報が含まれています。
  - 統計プロファイル名
  - QCI と ARP の両方に対するパケットドロップ設定
  - StarOS が詳細な ARP 統計を収集する QCI ARP の組み合わせ

上記の設定のいずれかが正しくない場合は、設定手順を再度実行して、適切な設定で統計プロファイルを再設定します。

QCI ごとのパケットドロップカウンタと QCI レベルカウンタの ARP 精度のモニタリング

この項では、QCI ごとのパケットドロップカウンタと QCI レベルカウンタの ARP 精度機能をモニタリングする方法について説明します。

バルク統計

この項では、ARP 精度および QCI ごとのパケットドロップカウンタ機能をサポートするために追加されたバルク統計を示します。

APN スキーマ

新しい標準 QCI 機能をサポートするために、次のバルク統計が S-GW スキーマに追加されました。

```
qci65-actbear
qci65-setupbear
qci65-relbear
```

```
qci65-uplinkpkt-fwd
qci65-dwlinkpkt-fwd
qci65-uplinkbyte-fwd
qci65-dwlinkbyte-fwd
qci65-uplinkpkt-drop
qci65-dwlinkpkt-drop
qci65-uplinkbyte-drop
qci65-dwlinkbyte-drop
qci65-uplinkpkt-drop-mbrexcd
qci65-dwlinkpkt-drop-mbrexcd
qci65-uplinkbyte-drop-mbrexcd
qci65-dwlinkbyte-drop-mbrexcd
qci65-rejbearer
qci66-actbear
qci66-setupbear
qci66-relbear
qci66-uplinkpkt-fwd
qci66-dwlinkpkt-fwd
qci66-uplinkbyte-fwd
qci66-dwlinkbyte-fwd
qci66-uplinkpkt-drop
qci66-dwlinkpkt-drop
qci66-uplinkbyte-drop
qci66-dwlinkbyte-drop
qci66-uplinkpkt-drop-mbrexcd
qci66-dwlinkpkt-drop-mbrexcd
qci66-uplinkbyte-drop-mbrexcd
qci66-dwlinkbyte-drop-mbrexcd
qci66-rejbearer
qci69-actbear
qci69-setupbear
qci69-relbear
qci69-uplinkpkt-fwd
qci69-dwlinkpkt-fwd
qci69-uplinkbyte-fwd
qci69-dwlinkbyte-fwd
qci69-uplinkpkt-drop
qci69-dwlinkpkt-drop
qci69-uplinkbyte-drop
qci69-dwlinkbyte-drop
qci69-uplinkpkt-drop-mbrexcd
qci69-dwlinkpkt-drop-mbrexcd
qci69-uplinkbyte-drop-mbrexcd
qci69-dwlinkbyte-drop-mbrexcd
qci69-rejbearer
qci70-actbear
qci70-setupbear
qci70-relbear
qci70-uplinkpkt-fwd
qci70-dwlinkpkt-fwd
qci70-uplinkbyte-fwd
qci70-dwlinkbyte-fwd
qci70-uplinkpkt-drop
qci70-dwlinkpkt-drop
qci70-uplinkbyte-drop
qci70-dwlinkbyte-drop
qci70-uplinkpkt-drop-mbrexcd
qci70-dwlinkpkt-drop-mbrexcd
qci70-uplinkbyte-drop-mbrexcd
qci70-dwlinkbyte-drop-mbrexcd
qci70-rejbearer
sessstat-bearrel-ded-admin-clear-qci65
sessstat-bearrel-ded-admin-clear-qci66
```

```
sessstat-bearrel-ded-admin-clear-qci69
sessstat-bearrel-ded-admin-clear-qci70
```

コマンドの表示

ここでは、パケット単位の QCI ドロップカウンタと、QCI レベルカウンタの ARP 精度機能をサポートするために使用できる EXEC モードの show コマンドについて説明します。

show apn statistics

qci および **arp** キーワードがこのコマンドに追加されました。これらの新しいキーワードを使用して、オペレータは、QCI レベルカウンタの ARP 精度機能に適用される 4 つの基本シナリオの出力を表示できます。

シナリオ 1

単一の APN について、QCI/ARP レベルの精度でパケットドロップカウンタを表示します。このコマンドの出力は、パケットドロップに影響を与える可能性のあるネットワークの問題を切り分けるのに役立ちます。

show apn statistics name *apn_name* **qci { all | 1-9 | non-std { gbr | non-gbr } } arp { all | 1-15 }**

注：

- *apn_name*：*APN* コンフィギュレーション モードで作成された設定済み APN の名前である必要があります。
- **qci**：指定した QCI のパケットドロップ統計を表示します。
- **all**：すべての QCI のパケットドロップ統計を表示します。
- **1-9**：QCI <n> のパケットドロップ統計を表示します。1 ～ 9 の QCI 番号にする必要があります。
- **non-std**：非標準 QCI のパケットドロップ統計を表示します。
- **non-gbr**：非標準の非 GBR QCI のパケットドロップ統計を表示します。
- **gbr**：非標準 GBR QCI のパケットドロップ統計を表示します。
- **arp**：指定した ARP 優先順位レベルの統計を表示します。
- **all**：すべての ARP 優先順位レベルのパケットドロップ統計を表示します。
- **1-15**：指定した ARP 優先順位レベルの統計を表示します。

シナリオ 2

すべての APN について、QCI/ARP レベルの精度でパケットドロップカウンタを表示します。

show apn statistics qci { all | 1-9 | non-std { gbr | non-gbr } } arp { all | 1-15 }

注：

- *apn_name*：*APN* コンフィギュレーション モードで作成された設定済み APN の名前である必要があります。
- **qci**：指定した QCI のパケットドロップ統計を表示します。
- **all**：すべての QCI のパケットドロップ統計を表示します。
- **1-9**：QCI <n> のパケットドロップ統計を表示します。1 ～ 9 の QCI 番号にする必要があります。
- **non-std**：非標準 QCI のパケットドロップ統計を表示します。
- **non-gbr**：非標準の非 GBR QCI のパケットドロップ統計を表示します。
- **gbr**：非標準 GBR QCI のパケットドロップ統計を表示します。
- **arp**：指定した ARP 優先順位レベルの統計を表示します。
- **all**：すべての ARP 優先順位レベルのパケットドロップ統計を表示します。
- **1-15**：指定した ARP 優先順位レベルの統計を表示します。

シナリオ 3

QCI レベルの精度で新しいパケットドロップカウンタを表示し、指定された APN の既存の QCI レベルのカウンタを表示します。

show apn statistics name *apn_name* **qci { all | 1-9 | non-std { gbr | non-gbr } }**

注：

- *apn_name*：*APN* コンフィギュレーション モードで作成された設定済み APN の名前である必要があります。
- **qci**：指定した QCI のパケットドロップ統計を表示します。
- **all**：すべての QCI のパケットドロップ統計を表示します。
- **1-9**：QCI <n> のパケットドロップ統計を表示します。1 ～ 9 の QCI 番号にする必要があります。
- **non-std**：非標準 QCI のパケットドロップ統計を表示します。
- **non-gbr**：非標準の非 GBR QCI のパケットドロップ統計を表示します。
- **gbr**：非標準 GBR QCI のパケットドロップ統計を表示します。
- **arp**：指定した ARP 優先順位レベルの統計を表示します。
- **all**：すべての ARP 優先順位レベルのパケットドロップ統計を表示します。
- **1-15**：指定した ARP 優先順位レベルの統計を表示します。

シナリオ 4

QCI レベルの精度でパケットドロップカウンタを表示し、すべての APN の統合された既存の QCI カウンタを表示します。

show apn statistics qci { all | 1-9 | non-std { gbr | non-gbr } }

注：

- *apn_name*：*APN* コンフィギュレーション モードで作成された設定済み APN の名前である必要があります。
- **qci**：指定した QCI のパケットドロップ統計を表示します。
- **all**：すべての QCI のパケットドロップ統計を表示します。
- **1-9**：QCI <n> のパケットドロップ統計を表示します。1 ～ 9 の QCI 番号にする必要があります。
- **non-std**：非標準 QCI のパケットドロップ統計を表示します。
- **non-gbr**：非標準の非 GBR QCI のパケットドロップ統計を表示します。
- **gbr**：非標準 GBR QCI のパケットドロップ統計を表示します。
- **arp**：指定した ARP 優先順位レベルの統計を表示します。
- **all**：すべての ARP 優先順位レベルのパケットドロップ統計を表示します。
- **1-15**：指定した ARP 優先順位レベルの統計を表示します。

show apn statistics name *apn_name* **qci all arp all** コマンドの出力が拡張され、次の新しい統計が表示されるようになりました。

```
Data Statistics:

    Uplink Bytes:                0   Downlink Bytes:                          0
    Uplink Pkts:                 0   Downlink Pkts:                           0
    Uplink Bytes dropped:        0   Downlink Bytes dropped:                  0
    Uplink Pkts dropped:         0   Downnlink Pkts dropped:                  0

  Uplink Dropped:                        Downlink Dropped:
    MBR Exceeded(Bytes):               0  MBR Exceeded(Bytes):                0
    MBR Exceeded(Pkts):                0  MBR Exceeded(Pkts):                 0
    AMBR Exceeded(Bytes):              0  AMBR Exceeded(Bytes):               0
    AMBR Exceeded(Pkts):               0  AMBR Exceeded(Pkts):                0
    Miscellaneous(Bytes):              0  Miscellaneous(Bytes):               0
    Miscellaneous(Pkts):               0  Miscellaneous(Pkts):                0
    Overcharge Prtctn(Bytes)           0  Overcharge Prtctn(Bytes):           0
    Overcharge Prtctn(Pkts):           0  Overcharge Prtctn(Pkts):            0
    SGW Restoration(Bytes):            0  SGW Restoration(Bytes):             0
    SGW Restoration(Pkts):             0  SGW Restoration(Pkts):              0
    SDF Gate(Bytes):                   0  SDF Gate(Bytes):                    0
    SDF Gate(Pkts):                    0  SDF Gate(Pkts):                     0
    ITC Gate(Bytes):                   0  ITC Gate(Bytes):                    0
    ITC Gate(Pkts):                    0  ITC Gate(Pkts):                     0
    Flow Terminated(Bytes):            0  Flow Terminated(Bytes):             0
    Flow Terminated(Pkts):             0  Flow Terminated(Pkts):              0
    Subsession Terminated(Bytes):      0  Subsession Terminated(Bytes):       0
    Subsession Terminated(Pkts):       0  Subsession Terminated(Pkts):        0
    Call Terminated(Bytes):            0  Call Terminated(Bytes):             0
    Call Terminated(Pkts):             0  Call Terminated(Pkts):              0
```

```
    DCCA Discard(Bytes):                    0  DCCA Discard(Bytes):                    0
    DCCA Discard(Pkts):                     0  DCCA Discard(Pkts):                     0
    No Rule Match(Bytes):                   0  No Rule Match(Bytes):                   0
    No Rule Match(Pkts):                    0  No Rule Match(Pkts):                    0
    ICAP(Bytes):                            0  ICAP(Bytes):                          N/A
    ICAP(Pkts):                             0  ICAP(Pkts):                           N/A
    SFW(Bytes):                             0  SFW(Bytes):                             0
    SFW(Pkts):                              0  SFW(Pkts):                              0
    Hierarchical ENF(Bytes):                0  Hierarchical ENF(Bytes):                0
    Hierarchical ENF(Pkts):                 0  Hierarchical ENF(Pkts):                 0
    Dynamic CA Gate(Bytes):                 0  Dynamic CA Gate(Bytes):    :            0
    Dynamic CA Gate(Pkts):                  0  Dynamic CA Gate(Pkts):                  0
    NAT64 Cancel(Bytes):                    0  NAT64 Cancel(Bytes):                    0
    NAT64 Cancel(Pkts):                     0  NAT64 Cancel(Pkts):                     0
    Bearer Not Found(Bytes):                0  Bearer Not Found(Bytes):                0
    Bearer Not Found(Pkts):                 0  Bearer Not Found(Pkts):                 0


4G Bearers Released By Reasons:
                 QCI1  QCI2  QCI3  QCI4  QCI5  QCI6  QCI7  QCI8  QCI9

Admin disconnect: 0      0    0      0    0      0     0     0    0


  ARP level distribution of 4G Bearer Released By Reasons:

    Admin disconnect:
    QCI 1:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0
.
.
.

    QCI 9:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0
```

```
Subscriber QoS Statistics:


4G Bearers Released By Reasons:
                QCI1  QCI2  QCI3  QCI4  QCI5  QCI6  QCI7  QCI8  QCI9

Admin disconnect: 0      0    0      0    0      0     0     0    0


  ARP level distribution of 4G Bearer Released By Reasons:

    Admin disconnect:
    QCI 1:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0
.
.
.

    QCI 9:
       ARP  1:            0
       ARP  2:            0
       ARP  3:            0
       ARP  4:            0
       ARP  5:            0
       ARP  6:            0
       ARP  7:            0
       ARP  8:            0
       ARP  9:            0
       ARP 10:            0
       ARP 11:            0
       ARP 12:            0
       ARP 13:            0
       ARP 14:            0
       ARP 15:            0

  QCI 1:
   ARP 1:
    Bearer Active:               0   Bearer setup:                                2
    Bearer Released:             2   Bearer Rejected:                             0

    Uplink Bytes forwarded:      0   Downlink Bytes forwarded:                    0
    Uplink Pkts forwarded:       0   Downlink Pkts forwarded:                     0
    Uplink Bytes dropped:        0   Downlink Bytes dropped:                      0
    Uplink Pkts dropped:         0   Downlink Pkts dropped:                       0
  Uplink Dropped:                          Downlink Dropped:
    MBR Exceeded(Bytes):                0  MBR Exceeded(Bytes):                  0
    MBR Exceeded(Pkts):                 0  MBR Exceeded(Pkts):                   0
```

```
    AMBR Exceeded(Bytes):                  0  AMBR Exceeded(Bytes):                  0
    AMBR Exceeded(Pkts):                   0  AMBR Exceeded(Pkts):                   0
    Miscellaneous(Bytes):                  0  Miscellaneous(Bytes):                  0
    Miscellaneous(Pkts):                   0  Miscellaneous(Pkts):                   0
    Overcharge Prtctn(Bytes)               0  Overcharge Prtctn(Bytes):               0
    Overcharge Prtctn(Pkts):               0  Overcharge Prtctn(Pkts):                0
    SGW Restoration(Bytes):                0  SGW Restoration(Bytes):                 0
    SGW Restoration(Pkts):                 0  SGW Restoration(Pkts):                  0
    SDF Gate(Bytes):                       0  SDF Gate(Bytes):                        0
    SDF Gate(Pkts):                        0  SDF Gate(Pkts):                         0
    ITC Gate(Bytes):                       0  ITC Gate(Bytes):                        0
    ITC Gate(Pkts):                        0  ITC Gate(Pkts):                         0
    Flow Terminated(Bytes):                0  Flow Terminated(Bytes):                 0
    Flow Terminated(Pkts):                 0  Flow Terminated(Pkts):                  0
    Subsession Terminated(Bytes):          0  Subsession Terminated(Bytes):           0
    Subsession Terminated(Pkts):           0  Subsession Terminated(Pkts):            0
    Call Terminated(Bytes):                0  Call Terminated(Bytes):                 0
    Call Terminated(Pkts):                 0  Call Terminated(Pkts):                  0
    DCCA Discard(Bytes):                   0  DCCA Discard(Bytes):                    0
    DCCA Discard(Pkts):                    0  DCCA Discard(Pkts):                     0
    No Rule Match(Bytes):                  0  No Rule Match(Bytes):                   0
    No Rule Match(Pkts):                   0  No Rule Match(Pkts):                    0
    ICAP(Bytes):                           0  ICAP(Bytes):                          N/A
    ICAP(Pkts):                            0  ICAP(Pkts):                           N/A
    SFW(Bytes):                            0  SFW(Bytes):                             0
    SFW(Pkts):                             0  SFW(Pkts):                              0
    Hierarchical ENF(Bytes):               0  Hierarchical ENF(Bytes):                0
    Hierarchical ENF(Pkts):                0  Hierarchical ENF(Pkts):                 0
    Dynamic CA Gate(Bytes):                0  Dynamic CA Gate(Bytes):    :           0
    Dynamic CA Gate(Pkts):                 0  Dynamic CA Gate(Pkts):                  0
    NAT64 Cancel(Bytes):                   0  NAT64 Cancel(Bytes):                    0
    NAT64 Cancel(Pkts):                    0  NAT64 Cancel(Pkts):                     0
    Bearer Not Found(Bytes):               0  Bearer Not Found(Bytes):                0
    Bearer Not Found(Pkts):                0  Bearer Not Found(Pkts):                 0
  QCI 1:
    ARP 2:
    Bearer Active:                     0   Bearer setup:                               2
    Bearer Released:                   2   Bearer Rejected:                            0

    Uplink Bytes forwarded:            0   Downlink Bytes forwarded:                   0
    Uplink Pkts forwarded:             0   Downlink Pkts forwarded:                    0
    Uplink Bytes dropped:              0   Downlink Bytes dropped:                     0
    Uplink Pkts dropped:               0   Downlink Pkts dropped:                      0
   Uplink Dropped:                             Downlink Dropped:
    MBR Exceeded(Bytes):               0  MBR Exceeded(Bytes):                    0
    MBR Exceeded(Pkts):                0  MBR Exceeded(Pkts):                     0
    AMBR Exceeded(Bytes):              0  AMBR Exceeded(Bytes):                   0
    AMBR Exceeded(Pkts):               0  AMBR Exceeded(Pkts):                    0
    Miscellaneous(Bytes):              0  Miscellaneous(Bytes):                   0
    Miscellaneous(Pkts):               0  Miscellaneous(Pkts):                    0
    Overcharge Prtctn(Bytes)           0  Overcharge Prtctn(Bytes):               0
    Overcharge Prtctn(Pkts):           0  Overcharge Prtctn(Pkts):                0
    SGW Restoration(Bytes):            0  SGW Restoration(Bytes):                 0
    SGW Restoration(Pkts):             0  SGW Restoration(Pkts):                  0
    SDF Gate(Bytes):                   0  SDF Gate(Bytes):                        0
    SDF Gate(Pkts):                    0  SDF Gate(Pkts):                         0
    ITC Gate(Bytes):                   0  ITC Gate(Bytes):                        0
    ITC Gate(Pkts):                    0  ITC Gate(Pkts):                         0
    Flow Terminated(Bytes):            0  Flow Terminated(Bytes):                 0
    Flow Terminated(Pkts):             0  Flow Terminated(Pkts):                  0
    Subsession Terminated(Bytes):      0  Subsession Terminated(Bytes):           0
    Subsession Terminated(Pkts):       0  Subsession Terminated(Pkts):            0
    Call Terminated(Bytes):            0  Call Terminated(Bytes):                 0
    Call Terminated(Pkts):             0  Call Terminated(Pkts):                  0
```

```
    DCCA Discard(Bytes):            0  DCCA Discard(Bytes):                  0
    DCCA Discard(Pkts):             0  DCCA Discard(Pkts):                   0
    No Rule Match(Bytes):           0  No Rule Match(Bytes):                 0
    No Rule Match(Pkts):            0  No Rule Match(Pkts):                  0
    ICAP(Bytes):                    0  ICAP(Bytes):                        N/A
    ICAP(Pkts):                     0  ICAP(Pkts):                         N/A
    SFW(Bytes):                     0  SFW(Bytes):                           0
    SFW(Pkts):                      0  SFW(Pkts):                            0
    Hierarchical ENF(Bytes):        0  Hierarchical ENF(Bytes):              0
    Hierarchical ENF(Pkts):         0  Hierarchical ENF(Pkts):               0
    Dynamic CA Gate(Bytes):         0  Dynamic CA Gate(Bytes):    :          0
    Dynamic CA Gate(Pkts):          0  Dynamic CA Gate(Pkts):                0
    NAT64 Cancel(Bytes):            0  NAT64 Cancel(Bytes):                  0
    NAT64 Cancel(Pkts):             0  NAT64 Cancel(Pkts):                   0
    Bearer Not Found(Bytes):        0  Bearer Not Found(Bytes):              0
    Bearer Not Found(Pkts):         0  Bearer Not Found(Pkts):               0
```

show apn statistics name *apn_name* **qci all** コマンドの出力が拡張され、次の新しい統計が表示されるようになりました。

```
Data Statistics:

    Uplink Bytes:                   0   Downlink Bytes:                       0
    Uplink Pkts:                    0   Downlink Pkts:                        0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:               0
    Uplink Pkts dropped:            0   Downnlink Pkts dropped:               0

  Uplink Dropped:                         Downlink Dropped:
    MBR Exceeded(Bytes):                0  MBR Exceeded(Bytes):               0
    MBR Exceeded(Pkts):                 0  MBR Exceeded(Pkts):                0
    AMBR Exceeded(Bytes):               0  AMBR Exceeded(Bytes):              0
    AMBR Exceeded(Pkts):                0  AMBR Exceeded(Pkts):               0
    Miscellaneous(Bytes):               0  Miscellaneous(Bytes):              0
    Miscellaneous(Pkts):                0  Miscellaneous(Pkts):               0
    Overcharge Prtctn(Bytes)            0  Overcharge Prtctn(Bytes):          0
    Overcharge Prtctn(Pkts):            0  Overcharge Prtctn(Pkts):           0
    SGW Restoration(Bytes):             0  SGW Restoration(Bytes):            0
    SGW Restoration(Pkts):              0  SGW Restoration(Pkts):             0
    SDF Gate(Bytes):                    0  SDF Gate(Bytes):                   0
    SDF Gate(Pkts):                     0  SDF Gate(Pkts):                    0
    ITC Gate(Bytes):                    0  ITC Gate(Bytes):                   0
    ITC Gate(Pkts):                     0  ITC Gate(Pkts):                    0
    Flow Terminated(Bytes):             0  Flow Terminated(Bytes):            0
    Flow Terminated(Pkts):              0  Flow Terminated(Pkts):             0
    Subsession Terminated(Bytes):       0  Subsession Terminated(Bytes):      0
    Subsession Terminated(Pkts):        0  Subsession Terminated(Pkts):       0
    Call Terminated(Bytes):             0  Call Terminated(Bytes):            0
    Call Terminated(Pkts):              0  Call Terminated(Pkts):             0
    DCCA Discard(Bytes):                0  DCCA Discard(Bytes):               0
    DCCA Discard(Pkts):                 0  DCCA Discard(Pkts):                0
    No Rule Match(Bytes):               0  No Rule Match(Bytes):              0
    No Rule Match(Pkts):                0  No Rule Match(Pkts):               0
    ICAP(Bytes):                        0  ICAP(Bytes):                     N/A
    ICAP(Pkts):                         0  ICAP(Pkts):                      N/A
    SFW(Bytes):                         0  SFW(Bytes):                        0
    SFW(Pkts):                          0  SFW(Pkts):                         0
    Hierarchical ENF(Bytes):            0  Hierarchical ENF(Bytes):           0
    Hierarchical ENF(Pkts):             0  Hierarchical ENF(Pkts):            0
    Dynamic CA Gate(Bytes):             0  Dynamic CA Gate(Bytes):    :       0
    Dynamic CA Gate(Pkts):              0  Dynamic CA Gate(Pkts):             0
    NAT64 Cancel(Bytes):                0  NAT64 Cancel(Bytes):               0
    NAT64 Cancel(Pkts):                 0  NAT64 Cancel(Pkts):                0
    Bearer Not Found(Bytes):            0  Bearer Not Found(Bytes):           0
    Bearer Not Found(Pkts):             0  Bearer Not Found(Pkts):            0
```

```
4G Bearers Released By Reasons:

                      QCI1  QCI2  QCI3  QCI4  QCI5  QCI6  QCI7  QCI8    QCI9
   Admin disconnect:     0     0     0     0     0     0     0     0       0


Subscriber QoS Statistics:

  QCI 1:
    Bearer Active:                    0   Bearer setup:                              0
    Bearer Released:                  0   Bearer Rejected:                           0

    Uplink Bytes forwarded:           0   Downlink Bytes forwarded:                  0
    Uplink Pkts forwarded:            0   Downlink Pkts forwarded:                   0
    Uplink Bytes dropped:             0   Downlink Bytes dropped:                    0
    Uplink Pkts dropped:              0   Downlink Pkts dropped:                     0
  Uplink Dropped:                             Downlink Dropped:
    MBR Exceeded(Bytes):                  0   MBR Exceeded(Bytes):                   0
    MBR Exceeded(Pkts):                   0   MBR Exceeded(Pkts):                    0
    AMBR Exceeded(Bytes):                 0   AMBR Exceeded(Bytes):                  0
    AMBR Exceeded(Pkts):                  0   AMBR Exceeded(Pkts):                   0
    Miscellaneous(Bytes):                 0   Miscellaneous(Bytes):                  0
    Miscellaneous(Pkts):                  0   Miscellaneous(Pkts):                   0
    Overcharge Prtctn(Bytes)              0   Overcharge Prtctn(Bytes):              0
    Overcharge Prtctn(Pkts):              0   Overcharge Prtctn(Pkts):               0
    SGW Restoration(Bytes):               0   SGW Restoration(Bytes):                0
    SGW Restoration(Pkts):                0   SGW Restoration(Pkts):                 0
    SDF Gate(Bytes):                      0   SDF Gate(Bytes):                       0
    SDF Gate(Pkts):                       0   SDF Gate(Pkts):                        0
    ITC Gate(Bytes):                      0   ITC Gate(Bytes):                       0
    ITC Gate(Pkts):                       0   ITC Gate(Pkts):                        0
    Flow Terminated(Bytes):               0   Flow Terminated(Bytes):                0
    Flow Terminated(Pkts):                0   Flow Terminated(Pkts):                 0
    Subsession Terminated(Bytes):         0   Subsession Terminated(Bytes):          0
    Subsession Terminated(Pkts):          0   Subsession Terminated(Pkts):           0
    Call Terminated(Bytes):               0   Call Terminated(Bytes):                0
    Call Terminated(Pkts):                0   Call Terminated(Pkts):                 0
    DCCA Discard(Bytes):                  0   DCCA Discard(Bytes):                   0
    DCCA Discard(Pkts):                   0   DCCA Discard(Pkts):                    0
    No Rule Match(Bytes):                 0   No Rule Match(Bytes):                  0
    No Rule Match(Pkts):                  0   No Rule Match(Pkts):                   0
    ICAP(Bytes):                          0   ICAP(Bytes):                         N/A
    ICAP(Pkts):                           0   ICAP(Pkts):                          N/A
    SFW(Bytes):                           0   SFW(Bytes):                            0
    SFW(Pkts):                            0   SFW(Pkts):                             0
    Hierarchical ENF(Bytes):              0   Hierarchical ENF(Bytes):               0
    Hierarchical ENF(Pkts):               0   Hierarchical ENF(Pkts):                0
    Dynamic CA Gate(Bytes):               0   Dynamic CA Gate(Bytes):    :           0
    Dynamic CA Gate(Pkts):                0   Dynamic CA Gate(Pkts):                 0
    NAT64 Cancel(Bytes):                  0   NAT64 Cancel(Bytes):                   0
    NAT64 Cancel(Pkts):                   0   NAT64 Cancel(Pkts):                    0
    Bearer Not Found(Bytes):              0   Bearer Not Found(Bytes):               0
    Bearer Not Found(Pkts):               0   Bearer Not Found(Pkts):                0

.
.
.
QCI 9:
    Bearer Active:                    0   Bearer setup:                              0
    Bearer Released:                  0   Bearer Rejected:                           0

    Uplink Bytes forwarded:           0   Downlink Bytes forwarded:                  0
```

```
Uplink Pkts forwarded:          0   Downlink Pkts forwarded:                    0
Uplink Bytes dropped:           0   Downlink Bytes dropped:                     0
Uplink Pkts dropped:            0   Downlink Pkts dropped:
```

show configuration

このコマンドの出力が拡張され、統計プロファイルの設定が表示されるようになりました。

- stats-profile <*stats_profile_name*>
- qci <*qci number*> arp <*arp number*>
- packet-drop（*packet-drop* が有効になっている場合）

show stats-profile name

Exec モードのこの新しいコマンドは、指定された統計プロファイルの設定内容を表示します。

- 統計プロファイル名：<*stats_profile_name*>
- qci <*qci number*> arp <*arp_number(s)*>
- packet-drop <*if packet drop is enabled*>

QCI 値と ARP 値の両方に基づく DSCP マーキング

機能説明

P-GW では、QoS クラス識別子（QCI）値に基づいて DSCP マーキングを実行できます。この機能が拡張され、割り当ておよび保持プライオリティ（ARP）の優先順位レベル（PL）値（1 ～ 15）が追加されました。これにより、QCI 値が同じで ARP 優先順位値が異なるベアラーに異なる DSCP 値を割り当てることができます。たとえば、QCI+ARP に基づいて DSCP 値を割り当てる機能を使用して、VoLTE を介した優先コールと緊急コールに関するコンプライアンスを満たすことができます。

次のインターフェイスの P-GW に適用されます。

- S5
- S8
- SGi
- S2b

次のインターフェイスの S-GW に適用されます。

- S1-U
- S5
- S8

- S11
- S4

他の機能との関係

ECS は、内部 IP ヘッダーに DSCP 値を入力します。これらの値は、sessmanager API を使用して DSCP テーブルから取得されます。DSCP 値が QCI と ARP の組み合わせで使用できるようになったため、API は、QCI と ARP の両方を受け入れ、新しいデータ構造で ECS に DSCP 値を提供するラッパー API に置き換えられます。

API は、次のシナリオで正しい値を返します。

1. QCI-DSCP テーブルが設定されていないか、このセッションに関連付けられていません。

   API は、テーブルが見つからなかったという通知を ECS に返します。

2. テーブルは設定されていますが、指定された QCI 値のエントリがテーブルに存在しません。

   API は構造に入力せず、構造は変更されずに同じ状態に保たれます。

3. 特定の QCI のエントリが存在しますが、特定の QCI-ARP ペアでは使用できません。

   特定の QCI のデフォルト DSCP 値が応答の構造に入力されます。

4. 特定の QCI と ARP の組み合わせのエントリが存在します。

   特定の QCI と ARP の組み合わせの DSCP 値が応答の構造に入力されます。

SM から値を受信すると、ECS はこれらの値をキャッシュし、キャッシュされた値を使用して以降のパケットをマークします。テーブルへの追加のルックアップは、現在キャッシュされている QCI-ARP 値と現在のパケットの QCI-ARP 値の間に不一致がある場合にのみ実行されます。したがって、QCI-ARP テーブルでの変更は、QCI または ARP が変更された場合にのみ、既存のフローの内部 DSCP マーキングの影響を受けます。

ライセンス

DSCP マーキング機能を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

機能の仕組み

同じ QCI を持ち異なる APR 値を持つベアラーに異なる DSCP 値を割り当てることができるように機能が拡張され、次のように機能します。

- QCI+ARP の組み合わせに基づくパケットの DSCP マーキングが許可されます。
- QCI+ARP の設定により、その QCI+ARP の組み合わせに対する DSCP エントリがすべてオーバーライドされます。

- QCI のみの DSCP エントリにより、既存の QCI+ARP 設定がすべてオーバーライドされます。
- アップリンクおよびダウンリンク機能のための QCI+ARP に関連する DSCP マーキングの適用も許可されます。

QCI 値と ARP 値の両方に基づく DSCP マーキングの設定

このセクションでは、QCI 値と ARP 値の両方に基づいて DSCP マーキングを設定する方法について説明します。

QCI-QoS マッピングの設定

QCI および ARP 値を作成して、強制可能な Quality of Service（QoS）パラメータにマッピングするには、次の例に示すコマンドを使用します。

```
configure
   qci-qos-mapping name
     qci num [ arp-priority-level arp_value ] [ downlink [ encaps-header
{ copy-inner | dscp-marking dscp-marking-value } ] [ internal-qos priority
 priority ] [ user-datagram dscp-marking dscp-marking-value  ] ] [ uplink [
 downlink] [ encaps-header { copy-inner | dscp-marking dscp-marking-value
 } ] [ internal-qos priority priority ]  [ user-datagram dscp-marking
dscp-marking-value  ] ]
     end
```

注：

- 有効なライセンスキーがインストールされていない場合、P-GW は非標準の QCI 値をサポートしません。

  QCI 値 1 ～ 9 は、3GPP TS 23.203 で定義されている標準値です。P-GW はこれらの標準値をサポートします。また、QCI 値 65、66、69、70 は、StarOS リリース 21.0 以降で使用できます。

  3GPP リリース 8 以降では、通信事業者固有/非標準の QCI がサポートされ、キャリアは QCI 128- 254 を定義できます。

- **arp-priority-level** *arp_value*：Address Retention Priority（ARP）の優先順位レベルを指定します。

  arp_value は、1 から 15 までの整数値にする必要があります。

- 上記の設定は、1 つのキーワードの例のみを示しています。**qci** コマンドおよびサポートされるその他のキーワードの詳細については、『*Command Line Interface Reference*』の「*QCI - QOS Mapping Configuration Mode Commands*」[英語] の章を参照してください。

QCI および ARP 値を無効にするには、次の例に示すコマンドを使用します。

```
configure
   qci-qos-mapping name
```

```
no qci num [ arp-priority-level arp_value ]
end
```

QCI-QoS マッピング設定の関連付け

次の例を使用して、P-GW サービスが既存の QCI-QoS マッピング設定に関連付けられることを指定します。

```
configure
  contextcontext_name
    pgw-service pgw_service_name
      associate qci-qos-mapping name
      end
```

注：

- QCI-QoS マッピング設定は AAA コンテキストで作成されます。

次の例を使用して、S-GW サービスが既存の QCI-QoS マッピング設定に関連付けられることを指定します。

```
configure
  contextcontext_name
    sgw-service sgw_service_name
      associate qci-qos-mapping name
      end
```

注：

- QCI-QoS マッピング設定は AAA コンテキストで作成されます。

GTP-C の CS5 マーキングの設定

制御パケットで DSCP を CS5 より優先処理するとマーク付けするには、次の例に示すコマンドを使用します。

```
configure
  contextcontext_name
    ggsn-service ggsn_service_name
      ip qos-dscp gtpc cs5
      end
```

注：

- GTP-C パケットでは、クラスセレクタ 5 DSCP の優先順位を指定します。

設定の確認

設定を表示または確認するには、Exec モードで次のコマンドを使用します。

```
show configuration
```

QCI 値と ARP 値の両方に基づく DSCP マーキングのモニター

show コマンドの出力

ここでは、QCI 値と ARP 値の両方に基づく DSCP マーキングをサポートするための show コマンドとその出力について説明します。

show qci-qos-mapping table all

このコマンドの出力が拡張され、次の ARP 値が表示されるようになりました。

- arp-priority-level

新しい標準 QCI のサポート

CDETS：CSCuy20910 - 新しい標準 QCI（65、66、69、70）のサポート

該当する製品：P-GW、SAEGW、S-GW

機能説明

P-GW/SAEGW/S-GW は、新しい 3GPP 定義の標準 QCI をサポートするようになりました。QCI 65、66、69、70 は、ミッションクリティカルおよびプッシュツートーク（MC/PTT）アプリケーションをサポートするようになりました。これらの新しい標準 QCI は、これまでサポートされていた QCI 1 ～ 9、および通信事業者が定義する QCI 128 ～ 254 に加えてサポートされます。

StarOS は PCRF から送信される QCI 10 ～ 127 を引き続き拒否します。

ライセンス

重要 新しい標準 QCI サポートはライセンスで供与される機能です。ライセンスの詳細については、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

機能の仕組み

3GPP 仕様には QCI 65 と QCI 69 のみが共存可能であると記載されていますが、PCRF に適用されるため、この機能の StarOS 実装における QCI には厳しい制限はありません。P-GW は、パススルーノードとして機能し、異なる QCI の組み合わせが PCRF から要求された場合、QCI 65 と QCI 69 を許可します。

標準 QCI 65、66、69、および 70 の存在がサポートされているため、この実装には、次の StarOS インターフェイスを介したサポートも追加されています。

- **Gx**：Gx は、デフォルトベアラー QoS とルール検証を処理し、新しいミッションクリティカル（MC）/プッシュツートーク（PTT）QCI を許可します。MC/PTT ビットが PCRF とネゴシエートされない場合、PCEF は、ベアラーの作成を拒否するか、コールセットアップを拒否します。
- **sessmgr**：P-GW sessmgr は、QoS の更新と変更を処理するようになりました。P-GW は、新しい標準 QCI に対するすべての UE 開始 BRC 作成を拒否します。
- **ECS**：ECS は、PCRF から新しい標準 QCI を受信した場合はそれらを受け入れ、ライセンスが設定されていないか 3G で同じものを受信した場合はそれらを拒否します。ECS は、この QoS 変更でデフォルトのベアラーを更新したり、新しい標準 QCI の専用ベアラーを作成することができます。

ハンドオフ動作

Gn/Gp ハンドオフの場合、CLI によるローカルマッピングがサポートされており、それによって P-GW/SAEGW/S-GW が MME から SGSN へのコンテキスト転送と同期化されます。次のシナリオがサポートされています。

ローカル QoS マッピングが存在しない：新しい QCI のローカルマッピングが存在しない場合、4G から 3G へのコールハンドオフは拒否されます。

ローカル QoS マッピングが存在する：ローカルマッピングが存在する場合、次の 3 つのシナリオがサポートされます。

- **同期していない MME-SGSN と PCRF のローカルマッピングが存在する**：ローカルマッピングが存在する場合は、P-GW の QoS マッピングが MME から SGSN へのマッピングと同期していると見なされます。Gn/Gp ハンドオフ中に転送された PDP の 1 つの QoS マッピングが MME-SGSN マッピングと同期していない場合でも、P-GW/SAW/S-GW は、ローカルマッピングが存在する状態でハンドオフを続行します。ただし、ハンドオフ時に PCRF 応答を待機している間に生成された CDR は、ハンドオフ後に受信した CDR と同期しません。
- **同期している MME-SGSN と PCRF のマッピングが存在する**：ローカルマッピングが MME-SGSN と同期している場合、ハンドオフ後に生成された CDR に違いはありません。
- **部分的なマッピングが存在する**：部分的なマッピングは、一部の MC/PTT QCI にマッピングがあり、残りの MC/PTT QCI にマッピングがない場合に発生します。この場合、コールはドロップされます。

想定されるコールフロー出力

ここでは、新しい標準 QCI サポート機能を使用するさまざまな新しいシナリオで想定されるコールフロー出力の詳細について説明します。

- 新しいコールプロシージャ
- ハンドオフプロシージャ
- UE 開始ベアラー作成

- ベアラーの作成
- ベアラーの更新

ここでは、新しい動作を説明するとともに、この機能での動作を詳細に説明します。説明のない動作は、標準 QCI の場合と同じです。

新しいコールプロシージャ

ここでは、新しい標準QCIサポート機能を使用するさまざまな新しいコールプロシージャシナリオで想定されるコールフロー出力の詳細について説明します。

表 *52 :* 想定されるコールフロー出力：新しいコールプロシージャ

手順	事前条件	コール QCI の変更	メッセージ タイプ	QCI タイプの要求	PGW ライセンス	Gx インターフェイス（受信した、再マッピングされた QCI タイプ）			予想される動作
						CCA-I	CCA-U	RAR	
3G の設定（GGSN）	該当なし	該当なし	PDP 作成要求	標準 QCI	有効	MC/PTT 標準 QCI	該当なし	該当なし	アプリケーションによって拒否されたコール
eHRPD の設定	該当なし	該当なし	PBU	標準 QCI	有効	MC/PTT 標準 QCI	該当なし	該当なし	このルールで受け入れおよび作成されたコール
4G の設定（RAT：S4-SGSN）	該当なし	該当なし	セッション作成要求	標準 QCI	有効	MC/PTT 標準 QCI	該当なし	該当なし	このルールで受け入れおよび作成されたコール

ハンドオフプロシージャ

ここでは、新しい標準 QCI サポート機能を使用するさまざまなハンドオフ プロシージャ シナリオで想定されるコールフロー出力の詳細について説明します。

表 *53 :* 想定されるコールフロー出力：ハンドオフプロシージャ

手順	事前条件	コール QCI の変更	メッセージ タイプ	QCI タイプの要求	PGW ライセンス	Gx インターフェイス（受信した、再マッピングされた QCI タイプ）			予想される動作
						CCA-I	CCA-U	RAR	
Wi-Fi に存在するデフォルトベアラー	MC/PTT QCI が設定された既存のコールを MC/PTT QCI にハンドオフするよう要求された	セッション作成要求	MC/PTT QCI	イネーブル	該当なし	MC/PTT：デフォルトベアラーで標準 QCI を受信	該当なし	ハンドオフが承認され、ダウンロードされた MC/PTT 標準 QCI が適用される	

手順	事前条件	コール QCI の変更	メッセージ タイプ	QCI タイプの要求	PGW ライセンス	Gx インターフェイス（受信した、再マッピングされた QCI タイプ）			予想される動作
						CCA-I	CCA-U	RAR	
GnGp のハンドオフ（4G（LTE）から 3G（GGSN）へ）	プライマリ PDP で PDP 更新要求を受信し、応答保留中（ローカルマッピングあり）	MC/PTT QCI が設定された既存のコールを標準 QCI にするよう要求され、一部の MC/PTT QCI ベアラーでマッピングが受信されない	PDP 更新要求	MC/PTT QCI を標準 QCI にするための部分的なマッピングを PCRF から受信	イネーブル	該当なし	MC/PTT QCI の部分的にマッピングされた標準 QCI を受信。一部の PDP ベアラーでマッピングが受信されない。	該当なし	ハンドオフが拒否され、コールドロップが開始される
	プライマリ PDP で PDP 更新要求を受信し、応答保留中（ローカルマッピングあり）	MC/PTT QCI が設定された既存のコールを標準 QCI にするよう要求され、一部の MC/PTT QCI ベアラーでマッピングが受信されない	PDP 更新要求	MC/PTT QCI を標準 QCI にするための部分的なマッピングを PCRF から受信しない	イネーブル	該当なし	マッピングが受信されない	該当なし	ハンドオフが拒否され、コールドロップが開始される
			PDP 更新要求	該当なし	イネーブル	該当なし	標準 QCI 専用ベアラーで MC/PTT 更新ルールを受信	該当なし	MC/PTT QCI マッピングルールに関連付けられた専用ベアラーが消去され、ハンドオフが許可される

手順	事前条件	コール QCI の変更	メッセージ タイプ	QCI タイプの要求	PGW ライセンス	Gx インターフェイス（受信した、再マッピングされた QCI タイプ）			予想される動作
						CCA-I	CCA-U	RAR	
	プライマリ PDP で PDP 更新要求を受信し、応答保留中 （ローカル マッピングなし）	標準プライマリ PDP と MC/PTT QCI が設定された既存のコールを標準 QCI にするよう要求された							
	プライマリ PDP で PDP 更新要求を受信し、応答保留中 （ローカル マッピングなし）	MC/PTT プライマリ PDP が設定された既存のコール	PDP 更新要求	該当なし	イネーブル	該当なし	該当なし	該当なし	ハンドオフが拒否され、コールドロップが開始される（ハンドオフのために CCA-U を開始する前にドロップされる）
	プライマリ PDP で PDP 更新要求を受信し、応答保留中 （ローカル マッピングあり）	MC/PTT QCI が設定された既存のコールを標準 QCI にするよう要求された	PDP 更新要求	PCRF はタイムアウトし、応答を受信しない	イネーブル	該当なし	PCRF から応答なし/CCA-U はタイムアウト	該当なし	ハンドオフが拒否され、コールドロップが開始される
			PDP 更新要求		イネーブル	該当なし	PCRF からすべてのマッピングを受信	該当なし	ハンドオフが承認される

手順	事前条件	コール QCI の変更	メッセージ タイプ	QCI タイプの要求	PGW ライセンス	Gx インターフェイス（受信した、再マッピングされた QCI タイプ）			予想される動作
						CCA-I	CCA-U	RAR	
	プライマリ PDP で PDP 更新要求を受信し、応答保留中。BCM モードが混合している。（ローカルマッピングが存在し、HO 中に UPC で取得される QCI 値と同じ）	MC/PTT QCI が設定された既存のコールを標準 QCI にするよう要求された		MC/PTT QCI を標準 QCI にするためのマッピングを PCRF から受信					
	プライマリ PDP で PDP 更新要求を受信し、応答保留中。BCM モードが混合している。（ローカルマッピングが存在し、HO 中に UPC で取得される QCI 値と異なる）	MC/PTT QCI が設定された既存のコールを標準 QCI にするよう要求された	PDP 更新要求	該当なし	イネーブル	該当なし	該当なし	該当なし	ハンドオフが拒否され、コールドロップが開始される
			PDP 更新要求		イネーブル	該当なし		該当なし	ハンドオフが承認される

手順	事前条件	コール QCI の変更	メッセージ タイプ	QCI タイプの要求	PGW ライセンス	Gx インターフェイス（受信した、再マッピングされた QCI タイプ）			予想される動作
						CCA-I	CCA-U	RAR	
	プライマリ PDP で PDP 更新要求を受信し、応答保留中。BCM モードは UE のみ。 （ローカルマッピングが存在し、HO 中に UPC で取得される QCI 値と同じ）	MC/PTT QCI が設定された既存のコールを標準 QCI にするよう要求された		MC/PTT QCI を標準 QCI にするためのマッピングを PCRF から受信			PCRF からすべてのマッピングを受信		
	プライマリ PDP で PDP 更新要求を受信し、応答保留中。BCM モードは UE のみ。 （ローカルマッピングが存在し、HO 中に UPC で取得される QCI 値と異なる）	MC/PTT QCI が設定された既存のコールを標準 QCI にするよう要求された	PDP 更新要求	MC/PTT QCI を標準 QCI にするためのマッピングを PCRF から受信	イネーブル	該当なし	PCRF からすべてのマッピングを受信	該当なし	ハンドオフが承認される
			PDP 更新要求	該当なし	イネーブル	該当なし	該当なし	該当なし	

手順	事前条件	コール QCI の変更	メッセージ タイプ	QCI タイプの要求	PGW ライセンス	Gx インターフェイス（受信した、再マッピングされた QCI タイプ）			予想される動作
						CCA-I	CCA-U	RAR	
	プライマリ PDP で PDP 更新要求を受信し、応答保留中（ローカルマッピングあり/なし）	MC/PTT QCI が設定された既存のコールを標準 QCI にするよう要求された。また、suppress-NRUPC UPC が GGSN サービスレベルで設定されている。							ハンドオフが拒否され、コールドロップが開始される
	プライマリ PDP で PDP 更新要求を受信し、応答を送信（ローカルマッピングあり）	MC/PTT QCI が設定された既存のコールを標準 QCI にするよう要求され、すべての MC/PTT QCI ベアラーでマッピングを受信	PDP 更新要求	MC/PTT QCI から標準 QCI への完全なマッピングを PCRF から受信（ローカル MC/PTT から標準 QCI へのマッピングと同じ）	イネーブル	該当なし	MC/PTT QCI ですべて標準 QCI にマッピングされる	該当なし	ハンドオフが承認される
			PDP 更新要求		イネーブル	該当なし	MC/PTT QCI ですべて標準 QCI にマッピングされる	該当なし	

手順	事前条件	コール QCI の変更	メッセージ タイプ	QCI タイプの要求	PGW ライセンス	Gx インターフェイス（受信した、再マッピングされた QCI タイプ）			予想される動作
						CCA-I	CCA-U	RAR	
	プライマリ PDP で PDP 更新要求を受信し、応答を送信（ローカル マッピングあり）	MC/PTT QCI が設定された既存のコールを標準 QCI にするよう要求され、すべての MC/PTT QCI ベアラーでマッピングを受信		MC/PTT QCI から標準 QCI への完全なマッピングを PCRF から受信（ローカル MC/PTT から標準 QCI へのマッピングと異なる）					ハンドオフが承認され、すべてのベアラーで PDP 更新応答が送信される
eHRPD -> LTE	ho_ind = 1 でセッション作成要求を受信	コールに 1 つのベアラーのみが存在	セッション作成要求	MC/PTT QCI	イネーブル	該当なし	ルールで MC/PTT 標準 QCI を受信	該当なし	ハンドオフが受信され、受信した MC/PTT 標準 QCI で専用ベアラーが作成される。
LTE -> eHRPD	LTE 用に存在するデフォルト + 専用ベアラー	MC/PTT QCI が設定された既存のコール	PBU	該当なし	イネーブル	該当なし	該当なし	該当なし	ハンドオフが承認されて、PBA が送信されると、専用ベアラールールがシングルベアラーの下に追加されます

UE 開始ベアラー作成

このセクションでは、新しい標準 QCI サポート機能を使用したさまざまな UE 開始ベアラー作成シナリオで予想されるコールフロー出力に関する詳細情報を提供します。

表 *54 :* 予想されるコールフロー出力：*UE* 開始ベアラー作成

手順 (3GPP/GSM)	事前条件	コール QCI の変更	メッセージ タイプ	QCI タイプの要求	PGW ライセンス	Gx インターフェイス（受信した、再マッピングされた QCI タイプ）			予想される動作
						CCA-I	CCA-U	RAR	
LTE UE 開始 ベアラー	LTE 用に存在するデフォルトのベアラー	該当なし	ベアラーリソースコマンド	MC/PTT 標準 QCI	該当なし	該当なし	該当なし	該当なし	アプリケーションにより BRC を拒否
	LTE 用に存在するデフォルトのベアラー	該当なし	ベアラーリソースコマンド	標準 QCI	無効	該当なし	MC/PTT 標準専用 QCI	該当なし	BRC を拒否/リソース割り当ての失敗によりルールを拒否
	LTE 用に存在するデフォルトのベアラー	該当なし	ベアラーリソースコマンド	標準 QCI	イネーブル	該当なし	MC/PTT 標準専用 QCI	該当なし	BRC を拒否/MC/PTT 標準 QCI で CBReq を開始

ベアラーの作成

ここでは、新しい標準QCIサポート機能を使用するベアラー作成シナリオで想定されるコールフロー出力の詳細について説明します。

表 *55 :* 予想されるコールフロー出力：ベアラー作成

手順 (3GPP/GSM)	事前条件	コール QCI の変更	メッセージ タイプ	QCI タイプの要求	PGW ライセンス	Gx インターフェイス（受信した、再マッピングされた QCI タイプ）			予想される動作
						CCA-I	CCA-U	RAR	
GGSN セカンダリ PDP の作成	プライマリ PDP が GGSN 用に存在	MC/PTT 標準 QCI で要求される新しいセカンダリ PDP	RAR プロシージャ	該当なし	イネーブル	該当なし	該当なし	MC/PTT 標準 QCI で受信されるルール	PCRF に送信されるセカンダリ PDP に関する CCR-I リソース割り当てに失敗

ベアラーの更新

ここでは、新しい標準QCIサポート機能を使用するベアラー更新シナリオで想定されるコールフロー出力の詳細について説明します。

表 *56 :* 想定されるコールフロー出力：ベアラー更新

手順	事前条件	コール QCI の変更	メッセージ タイプ	QCI タイプの要求	PGW ライセンス	Gxインターフェイス（受信した、再マッピングされた QCI タイプ）			予想される動作
						CCA-I	CCA-U	RAR	
GGSN プライマリ PDP QoS の変更	プライマリ PDP が GGSN用に存在	標準 QCI の既存のコールを MC/PTT 標準 QCI に変更するよう要求	RAR プロシージャ	MC/PTT 標準 QCI	イネーブル	該当なし	該当なし	プライマリ PDP の MC/PTT 標準 QCI を受信	プライマリ PDP QoS 変更が拒否されたため CCR-I QoS 変更失敗
GGSN セカンダリ PDP の QoS 変更	プライマリ PDP とセカンダリ PDP が GGSN用に存在	標準 QCI の既存のコールをセカンダリ PDP 用の MC/PTT 標準 QCI に変更するよう要求	RAR プロシージャ	MC/PTT 標準 QCI	イネーブル	該当なし	該当なし	セカンダリ PDP の MC/PTT 標準 QCI とルールを受信	セカンダリ PDP の QoS 変更が送信されたため CCR-I リソース割り当てに失敗

新しい標準 QCI の設定

新しい標準 QCI の設定は、次のタスクで構成されています。

- QCI-QoS マッピングの設定
- Gn/Gp サポートのためのローカルマッピングの設定
- ネットワーク開始型セットアップ/ティアダウンイベントのトランザクションレートの設定
- ミッションクリティカルな QCI の有効化

QCI-QoS マッピングの設定

標準QCIオプション **65**、**66**、**69**、および **70** が、*QCI-QoS* マッピング コンフィギュレーション モードの **qci** コマンドに追加されました。

新しい標準 QCI の QCI-QoS マッピングを構成するには、次の手順を実行します。

```
configure
  qci-qos-mapping qci_qos_map_name
    qci { 1-9 | 65 | 66 | 69 | 70 }
    end
```

新しい標準 QCI の新しい QCI-QoS マッピングを無効にするには、次の手順を実行します。

```
configure
  qci-qos-mapping qci_qos_map_name
    no qci { 1-9 | 65 | 66 | 69 | 70 }
    end
```

注：

- **qci** オプション 65 と 66 は、保証ビットレート（GBR）ネットワークで開始される QCI 値にのみ使用できます。

  qci オプション 69 および 70 は、GBR 以外のネットワークで開始される QCI 値でのみ使用できます。

- **no** は、指定された標準 **qci** 値を無効にします。

Gn/Gp QoS サポートのためのローカル QCI マッピングの設定

Gn および Gp サポートのためのローカル QCI マッピングを設定するには、次の例を使用します。

```
configure
  qci-qos-mapping mapping_name
    qci  { 1-9 | 65 | 66 | 69 | 70 } pre-rel8-qos-mapping qci_value
    end
```

注：

- **qci**：MPS ライセンスが無効になっている場合、この値は 1 ～ 9 の標準 QoS クラス識別子（QCI）である必要があります。MPS ライセンスが有効になっている場合、この値は 1 ー 9 の標準 QCI、または 65、66、69、70 である必要があります。
- **qci** 65 と 66 はミッションクリティカルまたはプッシュトゥトーク（MC/PTT）GBR の値であり、値 69 と 70 は MC/PTT 非 GBR の値です。
- **qci** 値 65 および 66 は QCI 値 1 ー 4 にのみマッピングでき、QCI 値 69 および 70 は QCI 値 5 ー 9 にのみマッピングできます。

ネットワーク開始型セットアップ/ティアダウンイベントのトランザクションレートの設定

新しい標準 QCI 値の、ネットワーク開始型セットアップ/ティアダウンイベントのトランザクションレートを設定するには、次の手順を実行します。

```
configure
  transaction-rate nw-initiated-setup-teardown-events qci { 1-9 | 65
| 66 | 69 | 70 | 128-254 }
  end
```

新しい標準 QCI 値の、ネットワーク開始型セットアップ/ティアダウンイベントのトランザクションレートを無効にするには、次の手順を実行します。

```
configure
  no transaction-rate nw-initiated-setup-teardown-events qci qci_value
  end
```

注：

- **65** と **66** は、GBR のネットワーク開始型 QCI の値で使用できるオプションです。
- **69** と **70** は、GBR 以外のネットワーク開始型 QCI の値で使用できるオプションです。
- **no** は、指定された新しい標準 QCI 値の、ネットワーク開始型セットアップ/ティアダウンイベントのトランザクションレートを無効にします。

ミッションクリティカルな QCI の有効化

新しい標準 QCI サポートを PCEF と PCRF 間でサポートするには、**diameter encode-supported-features** コマンドに **mission-critical-qcis** キーワードが必要です。ポリシー制御コンフィギュレーション モードでミッションクリティカルな QCI を有効にするには、次の例を使用します。

```
configure
  context context_name
    ims-auth-service ims-ggsn-auth
      policy-control
        diameter encode-supported-features mission-critical-qcis
        end
```

この機能を無効にするには、次のコマンドを入力します。

```
configure
  context context_name
    ims-auth-service ims-ggsn-auth
      policy-control
        no diameter encode-supported-features
        end
```

注：



重要 **mission-critical-qcis** オプションを設定するには、LTE ワイヤレス優先機能セットを有効にする必要があります。LTE ワイヤレス優先機能セットは、ライセンス制御された機能です。ライセンスの詳細については、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

設定の確認

新しい標準 QCI 設定を確認するには、次の例を使用します。

show qci-qos-mapping table name *qci_qos_mapping_table_name*

注：

- コマンド出力には、新しい標準 QCI 番号を含む、すべての QCI-QoS マッピング属性が表示されます。属性のいずれかが正しくない場合は、この章の設定手順を繰り返して設定を修正してください。

機能の監視

この項では、新しい標準 QCI のサポート機能をモニターする方法について説明します。

バルク統計

ここでは、新しい標準QCI機能をサポートするために追加されたバルク統計のリストを示します。

APN スキーマ

新しい標準 QCI 機能をサポートするために、次のバルク統計が S-GW スキーマに追加されました。

```
qci65-actbear
qci65-setupbear
qci65-relbear
qci65-uplinkpkt-fwd
qci65-dwlinkpkt-fwd
qci65-uplinkbyte-fwd
qci65-dwlinkbyte-fwd
qci65-uplinkpkt-drop
qci65-dwlinkpkt-drop
qci65-uplinkbyte-drop
qci65-dwlinkbyte-drop
qci65-uplinkpkt-drop-mbrexcd
qci65-dwlinkpkt-drop-mbrexcd
qci65-uplinkbyte-drop-mbrexcd
qci65-dwlinkbyte-drop-mbrexcd
qci65-rejbearer
qci66-actbear
qci66-setupbear
qci66-relbear
qci66-uplinkpkt-fwd
qci66-dwlinkpkt-fwd
qci66-uplinkbyte-fwd
qci66-dwlinkbyte-fwd
qci66-uplinkpkt-drop
qci66-dwlinkpkt-drop
qci66-uplinkbyte-drop
qci66-dwlinkbyte-drop
qci66-uplinkpkt-drop-mbrexcd
qci66-dwlinkpkt-drop-mbrexcd
qci66-uplinkbyte-drop-mbrexcd
qci66-dwlinkbyte-drop-mbrexcd
```

```
qci66-rejbearer
qci69-actbear
qci69-setupbear
qci69-relbear
qci69-uplinkpkt-fwd
qci69-dwlinkpkt-fwd
qci69-uplinkbyte-fwd
qci69-dwlinkbyte-fwd
qci69-uplinkpkt-drop
qci69-dwlinkpkt-drop
qci69-uplinkbyte-drop
qci69-dwlinkbyte-drop
qci69-uplinkpkt-drop-mbrexcd
qci69-dwlinkpkt-drop-mbrexcd
qci69-uplinkbyte-drop-mbrexcd
qci69-dwlinkbyte-drop-mbrexcd
qci69-rejbearer
qci70-actbear
qci70-setupbear
qci70-relbear
qci70-uplinkpkt-fwd
qci70-dwlinkpkt-fwd
qci70-uplinkbyte-fwd
qci70-dwlinkbyte-fwd
qci70-uplinkpkt-drop
qci70-dwlinkpkt-drop
qci70-uplinkbyte-drop
qci70-dwlinkbyte-drop
qci70-uplinkpkt-drop-mbrexcd
qci70-dwlinkpkt-drop-mbrexcd
qci70-uplinkbyte-drop-mbrexcd
qci70-dwlinkbyte-drop-mbrexcd
qci70-rejbearer
sessstat-bearrel-ded-admin-clear-qci65
sessstat-bearrel-ded-admin-clear-qci66
sessstat-bearrel-ded-admin-clear-qci69
sessstat-bearrel-ded-admin-clear-qci70
```

GTPU スキーマ

新しい標準 QCI 機能をサポートするために、次のバルク統計が GTPU スキーマに追加されました。

```
qci65-uplink-pkts
qci65-uplink-bytes
qci65-dwlink-pkts
qci65-dwlink-byte
qci65-pkts-discard
qci65-bytes-discard
qci66-uplink-pkts
qci66-uplink-bytes
qci66-dwlink-pkts
qci66-dwlink-byte
qci66-pkts-discard
qci66-bytes-discard
qci69-uplink-pkts
qci69-uplink-bytes
qci69-dwlink-pkts
qci69-dwlink-byte
qci69-pkts-discard
qci69-bytes-discard
qci70-uplink-pkts
qci70-uplink-bytes
qci70-dwlink-pkts
```

```
qci70-dwlink-byte
qci70-pkts-discard
qci70-bytes-discard
```

P-GW スキーマ

新しい標準QCI機能をサポートするために、P-GW スキーマに次のバルク統計が追加されました。

```
subqosstat-bearact-qci65
subqosstat-bearact-qci66
subqosstat-bearact-qci69
subqosstat-bearact-qci70
subqosstat-bearsetup-qci65
subqosstat-bearsetup-qci66
subqosstat-bearsetup-qci69
subqosstat-bearsetup-qci70
subqosstat-bearrel-qci65
subqosstat-bearrel-qci66
subqosstat-bearrel-qci69
subqosstat-bearrel-qci70
subdatastat-uppktfwd-qci65
subdatastat-uppktfwd-qci66
subdatastat-uppktfwd-qci69
subdatastat-uppktfwd-qci70
subdatastat-upbytefwd-qci65
subdatastat-upbytefwd-qci66
subdatastat-upbytefwd-qci69
subdatastat-upbytefwd-qci70
subdatastat-downpktfwd-qci65
subdatastat-downpktfwd-qci66
subdatastat-downpktfwd-qci69
subdatastat-downpktfwd-qci70
subdatastat-downbytefwd-qci65
subdatastat-downbytefwd-qci66
subdatastat-downbytefwd-qci69
subdatastat-downbytefwd-qci70
subdatastat-uppktdrop-qci65
subdatastat-uppktdrop-qci66
subdatastat-uppktdrop-qci69
subdatastat-uppktdrop-qci70
subdatastat-upbytedrop-qci65
subdatastat-upbytedrop-qci66
subdatastat-upbytedrop-qci69
subdatastat-upbytedrop-qci70
subdatastat-downpktdrop-qci65
subdatastat-downpktdrop-qci66
subdatastat-downpktdrop-qci69
subdatastat-downpktdrop-qci70
subdatastat-downbytedrop-qci65
subdatastat-downbytedrop-qci66
subdatastat-downbytedrop-qci69
subdatastat-downbytedrop-qci70
subdatastat-uppktdropmbrexc-qci65
subdatastat-uppktdropmbrexc-qci66
subdatastat-uppktdropmbrexc-qci69
subdatastat-uppktdropmbrexc-qci70
subdatastat-upbytedropmbrexc-qci65
subdatastat-upbytedropmbrexc-qci66
subdatastat-upbytedropmbrexc-qci69
subdatastat-upbytedropmbrexc-qci70
subdatastat-downpktdropmbrexc-qci65
subdatastat-downpktdropmbrexc-qci66
subdatastat-downpktdropmbrexc-qci69
```

```
subdatastat-downpktdropmbrexc-qci70
subdatastat-downbytedropmbrexc-qci65
subdatastat-downbytedropmbrexc-qci66
subdatastat-downbytedropmbrexc-qci69
subdatastat-downbytedropmbrexc-qci70
```

SAEGW スキーマ

新しい標準QCI機能をサポートするために、SAEGW スキーマに次のバルク統計が追加されました。

```
sgw-totepsbearact-qci65
sgw-totepsbearact-qci66
sgw-totepsbearact-qci69
sgw-totepsbearact-qci70
sgw-totepsbearset-qci65
sgw-totepsbearset-qci66
sgw-totepsbearset-qci69
sgw-totepsbearset-qci70
sgw-totepsbearrel-qci65
sgw-totepsbearrel-qci66
sgw-totepsbearrel-qci69
sgw-totepsbearrel-qci70
sgw-totepsbearmod-qci65
sgw-totepsbearmod-qci66
sgw-totepsbearmod-qci69
sgw-totepsbearmod-qci70
sgw-totepsbearrel-dedrsn-pgw-qci65
sgw-totepsbearrel-dedrsn-pgw-qci66
sgw-totepsbearrel-dedrsn-pgw-qci69
sgw-totepsbearrel-dedrsn-pgw-qci70
sgw-totepsbearrel-dedrsn-s1err-qci65
sgw-totepsbearrel-dedrsn-s1err-qci66
sgw-totepsbearrel-dedrsn-s1err-qci69
sgw-totepsbearrel-dedrsn-s1err-qci70
sgw-totepsbearrel-dedrsn-s5err-qci65
sgw-totepsbearrel-dedrsn-s5err-qci66
sgw-totepsbearrel-dedrsn-s5err-qci69
sgw-totepsbearrel-dedrsn-s5err-qci70
sgw-totepsbearrel-dedrsn-s4err-qci65
sgw-totepsbearrel-dedrsn-s4err-qci66
sgw-totepsbearrel-dedrsn-s4err-qci69
sgw-totepsbearrel-dedrsn-s4err-qci70
sgw-totepsbearrel-dedrsn-s12err-qci65
sgw-totepsbearrel-dedrsn-s12err-qci66
sgw-totepsbearrel-dedrsn-s12err-qci69
sgw-totepsbearrel-dedrsn-s12err-qci70
sgw-totepsbearrel-dedrsn-local-qci65
sgw-totepsbearrel-dedrsn-local-qci66
sgw-totepsbearrel-dedrsn-local-qci69
sgw-totepsbearrel-dedrsn-local-qci70
sgw-totepsbearrel-dedrsn-pdn-qci65
sgw-totepsbearrel-dedrsn-pdn-qci66
sgw-totepsbearrel-dedrsn-pdn-qci69
sgw-totepsbearrel-dedrsn-pdn-qci70
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s1-u-qci70
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s5-u-qci70
sgw-totepsbearrel-dedrsn-pathfail-s5-qci65
```

sgw-totepsbearrel-dedrsn-pathfail-s5-qci66
sgw-totepsbearrel-dedrsn-pathfail-s5-qci69
sgw-totepsbearrel-dedrsn-pathfail-s5-qci70
sgw-totepsbearrel-dedrsn-pathfail-s11-qci65
sgw-totepsbearrel-dedrsn-pathfail-s11-qci66
sgw-totepsbearrel-dedrsn-pathfail-s11-qci69
sgw-totepsbearrel-dedrsn-pathfail-s11-qci70
sgw-totepsbearrel-dedrsn-pathfail-s12-qci65
sgw-totepsbearrel-dedrsn-pathfail-s12-qci66
sgw-totepsbearrel-dedrsn-pathfail-s12-qci69
sgw-totepsbearrel-dedrsn-pathfail-s12-qci70
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci65
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci66
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci69
sgw-totepsbearrel-dedrsn-pathfail-s4-u-qci70
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci65
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci66
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci69
sgw-totepsbearrel-dedrsn-inactivity-timeout-qci70
sgw-totepsbearrel-dedrsn-other-qci65
sgw-totepsbearrel-dedrsn-other-qci66
sgw-totepsbearrel-dedrsn-other-qci69
sgw-totepsbearrel-dedrsn-other-qci70
sgw-datastat-ul-qci65totbyte
sgw-datastat-ul-qci65totpkt
sgw-datastat-ul-qci66totbyte
sgw-datastat-ul-qci66totpkt
sgw-datastat-ul-qci69totbyte
sgw-datastat-ul-qci69totpkt
sgw-datastat-ul-qci70totbyte
sgw-datastat-ul-qci70totpkt
sgw-datastat-ul-dropstat-qci65totbyte
sgw-datastat-ul-dropstat-qci65totpkt
sgw-datastat-ul-dropstat-qci66totbyte
sgw-datastat-ul-dropstat-qci66totpkt
sgw-datastat-ul-dropstat-qci69totbyte
sgw-datastat-ul-dropstat-qci69totpkt
sgw-datastat-ul-dropstat-qci70totbyte
sgw-datastat-ul-dropstat-qci70totpkt
sgw-datastat-dl-qci65totbyte
sgw-datastat-dl-qci65totpkt
sgw-datastat-dl-qci66totbyte
sgw-datastat-dl-qci66totpkt
sgw-datastat-dl-qci69totbyte
sgw-datastat-dl-qci69totpkt
sgw-datastat-dl-qci70totbyte
sgw-datastat-dl-qci70totpkt
sgw-datastat-dl-dropstat-qci65totbyte
sgw-datastat-dl-dropstat-qci65totpkt
sgw-datastat-dl-dropstat-qci66totbyte
sgw-datastat-dl-dropstat-qci66totpkt
sgw-datastat-dl-dropstat-qci69totbyte
sgw-datastat-dl-dropstat-qci69totpkt
sgw-datastat-dl-dropstat-qci70totbyte
sgw-datastat-dl-dropstat-qci70totpkt
sgw-s1u-ul-qci65totbyte
sgw-s1u-ul-qci65totpkt
sgw-s1u-ul-qci66totbyte
sgw-s1u-ul-qci66totpkt
sgw-s1u-ul-qci69totbyte
sgw-s1u-ul-qci69totpkt
sgw-s1u-ul-qci70totbyte
sgw-s1u-ul-qci70totpkt
sgw-s1u-ul-drop-qci65totbyte

```
sgw-s1u-ul-drop-qci65totpkt
sgw-s1u-ul-drop-qci66totbyte
sgw-s1u-ul-drop-qci66totpkt
sgw-s1u-ul-drop-qci69totbyte
sgw-s1u-ul-drop-qci69totpkt
sgw-s1u-ul-drop-qci70totbyte
sgw-s1u-ul-drop-qci70totpkt
sgw-s1u-dl-qci65totbyte
sgw-s1u-dl-qci65totpkt
sgw-s1u-dl-qci66totbyte
sgw-s1u-dl-qci66totpkt
sgw-s1u-dl-qci69totbyte
sgw-s1u-dl-qci69totpkt
sgw-s1u-dl-qci70totbyte
sgw-s1u-dl-qci70totpkt
sgw-s1u-dl-drop-qci65totbyte
sgw-s1u-dl-drop-qci65totpkt
sgw-s1u-dl-drop-qci66totbyte
sgw-s1u-dl-drop-qci66totpkt
sgw-s1u-dl-drop-qci69totbyte
sgw-s1u-dl-drop-qci69totpkt
sgw-s1u-dl-drop-qci70totbyte
sgw-s1u-dl-drop-qci70totpkt
sgw-s4u-ul-qci65totbyte
sgw-s4u-ul-qci65totpkt
sgw-s4u-ul-qci66totbyte
sgw-s4u-ul-qci66totpkt
sgw-s4u-ul-qci69totbyte
sgw-s4u-ul-qci69totpkt
sgw-s4u-ul-qci70totbyte
sgw-s4u-ul-qci70totpkt
sgw-s4u-ul-drop-qci65totbyte
sgw-s4u-ul-drop-qci65totpkt
sgw-s4u-ul-drop-qci66totbyte
sgw-s4u-ul-drop-qci66totpkt
sgw-s4u-ul-drop-qci69totbyte
sgw-s4u-ul-drop-qci69totpkt
sgw-s4u-ul-drop-qci70totbyte
sgw-s4u-ul-drop-qci70totpkt
sgw-s4u-dl-qci65totbyte
sgw-s4u-dl-qci65totpkt
sgw-s4u-dl-qci66totbyte
sgw-s4u-dl-qci66totpkt
sgw-s4u-dl-qci69totbyte
sgw-s4u-dl-qci69totpkt
sgw-s4u-dl-qci70totbyte
sgw-s4u-dl-qci70totpkt
sgw-s4u-dl-drop-qci65totbyte
sgw-s4u-dl-drop-qci65totpkt
sgw-s4u-dl-drop-qci66totbyte
sgw-s4u-dl-drop-qci66totpkt
sgw-s4u-dl-drop-qci69totbyte
sgw-s4u-dl-drop-qci69totpkt
sgw-s4u-dl-drop-qci70totbyte
sgw-s4u-dl-drop-qci70totpkt
sgw-s12-ul-qci65totbyte
sgw-s12-ul-qci65totpkt
sgw-s12-ul-qci66totbyte
sgw-s12-ul-qci66totpkt
sgw-s12-ul-qci69totbyte
sgw-s12-ul-qci69totpkt
sgw-s12-ul-qci70totbyte
sgw-s12-ul-qci70totpkt
sgw-s12-ul-drop-qci65totbyte
```

```
sgw-s12-ul-drop-qci65totpkt
sgw-s12-ul-drop-qci66totbyte
sgw-s12-ul-drop-qci66totpkt
sgw-s12-ul-drop-qci69totbyte
sgw-s12-ul-drop-qci69totpkt
sgw-s12-ul-drop-qci70totbyte
sgw-s12-ul-drop-qci70totpkt
sgw-s12-dl-qci65totbyte
sgw-s12-dl-qci65totpkt
sgw-s12-dl-qci66totbyte
sgw-s12-dl-qci66totpkt
sgw-s12-dl-qci69totbyte
sgw-s12-dl-qci69totpkt
sgw-s12-dl-qci70totbyte
sgw-s12-dl-qci70totpkt
sgw-s12-dl-drop-qci65totbyte
sgw-s12-dl-drop-qci65totpkt
sgw-s12-dl-drop-qci66totbyte
sgw-s12-dl-drop-qci66totpkt
sgw-s12-dl-drop-qci69totbyte
sgw-s12-dl-drop-qci69totpkt
sgw-s12-dl-drop-qci70totbyte
sgw-s12-dl-drop-qci70totpkt
sgw-s5-ul-qci65totbyte
sgw-s5-ul-qci65totpkt
sgw-s5-ul-qci66totbyte
sgw-s5-ul-qci66totpkt
sgw-s5-ul-qci69totbyte
sgw-s5-ul-qci69totpkt
sgw-s5-ul-qci70totbyte
sgw-s5-ul-qci70totpkt
sgw-s5-ul-drop-qci65totbyte
sgw-s5-ul-drop-qci65totpkt
sgw-s5-ul-drop-qci66totbyte
sgw-s5-ul-drop-qci66totpkt
sgw-s5-ul-drop-qci69totbyte
sgw-s5-ul-drop-qci69totpkt
sgw-s5-ul-drop-qci70totbyte
sgw-s5-ul-drop-qci70totpkt
sgw-s5-dl-qci65totbyte
sgw-s5-dl-qci65totpkt
sgw-s5-dl-qci66totbyte
sgw-s5-dl-qci66totpkt
sgw-s5-dl-qci69totbyte
sgw-s5-dl-qci69totpkt
sgw-s5-dl-qci70totbyte
sgw-s5-dl-qci70totpkt
sgw-s5-dl-drop-qci65totbyte
sgw-s5-dl-drop-qci65totpkt
sgw-s5-dl-drop-qci66totbyte
sgw-s5-dl-drop-qci66totpkt
sgw-s5-dl-drop-qci69totbyte
sgw-s5-dl-drop-qci69totpkt
sgw-s5-dl-drop-qci70totbyte
sgw-s5-dl-drop-qci70totpkt
sgw-s8-ul-qci65totbyte
sgw-s8-ul-qci65totpkt
sgw-s8-ul-qci66totbyte
sgw-s8-ul-qci66totpkt
sgw-s8-ul-qci69totbyte
sgw-s8-ul-qci69totpkt
sgw-s8-ul-qci70totbyte
sgw-s8-ul-qci70totpkt
sgw-s8-ul-drop-qci65totbyte
```

```
sgw-s8-ul-drop-qci65totpkt
sgw-s8-ul-drop-qci66totbyte
sgw-s8-ul-drop-qci66totpkt
sgw-s8-ul-drop-qci69totbyte
sgw-s8-ul-drop-qci69totpkt
sgw-s8-ul-drop-qci70totbyte
sgw-s8-ul-drop-qci70totpkt
sgw-s8-dl-qci65totbyte
sgw-s8-dl-qci65totpkt
sgw-s8-dl-qci66totbyte
sgw-s8-dl-qci66totpkt
sgw-s8-dl-qci69totbyte
sgw-s8-dl-qci69totpkt
sgw-s8-dl-qci70totbyte
sgw-s8-dl-qci70totpkt
sgw-s8-dl-drop-qci65totbyte
sgw-s8-dl-drop-qci65totpkt
sgw-s8-dl-drop-qci66totbyte
sgw-s8-dl-drop-qci66totpkt
sgw-s8-dl-drop-qci69totbyte
sgw-s8-dl-drop-qci69totpkt
sgw-s8-dl-drop-qci70totbyte
sgw-s8-dl-drop-qci70totpkt
sgw-s5s8-ul-qci65totbyte
sgw-s5s8-ul-qci65totpkt
sgw-s5s8-ul-qci66totbyte
sgw-s5s8-ul-qci66totpkt
sgw-s5s8-ul-qci69totbyte
sgw-s5s8-ul-qci69totpkt
sgw-s5s8-ul-qci70totbyte
sgw-s5s8-ul-qci70totpkt
sgw-s5s8-ul-drop-qci65totbyte
sgw-s5s8-ul-drop-qci65totpkt
sgw-s5s8-ul-drop-qci66totbyte
sgw-s5s8-ul-drop-qci66totpkt
sgw-s5s8-ul-drop-qci69totbyte
sgw-s5s8-ul-drop-qci69totpkt
sgw-s5s8-ul-drop-qci70totbyte
sgw-s5s8-ul-drop-qci70totpkt
sgw-s5s8-dl-qci65totbyte
sgw-s5s8-dl-qci65totpkt
sgw-s5s8-dl-qci66totbyte
sgw-s5s8-dl-qci66totpkt
sgw-s5s8-dl-qci69totbyte
sgw-s5s8-dl-qci69totpkt
sgw-s5s8-dl-qci70totbyte
sgw-s5s8-dl-qci70totpkt
sgw-s5s8-dl-drop-qci65totbyte
sgw-s5s8-dl-drop-qci65totpkt
sgw-s5s8-dl-drop-qci66totbyte
sgw-s5s8-dl-drop-qci66totpkt
sgw-s5s8-dl-drop-qci69totbyte
sgw-s5s8-dl-drop-qci69totpkt
sgw-s5s8-dl-drop-qci70totbyte
sgw-s5s8-dl-drop-qci70totpkt
pgw-subqosstat-bearact-qci65
pgw-subqosstat-bearact-qci66
pgw-subqosstat-bearact-qci69
pgw-subqosstat-bearact-qci70
pgw-subqosstat-bearset-qci65
pgw-subqosstat-bearset-qci66
pgw-subqosstat-bearset-qci69
pgw-subqosstat-bearset-qci70
pgw-subqosstat-bearrel-qci65
```

```
pgw-subqosstat-bearrel-qci66
pgw-subqosstat-bearrel-qci69
pgw-subqosstat-bearrel-qci70
pgw-subdatastat-ulpktfwd-qci65
pgw-subdatastat-ulpktfwd-qci66
pgw-subdatastat-ulpktfwd-qci69
pgw-subdatastat-ulpktfwd-qci70
pgw-subdatastat-ulbytefwd-qci65
pgw-subdatastat-ulbytefwd-qci66
pgw-subdatastat-ulbytefwd-qci69
pgw-subdatastat-ulbytefwd-qci70
pgw-subdatastat-dlpktfwd-qci65
pgw-subdatastat-dlpktfwd-qci66
pgw-subdatastat-dlpktfwd-qci69
pgw-subdatastat-dlpktfwd-qci70
pgw-subdatastat-dlbytefwd-qci65
pgw-subdatastat-dlbytefwd-qci66
pgw-subdatastat-dlbytefwd-qci69
pgw-subdatastat-dlbytefwd-qci70
pgw-subdatastat-ulpktdrop-qci65
pgw-subdatastat-ulpktdrop-qci66
pgw-subdatastat-ulpktdrop-qci69
pgw-subdatastat-ulpktdrop-qci70
pgw-subdatastat-ulbytedrop-qci65
pgw-subdatastat-ulbytedrop-qci66
pgw-subdatastat-ulbytedrop-qci69
pgw-subdatastat-ulbytedrop-qci70
pgw-subdatastat-dlpktdrop-qci65
pgw-subdatastat-dlpktdrop-qci66
pgw-subdatastat-dlpktdrop-qci69
pgw-subdatastat-dlpktdrop-qci70
pgw-subdatastat-dlbytedrop-qci65
pgw-subdatastat-dlbytedrop-qci66
pgw-subdatastat-dlbytedrop-qci69
pgw-subdatastat-dlbytedrop-qci70
pgw-subdatastat-ulpktdropmbrexc-qci65
pgw-subdatastat-ulpktdropmbrexc-qci66
pgw-subdatastat-ulpktdropmbrexc-qci69
pgw-subdatastat-ulpktdropmbrexc-qci70
pgw-subdatastat-ulbytedropmbrexc-qci65
pgw-subdatastat-ulbytedropmbrexc-qci66
pgw-subdatastat-ulbytedropmbrexc-qci69
pgw-subdatastat-ulbytedropmbrexc-qci70
pgw-subdatastat-dlpktdropmbrexc-qci65
pgw-subdatastat-dlpktdropmbrexc-qci66
pgw-subdatastat-dlpktdropmbrexc-qci69
pgw-subdatastat-dlpktdropmbrexc-qci70
pgw-subdatastat-dlbytedropmbrexc-qci65
pgw-subdatastat-dlbytedropmbrexc-qci66
pgw-subdatastat-dlbytedropmbrexc-qci69
pgw-subdatastat-dlbytedropmbrexc-qci70
collapsed-subdatastat-ulpktfwd-qci65
collapsed-subdatastat-ulpktfwd-qci66
collapsed-subdatastat-ulpktfwd-qci69
collapsed-subdatastat-ulpktfwd-qci70
collapsed-subdatastat-ulbytefwd-qci65
collapsed-subdatastat-ulbytefwd-qci66
collapsed-subdatastat-ulbytefwd-qci69
collapsed-subdatastat-ulbytefwd-qci70
collapsed-subdatastat-dlpktfwd-qci65
collapsed-subdatastat-dlpktfwd-qci66
collapsed-subdatastat-dlpktfwd-qci69
collapsed-subdatastat-dlpktfwd-qci70
collapsed-subdatastat-dlbytefwd-qci65
```

```
collapsed-subdatastat-dlbytefwd-qci66
collapsed-subdatastat-dlbytefwd-qci69
collapsed-subdatastat-dlbytefwd-qci70
collapsed-subdatastat-ulpktdrop-qci65
collapsed-subdatastat-ulpktdrop-qci66
collapsed-subdatastat-ulpktdrop-qci69
collapsed-subdatastat-ulpktdrop-qci70
collapsed-subdatastat-ulbytedrop-qci65
collapsed-subdatastat-ulbytedrop-qci66
collapsed-subdatastat-ulbytedrop-qci69
collapsed-subdatastat-ulbytedrop-qci70
collapsed-subdatastat-dlpktdrop-qci65
collapsed-subdatastat-dlpktdrop-qci66
collapsed-subdatastat-dlpktdrop-qci69
collapsed-subdatastat-dlpktdrop-qci70
collapsed-subdatastat-dlbytedrop-qci65
collapsed-subdatastat-dlbytedrop-qci66
collapsed-subdatastat-dlbytedrop-qci69
collapsed-subdatastat-dlbytedrop-qci70
collapsed-subqosstat-bearact-qci65
collapsed-subqosstat-bearact-qci66
collapsed-subqosstat-bearact-qci69
collapsed-subqosstat-bearact-qci70
collapsed-subqosstat-bearset-qci65
collapsed-subqosstat-bearset-qci66
collapsed-subqosstat-bearset-qci69
collapsed-subqosstat-bearset-qci70
collapsed-subqosstat-bearrel-qci65
collapsed-subqosstat-bearrel-qci66
collapsed-subqosstat-bearrel-qci69
collapsed-subqosstat-bearrel-qci70
saegw-ggsn-subqosstat-bearact-qci65
saegw-ggsn-subqosstat-bearact-qci66
saegw-ggsn-subqosstat-bearact-qci69
saegw-ggsn-subqosstat-bearact-qci70
saegw-ggsn-subqosstat-bearset-qci65
saegw-ggsn-subqosstat-bearset-qci66
saegw-ggsn-subqosstat-bearset-qci69
saegw-ggsn-subqosstat-bearset-qci70
saegw-ggsn-subqosstat-bearrel-qci65
saegw-ggsn-subqosstat-bearrel-qci66
saegw-ggsn-subqosstat-bearrel-qci69
saegw-ggsn-subqosstat-bearrel-qci70
saegw-ggsn-subdatastat-ulpktfwd-qci65
saegw-ggsn-subdatastat-ulpktfwd-qci66
saegw-ggsn-subdatastat-ulpktfwd-qci69
saegw-ggsn-subdatastat-ulpktfwd-qci70
saegw-ggsn-subdatastat-ulbytefwd-qci65
saegw-ggsn-subdatastat-ulbytefwd-qci66
saegw-ggsn-subdatastat-ulbytefwd-qci69
saegw-ggsn-subdatastat-ulbytefwd-qci70
saegw-ggsn-subdatastat-dlpktfwd-qci65
saegw-ggsn-subdatastat-dlpktfwd-qci66
saegw-ggsn-subdatastat-dlpktfwd-qci69
saegw-ggsn-subdatastat-dlpktfwd-qci70
saegw-ggsn-subdatastat-dlbytefwd-qci65
saegw-ggsn-subdatastat-dlbytefwd-qci66
saegw-ggsn-subdatastat-dlbytefwd-qci69
saegw-ggsn-subdatastat-dlbytefwd-qci70
saegw-ggsn-subdatastat-ulpktdrop-qci65
saegw-ggsn-subdatastat-ulpktdrop-qci66
saegw-ggsn-subdatastat-ulpktdrop-qci69
saegw-ggsn-subdatastat-ulpktdrop-qci70
saegw-ggsn-subdatastat-ulbytedrop-qci65
```

```
saegw-ggsn-subdatastat-ulbytedrop-qci66
saegw-ggsn-subdatastat-ulbytedrop-qci69
saegw-ggsn-subdatastat-ulbytedrop-qci70
saegw-ggsn-subdatastat-dlpktdrop-qci65
saegw-ggsn-subdatastat-dlpktdrop-qci66
saegw-ggsn-subdatastat-dlpktdrop-qci69
saegw-ggsn-subdatastat-dlpktdrop-qci70
saegw-ggsn-subdatastat-dlbytedrop-qci65
saegw-ggsn-subdatastat-dlbytedrop-qci66
saegw-ggsn-subdatastat-dlbytedrop-qci69
saegw-ggsn-subdatastat-dlbytedrop-qci70
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci65
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci66
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci69
saegw-ggsn-subdatastat-ulpktdropmbrexc-qci70
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci65
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci66
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci69
saegw-ggsn-subdatastat-ulbytedropmbrexc-qci70
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci65
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci66
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci69
saegw-ggsn-subdatastat-dlpktdropmbrexc-qci70
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci65
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci66
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci69
saegw-ggsn-subdatastat-dlbytedropmbrexc-qci70
```

P-GW スキーマ

新しい標準QCI機能をサポートするために、S-GW スキーマに次のバルク統計が追加されました。

```
totepsbearactive-qci65
totepsbearactive-qci66
totepsbearactive-qci69
totepsbearactive-qci70
totepsbearsetup-qci65
totepsbearsetup-qci66
totepsbearsetup-qci69
totepsbearsetup-qci70
totepsbearrel-qci65
totepsbearrel-qci66
totepsbearrel-qci69
totepsbearrel-qci70
totepsbearmod-qci65
totepsbearmod-qci66
totepsbearmod-qci69
totepsbearmod-qci70
totepsbearrel-dedrsn-pgw-qci65
totepsbearrel-dedrsn-pgw-qci66
totepsbearrel-dedrsn-pgw-qci69
totepsbearrel-dedrsn-pgw-qci70
totepsbearrel-dedrsn-s1err-qci65
totepsbearrel-dedrsn-s1err-qci66
totepsbearrel-dedrsn-s1err-qci69
totepsbearrel-dedrsn-s1err-qci70
totepsbearrel-dedrsn-s5err-qci65
totepsbearrel-dedrsn-s5err-qci66
totepsbearrel-dedrsn-s5err-qci69
totepsbearrel-dedrsn-s5err-qci70
totepsbearrel-dedrsn-s4err-qci65
totepsbearrel-dedrsn-s4err-qci66
totepsbearrel-dedrsn-s4err-qci69
```

```
totepsbearrel-dedrsn-s4err-qci70
totepsbearrel-dedrsn-s12err-qci65
totepsbearrel-dedrsn-s12err-qci66
totepsbearrel-dedrsn-s12err-qci69
totepsbearrel-dedrsn-s12err-qci70
totepsbearrel-dedrsn-local-qci65
totepsbearrel-dedrsn-local-qci66
totepsbearrel-dedrsn-local-qci69
totepsbearrel-dedrsn-local-qci70
totepsbearrel-dedrsn-pdn-qci65
totepsbearrel-dedrsn-pdn-qci66
totepsbearrel-dedrsn-pdn-qci69
totepsbearrel-dedrsn-pdn-qci70
totepsbearrel-dedrsn-pathfail-s1-u-qci65
totepsbearrel-dedrsn-pathfail-s1-u-qci66
totepsbearrel-dedrsn-pathfail-s1-u-qci69
totepsbearrel-dedrsn-pathfail-s1-u-qci70
totepsbearrel-dedrsn-pathfail-s5-u-qci65
totepsbearrel-dedrsn-pathfail-s5-u-qci66
totepsbearrel-dedrsn-pathfail-s5-u-qci69
totepsbearrel-dedrsn-pathfail-s5-u-qci70
totepsbearrel-dedrsn-pathfail-s5-qci65
totepsbearrel-dedrsn-pathfail-s5-qci66
totepsbearrel-dedrsn-pathfail-s5-qci69
totepsbearrel-dedrsn-pathfail-s5-qci70
totepsbearrel-dedrsn-pathfail-s11-qci65
totepsbearrel-dedrsn-pathfail-s11-qci66
totepsbearrel-dedrsn-pathfail-s11-qci69
totepsbearrel-dedrsn-pathfail-s11-qci70
totepsbearrel-dedrsn-pathfail-s12-qci65
totepsbearrel-dedrsn-pathfail-s12-qci66
totepsbearrel-dedrsn-pathfail-s12-qci69
totepsbearrel-dedrsn-pathfail-s12-qci70
totepsbearrel-dedrsn-pathfail-s4-u-qci65
totepsbearrel-dedrsn-pathfail-s4-u-qci66
totepsbearrel-dedrsn-pathfail-s4-u-qci69
totepsbearrel-dedrsn-pathfail-s4-u-qci70
totepsbearrel-dedrsn-inactivity-timeout-qci65
totepsbearrel-dedrsn-inactivity-timeout-qci66
totepsbearrel-dedrsn-inactivity-timeout-qci69
totepsbearrel-dedrsn-inactivity-timeout-qci70
totepsbearrel-dedrsn-other-qci65
totepsbearrel-dedrsn-other-qci66
totepsbearrel-dedrsn-other-qci69
totepsbearrel-dedrsn-other-qci70
datastat-uplink-qci65totbyte
datastat-uplink-qci65totpkt
datastat-uplink-qci66totbyte
datastat-uplink-qci66totpkt
datastat-uplink-qci69totbyte
datastat-uplink-qci69totpkt
datastat-uplink-qci70totbyte
datastat-uplink-qci70totpkt
datastat-uplink-dropstat-qci65totbyte
datastat-uplink-dropstat-qci65totpkt
datastat-uplink-dropstat-qci66totbyte
datastat-uplink-dropstat-qci66totpkt
datastat-uplink-dropstat-qci69totbyte
datastat-uplink-dropstat-qci69totpkt
datastat-uplink-dropstat-qci70totbyte
datastat-uplink-dropstat-qci70totpkt
datastat-downlink-qci65totbyte
datastat-downlink-qci65totpkt
datastat-downlink-qci66totbyte
```

```
datastat-downlink-qci66totpkt
datastat-downlink-qci69totbyte
datastat-downlink-qci69totpkt
datastat-downlink-qci70totbyte
datastat-downlink-qci70totpkt
datastat-downlink-dropstat-qci65totbyte
datastat-downlink-dropstat-qci65totpkt
datastat-downlink-dropstat-qci66totbyte
datastat-downlink-dropstat-qci66totpkt
datastat-downlink-dropstat-qci69totbyte
datastat-downlink-dropstat-qci69totpkt
datastat-downlink-dropstat-qci70totbyte
datastat-downlink-dropstat-qci70totpkt
s1u-uplnk-qci65totbyte
s1u-uplnk-qci65totpkt
s1u-uplnk-qci66totbyte
s1u-uplnk-qci66totpkt
s1u-uplnk-qci69totbyte
s1u-uplnk-qci69totpkt
s1u-uplnk-qci70totbyte
s1u-uplnk-qci70totpkt
s1u-uplnk-drop-qci65totbyte
s1u-uplnk-drop-qci65totpkt
s1u-uplnk-drop-qci66totbyte
s1u-uplnk-drop-qci66totpkt
s1u-uplnk-drop-qci69totbyte
s1u-uplnk-drop-qci69totpkt
s1u-uplnk-drop-qci70totbyte
s1u-uplnk-drop-qci70totpkt
s1u-downlnk-qci65totbyte
s1u-downlnk-qci65totpkt
s1u-downlnk-qci66totbyte
s1u-downlnk-qci66totpkt
s1u-downlnk-qci69totbyte
s1u-downlnk-qci69totpkt
s1u-downlnk-qci70totbyte
s1u-downlnk-qci70totpkt
s1u-downlnk-drop-qci65totbyte
s1u-downlnk-drop-qci65totpkt
s1u-downlnk-drop-qci66totbyte
s1u-downlnk-drop-qci66totpkt
s1u-downlnk-drop-qci69totbyte
s1u-downlnk-drop-qci69totpkt
s1u-downlnk-drop-qci70totbyte
s1u-downlnk-drop-qci70totpkt
s4u-uplnk-qci65totbyte
s4u-uplnk-qci65totpkt
s4u-uplnk-qci66totbyte
s4u-uplnk-qci66totpkt
s4u-uplnk-qci69totbyte
s4u-uplnk-qci69totpkt
s4u-uplnk-qci70totbyte
s4u-uplnk-qci70totpkt
s4u-uplnk-drop-qci65totbyte
s4u-uplnk-drop-qci65totpkt
s4u-uplnk-drop-qci66totbyte
s4u-uplnk-drop-qci66totpkt
s4u-uplnk-drop-qci69totbyte
s4u-uplnk-drop-qci69totpkt
s4u-uplnk-drop-qci70totbyte
s4u-uplnk-drop-qci70totpkt
s4u-downlnk-qci65totbyte
s4u-downlnk-qci65totpkt
s4u-downlnk-qci66totbyte
```

```
s4u-downlnk-qci66totpkt
s4u-downlnk-qci69totbyte
s4u-downlnk-qci69totpkt
s4u-downlnk-qci70totbyte
s4u-downlnk-qci70totpkt
s4u-downlnk-drop-qci65totbyte
s4u-downlnk-drop-qci65totpkt
s4u-downlnk-drop-qci66totbyte
s4u-downlnk-drop-qci66totpkt
s4u-downlnk-drop-qci69totbyte
s4u-downlnk-drop-qci69totpkt
s4u-downlnk-drop-qci70totbyte
s4u-downlnk-drop-qci70totpkt
s12-uplnk-qci65totbyte
s12-uplnk-qci65totpkt
s12-uplnk-qci66totbyte
s12-uplnk-qci66totpkt
s12-uplnk-qci69totbyte
s12-uplnk-qci69totpkt
s12-uplnk-qci70totbyte
s12-uplnk-qci70totpkt
s12-uplnk-drop-qci65totbyte
s12-uplnk-drop-qci65totpkt
s12-uplnk-drop-qci66totbyte
s12-uplnk-drop-qci66totpkt
s12-uplnk-drop-qci69totbyte
s12-uplnk-drop-qci69totpkt
s12-uplnk-drop-qci70totbyte
s12-uplnk-drop-qci70totpkt
s12-downlnk-qci65totbyte
s12-downlnk-qci65totpkt
s12-downlnk-qci66totbyte
s12-downlnk-qci66totpkt
s12-downlnk-qci69totbyte
s12-downlnk-qci69totpkt
s12-downlnk-qci70totbyte
s12-downlnk-qci70totpkt
s12-downlnk-drop-qci65totbyte
s12-downlnk-drop-qci65totpkt
s12-downlnk-drop-qci66totbyte
s12-downlnk-drop-qci66totpkt
s12-downlnk-drop-qci69totbyte
s12-downlnk-drop-qci69totpkt
s12-downlnk-drop-qci70totbyte
s12-downlnk-drop-qci70totpkt
s5-uplnk-qci65totbyte
s5-uplnk-qci65totpkt
s5-uplnk-qci66totbyte
s5-uplnk-qci66totpkt
s5-uplnk-qci69totbyte
s5-uplnk-qci69totpkt
s5-uplnk-qci70totbyte
s5-uplnk-qci70totpkt
s5-uplnk-drop-qci65totbyte
s5-uplnk-drop-qci65totpkt
s5-uplnk-drop-qci66totbyte
s5-uplnk-drop-qci66totpkt
s5-uplnk-drop-qci69totbyte
s5-uplnk-drop-qci69totpkt
s5-uplnk-drop-qci70totbyte
s5-uplnk-drop-qci70totpkt
s5-downlnk-qci65totbyte
s5-downlnk-qci65totpkt
s5-downlnk-qci66totbyte
```

s5-downlnk-qci66totpkt
s5-downlnk-qci69totbyte
s5-downlnk-qci69totpkt
s5-downlnk-qci70totbyte
s5-downlnk-qci70totpkt
s5-downlnk-drop-qci65totbyte
s5-downlnk-drop-qci65totpkt
s5-downlnk-drop-qci66totbyte
s5-downlnk-drop-qci66totpkt
s5-downlnk-drop-qci69totbyte
s5-downlnk-drop-qci69totpkt
s5-downlnk-drop-qci70totbyte
s5-downlnk-drop-qci70totpkt
s8-uplnk-qci65totbyte
s8-uplnk-qci65totpkt
s8-uplnk-qci66totbyte
s8-uplnk-qci66totpkt
s8-uplnk-qci69totbyte
s8-uplnk-qci69totpkt
s8-uplnk-qci70totbyte
s8-uplnk-qci70totpkt
s8-uplnk-drop-qci65totbyte
s8-uplnk-drop-qci65totpkt
s8-uplnk-drop-qci66totbyte
s8-uplnk-drop-qci66totpkt
s8-uplnk-drop-qci69totbyte
s8-uplnk-drop-qci69totpkt
s8-uplnk-drop-qci70totbyte
s8-uplnk-drop-qci70totpkt
s8-downlnk-qci65totbyte
s8-downlnk-qci65totpkt
s8-downlnk-qci66totbyte
s8-downlnk-qci66totpkt
s8-downlnk-qci69totbyte
s8-downlnk-qci69totpkt
s8-downlnk-qci70totbyte
s8-downlnk-qci70totpkt
s8-downlnk-drop-qci65totbyte
s8-downlnk-drop-qci65totpkt
s8-downlnk-drop-qci66totbyte
s8-downlnk-drop-qci66totpkt
s8-downlnk-drop-qci69totbyte
s8-downlnk-drop-qci69totpkt
s8-downlnk-drop-qci70totbyte
s8-downlnk-drop-qci70totpkt
s5s8-uplnk-qci65totbyte
s5s8-uplnk-qci65totpkt
s5s8-uplnk-qci66totbyte
s5s8-uplnk-qci66totpkt
s5s8-uplnk-qci69totbyte
s5s8-uplnk-qci69totpkt
s5s8-uplnk-qci70totbyte
s5s8-uplnk-qci70totpkt
s5s8-uplnk-drop-qci65totbyte
s5s8-uplnk-drop-qci65totpkt
s5s8-uplnk-drop-qci66totbyte
s5s8-uplnk-drop-qci66totpkt
s5s8-uplnk-drop-qci69totbyte
s5s8-uplnk-drop-qci69totpkt
s5s8-uplnk-drop-qci70totbyte
s5s8-uplnk-drop-qci70totpkt
s5s8-downlnk-qci65totbyte
s5s8-downlnk-qci65totpkt
s5s8-downlnk-qci66totbyte

```
s5s8-downlnk-qci66totpkt
s5s8-downlnk-qci69totbyte
s5s8-downlnk-qci69totpkt
s5s8-downlnk-qci70totbyte
s5s8-downlnk-qci70totpkt
s5s8-downlnk-drop-qci65totbyte
s5s8-downlnk-drop-qci65totpkt
s5s8-downlnk-drop-qci66totbyte
s5s8-downlnk-drop-qci66totpkt
s5s8-downlnk-drop-qci69totbyte
s5s8-downlnk-drop-qci69totpkt
s5s8-downlnk-drop-qci70totbyte
s5s8-downlnk-drop-qci70totpkt
```

システムスキーマ

新しい標準QCI機能をサポートするために、システムスキーマに次のバルク統計が追加されました。

```
sess-bearerdur-5sec-qci65
sess-bearerdur-10sec-qci65
sess-bearerdur-30sec-qci65
sess-bearerdur-1min-qci65
sess-bearerdur-2min-qci65
sess-bearerdur-5min-qci65
sess-bearerdur-15min-qci65
sess-bearerdur-30min-qci65
sess-bearerdur-1hr-qci65
sess-bearerdur-4hr-qci65
sess-bearerdur-12hr-qci65
sess-bearerdur-24hr-qci65
sess-bearerdur-over24hr-qci65
sess-bearerdur-2day-qci65
sess-bearerdur-4day-qci65
sess-bearerdur-5day-qci65
sess-bearerdur-5sec-qci66
sess-bearerdur-10sec-qci66
sess-bearerdur-30sec-qci66
sess-bearerdur-1min-qci66
sess-bearerdur-2min-qci66
sess-bearerdur-5min-qci66
sess-bearerdur-15min-qci66
sess-bearerdur-30min-qci66
sess-bearerdur-1hr-qci66
sess-bearerdur-4hr-qci66
sess-bearerdur-12hr-qci66
sess-bearerdur-24hr-qci66
sess-bearerdur-over24hr-qci66
sess-bearerdur-2day-qci66
sess-bearerdur-4day-qci66
sess-bearerdur-5day-qci66
sess-bearerdur-5sec-qci69
sess-bearerdur-10sec-qci69
sess-bearerdur-30sec-qci69
sess-bearerdur-1min-qci69
sess-bearerdur-2min-qci69
sess-bearerdur-5min-qci69
sess-bearerdur-15min-qci69
sess-bearerdur-30min-qci69
sess-bearerdur-1hr-qci69
sess-bearerdur-4hr-qci69
sess-bearerdur-12hr-qci69
sess-bearerdur-24hr-qci69
sess-bearerdur-over24hr-qci69
```

```
sess-bearerdur-2day-qci69
sess-bearerdur-4day-qci69
sess-bearerdur-5day-qci69
sess-bearerdur-5sec-qci70
sess-bearerdur-10sec-qci70
sess-bearerdur-30sec-qci70
sess-bearerdur-1min-qci70
sess-bearerdur-2min-qci70
sess-bearerdur-5min-qci70
sess-bearerdur-15min-qci70
sess-bearerdur-30min-qci70
sess-bearerdur-1hr-qci70
sess-bearerdur-4hr-qci70
sess-bearerdur-12hr-qci70
sess-bearerdur-24hr-qci70
sess-bearerdur-over24hr-qci70
sess-bearerdur-2day-qci70
sess-bearerdur-4day-qci70
sess-bearerdur-5day-qci70
```

コマンドの表示

ここでは、新しい標準 QCI 機能をモニターするために使用できる show コマンドについて説明します。

show apn statistics all

このコマンドの出力が拡張され、新しい標準 QCI 65、66、69、および 70 の管理上の接続解除とベアラー統計が表示されるようになりました。新しい統計情報はイタリック体で強調表示されます。

```
...
4G Bearers Released By Reasons:

                     QCI1   QCI2   QCI3   QCI4   QCI5   QCI6   QCI7   QCI8   QCI9
   Admin disconnect:  0          0          0      0      0      0      0      0

                       QCI65      QCI66      QCI69      QCI70
   Admin disconnect:         0          0          0          0
...

  QCI 65:
    Bearer Active:                  0   Bearer setup:                                0
    Bearer Released:                0   Bearer Rejected:                             0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:                    0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:                     0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                      0
    Uplink pkts dropped:            0   Downlink pkts dropped:                       0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):            0
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):             0

  QCI 66:
    Bearer Active:                  0   Bearer setup:                                0
    Bearer Released:                0   Bearer Rejected:                             0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:                    0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:                     0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                      0
    Uplink pkts dropped:            0   Downlink pkts dropped:                       0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):            0
```

```
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):              0

  QCI 69:
    Bearer Active:                  0   Bearer setup:                               0
    Bearer Released:                0   Bearer Rejected:                            0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:                   0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:                    0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                     0
    Uplink pkts dropped:            0   Downlink pkts dropped:                      0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):           0
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):            0

  QCI 70:
    Bearer Active:                  0   Bearer setup:                               0
    Bearer Released:                0   Bearer Rejected:                            0

    Uplink Bytes forwarded:         0   Downlink Bytes forwarded:                   0
    Uplink pkts forwarded:          0   Downlink pkts forwarded:                    0
    Uplink Bytes dropped:           0   Downlink Bytes dropped:                     0
    Uplink pkts dropped:            0   Downlink pkts dropped:                      0
    Uplink Bytes dropped(MBR Excd): 0   Downlink Bytes dropped(MBR Excd):           0
    Uplink pkts dropped(MBR Excd):  0   Downlink pkts dropped(MBR Excd):         0
                          0
...
```

show gtpu statistics

このコマンドの出力が拡張され、QCI 値 65、66、69、70 のパケットおよびバイト情報が提供されるようになりました。新しい統計情報はイタリック体で示しています。

```
...
    QCI 9:
         Uplink Packets:              0  Uplink Bytes:               0
         Downlink Packets:            0  Downlink Bytes:             0
         Packets Discarded:           0  Bytes Discarded:            0

    QCI 65:
         Uplink Packets:              0  Uplink Bytes:               0
         Downlink Packets:            0  Downlink Bytes:             0
         Packets Discarded:           0  Bytes Discarded:            0

    QCI 66:
         Uplink Packets:              0  Uplink Bytes:               0
         Downlink Packets:            0  Downlink Bytes:             0
         Packets Discarded:           0  Bytes Discarded:            0


    QCI 69:
         Uplink Packets:              0  Uplink Bytes:               0
         Downlink Packets:            0  Downlink Bytes:             0
         Packets Discarded:           0  Bytes Discarded:            0

    QCI 70:
         Uplink Packets:              0  Uplink Bytes:               0
         Downlink Packets:            0  Downlink Bytes:             0
         Packets Discarded:           0  Bytes Discarded:            0

    Non-Std QCI(Non-GBR):
         Uplink Packets:              0  Uplink Bytes:               0
         Downlink Packets:            0  Downlink Bytes:             0
         Packets Discarded:           0  Bytes Discarded:            0
...
```

show pgw-service statistics all verbose

このコマンドの出力が拡張され、QoS 特性と IPv4v6 PDN データ統計による新しい標準 QCI 情報が表示されるようになりました。新しい統計情報はイタリック体で示しています。

```
Bearers By QoS characteristics:
  Active:                                  Setup:
    QCI 1:                          0        QCI 1:                          0
...
    QCI 65:                     0            QCI 65:                     0
    QCI 66:                         0        QCI 66:                         0
    QCI 69:                         0        QCI 69:                         0
    QCI 70:                         0        QCI 70:                         0
...

  Released:
    QCI 1:                          0
...
    QCI 65:                         0
    QCI 66:                         0
    QCI 69:                         0
    QCI 70:                         0
...

  IPv4v6 PDN Data Statistics:
    Uplink :                               Downlink :
...
      Packets:                                 Packets:
        QCI 1:                      0            QCI 1:                          0
...
        QCI 65:                 0                QCI 65:                     0
        QCI 66:                     0            QCI 66:                         0
        QCI 69:                     0            QCI 69:                         0
        QCI 70:                     0            QCI 70:                         0
```

show saegw-service statistics all verbose

このコマンドの出力が拡張され、新しい標準 QCI に関する情報が提供されるようになりました。新しい統計情報はイタリック体で示しています。

```
...

Bearers By QoS characteristics:
  Active:                                  Setup:
    QCI  1:                         0      QCI  1:                         0
    ...
    QCI  9:                         0      QCI  9:                         0
    QCI 65:                         0      QCI 65:                         0
    QCI 66:                         0      QCI 66:                         0
    QCI 69:                         0      QCI 69:                         0
    QCI 70:                         0      QCI 70:                         0
    Non-Std QCI:                    0      Non-Std QCI:                    0
  Released:
    QCI  1:                         0
   ...
    QCI  9:                         0
    QCI 65:                         0
    QCI 66:                         0
    QCI 69:                         0
    QCI 70:                         0
    Non-Std QCI:                    0

…
```

```
      Std QCI(Non-GBR):                0      Std QCI(Non-GBR):                0
      Std QCI(GBR):                    0      Std QCI(GBR):                    0

    Uplink :                                 Downlink :
      Packets:                                 Packets:
        QCI 1:                         0       QCI 1:                         0
...
        QCI 65:                        0       QCI 65:                        0
        QCI 66:                        0       QCI 66:                        0
        QCI 69:                        0       QCI 69:                        0
        QCI 70:                        0       QCI 70:                        0
        Non-Std QCI:                   0       Non-Std QCI:                   0

      Bytes:                                   Bytes:
        QCI 1:                         0       QCI 1:                         0
...
        QCI 65:                        0       QCI 65:                        0
        QCI 66:                        0       QCI 66:                        0
        QCI 69:                        0       QCI 69:                        0
        QCI 70:                        0       QCI 70:                        0
        Non-Std QCI:                   0       Non-Std QCI:                   0

      Dropped Packets:                         Dropped Packets:
        QCI 1:                         0       QCI 1:                         0\
...
        QCI 65:                        0       QCI 65:                        0
        QCI 66:                        0       QCI 66:                        0
        QCI 69:                        0       QCI 69:                        0
        QCI 70:                        0       QCI 70:                        0
        Non-Std QCI:                   0       Non-Std QCI:                   0

      Dropped Bytes:                           Dropped Bytes:
        QCI 1:                         0       QCI 1:                         0
...
        QCI 65:                        0       QCI 65:                        0
        QCI 66:                        0       QCI 66:                        0
        QCI 69:                        0       QCI 69:                        0
        QCI 70:                        0       QCI 70:                        0
        Non-Std QCI:                   0       Non-Std QCI:                   0
Setup Guard Timer Expired:        0
```

show sgw-service statistics all verbose

このコマンドの出力が拡張され、新しい標準QCI情報が提供されるようになりました。新しい統計情報はイタリック体で強調表示されます。

```
...

Bearers By QoS characteristics:
  Active:                                  Setup:
    QCI 1:                         0       QCI 1:                         0
...
    QCI 65:                        0       QCI 65:                        0
    QCI 66:                        0       QCI 66:                        0
    QCI 69:                        0       QCI 69:                        0
    QCI 70:                        0       QCI 70:                        0
...

  Released:                                Modified:
    QCI 1:                         0       QCI 1:                         0
...
    QCI 65:                        0       QCI 65:                        0
    QCI 66:                        0       QCI 66:                        0
    QCI 69:                        0       QCI 69:                        0
```

```
    QCI 70:                             0      QCI 70:                             0
...

Dedicated Bearers Released By Reason:
  PGW Ini:                              0    PCRF Ini:                             0
    QCI 1:                              0
...
    QCI 65:                         0
    QCI 66:                             0
    QCI 69:                             0
    QCI 70:                             0
    Non-Std QCI:                        0
...
  S1 Error Ind:                         0    S5 Error Ind:                         0
    QCI 1:                              0      QCI 1:                              0
...
    QCI 65:                         0      QCI 65:                             0
    QCI 66:                             0      QCI 66:                             0
    QCI 69:                             0      QCI 69:                             0
    QCI 70:                             0      QCI 70:                             0
    Non-Std QCI:                        0      Non-Std QCI:                        0

  S4 Error Ind:                         0    S12 Error Ind:                        0
    QCI 1:                              0      QCI 1:                              0
...
    QCI 65:                         0      QCI 65:                             0
    QCI 66:                             0      QCI 66:                             0
    QCI 69:                             0      QCI 69:                             0
    QCI 70:                             0      QCI 70:                             0
    Non-Std QCI:                        0      Non-Std QCI:                        0

  Local:                                0    PDN Down:                             0
    QCI 1:                              0      QCI 1:                              0
...
    QCI 65:                         0      QCI 65:                             0
    QCI 66:                             0      QCI 66:                             0
    QCI 69:                             0      QCI 69:                             0
    QCI 70:                             0      QCI 70:                             0
    Non-Std QCI:                        0      Non-Std QCI:                        0

  Path Failure S1-U:                    0    Path Failure S5-U:                    0
    QCI 1:                              0      QCI 1:                              0
    ...
    QCI 65:                         0      QCI 65:                             0
    QCI 66:                             0      QCI 66:                             0
    QCI 69:                             0      QCI 69:                             0
    QCI 70:                             0      QCI 70:                             0
    Non-Std QCI:                        0      Non-Std QCI:                        0

  Path Failure S5:                      0    Path Failure S11:                     0
    QCI 1:                              0      QCI 1:                              0
...
    QCI 65:                         0      QCI 65:                             0
    QCI 66:                             0      QCI 66:                             0
    QCI 69:                             0      QCI 69:                             0
    QCI 70:                             0      QCI 70:                             0
    Non-Std QCI:                        0      Non-Std QCI:                        0

  Path Failure S4-U:                    0    Path Failure S12:                     0
    QCI 1:                              0      QCI 1:                              0
...
    QCI 65:                         0      QCI 65:                             0
    QCI 66:                             0      QCI 66:                             0
    QCI 69:                             0      QCI 69:                             0
```

```
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

  Inactivity Timeout:                0    Other:                             0
    QCI 1:                           0      QCI 1:                           0
...
    QCI 65:                      0      QCI 65:                          0
    QCI 66:                          0      QCI 66:                          0
    QCI 69:                          0      QCI 69:                          0
    QCI 70:                          0      QCI 70:                          0
    Non-Std QCI:                     0      Non-Std QCI:                     0

 ...
 Data Statistics Per Interface:
  S1-U Total Data Statistics:
    Uplink :                                Downlink :
...
      Packets:                                Packets:
        QCI 1:                       0          QCI 1:                       0
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                          0          QCI 66:                          0
        QCI 69:                          0          QCI 69:                          0
        QCI 70:                          0          QCI 70:                          0
        Non-Std QCI:                     0          Non-Std QCI:                     0

      Bytes:                                  Bytes:
        QCI 1:                       0          QCI 1:                       0
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                          0          QCI 66:                          0
        QCI 69:                          0          QCI 69:                          0
        QCI 70:                          0          QCI 70:                          0
        Non-Std QCI:                     0          Non-Std QCI:                     0

      Dropped Packets:                        Dropped Packets:
        QCI 1:                       0          QCI 1:                       0
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                          0          QCI 66:                          0
        QCI 69:                          0          QCI 69:                          0
        QCI 70:                          0          QCI 70:                          0
        Non-Std QCI:                     0          Non-Std QCI:                     0

      Dropped Bytes:                          Dropped Bytes:
        QCI 1:                       0          QCI 1:                       0
...
        QCI 65:                      0          QCI 65:                      0
        QCI 66:                          0          QCI 66:                          0
        QCI 69:                          0          QCI 69:                          0
        QCI 70:                          0          QCI 70:                          0
        Non-Std QCI:                     0          Non-Std QCI:                     0

  S4-U Total Data Statistics:
    Uplink :                                Downlink :
      Total Pkts:                    0      Total Pkts:                      0
      Total Bytes:                   0      Total Bytes:                     0
      Dropped Pkts:                  0      Dropped Pkts:                    0
      Dropped Bytes:                 0      Dropped Bytes:                   0

      Packets:                                Packets:
        QCI 1:                       0          QCI 1:                       0
...
        QCI 65:                      0          QCI 65:                      0
```

```
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Bytes:                                     Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0            QCI 65:                     0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Packets:                           Dropped Packets:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0            QCI 65:                     0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Bytes:                             Dropped Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0            QCI 65:                     0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

  S12 Total Data Statistics:
    Uplink :                                   Downlink :
      Total Pkts:                       0      Total Pkts:                       0
      Total Bytes:                      0      Total Bytes:                      0
      Dropped Pkts:                     0      Dropped Pkts:                     0
      Dropped Bytes:                    0      Dropped Bytes:                    0

      Packets:                                   Packets:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0            QCI 65:                     0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Bytes:                                     Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0            QCI 65:                     0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Packets:                           Dropped Packets:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0            QCI 65:                     0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
```

```
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Bytes:                           Dropped Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0            QCI 65:                     0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

  S5-U Total Data Statistics:
    Uplink :                                   Downlink :
      Total Pkts:                       0        Total Pkts:                     0
      Total Bytes:                      0        Total Bytes:                    0
      Dropped Pkts:                     0        Dropped Pkts:                   0
      Dropped Bytes:                    0        Dropped Bytes:                  0

      Packets:                                 Packets:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0            QCI 65:                     0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Bytes:                                   Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0            QCI 65:                     0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Packets:                         Dropped Packets:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0            QCI 65:                     0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

      Dropped Bytes:                           Dropped Bytes:
        QCI 1:                          0        QCI 1:                          0
...
        QCI 65:                     0            QCI 65:                     0
        QCI 66:                         0        QCI 66:                         0
        QCI 69:                         0        QCI 69:                         0
        QCI 70:                         0        QCI 70:                         0
        Non-Std QCI:                    0        Non-Std QCI:                    0

  S8-U Total Data Statistics:
    Uplink :                                   Downlink :
      Total Pkts:                       0        Total Pkts:                     0
      Total Bytes:                      0        Total Bytes:                    0
      Dropped Pkts:                     0        Dropped Pkts:                   0
      Dropped Bytes:                    0        Dropped Bytes:                  0

      Packets:                                 Packets:
        QCI 1:                          0        QCI 1:                          0
...
```

```
        QCI 65:                    0        QCI 65:                    0
        QCI 66:                    0        QCI 66:                    0
        QCI 69:                    0        QCI 69:                    0
        QCI 70:                    0        QCI 70:                    0
        Non-Std QCI:               0        Non-Std QCI:               0

      Bytes:                               Bytes:
        QCI 1:                     0        QCI 1:                     0
...
        QCI 65:                    0        QCI 65:                    0
        QCI 66:                    0        QCI 66:                    0
        QCI 69:                    0        QCI 69:                    0
        QCI 70:                    0        QCI 70:                    0
        Non-Std QCI:               0        Non-Std QCI:               0

      Dropped Packets:                     Dropped Packets:
        QCI 1:                     0        QCI 1:                     0
...
        QCI 65:                    0        QCI 65:                    0
        QCI 66:                    0        QCI 66:                    0
        QCI 69:                    0        QCI 69:                    0
        QCI 70:                    0        QCI 70:                    0
        Non-Std QCI:               0        Non-Std QCI:               0

      Dropped Bytes:                       Dropped Bytes:
        QCI 1:                     0        QCI 1:                     0
...
        QCI 65:                    0        QCI 65:                    0
        QCI 66:                    0        QCI 66:                    0
        QCI 69:                    0        QCI 69:                    0
        QCI 70:                    0        QCI 70:                    0
        Non-Std QCI:               0        Non-Std QCI:               0
```

非標準 QCI のサポート

ここでは、非標準 QCI のサポート機能について説明します。

機能説明

通常、GGSN/P-GW/SAEGW/S-GW/ePDG では、1 ～ 9 の標準ベース QCI 値のみがサポートされます。ただし、ライセンスを使用すると、非標準の QCI（128 ～ 254）を P-GW/GGSN（スタンドアロン GGSN ではない）で使用できます。

ライセンス

非標準 QCI を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

機能の仕組み

3GPP リリース 8 以降では、通信事業者固有/非標準の QCI がサポートされ、キャリアは QCI 128 ～ 254 を定義できます。QCI 値 0 および 10 ～ 255 は次のように定義されています。

- 0：予約済み
- 10 ～ 127：予約済み
- 128 ～ 254：通信事業者固有/非標準 QCI
- 255：予約済み

通信事業者固有の QCI（128 ～ 254）を使用して、ネットワーク内のエンドユーザーに提供するさまざまなサービス/アプリケーションキャリアを区別できます。

制限事項

- 非標準 QCI は、S5/S8/S2a/S2b インターフェイスでのみサポートされます。
- Gn インターフェイスはサポートされていません。

標準準拠

- 3GPP 仕様 TS 23.203：Policy and charging control architecture
- 3GPP 仕様 TS 29.212：Policy and Charging Control over Gx reference point

非標準 QCI サポートの設定

QCI-QoS マッピング コンフィギュレーション モードでの **operator-defined-qci** コマンドは、P-GW に非標準 QCI を設定して、非標準 QCI 値が UE または PCRF から受信されたときにコールを受け入れられるようにします。一意の DSCP パラメータ（アップリンクとダウンリンク）と、GBR または非 GBR も設定できます。

GGSN では非標準 QCI はサポートされていないため、**pre-rel8-qos-mapping** が、3G コールまたは GnGp ハンドオーバー時に非標準 QCI 値を pre-rel8 QoS 値にマッピングするための参照先として使用されます。

P-GW での非標準 QCI サポートの設定

次のコマンドを使用して、P-GW での非標準 QCI サポートを設定して、UE または PCRF から非標準 QCI 値を受信したときにコールを受け入れることができるようにします。

```
configure
    qci-qos-mapping  name
        operator-defined-qci  num  { gbr | non-gbr }  [ { downlink |
uplink } [ encaps-header { copy-inner | copy-outer | dscp-marking
dscp-marking-value } [ internal-qos priority priority ] | internal-qos
priority priority | user-datagram dscp-marking dscp-marking-value [
encaps-header { copy-inner | copy-outer | dscp-marking dscp-marking-value
 } [ internal-qos priority priority ] ] | pre-rel8-qos-mapping num ]
        no operator-defined-qci  num
        end
```

注：

- このコマンドは、非標準QCIをサポートするライセンスキーがインストールされている場合にのみ表示されます。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。
- **operator-defined-qci** *num*：有効にする通信事業者定義の QCI 値を指定します。

  num は 128 ～ 254 の整数である必要があります。

  標準ベースの QCI 値 1 ～ 9 は、**qci** コマンドを使用して設定されます。
- **pre-rel8-qos-mapping** *num*：3G コールまたは GnGp ハンドオーバー時に、非標準 QCI を、望ましい pre-rel8 標準 QoS 値と同様な特性（TC、THP、SI、TD、SSD）を持つ標準 QCI にマップします。

  num は、GBR の場合は 1 ～ 4、非 GBR の場合は 5 ～ 9 の整数である必要があります。QCI 値 1 ～ 9 は、*3GPP Specification TS 23.203*「*Policy and charging control architecture*」で定義されています。

  3G GGSN コール

  pre-rel8-qos-mapping フィールドが GGSN に関連付けられた P-GW の非標準 QCI に設定されていない場合、3G コールは拒否されます。

  GnGp のハンドオフ

  1. **pre-rel8-qos-mapping** フィールドがデフォルトベアラーの非標準 QCI に設定されていない場合、ハンドオフは拒否されます。
  2. **pre-rel8-qos-mapping** フィールドが専用ベアラーの非標準 QCI に設定されていない場合、そのベアラーだけがハンドオフ時に拒否されます。
  3. それぞれ、次のシナリオの通りです。
     - 標準QCIまたは非標準QCIを使用するデフォルトベアラー（**pre-rel8-qos-mapping** が設定済み）
     - 複数の専用ベアラー（一部が標準QCIを使用し、他の一部が **pre-rel8-qos-mapping** を設定済みの非標準 QCI を使用し、さらに他の一部がマッピングなしの非標準 QCI を使用する）

     LTE から GnGp へのハンドオフ時：

     - マッピングのない非標準 QCI を使用するすべての専用ベアラーの UPC 要求は拒否されます
     - 残りのベアラーのハンドオフは成功します

非標準 QCI サポートのモニタリング

バルク統計

このセクションでは、非標準QCIサポートのサポートにおけるバルク統計に関する情報を提供します。

APN スキーマ

非標準 QCI（GBR および非 GBR）をサポートするために、次のカウンタが追加されました。

- nonstdqci-nongbr-uplinkpkt-drop-mbrexcd
- nonstdqci-nongbr-dwlinkpkt-drop-mbrexcd
- nonstdqci-nongbr-uplinkbyte-drop-mbrexcd
- nonstdqci-nongbr-dwlinkbyte-drop-mbrexcd
- nonstdqci-nongbr-rejbearer
- nonstdqci-gbr-uplinkpkt-drop-mbrexcd
- nonstdqci-gbr-dwlinkpkt-drop-mbrexcd
- nonstdqci-gbr-uplinkbyte-drop-mbrexcd
- nonstdqci-gbr-dwlinkbyte-drop-mbrexcd
- nonstdqci-gbr-rejbearer

show コマンドの出力

このセクションでは、非標準 QCI のサポートでの show コマンドやその出力について説明します。

show apn statistics

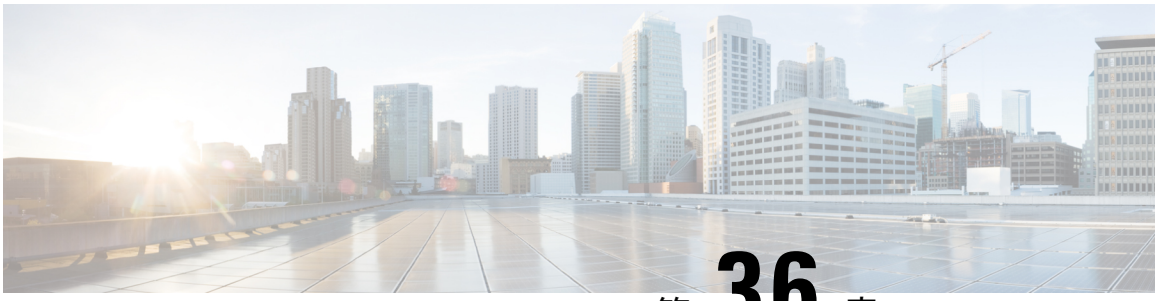
このコマンドの出力が拡張され、次の非標準 QCI カウンタ（GBR および非 GBR）が表示されるようになりました。

- 非標準 QCI（GBR 以外）
  - Bearer Rejected
  - Uplink Bytes dropped(MBR Excd)
  - Downlink Bytes dropped(MBR Excd)
  - Uplink pkts dropped(MBR Excd)
  - Downlink pkts dropped(MBR Excd)
- 非標準 QCI（GBR）
  - Bearer Rejected
  - Uplink Bytes dropped(MBR Excd)
  - Downlink Bytes dropped(MBR Excd)
  - Uplink pkts dropped(MBR Excd)
  - Downlink pkts dropped(MBR Excd)

show qci-qos-mapping table all

このコマンドの出力が拡張され、いつ非標準QCIが設定されたかが表示されるようになりました。

- Operator-defined-qci
- pre-rel8-qos-mapping



第 36 章

Gx インターフェイスでの 4G ネットワークのアップグレード

- 機能の概要と変更履歴 （631 ページ）
- 機能説明 （632 ページ）
- DRMP プライオリティ値の設定 （632 ページ）
- **発信タイムスタンプと最大待機時間** （633 ページ）
- モニタリングおよびトラブルシューティング （634 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• GGSN • P-GW • SAEGW
該当プラットフォーム	すべて（All）
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.23

機能説明

Diameter Overload Indication Conveyance（DOIC）仕様は、P-GW サーバーへのメッセージの転送中に過負荷情報を渡します。過負荷が発生した場合、スロットリングまたは破棄する必要があるメッセージを選択する特定の方法はありません。これにより、ネットワークで過剰なトラフィックが発生する可能性があります。ネットワーク内のトラフィックを削減するために、Diameter Routing Message Priority（DRMP）が新たに導入されました。DRMP を使用して、どのメッセージをスロットリングまたは廃棄するかに基づいて、メッセージの優先度を設定できます。

DRMP メッセージは、CCR メッセージおよび Gx インターフェイスの RAA でのみで送信できます。AVP で送信する値は、次のメッセージの設定コマンドを使用して設定できます。

メッセージ	説明
CCR -Initial	接続の作成中に送信される CCR メッセージ。
CCR- Update	CCR 更新中に送信される CCR メッセージ。
CCR-Termination	接続の削除中に送信される CCR メッセージ。
RAA	PCRF からの再承認要求への応答として送信される再承認応答メッセージ。

（注） DRMP機能が設定されていない場合、CCR/RAA メッセージに優先度は設定されません。DRMP が優先度（0 ～ 15）なしで設定されると、デフォルトの優先順位 10 が設定されます。

DRMP プライオリティ値の設定

DRMP のプライオリティ値を設定するには、次のコンフィギュレーション コマンドを使用します。

```
configure
    context context_name
      ims-auth-service ims_auth_service_name
        policy-control
          [ no ]diameter{ drmp [ ccr-i drmp_value| ccr-t drmp_value| ccr-u
```

```
drmp_value |rra  drmp_value]}
  end
```

（注） DRMP機能が設定されていない場合、CCR/RAAメッセージに優先度は設定されません。DRMPが優先度（0 ～ 15）なしで設定されると、デフォルトの優先順位 10 が設定されます。

発信タイムスタンプと最大待機時間

Origination-Time-Stamp

Origination-Time-Stamp（1536）は、P-GW から発信される CCR-I メッセージに追加される標準 AVP です。この AVP は、要求メッセージが P-GW から PCRF サーバーに送信される時刻（NTP 同期）を示します。Origination-Time-Stamp（1536）は、発信元エンティティが要求を開始し、64 ビット NTP タイムスタンプ形式でエンコードされる UTC 時刻を示します。ここでは、整数部分のバイナリエンコーディングは最初の 32 ビットで表され、小数部分のエンコーディングは、最後の 32 ビットで表されます。

Maximum-Wait-time

Maximum-Wait-time は Unsigned 32 タイプのの標準 AVP（コード 1537）です。メッセージが受信され、処理に時間がかかる場合、メッセージは PCRF によってドロップされるため、PCRF によって CCA-I が送信されません。この AVP は、Origination-Time-Stamp AVP とともに使用されます。Max-Wait-time（7103）は、Diameter Gx への CCR-I メッセージで使用される非標準 AVP であり、Maximum-Wait-Time（1537）標準 AVP と共に使用されます。

表 *57 :* 既存の *AVP*

AVP 名	AVP ID
Origination-Timestamp	7102
Max-Wait-Time	7103

表 *58 :* 新しい *AVP*

AVP 名	AVP ID
Origination-Time-Stamp	1536
Maximum-Wait-Time	1537

（注） このリリースでは、新しい AVP と既存の AVP の両方がサポートされています。

モニタリングおよびトラブルシューティング

ここでは、show コマンドとバルク統計について説明します。

show コマンドと出力

show ims-authorization service name <service_name>

このコマンドの出力に、以下の新しいフィールドが追加されました。

- Diameter Policy Control
  - DRMP：CCR-I CCR-U CCR-T RAA

show ims-authorization policy-control statistics

このコマンドの出力に、以下の新しいフィールドが追加されました。

- DPCA Experimental Result Code Stats
  - Late Overlapping Request
  - Time Out Request

show session disconnect-reasons

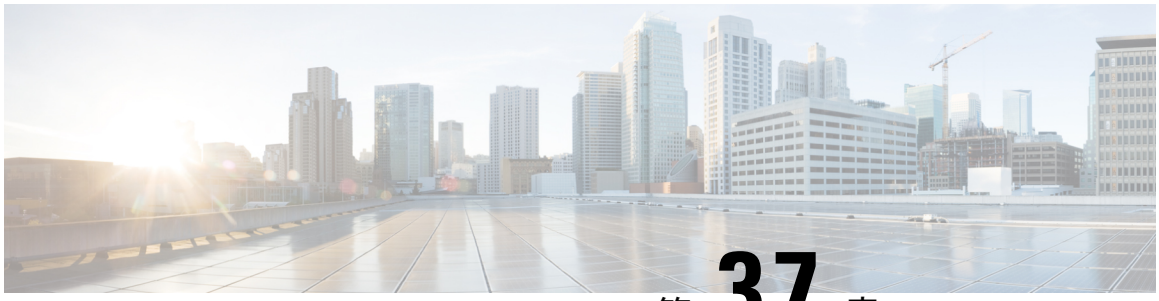
このコマンドの出力に、以下の新しいフィールドが追加されました。

- Disconnect Reason
  - newer-session-detected
  - late-overlapping-request

バルク統計

次のバルク統計が新たに追加されました。

バルク統計	説明
dpca-imsa-exp-late-overlapping-request	CCA メッセージで Diameter の実験結果コード DIAMETER_ERROR_LATE_OVERLAPPING_REQUEST(5453) を受信した合計回数を表示します。
dpca-imsa-exp-timed-out-request	CCA メッセージで Diameter の実験結果コード DIAMETER_ERROR_TIME_OUT_REQUEST(5454) を受信した合計回数を表示します。



第 37 章

GRE プロトコルインターフェイス

この章では、GGSN や P-GW サービスノードでの Generic Routing Encapsulation（GRE）プロトコルインターフェイスのサポートについて説明します。製品アドミニストレーションガイドには、システム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、それぞれの製品のアドミニストレーション ガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

重要 GREプロトコルインターフェイスのサポートは、ライセンス供与されたシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

重要 この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンドや、キーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

- はじめに （636 ページ）
- サポートされる標準 （637 ページ）
- サポート対象のネットワークとプラットフォーム （637 ページ）
- ライセンス （637 ページ）
- GRE インターフェイス上のサービスとアプリケーション （638 ページ）
- GRE インターフェイスサポートの仕組み （638 ページ）
- GRE インターフェイスの設定 （641 ページ）
- 設定の確認 （645 ページ）

はじめに

GRE プロトコル機能は、シスコのマルチメディア コア プラットフォーム（ASR 5500 以上）にもう 1 つのプロトコルを追加し、Generic Routing Encapsulation（GRE）を使用して企業ネットワークに接続するモバイルユーザーをサポートします。

企業顧客は、GRE トンネルを使用して、1）APN に対応する AAA パケットを、GRE トンネルを介して企業 AAA サーバーに転送し、2）企業サブスクライバパケットを、GRE トンネルを介して企業ゲートウェイに転送することができます。

企業サーバーはプライベート IP アドレスを持つことができるため、異なる企業に属するアドレスが重複する可能性があります。各企業は、「VRF」と呼ばれる一意の仮想ルーティングドメイン内に存在する必要があります。同じローカルエンドとリモートエンドのセット間のトンネルを区別するために、GRE キーが区別要因として使用されます。

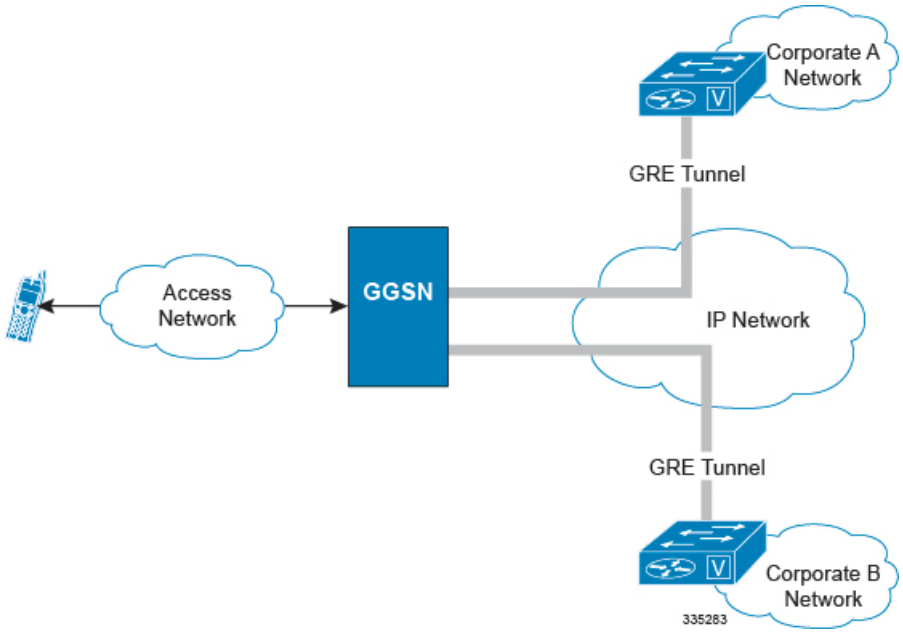
単一プロトコルバックボーン上でマルチプロトコル ローカル ネットワークを有効にし、非隣接ネットワークを接続して、WAN 間の仮想プライベートネットワークを有効にするのは一般的な手法です。このメカニズムでは、別のプロトコル内の 1 つのプロトコルからのデータパケットをカプセル化し、外部ネットワークでデータパケットを変更せずに転送します。（IPsec などのように）暗号化が含まれていないため、GRE トンネリングでは、カプセル化されたプロトコルが保護されないことに注意してください。

GRE トンネリングは、次の 3 種類の主要コンポーネントから構成されます。

- パッセンジャプロトコル：カプセル化されるプロトコル。CLNS、IPv4、IPv6 などです。
- キャリアプロトコル：カプセル化を実行するプロトコル。GRE、IP-in-IP、L2TP、MPLS、IPSec などです。
- トランスポートプロトコル：カプセル化したプロトコルを伝送するために使用するプロトコル。主なトランスポート プロトコルは IP です。

展開シナリオをごく簡潔な形式で次の図に示します。GGSN には、GRE トンネルを介して 2 つの企業ネットワークと通信する 2 つの APN があります。

図 *40 : GRE* インターフェイス展開シナリオ



サポートされる標準

このインターフェイスサポートに伴い、次の標準規格および Requests for Comments（RFC）のサポートが追加されました。

- RFC 1701：Generic Routing Encapsulation (GRE)
- RFC 1702：Generic Routing Encapsulation over IPv4 networks
- RFC 2784：Generic Routing Encapsulation (GRE)
- RFC 2890：Key and Sequence Number Extensions to GRE

サポート対象のネットワークとプラットフォーム

この機能は、コアネットワークサービスの GGSN サービスや SGSN サービスを実行している、StarOS リリース 9.0 以降のすべてのシステムをサポートしています。P-GW サービスは、StarOS リリース 12.0 以降でこの機能をサポートしています。

ライセンス

GRE プロトコルインターフェイスのサポートは、ライセンス供与されたシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シ

スコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

GRE インターフェイス上のサービスとアプリケーション

GRE インターフェイスを実装すると、GRE プロトコルのサポートとともに次の機能が提供されます。

GRE インターフェイスサポートの仕組み

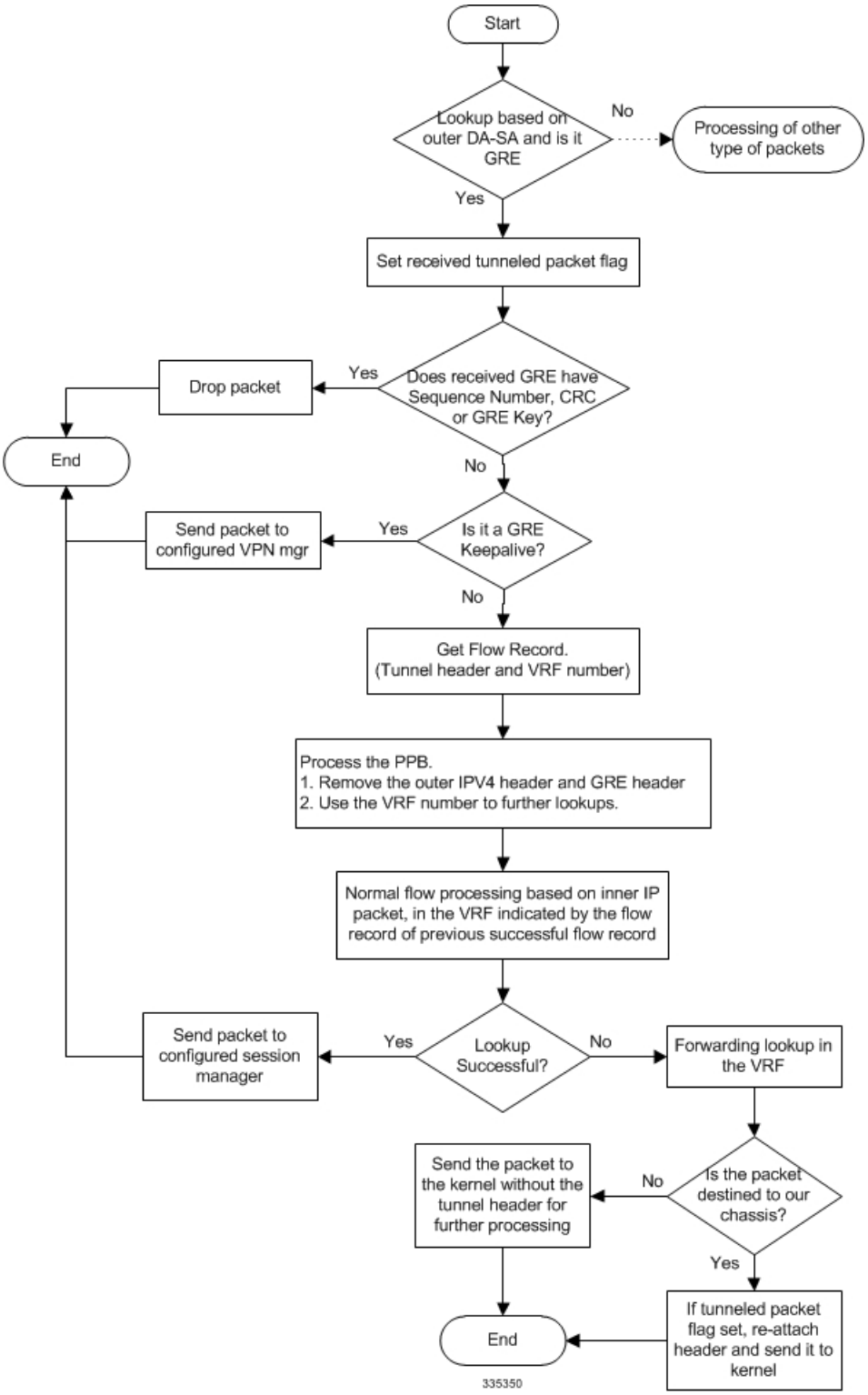
GRE インターフェイスでは、次の 2 種類のデータ処理が実行されます。1 つは入力パケットに関する処理、もう 1 つは出力パケットに関する処理です。

GRE インターフェイスでの入力パケット処理

次の図は、GRE インターフェイスでの着信パケットのプロセスのフローを示しています。

受信パケットが GRE キープアライブまたは ping パケットの場合、外側の IPV4 および GRE ヘッダーは削除されません（または再アタッチされません）が、代わりにパケットがそのまま VPN マネージャまたはカーネルにそれぞれ転送されることに注意してください。他のすべての GRE トンネルパケットの場合、新しいフロールックアップ用にパケットを送信する前に IPV4 および GRE ヘッダーが削除されます。

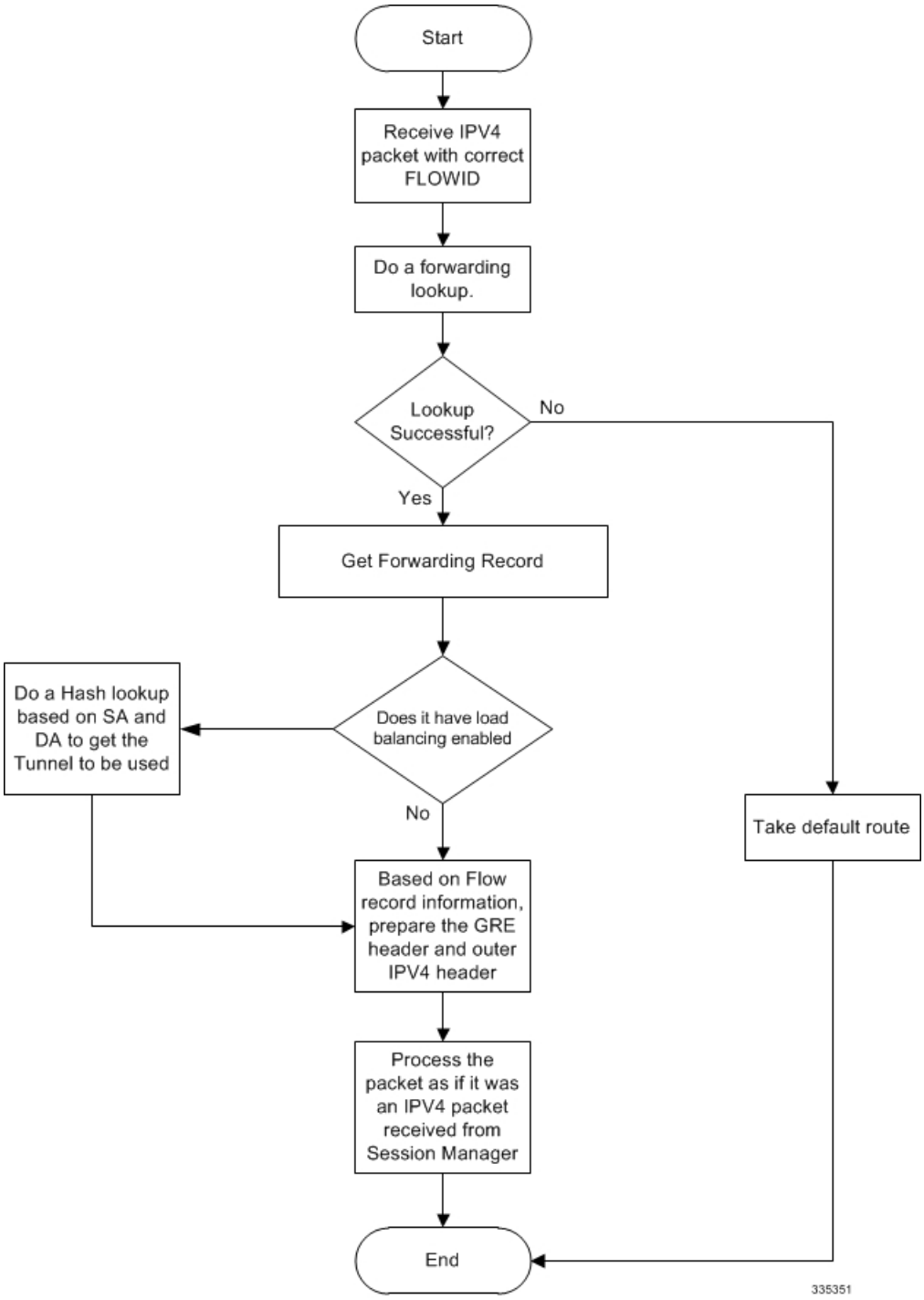
図 *41 : GRE* インターフェイスでの入力パケット処理



GRE インターフェイスでの出力パケット処理

次の図は、GRE インターフェイスでの発信パケットのプロセスのフローを示しています。

図 *42 : GRE* インターフェイスでの出力パケット処理



GRE インターフェイスの設定

ここでは、GGSN または P-GW サービスで GRE インターフェイスを使用してシステムを設定するための手順の概要と、関連する設定例について説明します。

重要 ここでは、GGSN または P-GW で GRE プロトコルインターフェイスのサポート機能を有効にするために最小限必要な手順を説明します。この機能に追加の機能を設定するコマンドについては、『*Command Line Interface Reference*』を参照してください。

以下の手順は、『システム管理ガイド』と各製品管理ガイドで説明されているシステムレベルの設定がすでに設定済みであることを前提としています。

GRE トンネルインターフェイスをサポートするようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 「Virtual Routing and Forwarding（VRF）の設定 （641 ページ）」に示されている設定例を適用して、コンテキスト内の仮想ルーティングおよび転送（VRF）を設定します。

ステップ 2 「GRE トンネルインターフェイスの設定 （642 ページ）」に示されている設定例を適用して、コンテキスト内の GRE トンネルインターフェイスを設定します。

ステップ 3 「VRF の OSPF の有効化 （643 ページ）」に示されている設定例を適用して、VRF および特定のネットワークの OSPF を有効にします。

ステップ 4 「IP プールおよび AAA グループと VRF の関連付け （643 ページ）」に示されている設定例を適用して、IP プールと AAA サーバーグループを VRF に関連付けます。

ステップ 5 「APN と VRF の関連付け （644 ページ）」に示されている設定例を適用して、AAA サーバーグループと IP プールを介して APN を VRF に関連付けます。

ステップ 6 オプションです。サーバーへのルートが OSPFv2 を介して企業から学習されない場合は、「スタティックルートの設定 （644 ページ）」に示されている設定例を適用して、スタティックルートを設定できます。

ステップ 7 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイスや、ネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

ステップ 8 設定の確認 （645 ページ） で提供されているコマンドを適用して、GRE および VRF 関連パラメータの設定を確認します。

Virtual Routing and Forwarding（VRF）の設定

ここでは、コンテキストで VRF を設定するための設定例を紹介します。

```
configure
  context <vpn_context_name> -noconfirm ]
    ip vrf <vrf_name>
      ip maximum-routes <max_routes>
      end
```

注：

- <*vpn_context_name*> は、VRF に使用するシステムコンテキストの名前です。詳細については、『*System Administration Guide*』を参照してください。
- コンテキストあたり最大 300 の VRF と、シャーシあたり最大 2,048 の VRF をシステムに設定できます。
- <*vrf_name*> は、各種インターフェイスに関連付けられる VRF の名前です。
- **ip maximum-routes** <*max_routes*> コマンドを使用して、最大 10000 のルートを設定できます。

GRE トンネルインターフェイスの設定

ここでは、GRE トンネルインターフェイスを設定し、VRF を GRE インターフェイスに関連付ける設定例を示します。

```
configure
  context <vpn_context_name>
    ip interface <intfc_name> tunnel
      ip vrf forwarding <vrf_name>
        ip address <internal_ip_address/mask>
        tunnel-mode gre
        source interface <non_tunn_intfc_to_corp>
        destination address <global_ip_address>
        keepalive interval <value> num-retry <retry>
        end
```

注：

- <*vpn_context_name*> は、GRE インターフェイス設定に使用するシステムコンテキストの名前です。詳細については、『*Command Line Interface Reference*』を参照してください。
- 最大 511 の GRE トンネル + 1 つの非トンネルインターフェイスを 1 つのコンテキストで設定できます。システムには、デフォルトとして少なくとも1つの非トンネルインターフェイスが必要です。
- <*intfc_name*> は、トンネルタイプのインターフェイスとして定義された IP インターフェイスの名前です。GRE トンネルインターフェイスに使用されます。
- <*vrf_name*> は、コンテキスト コンフィギュレーション モードで事前設定済みの VRF の名前です。
- <*internal_ip_address*/mask> は、VRF フォワーディングに使用されるサブネットマスクを含むネットワーク IP アドレスです。
- <*non_tunn_intfc_to_corp*> は、送信元インターフェイスとしてシステムに必要な、事前に設定された非トンネルインターフェイスの名前です。インターフェイスの設定の詳細については、『*System Administration Guide*』を参照してください。

- <*global_ip_address*> は、宛先アドレスとして使用されるグローバルに到達可能な IP アドレスです。

VRF の OSPF の有効化

ここでは、VRF の OSPF で GRE トンネルインターフェイスをサポートするための設定例を紹介します。

```
configure
   context <vpn_context_name>
      router ospf
         ip vrf <vrf_name>
         network <internal_ip_address/mask>
         end
```

注：

- <*vpn_context_name*> は、OSPF ルーティングに使用するシステムコンテキストの名前です。詳細については、このガイドの「ルーティング」を参照してください。
- <*vrf_name*> は、コンテキスト コンフィギュレーション モードで事前設定済みの VRF の名前です。
- <*internal_ip_address/mask*> は、OSPF ルーティングに使用される、サブネットマスクを含むネットワーク IP アドレスです。

IP プールおよび AAA グループと VRF の関連付け

ここでは、IP プールと AAA グループを VRF に関連付ける設定例を示します。

```
configure
   context <vpn_context_name>
      ip pool <ip_pool_name> <internal_ip_address/mask> vrf <vrf_name>
         exit
      aaa group <aaa_server_group>
         ip vrf <vrf_name>
         end
```

注：

- <*vpn_context_name*> は、IP プールと AAA サーバーグループに使用するシステムコンテキストの名前です。
- <*ip_pool_name*> は、事前設定済み IP プールの名前です。詳細については、『*System Administration Guide*』[英語] を参照してください。
- <*aaa_server_group*> は、事前設定済みの AAA サーバーグループの名前です。詳細については、『*AAA Interface Administration and Reference*』[英語] を参照してください。
- <*vrf_name*> は、コンテキスト コンフィギュレーション モードで事前設定済みの VRF の名前です。
- <*internal_ip_address/mask*> は、IP プールに使用されるサブネットマスクを含むネットワーク IP アドレスです。

APN と VRF の関連付け

このセクションでは、AAA グループと IP プールを介して APN を VRF に関連付ける設定例を示します。

```
configure
  context <vpn_context_name>
    apn <apn_name>
      aaa group <aaa_server_group>
      ip address pool name <ip_pool_name>
      end
```

注：

- *<vpn_context_name>* は、APN 設定に使用するシステムコンテキストの名前です。
- *<ip_pool_name>* は、事前設定済み IP プールの名前です。詳細については、『*System Administration Guide*』[英語] を参照してください。
- *<aaa_server_group>* は、事前設定済みの AAA サーバーグループの名前です。詳細については、『*AAA Interface Administration and Reference*』[英語] を参照してください。
- *<vrf_name>* は、コンテキスト コンフィギュレーション モードで事前設定済みの VRF の名前です。

スタティック ルートの設定

ここでは、サーバーへのルートが OSPFv2 を介して企業から学習されない場合にスタティックルートを設定するためのオプションの設定例を示します。

```
configure
  context <vpn_context_name>
    ip route <internal_ip_address/mask> tunnel <tunnel_intfc_name> vrf <vrf_name>

    end
```

注：

- *<vpn_context_name>* は、スタティックルート設定に使用するシステムコンテキストの名前です。
- *<internal_ip_address/mask>* は、スタティックルートとして使用される、サブネットマスクを含むネットワーク IP アドレスです。
- *<tunnel_intfc_name>* は、GRE トンネルインターフェイスに使用される定義済みのトンネルタイプ IP インターフェイスの名前です。
- *<vrf_name>* は、コンテキスト コンフィギュレーション モードで事前設定済みの VRF の名前です。

設定の確認

このセクションでは、システム アドミニストレーション ガイドの説明に従って .cfg ファイルに設定を保存した後に、それらの設定を表示して確認する方法と、サービスのアクティブな設定内のエラーおよび警告を取得する方法について説明します。

重要 ここに記載されているコマンドはすべてEXECモードで実行します。すべてのプラットフォームですべてのコマンドを使用できるわけではありません。

次の手順は、GRE インターフェイスの設定を確認するために使用されます。

手順

ステップ 1 Exec モードで次のコマンドを入力して、インターフェイスが正しく設定されていることを確認します。

show ip interface

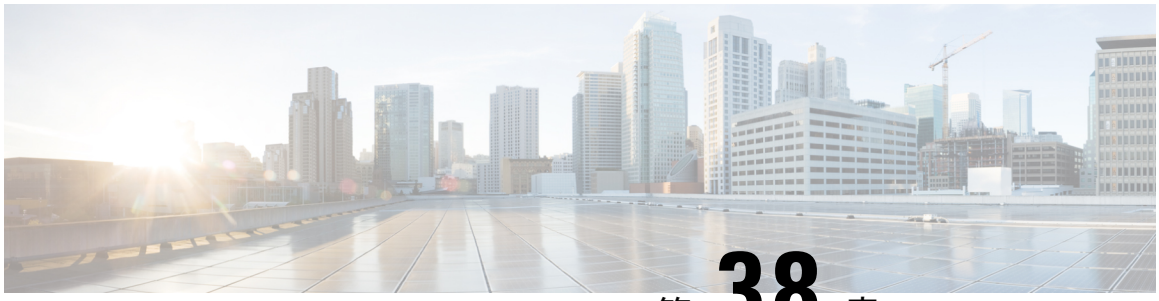
このコマンドの出力では、コンテキストに含まれるすべてのインターフェイスの設定が表示されます。

```
Intf Name:     foo1
Intf Type:             Broadcast
Description:
IP State:              UP (Bound to 17/2 untagged, ifIndex 285343745)
IP Address:            209.165.200.225         Subnet Mask:         255.255.255.0
Bcast Address:         209.165.200.254             MTU:                 1500
Resoln Type:           ARP                   ARP timeout:         60 secs
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 0
Intf Name:             foo2
Intf Type:             Tunnel (GRE)
Description:
VRF:                   vrf-tun
IP State:              UP (Bound to local address 209.165.200.225 (foo1), remote address
209.165.200.229)
IP Address:            209.165.200.228              Subnet Mask:         255.255.255.224
Intf Name:             foo3
Intf Type:             Tunnel (GRE)
Description:
IP State:              DOWN (<state explaining the reason of being down>)
IP Address:            209.165.200.232            Subnet Mask:         255.255.255.224
```

ステップ 2 Exec モードで次のコマンドを入力して、GRE キープアライブが正しく設定されていることを確認します。

show ip interface gre-keepalive

このコマンドの出力では、コンテキストで設定されているGREインターフェイスのキープアライブの設定が表示されます。



第 38 章

GGSN UPC のコリジョン処理

• GGSN UPC のコリジョン処理 （647 ページ）

GGSN UPC のコリジョン処理

機能説明

SGSN によって開始された UPC 要求と GGSN によって開始された UPC 要求の間でコリジョンが発生した場合、SGSN によって開始された UPC 要求がネットワーク運用（NRUPC）より優先されます。UPC コリジョン処理機能を使用すると、コール確立中やコール中のフェーズでコールやデータの損失は発生しません。この機能はCLI を使用して有効または無効にすることができますが、デフォルトで有効になっています。

- GGSN がプライマリ PDP コンテキスト上で、SGSN によって開始された UPC 要求と NRUPC との間のコリジョンを検出すると、UPC 応答の送信後に NRUPC が（異なるシーケンス番号で）再試行されます。
- GGSN が SGSN 間のハンドオフで、SGSN によって開始された UPC 要求と TFT による NRUPC との間のコリジョンを検出し、ハンドオフ後に BCM モードが混合モードから MS 専用モードに変更された場合、UPC 応答を TFT なしで送信後に NRUPC が（異なるシーケンス番号で）再試行されま 。
- GGSN がセカンダリ PDP コンテキストで、SGSN によって開始された UPC と NRUPC との間のコリジョンを検出した場合、NRUPC は中止され、PCRF が通知されます。GGSN で複数の CCR-U サポートが有効になっていない場合、（セカンダリ PDP コンテキストで）中止された NRUPC の CCR-U は PCRF に通知されません。この場合、PCRF はこの中止されたトランザクション（ルール失敗）を認識しません。

（注） S2bGTP から LTE へのハンドオフプロシージャ中に保留中のトランザクションがすでにあり、SAE-GW がハンドオフ要求を受信すると、次のメッセージを付けてハンドオフが拒否されます。

```
Rejecting S2b/LTE Handoff as only one pending transaction is supported
```

制限事項

- このリリースでは、この機能に対応するように GnGp GGSN の動作が変更されています。GGSN の動作に変更はありません。
- （「ダイレクトトンネルエラー通知」により）ダイレクトトンネルから受信した NRUPC が、SGSN によって開始された UPC 要求と競合すると、NRUPC は中止され、再試行されません。アクセス側から「ダイレクトトンネルエラー通知」を受信すると NRUPC が再度トリガーされるため、これは機能には影響しません。
- NRUPC 応答を受信する前に LTE へのハンドオフ要求を受信した場合、動作は変更されません。この場合、保留中の NRUPC 要求は中止されます。受信した NRUPC 要求がルールのインストールのためである場合、その要求は保留状態のままになり、ルールはインストールされません。静的ルールがなく、ルールインストール要求が保留状態であるため、PDP コンテキストは、インストールされたルールない状態で稼働したままになります。

GGSN UPC コリジョン処理の設定

オペレータは、コマンドライン インターフェイス（CLI）を使用して、SGSN によって開始された UPC 要求とネットワークによって開始された UPC 要求とのコリジョンの処理を設定できます。

gtpc handle-collision

サービス コンフィギュレーション モードでこのコマンドを使用すると、SGSN によって開始された UPC 要求とネットワークによって開始された UPC 要求とのコリジョンを処理できます。

GGSN サービス

```
configure
     context context_name
       ggsn-service service_name
          [ no | default ] gtpc handle-collision upc nrupc
          end
```

P-GW サービス

```
configure
     context context_name
```

```
pgw-service service_name
  [ no | default ] gtpc handle-collision upc nrupc
  end
```

S-GW サービス

```
configure
     context context_name
       sgw-service service_name
         [ no | default ] gtpc handle-collision upc nrupc
         end
```

SAEGW サービス

```
configure
     context context_name
       saegw-service service_name
         [ no | default ] gtpc handle-collision upc nrupc
         end
```

注：

- **no:** SGSN によって開始された UPC 要求と NRUPC 要求間のコリジョン処理を無効にします。
- **default:** SGSN によって開始された UPC 要求と NRUPC 要求間のデフォルトのコリジョン処理動作を設定します。デフォルトでは、コリジョン処理が有効になっています。
- **handle-collision upc nrupc:** SGSN によって開始された UPC とネットワークによって要求された UPC 間のコリジョン処理を有効/無効にします。デフォルトでは、コリジョン処理が有効になっています。

設定の確認

この機能の設定は、EXEC モードで次のコマンドを使用して確認できます。

- **show configuration**
- **show configuration verbose**

コマンド出力については、「GGSN UPC コリジョン処理のモニタリングとトラブルシューティング」を参照してください。

GGSN UPC コリジョン処理のモニタリングと障害対応

ここでは、GGSN UPC コリジョン処理をモニターするために使用できるコマンドについて説明します。

GGSN UPC コリジョン処理の show コマンド

show configuration

このコマンドを実行すると、次の出力が表示されます。

```
ggsn-service ggsn-service
associate gtpu-service gtpu-service
associate pgw-service pgw_service
associate peer-map map_ggsn

no gtpc handle-collision upc nrupc
```

ユーザーが [support record] セクションを指定していない場合は、show configuration verbose

このコマンドを実行すると、次の出力が表示されます。

```
ggsn-service ggsn-service
associate gtpu-service gtpu-service
associate pgw-service pgw_service
associate peer-map map_ggsn

no gtpc handle-collision upc nrupc
```

show ggsn-service name *service_name*

このコマンドを実行すると、次の出力が表示されます。

```
Service name:                      ggsn-service
Context:                           ingress
…
Suppress NRUPC triggered by UPC:   Disabled

Collision handling for UPC-NRUPC:  Enabled/Disabled
```

show gtpc statistics

このコマンドは、GGSN サービスのプライマリおよびセカンダリ PDP コンテキストで発生している、NRUPC および SGSN によって開始された UPC コリジョンの数を表示します。このコマンドを実行すると、次の出力が表示されます。

```
Active Subscribers:
  Total:                           1
  2G:                              0
  3G:                              1
…
…
MS Info Change Reporting Messages:
  MS Info Chng Notif Req:          0   Accepted:                      0
  Denied:                          0   Discarded:                     0

NRUPC UPC Collision:
  Primary PDP ctxt:                3   Secondary PDP ctxt:            0

QoS negotiation:
  CPC QoS Accepted:                3   CPC QoS Downgraded:            0
  UPC QoS Accepted:                3   UPC QoS Downgraded:            0
```

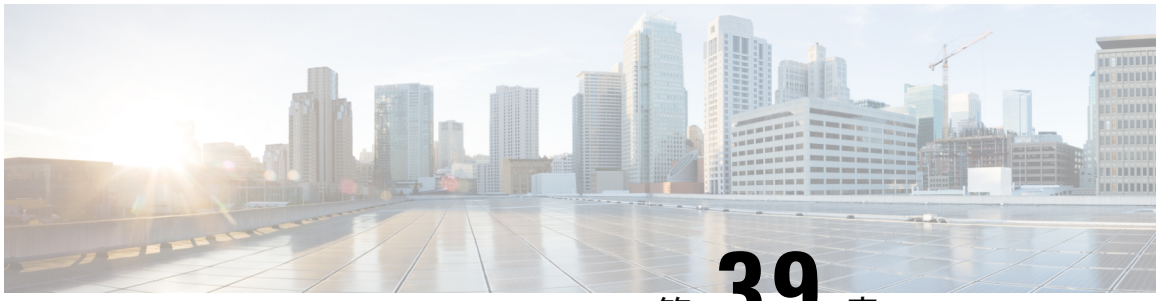
show gtpc statistics [format1 | ggsn-service *service_name* | verbose]

このコマンドは、GGSN サービスのプライマリおよびセカンダリ PDP コンテキストで発生している、NRUPC および SGSN によって開始された UPC コリジョンの数を表示します。このコマンドを実行すると、次の出力が表示されます。

```
Active Subscribers:
  Total:                          1
  2G:                             0
  3G:                             1
…
…
MS Info Change Reporting Messages:
  MS Info Chng Notif Req:         0   Accepted:                       0
  Denied:                         0   Discarded:                      0

NRUPC UPC Collision:
  Primary PDP ctxt:               3   Secondary PDP ctxt:             0

QoS negotiation:
  CPC QoS Accepted:               3   CPC QoS Downgraded:             0
  UPC QoS Accepted:               3   UPC QoS Downgraded:             0
```



第 39 章

P-GW および SAEGW での GTP ベース S2b インターフェイスのサポート

この章では、スタンドアロン P-GW および SAEGW での GTP ベース S2b インターフェイスのサポート機能について説明します。

- 機能説明 （653 ページ）
- S2b アーキテクチャの動作の仕組み （656 ページ）
- S2a アーキテクチャの動作の仕組み （682 ページ）
- P-GW および SAEGW 上の GTP ベース S2b インターフェイスの設定 （696 ページ）
- GTP ベースの S2b インターフェイス機能のモニタリング （697 ページ）
- GTP ベースの S2a インターフェイス機能のモニタリング （700 ページ）

機能説明

このセクションでは、P-GW および SAEGW での GTP ベースの S2a/S2b インターフェイスの導入について説明します。

スタンドアロン P-GW および SAEGW での GTP ベース S2b インターフェイスのサポート

重要 GTP ベース S2b インターフェイスのサポート機能は、ライセンスで制御されています。ライセンスについては、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

S2b インターフェイス参照ポイントは、スタンドアロン P-GW を ePDG に接続し、SAEGW の P-GW を ePDG に接続します。信頼できない非 3GPP ePDG（Evolved Packet Data Gateway）と P-GW の間で通信が実行されると、P-GW は PMIPv6（プロキシモバイル IP バージョン 6）を使用して EPC へのアクセスを提供します。GTPv2-C は、S2b で使用されるシグナリングプロトコルです。S2b インターフェイスは、3GPP TS 29.274 に基づいています。

S2b インターフェイスは、PMIPv6 プロトコルを使用して、P-GW との WLAN UE セッションを確立します。また、WLAN UE によって実行される P-CSCF 検出の一環として、PBU（プロキシ MIP バインディング更新）および PBA（プロキシ MIP バインディング確認応答）メッセージの P-CSCF 属性と DNS 属性の転送もサポートします。P-CSCF アドレス情報がない場合、P-CSCF 検出が S4-SGSN から LTE（およびその逆）へのハンドオフ時に開始されます。P-CSCF アドレス情報がすでに利用可能な場合は、S4-SGSN から LTE（およびその逆）へのハンドオフ時に、P-CSCF 検出を改めて明示的にトリガーする必要はありません。

例：UE は、ホームネットワークが同時接続をサポートしている場合にのみ、異なるアクセスネットワーク経由で異なる APN への同時接続を試みます。UE は、APN 単位のシステム間ルーティングポリシーでプロビジョニングされているか、このポリシーを受信済みの場合に、ネットワークが複数のアクセスでのこのような同時接続をサポートしていると判断します。したがって、UE は、複数のアクセスタイプによる個別の PDN 接続を確立できます。

サポートされるアクセスタイプは 4G と Wi-Fi です。

P-GW および SAEGW での S2b インターフェイスの実装では、次の機能をサポートしています。

- Wi-Fi アクセスを介して PDN に接続する UE
- UE の複数 PDN 接続
- 初回アタッチ
- LTE から Wi-Fi へのハンドオフ
- Wi-Fi から LTE へのハンドオフ

スタンドアロン P-GW および SAEGW での GTP ベース S2a インターフェイスのサポート

重要 GTP ベース S2a インターフェイスのサポートは、ライセンスで制御される機能です。ライセンスの詳細については、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

GTP ベース S2a インターフェイスのサポートは、P-GW および SAEGW で利用できます。SAEGW を使用して展開している通信事業者は、この機能を使用して信頼できる Wi-Fi ネットワーク機能を統合できるようになりました。

S2a インターフェイスは、SAEGW のスタンドアロン P-GW と P-GW を eHRPD の HSGW に接続します。具体的には、S2a インターフェイスは、信頼できる非 3GPP アクセスポイント（HSGW）と SAEGW のスタンドアロン P-GW または P-GW 間のシグナリングとモビリティのサポートを提供することで、ベアラーインターフェイスをサポートします。これはプロキシモバイル IP に基づいていますが、PMIP をサポートしない信頼できる非 3GPP IP アクセスポイントへの接続を可能にするクライアントモバイル IPv4 FA モードもサポートしています。

WLAN が通信事業者によって信頼されていると見なされると、信頼できる WLAN アクセスネットワーク（TWAN）が、P-GW への S2a インターフェイスを介して、信頼できる非 3GPP アク

セスとして EPC とインターフェイス接続されます。SAEGW サービスの Make と Break を使用して、Wi-Fi から LTE へのハンドオーバーのサポートが拡張されました。マルチ PDN ハンドオーバーも、この機能の一部としてサポートされています。

以下のような機能がサポートされています。

- 初回アタッチ
- Wi-Fi から LTE へのハンドオーバー
- LTE から WiFi へのハンドオーバー
- マルチ PDN ハンドオーバー

以下のようなプロトコルがサポートされています。

- トランスポート層：UDP、TCP
- トンネリング：GRE IPv6
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット

他の機能との関係

ここでは、GTP ベースの S2b および S2a インターフェイスサポート機能が他の機能とどのように関連するかについて説明します。

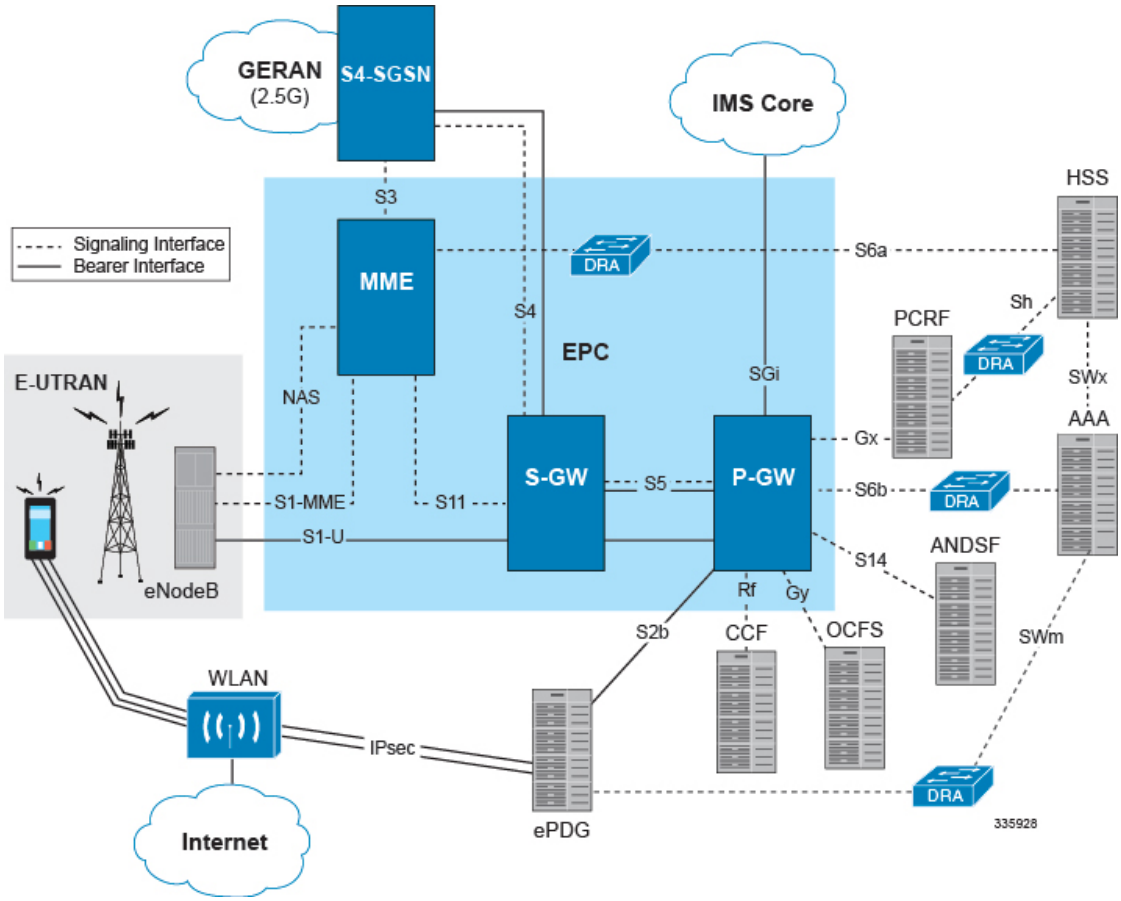
- スタンドアロン P-GW および SAEGW で GTP ベースの s2b インターフェイスサポートを設定するには、事前に P-GW サービスが設定され、動作可能になっている必要があります。
- この機能をサポートするには、ePDG で GTP ベースの S2b インターフェイスサポートも設定され、動作可能になっている必要があります。
- スタンドアロン P-GW および SAEGW で GTP ベースの s2a インターフェイスサポートを設定するには、事前に P-GW サービスが設定され、動作可能になっている必要があります。

S2b アーキテクチャの動作の仕組み

S2bインターフェイスのスタンドアロンP-GWアーキテクチャのサポート

GTP ベースの S2b インターフェイスアーキテクチャは、E-UTRAN および EPC ネットワークの P-GW 展開の一部です。P-GW は S2b インターフェイスを介して ePDG と通信し、ePDG は IPSec インターフェイスを介して WLAN オフロードアーキテクチャに接続します。

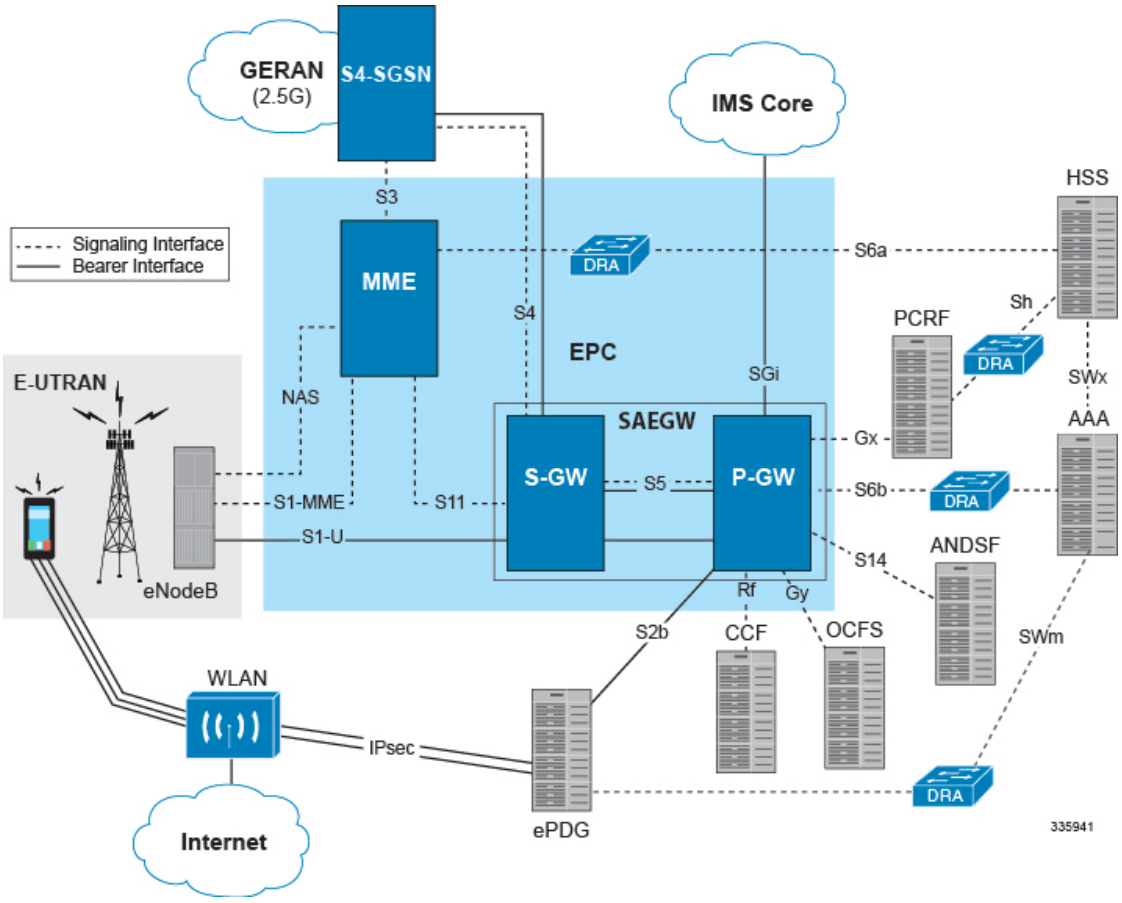
図 *43 : スタンドアロン P-GW* : *E-UTRAN* および *EPC* ネットワークでの *GTP* ベース *S2b* インターフェイスの実装



S2b インターフェイスをサポートするための SAEGW アーキテクチャ

GTP ベースの S2b インターフェイス アーキテクチャは、E-UTRAN/EPC ネットワーク内の SAEGW 展開の一部です。SAEGW の P-GW は S2b インターフェイスを介して ePDG と通信し、ePDG は IPSec インターフェイスを介して WLAN オフロードアーキテクチャに接続します。

図 *44 : SAEGW* : *E-UTRAN/EPC* ネットワーク内での *GTP* ベースの *S2b* インターフェイスの実装



P-GW および SAEGW の S2b インターフェイスサポートの制限事項

P-GW および SAEGW 上の GTP ベースの S2b インターフェイス実装では、次の制限事項に注意してください。

- Wi-Fi オフロードおよび VLC フローからの次のインターフェイス/アクセスタイプのみがサポートされます。
- アクセスタイプ：
  - Wi-Fi
  - LTE
- インターフェイス：
  - S6b
  - Gy
  - Rf
  - Gx
  - GTPv2（S2b）

- 従来の合法的傍受は、スタンドアロン P-GW の S2b インターフェイスでサポートされますが、現時点では、SAEGW の S2b インターフェイスでは認定されていません。

スタンドアロン P-GW コールフロー

ここでは、スタンドアロン P-GW での GTP ベース S2b インターフェイスサポートの基本機能を示すコールフローを提供します。

図 *45 :* 初期接続コールフロー：*P-GW*

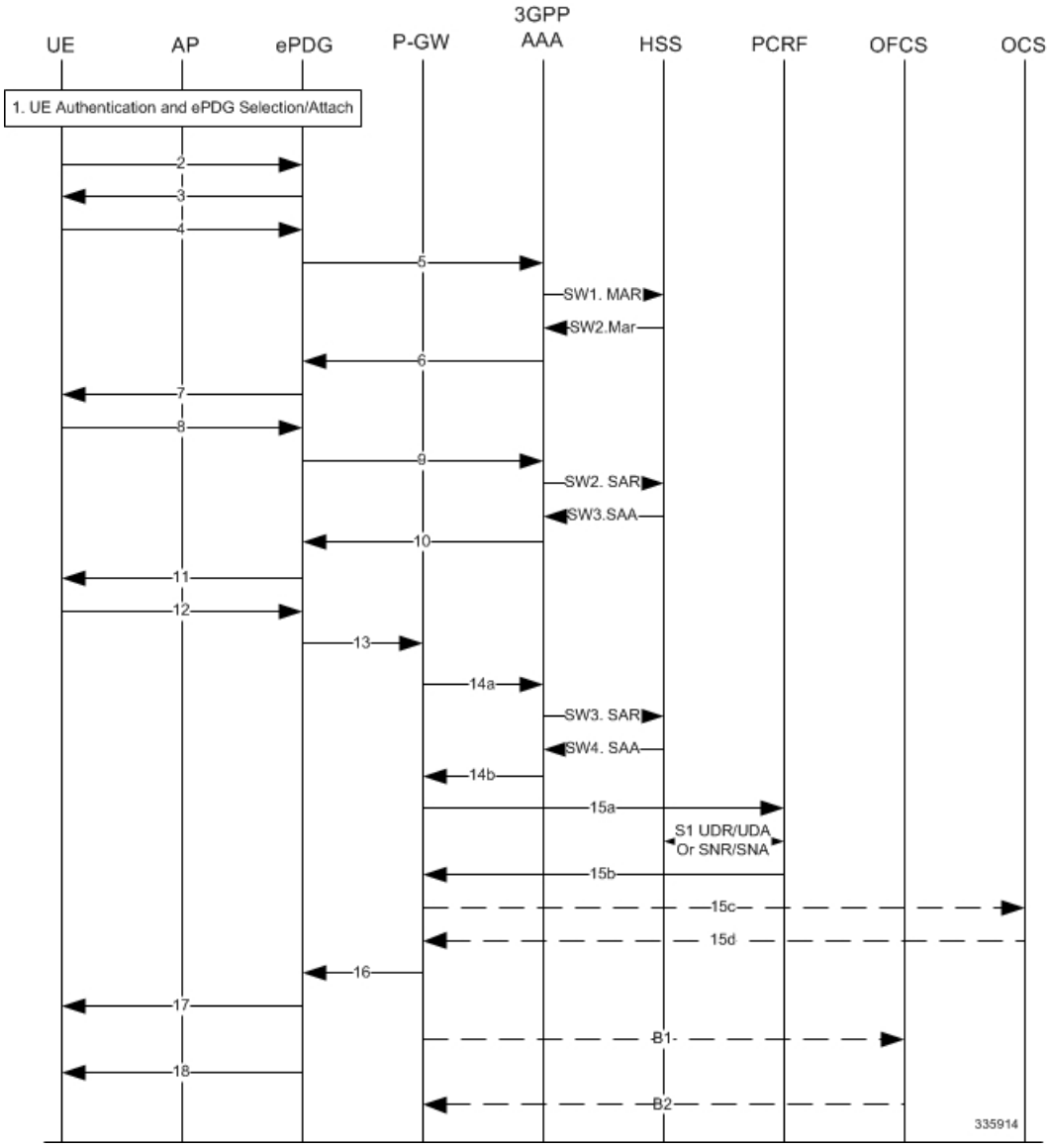


表 *59 :* 初期接続：*P-GW*

ステップ	説明
1	UUE が、必要に応じて、初期アクセスポイントの関連付けと認証を実行します。
2 ～ 11	UE が、ePDG との接続を確立します。
12	UE が、IKE_AUTH 要求（AUTH）を送信します。UE が、MSK の独自のコピーを入力として取得し、最初の IKE_SA_INIT メッセージを認証するための AUTH パラメータを生成します。
13	ePDG が、ノード選択オプションに基づいて P-GW を選択します。ePDG が、セッション作成要求を送信します。
14a	P-GW が、3GPP AAA に AAR を送信して、サブスクライバの PDN を承認し、APN の HSS 上の P-GW アドレスを更新します。
SW3	3GPP AAA が、APN の P-GW アドレスで HSS を更新し、HSS からサブスクライバ APN プロファイルを取得します。
SW4	HSS が、Server-Assignment-Answer（Session-Id、Result-Code、Experimental-Result（Vendor-Id、Experimental-Result-Code））を送信します。
14b	3GPP AAA が、AAA を送信します。
15a	P-GW が、新しい IP CAN セッションの確立を示すために、IP-CAN 確立の表示を CCR によって PCRF に送信します。
S1	PCRF が、ユーザープロファイルをダウンロード（およびキャッシュ）します（Sh: UDR（User-Identity、Service-Indication、Data-Reference）を送信し、Sh: UDA（Result-Code、User-Data）を受信することにより）。
S2	PCRF が、プロファイル更新通知を登録できます。
15b	PCRF が、CCA メッセージで IP CAN セッション確立を確認応答します。
15c	Online AVP が PCRF（UC ユーザー/CF/RTR）からの CCA に設定されている場合、P-GW が、条件に応じて CCR-Initial を送信します。
15d	OCS が、P-GW に CCA で応答します。
16	P-GW が、要求された IP アドレスセッションを割り当て、セッション作成応答メッセージで ePDG に応答します。
17	ePDG が、設定ペイロード（CFG_REPLY）で、割り当てられた IP アドレスを送信します。AUTH パラメータが、設定ペイロード、セキュリティ アソシエーション、および残りの IKEv2 パラメータとともに UE に送信され、IKEv2 ネゴシエーションが終了します。

ステップ	説明
18	ePDG が、IP スタックが完全に初期化されていることを確認するためにルータアドバタイズメントを送信します。P-GW が、UE へのルータアドバタイズメントを無効にします。
B1	Offline AVP が PCRF からの CCA に設定されている場合、IP-CAN セッション確立手順の完了後に、P-GW が、ACR-Start を OFCS に送信します。
B2	OFCS が、P-GW に ACA で応答します。

図 *46 : P-GW* : *LTE* から *Wi-Fi* へのハンドオフのコールフロー

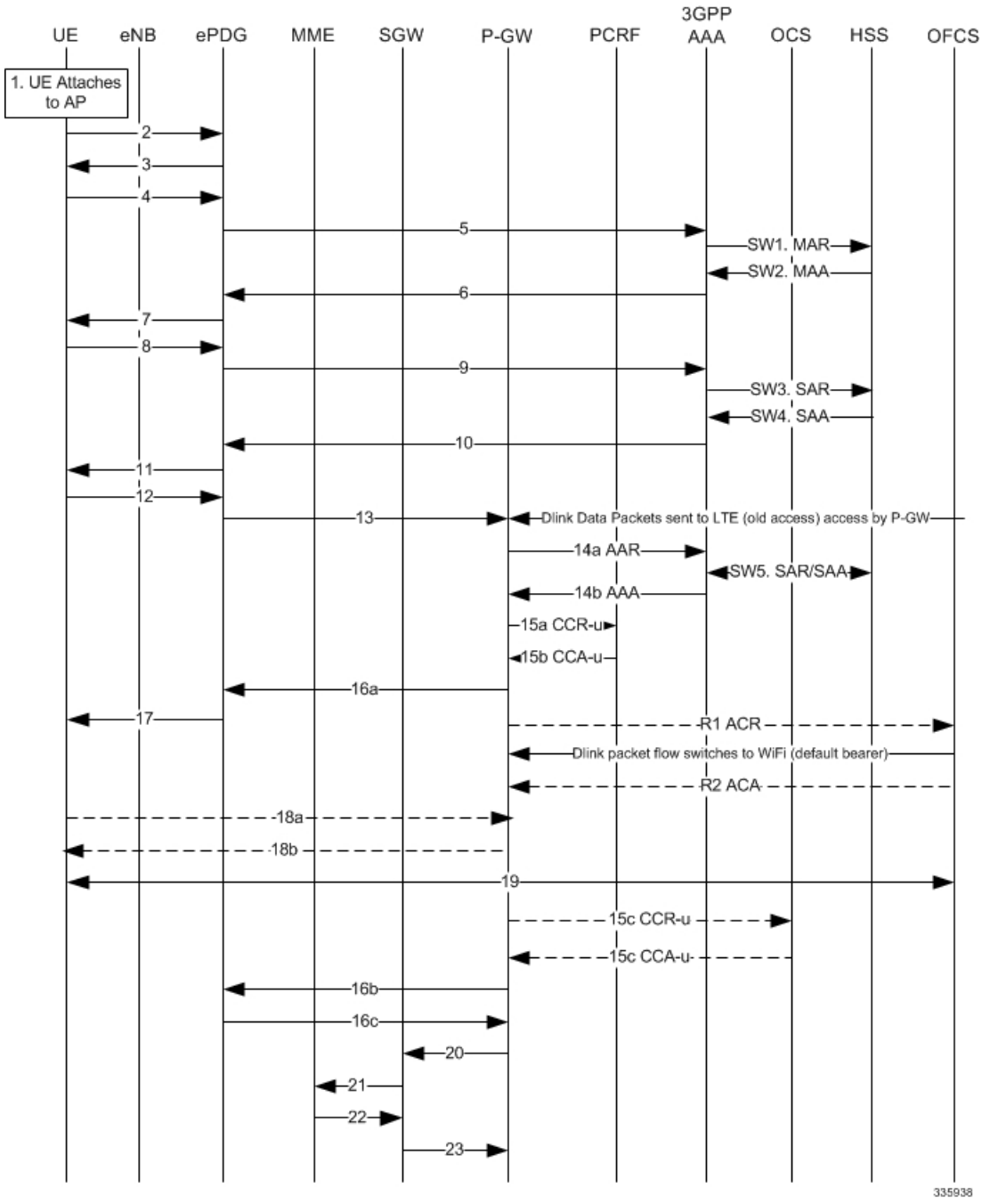


表 *60 : P-GW LTE* から *Wi-Fi* へのハンドオフ

ステップ	説明
1	認証と ePDG の選択。UUE が、必要に応じて、初期アクセスポイントの関連付けと認証を実行します。

ステップ	説明
2	UE から ePDG：IKEv2 SA_INIT。UE が、IKE_SA_INIT 要求を送信します。
3	ePDG から UE：INIT 応答。ePDG が、IKE_SA_INIT 応答で応答します。ePDG が、IKE_SA_INIT 応答を送信するときに IKEv2 セットアップタイマーを開始します。
4	UE が、Auth_Request を送信します。
5	ePDG から AAA：DER。ePDG が、3GPP AAA サーバーに DER メッセージを送信します。NAI には、IKE メッセージで受信されたユーザー名で送信された AP MAC アドレスを含めないでください。
SW1. MAR	AAA から HSS：MAR。3GPP AAA サーバーが、SWx を介して HSS からユーザープロファイルと認証ベクトルを取得します。3GPP AAA サーバーが、受信したユーザーアイデンティティに基づいて認証済みユーザーの IMSI のルックアップを実行し、HSS に送信される要求に、要求される認証方法として EAP-AKA を含めます。 AAA が、Multimedia-Auth-Request MAR、Origin-Host、Origin-Realm、Destination-Realm、Destination-Host、User-Name、RAT-Type、SIP-Auth-Data-Item、SIP-Number-Auth-Items、および Routing-Information を送信します。
SW2. MAA	HSS から AAA：MAA。その後、HSS が、AMF 分離ビット = 0 の認証ベクトルを生成し、それらを 3GPP AAA サーバーに送り返します。 HSS が、Multimedia-Auth-Answer MAA を送信します。
6	AAA から ePDG：DEA。3GPP AAA サーバーが、認証チャレンジを開始し、DEA で応答します。
7	ePDG から UE：IKE_AUTH。ePDG が、IKE_AUTH で応答します。このアイデンティティは ePDG の IP アドレスです。AUTH ペイロードが、最初の IKE_SA_INIT 応答を認証します。UE が証明書を要求した場合は、CERT が含まれます。IKEv2 を介した EAP 手順を開始するために、3GPP AAA サーバーから受信された EAP メッセージが含められます。
8	UE から ePDG：IKE_AUTH 要求。UE が、認証パラメータを確認し、認証チャレンジに応答します。IKEv2 メッセージの唯一のペイロード（ヘッダーを除く）は、EAP メッセージの IKE_AUTH 要求（EAP）です。
9	ePDG から AAA：DER。ePDG が、DER（基本 AVP、認証要求タイプ、EAP ペイロード、Auth-Session-State、サービス選択）を 3GPP AAA サーバーに送信します。

ステップ	説明
SW3. SAR	AAA から HSS：SAR。3GPP AAA が、認証されたユーザーの 3GPP AAA サーバーアドレス情報で HSS を更新します。AAA が、Server-Assignment-Request、Origin-Host、Origin-Realm、Destination-Host、Destination-Realm、User-Name（IMSI-NAI）、Server-Assignment-Type（REGISTRATION）を送信します。
SW4 SAA	HSS から AAA：SAA。HSS が、Server-Assignment-Answer を送信します。
10	AAA から ePDG：DEA。3GPP AAA サーバーが、EAP 成功を送信します。 3GPP AAA サーバーが、DEA で応答する前に、ユーザーが 3GPP 以外のアクセスについて承認されているかどうかをユーザーのサブスクリプションで確認します。
11	ePDG から UE：IKE_AUTH_Response。ePDG が、IKE_AUTH_Response（EAP）を送信します。
12	UE から ePDG：IKE_AUTH_Request。UE が、IKE_AUTH 要求（AUTH）を送信します。UE が、MSK の独自のコピーを入力として取得し、最初の IKE_SA_INIT メッセージを認証するための AUTH パラメータを生成します。
13	ePDG から P-GW：セッション作成要求。ePDG が、セッション作成要求を P-GW に送信します。UE が IKE Config 要求で P-CSCF を要求した場合は、P-CSCF が要求されます。
14a	P-GW から 3GPP-AAA：AAR。P-GW が、3GPP AAA に AAR を送信して、サブスクライバの APN を承認し、APN の HSS 上の P-GW アドレスを更新します。
SW5. SAR/SAA	AAA から HSS：SAR。3GPP AAA が、APN の P-GW アドレスで HSS を更新します。AAA が、Server-Assignment-Request を送信します。
14b AAA	3GPP AAA から P-GW：AAA。3GPP AAA が、AAA を P-GW に送信します。
15a CCR-u	P-GW から PCRF：CCR-U。P-GW が、IP-CAN セッションの変更を示すために、IP-CAN 変更の表示を CCR によって PCRF に送信します。
15b CCA-u	PCRF から P-GW：CCA。PCRF が、CCA メッセージで IP-CAN セッション変更を確認応答します。このメッセージには、P-GW が実施するポリシーおよび課金ルールと、P-GW で報告する必要があるイベントのトリガーが含まれます。
16a	P-GW から ePDG：セッション作成応答。P-GW が、S5 セッションを識別し、要求された IP アドレスセッションを再割り当てして、セッション作成応答メッセージで ePDG に応答します。ePDG がメッセージ 13 に P-CSCF 要求を含めていた場合は、P-CSCF プライベート IE が含まれます。
17	ePDG から UE：IKE_AUTH。ePDG が、IKE_AUTH を送信します。
R1 ACR	P-GW から OFCS：ACR。P-GW が、OFCS に ACR-Interim を送信します。

ステップ	説明
R2 ACA	OFCS から P-GW：ACA。OFCS が、P-GW に ACA で応答します。
18a	UE が、ルータ送信要求メッセージを送信します。
18b	P-GW が、ルータアドバタイズメントを送信し、以前に割り当てられたグローバルに一意の /64 IPv6 プレフィックスを含めます。
19	アクセスネットワークが変更されたことを正常に識別すると、UE が、P-CSCF への RAT 変更と、割り当て済みの IP アドレスは変更されないことを示す SIP Re-Register を送信します。UE は、PAN ヘッダーに 802.11 a/b/g/n を含めます。IMS の場合、P-CSCF からの課金が使用されないため、SIP の再登録は、P-CSCF の課金方法には影響しません。
15c CCR-u	P-GW から OCS：CCR-U。Online AVP が PCRF からの CCA に設定されている場合、P-GW が、条件に応じて CCR-Update を OCS に送信し、PDN セッションのオンライン課金クォータを要求します。
15d CCA-u	OCS から P-GW：CCA。OCS が、P-GW に CCA で応答します。
16b	P-GW から ePDG：ベアラー作成要求。IMS PDN には、ハンドオフ前に確立された 1 つ以上の専用ベアラーがあり、P-GW が、ベアラー作成要求も ePDG に送信します。課金 ID は S2b では送信されないことに注意してください。
16c	ePDG から P-GW：ベアラー作成応答。ePDG が、ベアラー作成応答メッセージを送信します。
20	P-GW から S-GW：ベアラー削除要求。P-GW が、S-GW にベアラー削除要求（リンクされた EPS ベアラー ID（最後のベアラーの場合）または EPS ベアラー ID、原因（RAT が 3GPP から非 3GPP に変更された））を送信します。このメッセージは、メッセージ 13（セッション作成要求）の後であればいつでも送信できます。
21	S-GW から MME：ベアラー削除要求。S-GW が、MME にベアラー削除要求（リンクされた EPS ベアラー ID（最後のベアラーの場合）または EPS ベアラー ID、原因（RAT が 3GPP から非 3GPP に変更された））を送信します。 MME が、E-UTRAN ベアラーをリリースします（まだリリースされていない場合）。原因 IE は非 3GPP への RAT の変更であるため、MME は、この時点では HSS に通知要求を送信しません。MME は、UE をページングしないか NAS シグナリングを開始せず、ローカルに保存された PDN 状態を削除し、eNodeB に対して S1 コンテキストリリースを実行します（eNodeB によってまだトリガーされていない場合）。最後の PDN の場合、MME が、ローカルに保存されているすべての UE 状態を削除します。
22	MME から S-GW：ベアラー削除応答。MME が、S-GW にベアラー削除応答を送信します。

ステップ	説明
23	S-GW から P-GW：ベアラー削除応答。S-GW が、P-GW にベアラー削除応答を送信します。

図 *47 : P-GW* : *Wi-Fi* から *LTE* へのハンドオフ

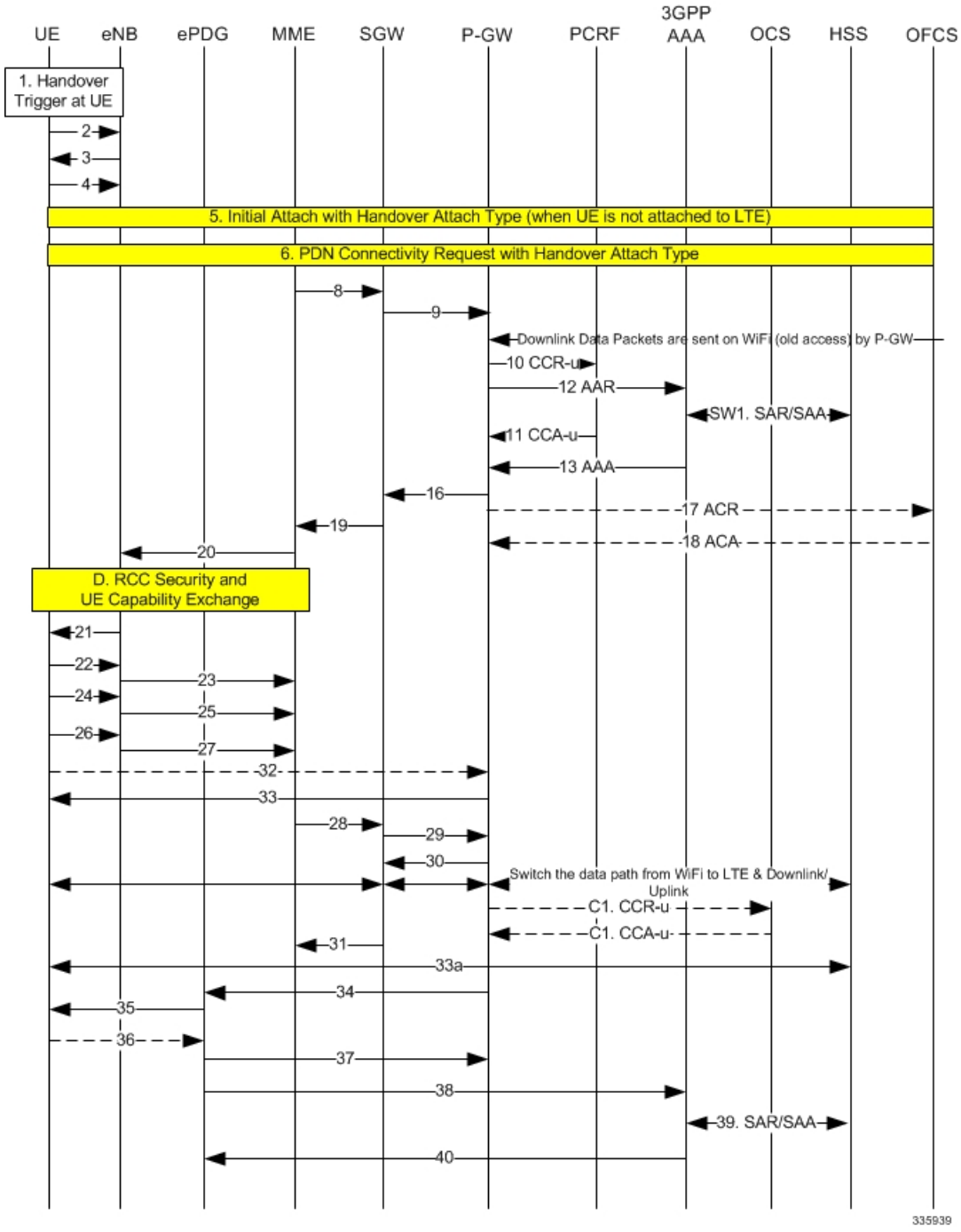


表 *61 : P-GW Wi-Fi* から *LTE* へのハンドオフ手順

ステップ	説明
1	UE でハンドオーバートリガーが発生します。
2、3	RRC 接続要求/接続セットアップ。UE と eNodeB が、RRC 接続（5.3.3、TS 36.331）をセットアップするためにシグナリングを交換します。
4	RRC 接続セットアップ完了 [アタッチ要求]。UE が、eNodeB に RRC 接続セットアップ完了メッセージを送信します。
5	eNB から MME へのアタッチ要求。UE が、LTE へのアタッチ要求で、これがハンドオーバーアタッチであることを示します。eNodeB が、MME を選択します。eNodeB が、初期 UE メッセージでアタッチ要求メッセージを MME に転送します。
6	MME が、HSS 提供の PGW FQDN に基づいて同じ P-GW を選択し、セッション作成要求を送信します。
8	MME が、PGW/SGW を選択します。MME が、RAT を EUTRAN とし、ハンドオフインジケータが TRUE に設定された、セッション作成要求を SGW に送信します。
9	SGW が、ハンドオフを確立するために、セッション作成要求を PDN GW に送信します（handoffindicator を true に設定）。RAT タイプは E-UTRAN です。
10	P-GW から PCRF への CCR IP-CAN セッション変更手順。PCEF が、CC-Request-Type が UPDATE_REQUEST に設定された CC-Request（CCR）コマンドを送信します。APN-AMBR が QoS-information AVP に含まれます。
12	P-GW が、AAR を 3GPP-AAA に送信し、新しい接続の RAT タイプを含めます。
SW1. SAR/SAA	3GPP-AAA が、ユーザープロファイルを取得するために SAR を HSS に送信し、HSS が、SAA を返します。3GPP-AAA がこのユーザーについて登録されていないため、P-GW-FQDN は更新されません。
11	PCRF から P-GW：CCA IP-CAN セッション変更手順。CCR を受信すると、PCRF が、設定および確立されたすべてのベアラーに PCC ルールとイベントトリガーをインストールするための CC-Answer（CCA）コマンドを送信します。QoS-Information AVP には APN-AMBR-UL と APN-AMBR-DL が含まれます。
13	3GPP-AAA が、AAA で応答します。
16	P-GW から S-GW：セッション作成応答 + ベアラー作成要求。P-GW が、セッション作成応答メッセージで S-GW に応答します。P-GW が、IPv6 プレフィックスを提供します。 通信事業者の設定に応じて、P-GW がダウンリンクデータの転送を開始でき、S-GW がすべてのダウンリンクデータパケットをバッファします。

ステップ	説明
17	P-GW から OFCS：ACR。P-GW が、PBA を送信した後に、ACR-Interim を OFCS に送信します。
18	OFCS から P-GW：ACA。OFCS が、P-GW に ACA で応答します。
19	セッション作成応答。S-GW が、セッション作成応答を MME に送信します。
20	初期コンテキストセットアップ要求/アタッチ承認。アタッチ承認が、MME から eNodeB に、初期コンテキストセットアップ要求で NAS PDU として送信されます。アタッチ承認メッセージには新しい GUTI が含まれます。
D	これらの手順は、ロケーション手順とは独立して実行されます。これらの手順は、初期アタッチシナリオにのみ適用されます。
21	RRC 接続再設定。eNodeB が、EPS 無線ベアラー ID を含む RRC 接続再設定メッセージを UE に送信し、アタッチ承認メッセージを UE に送信します。アクティブ化されたデフォルトベアラーが関連付けられている APN を UE に通知するために、APN が UE に提供されます。
22	RRC 接続再設定完了。UE が、RRC 接続再設定完了メッセージを eNodeB に送信します。
23	初期コンテキストセットアップ応答。eNodeB が、初期コンテキストセットアップ応答を MME に送信します。
24	アップリンク情報転送。UE が、アップリンク情報転送メッセージを送信します。
25	アタッチ完了。eNodeB が、受信したアタッチ完了メッセージを NAS PDU の一部としてアップリンク NAS トランスポートで転送します。
26	アップリンク情報転送。UE が、アタッチ承認メッセージで専用 EPS ベアラー コンテキスト アクティブ化要求メッセージを受信したときに、アップリンク情報転送メッセージで専用 EPS ベアラー コンテキスト アクティブ化承認メッセージを送信します。
27	UL NAS トランスポート。eNB が、ステップ 14.b で受信した専用ベアラー コンテキスト アクティブ化承認メッセージを、UL NAS トランスポートメッセージで MME に渡します。この時点で、専用ベアラーでアップリンクデータを送信できます。
32	ルータ送信要求。このステップは、ステップ 26 の後であれば任意の時点で実行される可能性があります。IPv6 PDN の場合は、UE が、ルータ送信要求を P-GW に送信する可能性があります。

ステップ	説明
33	ルータアドバタイズメント。UE が IPv4v6 または IPv6 PDN タイプを要求した場合、このステップは、ステップ 29 の後であれば任意の時点で実行される可能性があります。RS の受信時点またはその前に、P-GW が、ルータアドバタイズメントを送信し、以前に割り当てられたグローバルに一意の /64 IPv6 プレフィックスを含めます。
28	ベアラー変更要求/ベアラー作成応答。初期コンテキストセットアップ応答とアタッチ完了の両方を受信すると、MMEが、ベアラー変更要求メッセージをS-GWに送信します。 MMEが、ベアラー作成応答メッセージでベアラー変更要求メッセージをピギーバックします。
29	S-GW が、各メッセージを個別に処理します。S-GW が、ベアラー作成応答を P-GW に転送します。この時点で、P-GW は、IMS トラフィック専用ベアラーでダウンリンクデータを送信できます。 ベアラー変更要求でハンドオーバー指示がTRUEに設定されているため、S-GWが、ベアラー変更要求を P-GW に個別に送信します。 TS 23.401 に基づいて、P-GW は、このメッセージを受信すると、ダウンリンクトラフィックをS5に切り替えます。ただし、通信事業者の設定によっては、この切り替えが、上記（C3）のセッション作成要求時に発生します。
30	P-GW が、ベアラー変更応答（原因）メッセージを S-GW に送信します。
C1. CCR-u	P-GW から OCS：CCR-U。Online AVP が PCRF からの CCA に設定されている場合、P-GW が、条件に応じて CCR-Update を OCS に送信し、PDN セッションのオンライン課金クォータを要求します。
C1. CCA-u	OCS から P-GW：CCA。OCS が、P-GW に CCA で応答します。
31	S-GW が、ベアラー変更応答を MME に送信します。S1 S-GW F-TEID は、セッション作成応答で S-GW から MME に送信される S1-U S-GW F-TEID と同じです。 S-GW は eNB へのダウンリンクパケットの送信を開始できるようになり、Wi-Fi から LTE へのデータパスの切り替えは、ベアラー変更応答の後に発生します。
33a	SIP 再登録 RAT 変更。UE が、RAT 変更を検出したことと、割り当てられた IP アドレスが変更されていないことを示す SIP Re-Register を P-CSCF に送信します。
34	P-GWからePDG：ベアラー削除要求。P-GWが、セッションを切断するために、ベアラー削除要求を ePDG に送信します。
35	ePDGからUE：IKEv2情報削除要求。ePDGが、セッションを切断するために、IKEv2 情報削除要求（）を UE に送信します。

ステップ	説明
34	UE から ePDG：IKEv2 情報削除応答。UE が、IKEv2 情報削除応答（）で応答し、無線インターフェイスのリソース解放を開始します。このステップは条件付きであり、UE はこの応答を送信しない場合があります。
37	ePDG から P-GW：ベアラー削除応答。ePDG が、ベアラー削除応答を P-GW に送信します。
38	ePDG から AAA：セッション終了要求。ePDG が、STR を 3GPP AAA に送信します。
39	AAA から HSS：サーバー割り当て要求。AAA が、登録解除のために Server-Assignment-Request を送信します。 HSS から AAA：SAA。HSS が、Server-Assignment-Answer を送信します。
40	AAA から ePDG：セッション終了応答。AAA が、STA を ePDG に送信します。

SAEGW GTP ベース S2b コールフロー

このセクションでは、SAEGW での GTP ベース S2b インターフェイスサポートの基本機能を示すコールフローを示します。

図 *48 :* 初回アタッチコールフロー：***SAEGW***

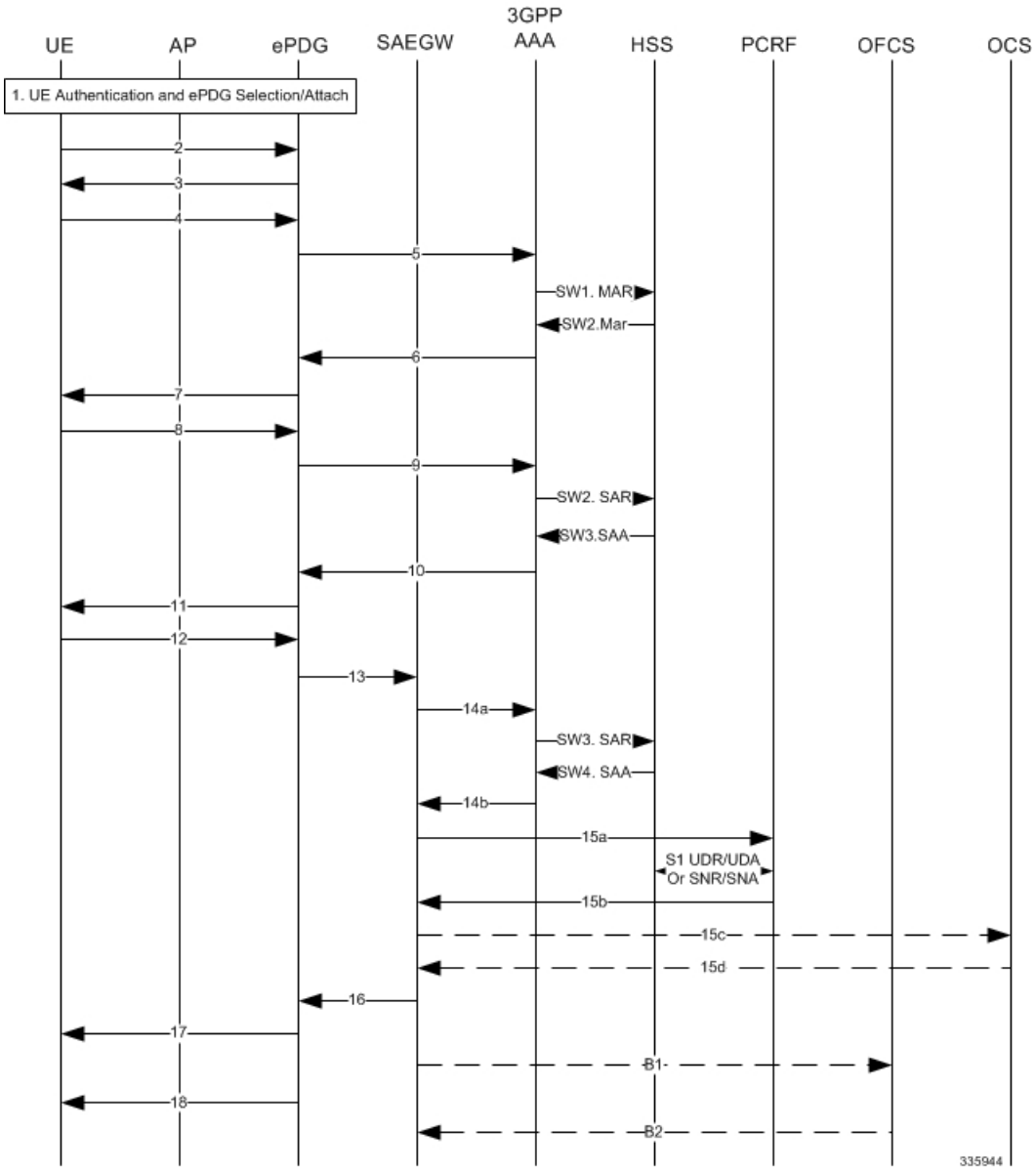


表 *62 :* 初回アタッチ：***SAEGW***

ステップ	説明
1	UUE が、必要に応じて、初期アクセスポイントの関連付けと認証を実行します。
2 ～ 11	UE が、ePDG との接続を確立します。

ステップ	説明
12	UE が、IKE_AUTH 要求（AUTH）を送信します。UE が、MSK の独自のコピーを入力として取得し、最初の IKE_SA_INIT メッセージを認証するための AUTH パラメータを生成します。
13	ePDG が、ノード選択オプションに基づいて SAEGW の P-GW を選択します。ePDG が、セッション作成要求を送信します。
14a	SAEGW の P-GW が、3GPP AAA に AAR を送信して、サブスクライバの PDN を承認し、APN の HSS 上の P-GW アドレスを更新します。
SW3	3GPP AAA が、APN 用の SAEGW の P-GW アドレスで HSS を更新し、HSS からサブスクライバ APN プロファイルを取得します。
SW4	HSS が、Server-Assignment-Answer（Session-Id、Result-Code、Experimental-Result（Vendor-Id、Experimental-Result-Code））を送信します。
14b	3GPP AAA が、AAA を送信します。
15a	SAEGW の P-GW が、IP-CAN の確立を示すために、新しい IP CAN セッション確立の通知を CCR で PCRF に送信します。
S1	PCRF が、ユーザープロファイルをダウンロード（およびキャッシュ）します（Sh: UDR（User-Identity、Service-Indication、Data-Reference）を送信し、Sh: UDA（Result-Code、User-Data）を受信することにより）。
S2	PCRF が、プロファイル更新通知を登録できます。
15b	PCRF が、CCA メッセージで IP CAN セッション確立を確認応答します。
15c	Online AVP が PCRF（UC ユーザー/CF/RTR）からの CCA に設定されている場合、P-GW が、条件に応じて CCR-Initial を送信します。
15d	OCS が、P-GW に CCA で応答します。
16	SAEGW の P-GW が、要求された IP アドレスセッションを割り当て、セッション作成応答メッセージで ePDG に応答します。
17	ePDG が、設定ペイロード（CFG_REPLY）で、割り当てられた IP アドレスを送信します。AUTH パラメータが、設定ペイロード、セキュリティ アソシエーション、および残りの IKEv2 パラメータとともに UE に送信され、IKEv2 ネゴシエーションが終了します。
18	ePDG が、IP スタックが完全に初期化されていることを確認するためにルータアドバタイズメントを送信します。SAEGW の P-GW が、UE へのルータアドバタイズメントを無効にします。
B1	Offline AVP が PCRF からの CCA に設定されている場合、IP-CAN セッション確立手順の完了後に、SAEGW の P-GW が、ACR-Start を OFCS に送信します。

ステップ	説明
B2	OFCS が、SAEGW の P-GW に ACA で応答します。

図 *49 : SAEGW* : *LTE* から *Wi-Fi* へのハンドオフのコールフロー

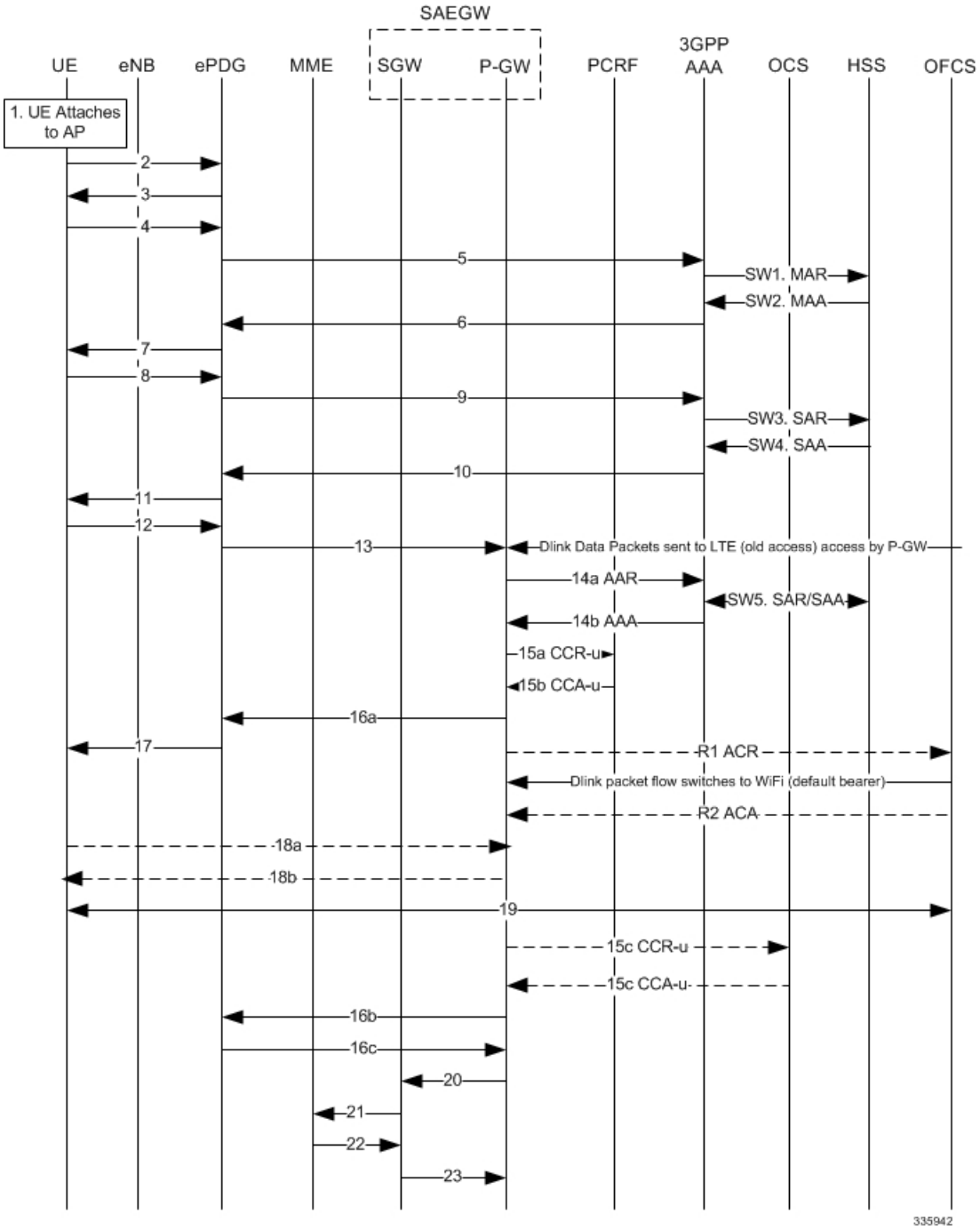


表 *63 : SAEGW LTE* から *Wi-Fi* へのハンドオフ

ステップ	説明
1	認証と ePDG の選択。UUE が、必要に応じて、初期アクセスポイントの関連付けと認証を実行します。
2	UE から ePDG：IKEv2 SA_INIT。UE が、IKE_SA_INIT 要求を送信します。
3	ePDG から UE：INIT 応答。ePDG が、IKE_SA_INIT 応答で応答します。ePDG が、IKE_SA_INIT 応答を送信するときに IKEv2 セットアップタイマーを開始します。
4	UE が、Auth_Request を送信します。
5	ePDG から AAA：DER。ePDG が、3GPP AAA サーバーに DER メッセージを送信します。NAI には、IKE メッセージで受信されたユーザー名で送信された AP MAC アドレスを含めないでください。
SW1. MAR	AAA から HSS：MAR。3GPP AAA サーバーが、SWx を介して HSS からユーザープロファイルと認証ベクトルを取得します。3GPP AAA サーバーが、受信したユーザーアイデンティティに基づいて認証済みユーザーの IMSI のルックアップを実行し、HSS に送信される要求に、要求される認証方法として EAP-AKA を含めます。 AAA が、Multimedia-Auth-Request MAR、Origin-Host、Origin-Realm、Destination-Realm、Destination-Host、User-Name、RAT-Type、SIP-Auth-Data-Item、SIP-Number-Auth-Items、および Routing-Information を送信します。
SW2. MAA	HSS から AAA：MAA。その後、HSS が、AMF 分離ビット = 0 の認証ベクトルを生成し、それらを 3GPP AAA サーバーに送り返します。 HSS が、Multimedia-Auth-Answer MAA を送信します。
6	AAA から ePDG：DEA。3GPP AAA サーバーが、認証チャレンジを開始し、DEA で応答します。
7	ePDG から UE：IKE_AUTH。ePDG が、IKE_AUTH で応答します。このアイデンティティは ePDG の IP アドレスです。AUTH ペイロードが、最初の IKE_SA_INIT 応答を認証します。UE が証明書を要求した場合は、CERT が含まれます。IKEv2 を介した EAP 手順を開始するために、3GPP AAA サーバーから受信された EAP メッセージが含められます。
8	UE から ePDG：IKE_AUTH 要求。UE が、認証パラメータを確認し、認証チャレンジに応答します。IKEv2 メッセージの唯一のペイロード（ヘッダーを除く）は、EAP メッセージの IKE_AUTH 要求（EAP）です。
9	ePDG から AAA：DER。ePDG が、DER（基本 AVP、認証要求タイプ、EAP ペイロード、Auth-Session-State、サービス選択）を 3GPP AAA サーバーに送信します。

ステップ	説明
SW3. SAR	AAA から HSS：SAR。3GPP AAA が、認証されたユーザーの 3GPP AAA サーバーアドレス情報で HSS を更新します。AAA が、Server-Assignment-Request、Origin-Host、Origin-Realm、Destination-Host、Destination-Realm、User-Name（IMSI-NAI）、Server-Assignment-Type（REGISTRATION）を送信します。
SW4 SAA	HSS から AAA：SAA。HSS が、Server-Assignment-Answer を送信します。
10	AAA から ePDG：DEA。3GPP AAA サーバーが、EAP 成功を送信します。 3GPP AAA サーバーが、DEA で応答する前に、ユーザーが 3GPP 以外のアクセスについて承認されているかどうかをユーザーのサブスクリプションで確認します。
11	ePDG から UE：IKE_AUTH_Response。ePDG が、IKE_AUTH_Response（EAP）を送信します。
12	UE から ePDG：IKE_AUTH_Request。UE が、IKE_AUTH 要求（AUTH）を送信します。UE が、MSK の独自のコピーを入力として取得し、最初の IKE_SA_INIT メッセージを認証するための AUTH パラメータを生成します。
13	ePDG から SAEGW の P-GW：セッション作成要求。ePDG が、セッション作成要求を SAEGW の P-GW に送信します。UE が IKE Config 要求で P-CSCF を要求した場合は、P-CSCF が要求されます。
14a	P-GW から 3GPP-AAA：AAR。SAEGW の P-GW が、3GPP AAA に AAR を送信して、サブスクライバの APN を承認し、APN の HSS 上の P-GW アドレスを更新します。
SW5. SAR/SAA	AAA から HSS：SAR。3GPP AAA が、APN の P-GW アドレスで HSS を更新します。AAA が、Server-Assignment-Request を送信します。
14b AAA	3GPP AAA から P-GW：AAA。3GPP AAA が、AAA を SAEGW の P-GW に送信します。
15a CCR-u	SAEGW の P-GW から PCRF：CCR-U。P-GW が、IP-CAN セッションの変更を示すために、IP-CAN 変更の通知を CCR で PCRF に送信します。
15b CCA-u	PCRF から SA の P-GW：CCA。PCRF が、CCA メッセージで IP-CAN セッション変更を確認応答します。このメッセージには、P-GW が実施するポリシーおよび課金ルールと、P-GW で報告する必要があるイベントのトリガーが含まれます。
16a	SAEGW の P-GW から ePDG：セッション作成応答。SAEGW の P-GW が、S5 セッションを識別し、要求された IP アドレスセッションを再割り当てして、セッション作成応答メッセージで ePDG に応答します。ePDG がメッセージ 13 に P-CSCF 要求を含めていた場合は、P-CSCF プライベート IE が含まれます。

ステップ	説明
17	ePDG から UE：IKE_AUTH。ePDG が、IKE_AUTH を送信します。
R1 ACR	P-GW から OFCS：ACR。P-GW が、OFCS に ACR-Interim を送信します。
R2 ACA	OFCS から P-GW：ACA。OFCS が、SAEGW の P-GW に ACA で応答します。
18a	UE が、ルータ送信要求メッセージを送信します。
18b	SAEGW の P-GW が、ルータアドバタイズメントを送信し、以前に割り当てられたグローバルに一意の /64 IPv6 プレフィックスを含めます。
19	アクセスネットワークが変更されたことを正常に識別すると、UE が、P-CSCF への RAT 変更と、割り当て済みの IP アドレスは変更されないことを示す SIP Re-Register を送信します。UE は、PAN ヘッダーに 802.11 a/b/g/n を含めます。IMS の場合、P-CSCF からの課金が使用されないため、SIP の再登録は、P-CSCF の課金方法には影響しません。
15c CCR-u	SAEGW の P-GW から OCS：CCR-U。Online AVP が PCRF からの CCA に設定されている場合、P-GW が、条件に応じて CCR-Update を OCS に送信し、PDN セッションのオンライン課金クォータを要求します。
15d CCA-u	OCS から P-GW：CCA。OCS が、SAEGW の P-GW に CCA で応答します。
16b	SAEGW の P-GW から ePDG：ベアラー作成要求。IMS PDN には、ハンドオフ前に確立された 1 つ以上の専用ベアラーがあり、SAEGW の P-GW が、ベアラー作成要求も ePDG に送信します。課金 ID は S2b では送信されないことに注意してください。 （注） コリジョンがある状況で、すでに 1 つのトランザクションが保留中でハンドオフ要求が受信されている場合、ハンドオフは拒否され、「Rejecting S2b/LTE Handoff as only one pending transaction is supported」というメッセージが表示されます。
16c	ePDG から P-GW：ベアラー作成応答。ePDG が、ベアラー作成応答メッセージを送信します。
20	SAEGW の P-GW から SAEGW の S-GW：ベアラー削除要求。P-GW が、S-GW にベアラー削除要求（リンクされた EPS ベアラー ID（最後のベアラーの場合）または EPS ベアラー ID、原因（RAT が 3GPP から非 3GPP に変更された））を送信します。このメッセージは、メッセージ 13（セッション作成要求）の後であればいつでも送信できます。

ステップ	説明
21	SAEGW の S-GW から MME：ベアラー削除要求。SAEGW の S-GW が、MME にベアラー削除要求（リンクされた EPS ベアラー ID（最後のベアラーの場合）または EPS ベアラー ID、原因（RAT が 3GPP から非 3GPP に変更された））を送信します。 MME が、E-UTRAN ベアラーをリリースします（まだリリースされていない場合）。原因 IE は非 3GPP への RAT の変更であるため、MME は、この時点では HSS に通知要求を送信しません。MME は、UE をページングしないか NAS シグナリングを開始せず、ローカルに保存された PDN 状態を削除し、eNodeB に対して S1 コンテキストリリースを実行します（eNodeB によってまだトリガーされていない場合）。最後の PDN の場合、MME が、ローカルに保存されているすべての UE 状態を削除します。
22	MME から SAEGW の S-GW：ベアラー削除応答。MME が、SAEGW の S-GW にベアラー削除応答を送信します。
23	SAEGW の S-GW から SAEGW の P-GW：ベアラー削除応答。SAEGW の S-GW が、SAEGW の P-GW にベアラー削除要求を送信します。

図 *50 : SAEGW Wi-Fi* から *LTE* へのハンドオフ

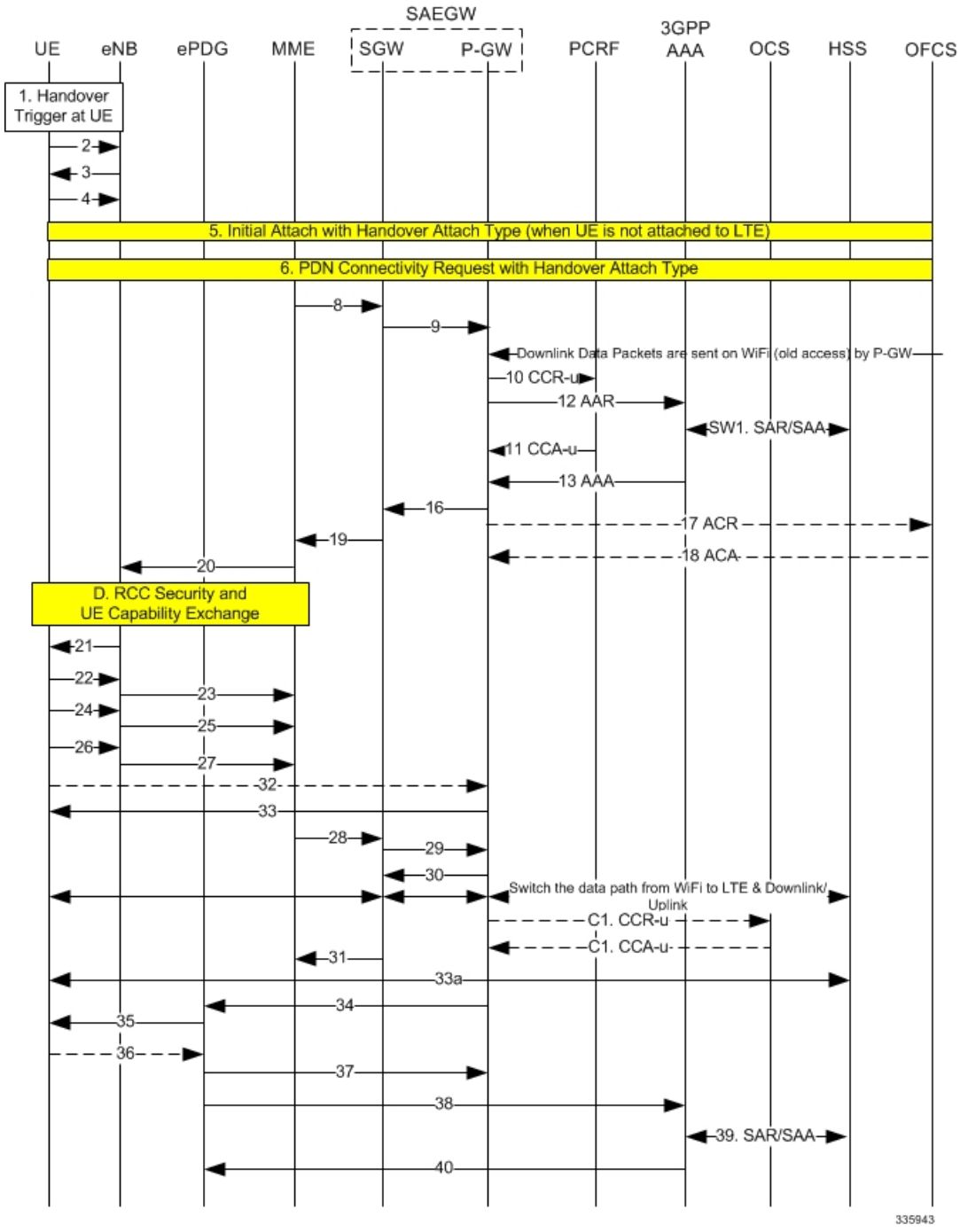


表 *64 : SAEGW Wi-Fi* から *LTE* へのハンドオフ手順

ステップ	説明
1	UE でハンドオーバートリガーが発生します。

ステップ	説明
2、3	RRC 接続要求/接続セットアップ。UE と eNodeB が、RRC 接続（5.3.3、TS 36.331）をセットアップするためにシグナリングを交換します。
4	RRC 接続セットアップ完了 [アタッチ要求]。UE が、eNodeB に RRC 接続セットアップ完了メッセージを送信します。
5	eNB から MME へのアタッチ要求。UE が、LTE へのアタッチ要求で、これがハンドオーバーアタッチであることを示します。eNodeB が、MME を選択します。eNodeB が、初期 UE メッセージでアタッチ要求メッセージを MME に転送します。
6	MME が、HSS 提供の PGW FQDN に基づいて同じ SAEGW の P-GW を選択し、セッション作成要求を送信します。
8	MME が、SAEGW の PGW/SGW を選択します。MME が、RAT を EUTRAN とし、ハンドオフインジケータが TRUE に設定されたセッション作成要求を SAEGW の SGW に送信します。
9	SAEGW の SGW が、ハンドオフを確立するために、セッション作成要求を PDN GW に送信します（handoffindicator を true に設定）。RAT タイプは E-UTRAN です。
10	SAEGW の P-GW から PCRF への CCR IP-CAN セッション変更手順。PCEF が、CC-Request-Type が UPDATE_REQUEST に設定された CC-Request（CCR）コマンドを送信します。APN-AMBR が QoS-information AVP に含まれます。
12	SAEGW の P-GW が、AAR を 3GPP-AAA に送信し、新しい接続の RAT タイプを含めます。
SW1. SAR/SAA	3GPP-AAA が、ユーザープロファイルを取得するために SAR を HSS に送信し、HSS が、SAA を返します。3GPP-AAA がこのユーザーについて登録されていないため、P-GW-FQDN は更新されません。
11	PCRF から SAEGW の P-GW：CCA IP-CAN セッション変更手順。CCR を受信すると、PCRF が、設定および確立されたすべてのベアラーに PCC ルールとイベントトリガーをインストールするための CC-Answer（CCA）コマンドを送信します。QoS-Information AVP には APN-AMBR-UL と APN-AMBR-DL が含まれます。
13	3GPP-AAA が、AAA で応答します。

ステップ	説明
16	SAEGW の P-GW から SAEGW の S-GW：セッション作成応答＋ベアラー作成要求。SAEGW の P-GW が、セッション作成応答メッセージで SAEGW の S-GW に応答します。SAEGW の P-GW が、IPv6 プレフィックスを提供します。 オペレータの設定に応じて、SAEGW の P-GW がダウンリンクデータの転送を開始でき、SAEGW の S-GW がすべてのダウンリンクデータパケットをバッファします。
17	SAEGW の P-GW から OFCS：ACR。SAEGW の P-GW が PBA を送信した後に、SAEGW の P-GW は OFCS に ACR-Interim を送信します。
18	OFCS から SAEGW の P-GW：ACA。OFCS が、P-GW に ACA で応答します。
19	セッション作成応答。SAEGW の S-GW が、セッション作成応答を MME に送信します。
20	初期コンテキストセットアップ要求/アタッチ承認。アタッチ承認が、MME から eNodeB に、初期コンテキストセットアップ要求で NAS PDU として送信されます。アタッチ承認メッセージには新しい GUTI が含まれます。
D	これらの手順は、ロケーション手順とは独立して実行されます。これらの手順は、初期アタッチシナリオにのみ適用されます。
21	RRC 接続再設定。eNodeB が、EPS 無線ベアラー ID を含む RRC 接続再設定メッセージを UE に送信し、アタッチ承認メッセージを UE に送信します。アクティブ化されたデフォルトベアラーが関連付けられている APN を UE に通知するために、APN が UE に提供されます。
22	RRC 接続再設定完了。UE が、RRC 接続再設定完了メッセージを eNodeB に送信します。
23	初期コンテキストセットアップ応答。eNodeB が、初期コンテキストセットアップ応答を MME に送信します。
24	アップリンク情報転送。UE が、アップリンク情報転送メッセージを送信します。
25	アタッチ完了。eNodeB が、受信したアタッチ完了メッセージを NAS PDU の一部としてアップリンク NAS トランスポートで転送します。
26	アップリンク情報転送。UE が、アタッチ承認メッセージで専用 EPS ベアラー コンテキスト アクティブ化要求メッセージを受信したときに、アップリンク情報転送メッセージで専用 EPS ベアラー コンテキスト アクティブ化承認メッセージを送信します。

ステップ	説明
27	UL NAS トランスポート。eNB が、ステップ 14.b で受信した専用ベアラー コンテキスト アクティブ化承認メッセージを、UL NAS トランスポートメッセージで MME に渡します。この時点で、専用ベアラーでアップリンクデータを送信できます。
32	ルータ送信要求。このステップは、ステップ 26 の後であれば任意の時点で実行される可能性があります。IPv6 PDN の場合は、UE が、ルータ送信要求を P-GW に送信する可能性があります。
33	ルータアドバタイズメント。UE が IPv4v6 または IPv6 PDN タイプを要求した場合、このステップは、ステップ 29 の後であれば任意の時点で実行される可能性があります。RS の受信時点またはその前に、SAEGW の P-GW が、ルータアドバタイズメントを送信し、以前に割り当てられたグローバルに一意の /64 IPv6 プレフィックスを含めます。
28	ベアラー変更要求/ベアラー作成応答。初期コンテキストセットアップ応答とアタッチ完了の両方を受信すると、MME が、ベアラー変更要求メッセージを SAEGW の S-GW に送信します。 MME が、ベアラー作成応答メッセージでベアラー変更要求メッセージをピギーバックします。
29	SAEGW の S-GW が、各メッセージを個別に処理します。SAEGW の S-GW が、ベアラー作成応答を P-GW に転送します。この時点で、SAEGW の P-GW は、IMS トラフィック専用ベアラーでダウンリンクデータを送信できます。 ベアラー変更要求でハンドオーバー通知が TRUE に設定されているため、SAEGW の S-GW が、ベアラー変更要求を SAEGW の P-GW に個別に送信します。 TS 23.401 に基づいて、SAEGW の P-GW は、このメッセージを受信すると、ダウンリンクトラフィックを S5 に切り替えます。ただし、通信事業者の設定によっては、この切り替えが、上記（C3）のセッション作成要求時に発生します。
30	SAEGW の P-GW が、ベアラー変更応答（原因）メッセージを S-GW に送信します。
C1. CCR-u	SAEGW の P-GW から OCS：CCR-U。Online AVP が PCRF からの CCA に設定されている場合、SAEGW の P-GW が、条件に応じて CCR-Update を OCS に送信し、PDN セッションのオンライン課金クォータを要求します。
C1. CCA-u	OCS から SAEGW の P-GW：CCA。OCS が、SAEGW の P-GW に CCA で応答します。

ステップ	説明
31	SAEGW の S-GW が、ベアラー変更応答を MME に送信します。S1 S-GW F-TEID は、セッション作成応答で SAEGW の S-GW から MME に送信される S1-U S-GW F-TEID と同じです。 SAEGW の S-GW は eNB へのダウンリンクパケットの送信を開始できるようになり、Wi-Fi から LTE へのデータパスの切り替えは、ベアラー変更応答の後に発生します。
33a	SIP 再登録 RAT 変更。UE が、RAT 変更を検出したことと、割り当てられた IP アドレスが変更されていないことを示す SIP Re-Register を P-CSCF に送信します。
34	SAEGW の P-GW から ePDG：ベアラー削除要求。SAEGW の P-GW が、セッションを切断するために、ベアラー削除要求を ePDG に送信します。
35	ePDG から UE：IKEv2 情報削除要求。ePDG が、セッションを切断するために、IKEv2 情報削除要求（）を UE に送信します。
34	UE から ePDG：IKEv2 情報削除応答。UE が、IKEv2 情報削除応答（）で応答し、無線インターフェイスのリソース解放を開始します。このステップは条件付きであり、UE はこの応答を送信しない場合があります。
37	ePDG から SAEGW の P-GW：ベアラー削除応答。ePDG が、ベアラー削除応答を P-GW に送信します。
38	ePDG から AAA：セッション終了要求。ePDG が、STR を 3GPP AAA に送信します。
39	AAA から HSS：サーバー割り当て要求。AAA が、登録解除のために Server-Assignment-Request を送信します。 HSS から AAA：SAA。HSS が、Server-Assignment-Answer を送信します。
40	AAA から ePDG：セッション終了応答。AAA が、STA を ePDG に送信します。

標準準拠

ここでは、P-GW および SAEGW に GTP ベースの S2b インターフェイスを実装する際に使用された業界標準と参考資料を紹介します。

GTP ベースの S2b インターフェイスのサポート機能を開発する工程では、次の標準規格と参考資料が使用されています。

- 3GPP TS 23.003-a.1.0 Numbering, addressing and identification
- 3GPP TS 23.234-a.0.0, 3GPP system to Wireless Local Area Network (WLAN) Interworking
- 3GPP TS 23.261-a.1.0, IP flow mobility and seamless Wireless Local Area Network (WLAN) Offload
- 3GPP TS 23.401: GPRS Enhancement for E-UTRAN Access

- 3GPP TS 23.402-a.4.0 Architecture Enhancements for non-3GPP Accesses
- 3GPP TS 24.302-a.4.0: Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks.
- 3GPP TS 24.312-a.3.0 Access Network Discovery and Selection Function (ANDSF) Management Object (MO)
- 3GPP TS 29.273-a.3.0 Evolved Packet System (EPS); 3GPP EPS AAA interfaces
- 3GPP TS 29.274- Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP TS 33.234-a.0.0 Wireless Local Area Network (WLAN) interworking security
- 3GPP TS 33.402-a.0.0 Security aspects of non-3GPP accesses
- IETF RFC 3588：Diameter Base Protocol.
- IETF RFC 3602：The AES-CBC Cipher Algorithm and Its Use with IPSec
- IETF RFC 3715：IPSec-Network Address Translation (NAT) Compatibility Requirements
- IETF RFC 3748：Extensible Authentication Protocol (EAP)
- IETF RFC 3948：UDP Encapsulation of IPSec ESP Packets.
- IETF RFC 4187：Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
- IETF RFC 4303：IP Encapsulating Security Payload (ESP).
- IETF RFC 4306：Internet Key Exchange Protocol Version 2
- IETF RFC 4739：Multiple Authentication Exchange in IKEv2 protocol
- IETF RFC 5996：Internet Key Exchange Protocol Version 2 (IKEv2)

S2a アーキテクチャの動作の仕組み

ここでは、スタンドアロン P-GW および SAEGW の S2a インターフェイス アーキテクチャについて説明します。

S2a インターフェイスをサポートするためのスタンドアロン P-GW および SAEGW アーキテクチャ

スタンドアロン P-GW および SAEGW の S2a インターフェイス アーキテクチャの図を以下に示します。

S2a インターフェイスは、SAEGW のスタンドアロン P-GW と P-GW を eHRPD の HSGW に接続します。具体的には、S2a インターフェイスは、信頼できる非 3GPP アクセスポイント（HSGW）と SAEGW のスタンドアロン P-GW または P-GW 間のシグナリングとモビリティのサポートを提供することで、ベアラーインターフェイスをサポートします。これはプロキシモバイル IP に基づいていますが、PMIP をサポートしない信頼できる非 3GPP IP アクセスポイントへの接続を可能にするクライアントモバイル IPv4 FA モードもサポートしています。

図 *51* : スタンドアロン *P-GW* の *S2a* インターフェイス アーキテクチャ

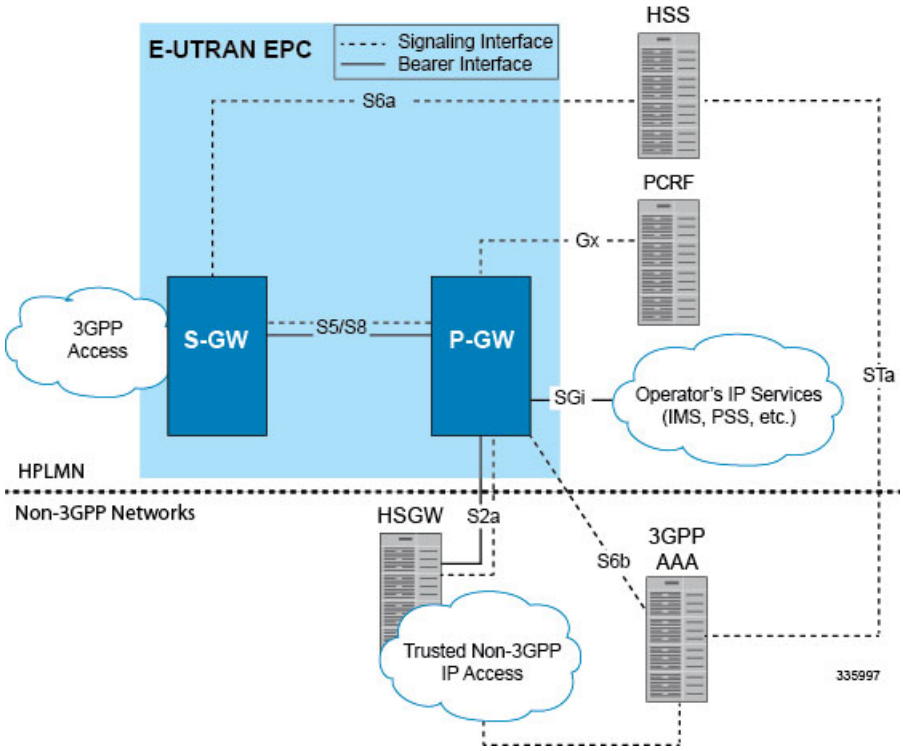
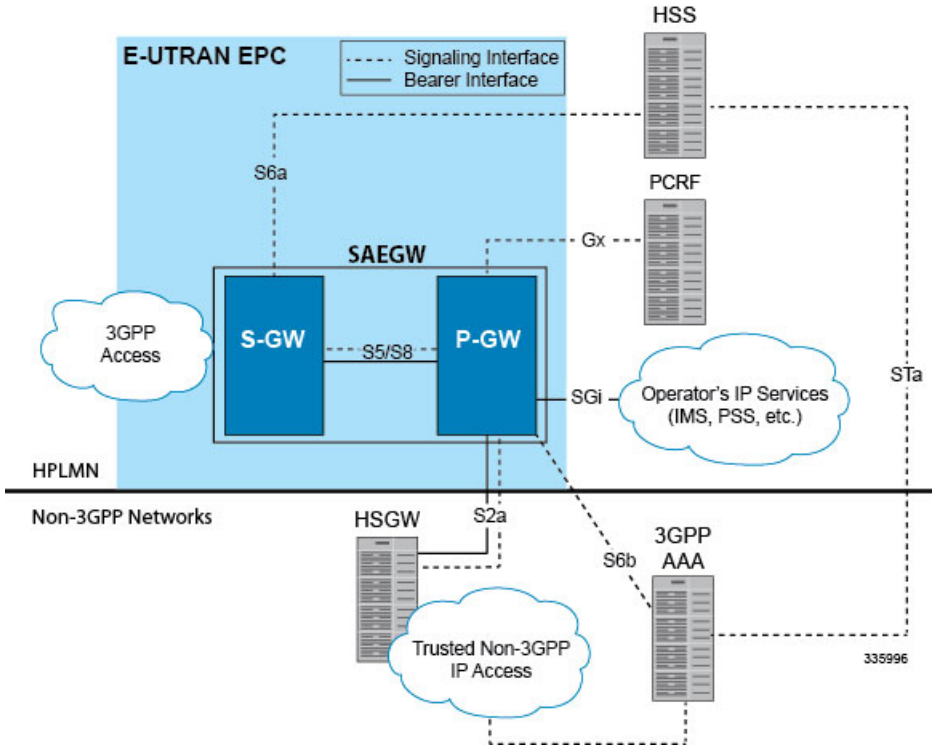


図 *52* : *SAEGW* の *S2a* インターフェイス アーキテクチャ



P-GW および SAEGW 上の S2a インターフェイスサポートの制限事項

P-GW および SAEGW 上の GTP ベースの S2a インターフェイス実装では、次の制限事項に注意してください。

- サポートされているアクセスタイプテクノロジーは、WiFi および LTE です。
- サポートされるインターフェイスは次のとおりです。
  - S6b
  - Gy
  - Rf
  - Gx
  - GTPv2

スタンドアロン P-GW S2a コールフロー

次のコールフロー図は、スタンドアロン P-GW アーキテクチャに展開されている場合の、S2a インターフェイスの基本機能を示しています。

図 *53* : スタンドアロン *P-GW* での *S2a* の初期接続

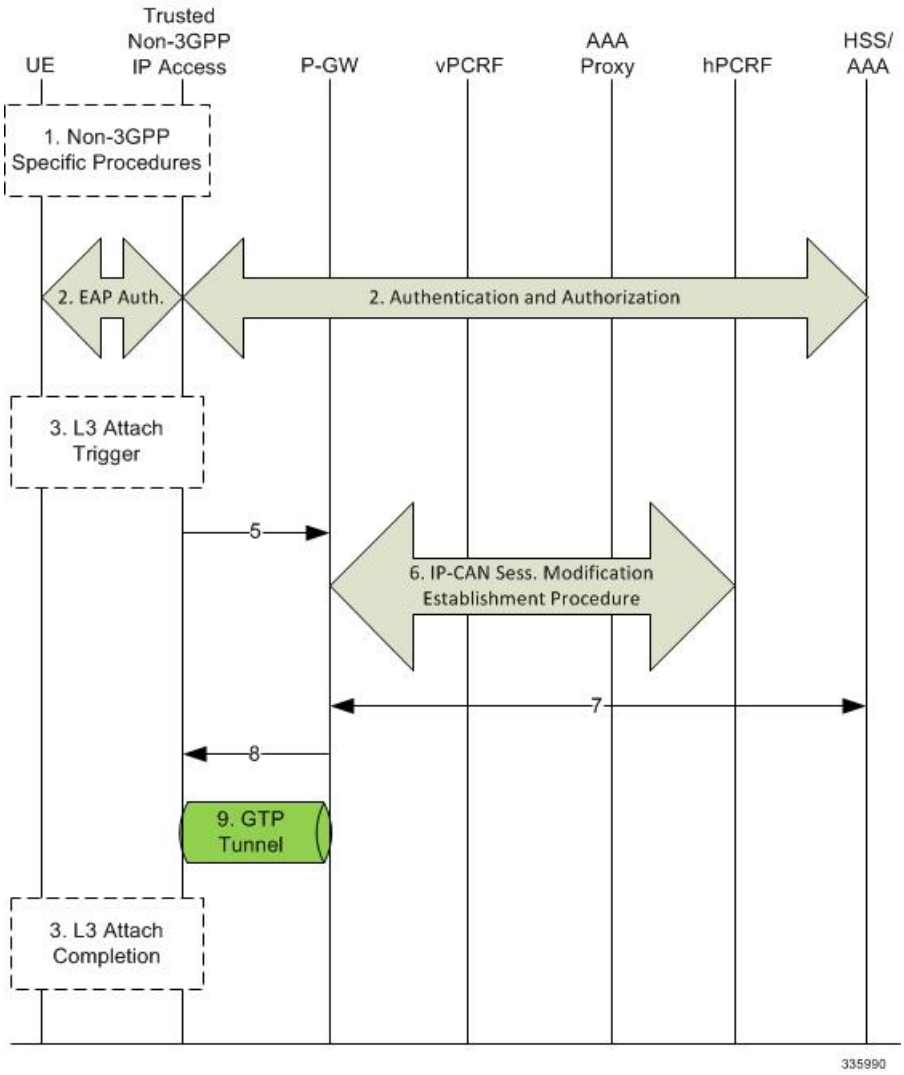


表 *65* : スタンドアロン *P-GW* での *S2a* の初期接続

ステップ	説明
1	
2	
3	
4	

ステップ	説明
5	信頼できる非 3GPP IP アクセスにより、セッション作成要求メッセージが P-GW に送信されます。RAT タイプは、非 3GPP IP アクセステクノロジータイプを示します。PDN タイプは、要求された IP アドレスタイプとサブスクリプション プロファイルに基づいて、E-UTRAN 初期接続時に PDN タイプが選択されたのと同じ方法で設定する必要があります。
6	P-GW が、PCRF を使用して IP-CAN セッション確立手順を開始します。
7	選択された P-GW が、その P-GW ID と、UE の PDN 接続に対応する APN を 3GPP AAA サーバーに通知します。メッセージには、PDN GW がある PLMN を識別する情報が含まれます。この情報は HSS に登録されます。
8	P-GW が、UE に割り当てられた IP アドレスを含むセッション作成応答メッセージを TWAN に返します。
9	GTP トンネルが TWAN と P-GW の間に設定されます。
10	初回接続が完了します。

図 *54* : スタンドアロン *P-GW* での *S2a LTE* から *Wi-Fi* へのハンドオーバー

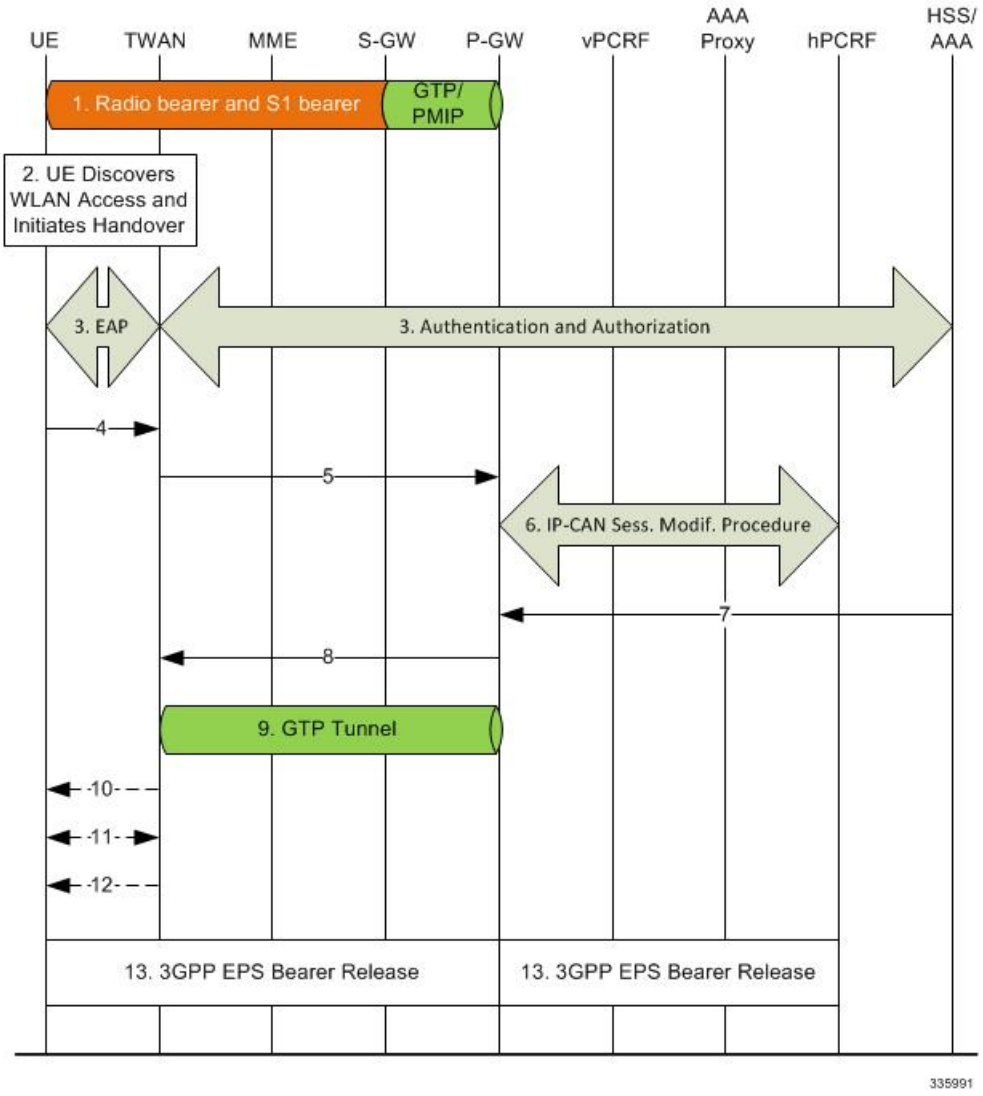


表 *66* : スタンドアロン *P-GW* での *S2a Wi-Fi* から *LTE* へのハンドオーバー

ステップ	説明
1	
2 ～ 4	UE が WLAN アクセスを検出し、ハンドオーバーを開始します。TWAN が AAA サーバーから許可を受け取ります。

ステップ	説明
5	TWAN が、セッション作成要求（IMSI、APN、RAT タイプ）メッセージを P-GW に送信します。RAT タイプ WLAN は、非 3GPP IP アクセステクノロジータイプを示します。TWAN は「ハンドオーバー指示」ビットを設定しません。代わりに、P-GW は、IMSI、APN、および RAT タイプに基づいて、TWAN からのハンドオーバーの可能性の有無を判断します。P-GW が、3GPP IP アクセスに接続されていたときに UE に割り当てられたのと同じ IPv4 アドレスまたは IPv6 アドレスを再度割り当てます。
6	P-GW が、RAT タイプが WLAN として PCRF を使用して PCEF 開始の IP-CAN セッション変更手順を実行します。
7	P-GW が、3GPP AAA サーバーに、P-GW ID と UE の PDN に対応する APN を通知し、3GPP AAA サーバーから承認情報を取得します。3GPP AAA サーバーは、認証フェーズで提供された UE 機能に従って、P-GW ID を更新するかどうかを決定します。
8	P-GW が、セッション作成応答を使用して TWAN に応答します。セッション作成応答には、UE が 3GPP IP アクセスに接続されている間に UE に割り当てられた IPv4 アドレスまたは IPv6 アドレスが含まれます。
9	GTP トンネルが TWAN と P-GW の間に設定されます。
10	
11	
12	
13	P-GW が、GTP-S5/S8 の TS 23.401 [6]、条項 5.4.4.1 で定義されている「P-GW 開始のベアラーの非アクティブ化」手順を開始します。

図 *55* : スタンドアロン *P-GW* での *S2a Wi-Fi* から *LTE* へのハンドオーバー

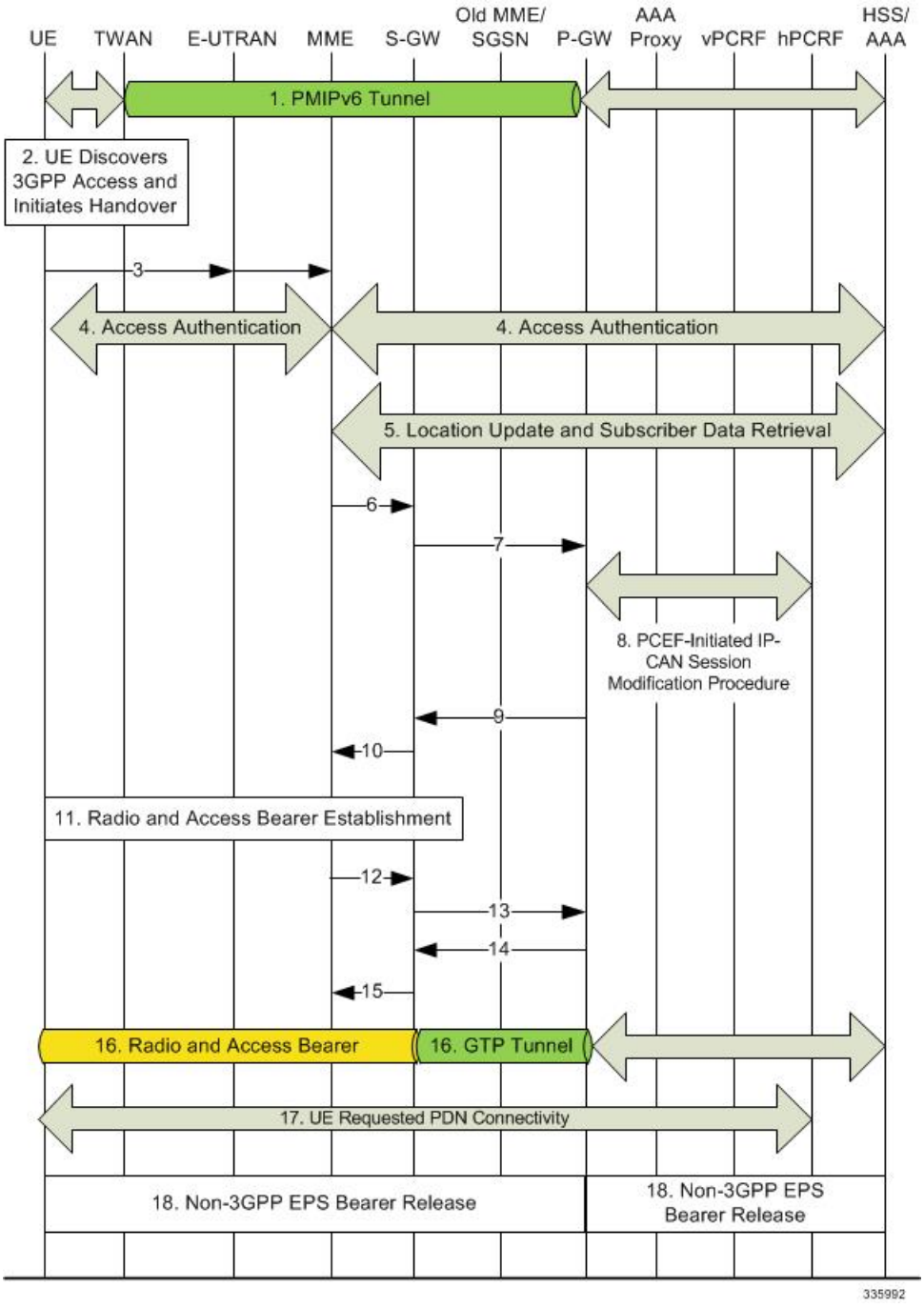


表 *67* : スタンドアロン *P-GW* での *S2a Wi-Fi* から *LTE* へのハンドオーバー

ステップ	説明
1	

ステップ	説明
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	

SAEGW S2a コールフロー

この項のコールフロー図は、SAEGW における S2a インターフェイスサポートの基本的な機能について説明しています。これには次のものが含まれます。

- 初期接続
- LTE から WiFi へのハンドオーバー
- Wi-Fi から LTE へのハンドオーバー

図 *56 : SAEGW* での *S2a* 初期接続

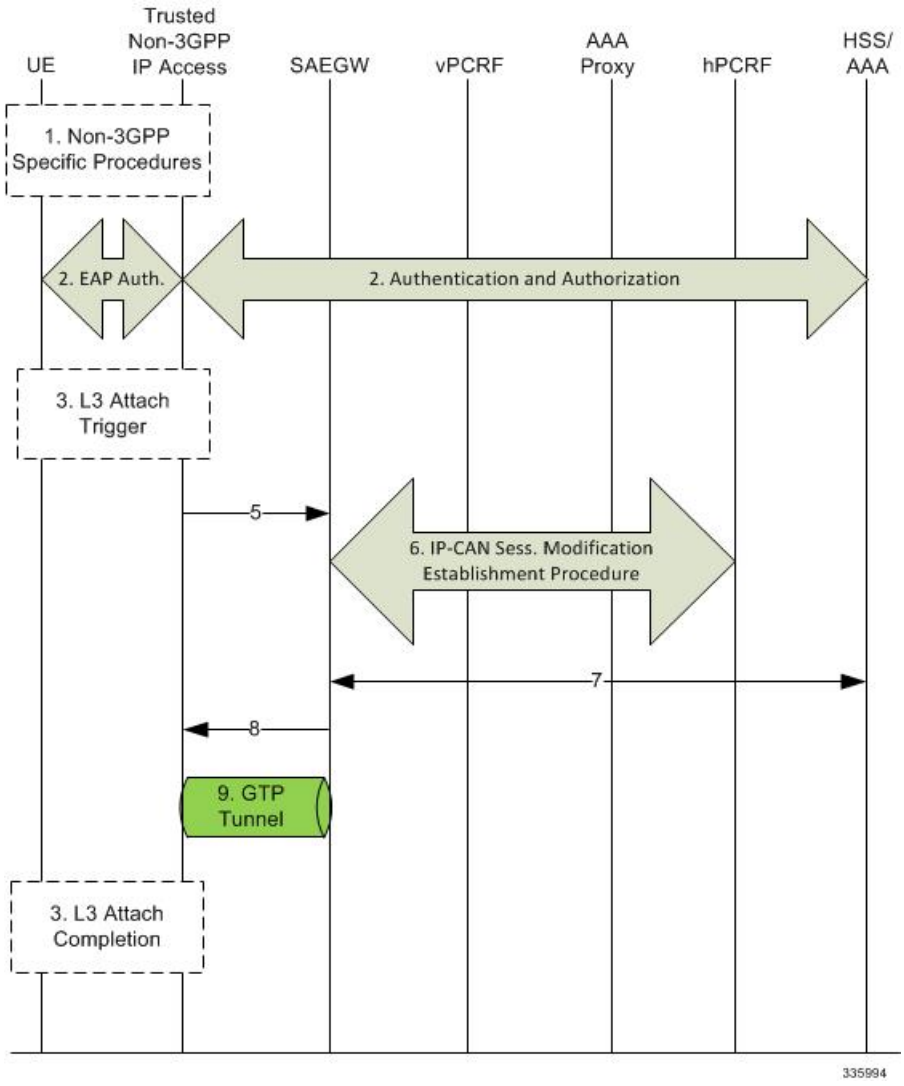


表 *68 : SAEGW* での *S2a* 初期接続

ステップ	説明
1	
2	
3	
4	

ステップ	説明
5	信頼できる非 3GPP IP アクセスにより、セッション作成要求（CSReq）メッセージが P-GW に送信されます。RAT タイプは、非 3GPP IP アクセステクノロジータイプを示します。PDN タイプは、要求された IP アドレスタイプとサブスクリプション プロファイルに基づいて、E-UTRAN 初期接続時に PDN タイプが選択されたのと同じ方法で設定する必要があります。 SAEGW の P-GW は、そのベアラー コンテキスト テーブルに新しいエントリを作成し、課金 ID を生成します。新しいエントリが作成されると、SAEGW の P-GW は、信頼できる非 3GPP IP アクセスネットワークとパケットデータネットワーク間でユーザープレーン PDU をルーティングし、課金プロセスを開始できます。
6	P-GW が、PCRF を使用して IP-CAN セッション確立手順を開始します。
7	SAEGW の選択された P-GW が、その P-GW ID と、UE の PDN 接続に対応する APN を 3GPP AAA サーバーに通知します。メッセージには、P-GW がある PLMN を識別する情報が含まれます。この情報は HSS に登録されます。
8	P-GW が、UE に割り当てられた IP アドレスを含むセッション作成応答（CSResp）メッセージを TWAN に返します。
9	GTP トンネルが TWAN と P-GW の間に設定されます。 初回接続が完了します。

図 *57 : SAEGW* での *S2a LTE* から *Wi-Fi* へのハンドオーバー

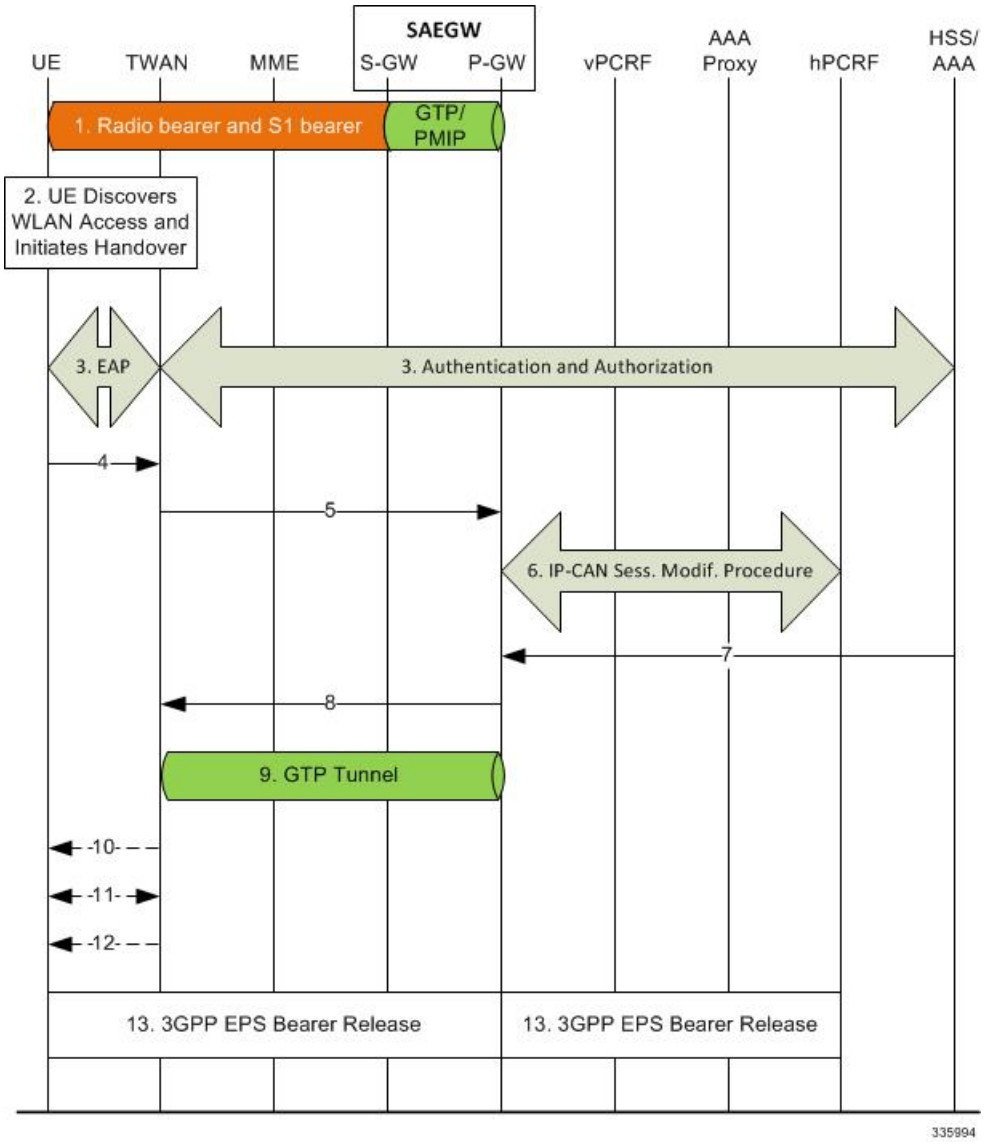


表 *69 : SAEGW* での *S2a LTE* から *Wi-Fi* へのハンドオーバー

ステップ	説明
1	
2 ～ 4	ステップ 2 ～ 4 では、UE が WLAN アクセスを検出し、ハンドオーバーを開始します。TWAN が AAA サーバーから許可を受け取ります。

ステップ	説明
5	TWAN が、セッション作成要求（IMSI、APN、RAT タイプなど）メッセージを SAEGW の P-GW に送信します。 RAT タイプ WLAN は、非 3GPP IP アクセステクノロジータイプを示します。TWAN は「ハンドオーバー指示」ビットを設定しません。代わりに、SAEGW の P-GW は、IMSI、APN、および RAT タイプに基づいて、TWAN からのハンドオーバーの可能性の有無を判断します。 SAEGW の P-GW が、3GPP IP アクセスに接続されていたときに UE に割り当てられたのと同じ IPv4 アドレスまたは IPv6 アドレスを再度割り当てます。
6	SAEGW の P-GW が、RAT タイプが WLAN として PCRF を使用して PCEF 開始の IP-CAN セッション変更手順を実行します。
7	SAEGW の P-GW が、3GPP AAA サーバーに、PDN GW ID および UE の PDN に対応する APN を通知し、3GPP AAA サーバーから承認情報を取得します。 3GPP AAA サーバーは、認証フェーズで提供された UE 機能に従って、PDN GW ID を更新するかどうかを決定します。
8	SAEGW の P-GW が、 セッション作成応答で TWAN に応答します。セッション作成応答には、UE が 3GPP IP アクセスに接続されている間に UE に割り当てられた IPv4 アドレスまたは IPv6 アドレスが含まれます。
9	GTP トンネルが TWAN と SAEGW の P-GW の間に設定されます。
10	
11	
12	
13	SAEGW の P-GW が、GTP-S5/S8 インターフェイスに関して TS 23.401 [6]、条項 5.4.4.1 で定義されている「P-GW 開始ベアラーの非アクティブ化」手順を開始します。

図 *58 : SAEGW* での *S2a WiFi* から *LTE* へのハンドオーバー

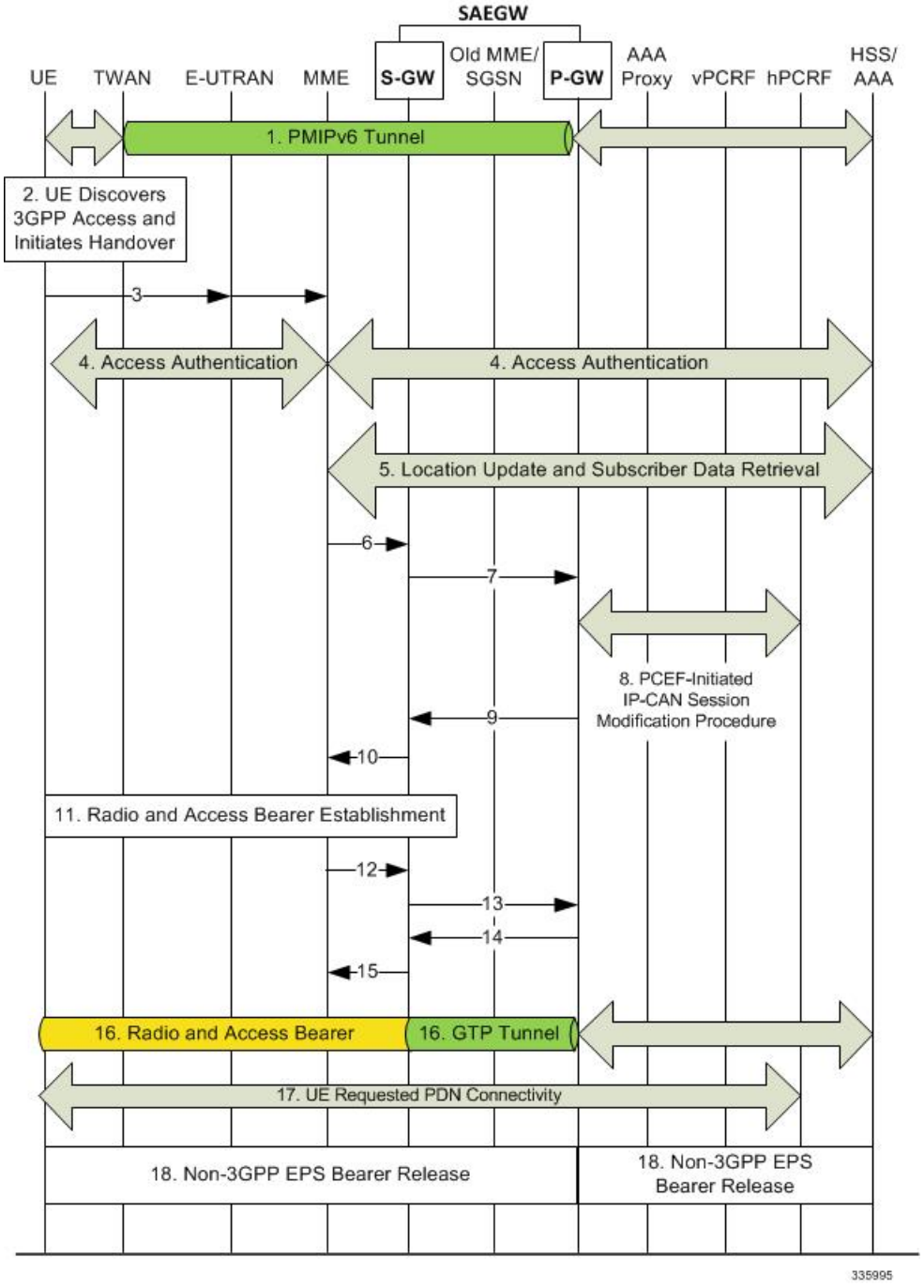


表 *70 : SAEGW* での *S2a WiFi* から *LTE* へのハンドオーバー

ステップ	説明
1	

ステップ	説明
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	

P-GW および SAEGW 上の GTP ベース S2b インターフェイスの設定

ここでは、GTP ベースの S2b インターフェイスサポート機能の設定方法を説明します。

GTP ベース S2b インターフェイスのサポートの設定

P-GW および SAEGW で GTP ベースの S2b インターフェイスのサポートを設定するには、次の例を使用します。

重要 P-GW および SAEGW での GTP ベースの S2a / S2b インターフェイスのサポートは、ライセンスで制御される機能です。ライセンスの詳細については、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

重要 **interface-type** コマンドを変更すると、親サービス（eGTP または GTP-U サービスが設定されているサービス）が自動的に再起動します。サービスを再起動すると、親サービスに関連付けられているアクティブコールがドロップされます。

```
config
   context ingress_context_name
      egtp-service egtp_service_name
         interface-type interface-pgw-ingress s2b
         end
```

次のコマンドを入力して、S2b インターフェイスサポートを無効にします。

```
config
   context ingress_context_name
      egtp-service egtp_service_name
         interface-type interface-pgw-ingress
         end
```

設定の確認

ここでは、P-GW および SAEGW での GTP ベースの S2a/S2b インターフェイス設定の確認方法について説明します。

Exec モードで **show configuration** コマンドを使用して、設定がアクティブであることを確認します。出力で、eGTP サービスの設定セクションを探します。

```
egtp-service EGTP
   interface-type interface-pgw-ingress s2a s2b
```

S2b ライセンスがインストールされ、アクティブになったら、Wi-Fi 初期接続コールを実行して、コールが正常に設定されたことを確認します。Exec モードで、**show subscribers all** コマンドを使用して、コールが成功したことを確認します。

GTP ベースの S2b インターフェイス機能のモニタリング

ここでは、通信事業者が P-GW および SAEGW で GTP ベースの S2b インターフェイス機能をモニターするために使用できるコマンドについて説明します。

GTP ベースの S2b インターフェイスの show コマンド

このセクションでは、GTP ベースの S2b インターフェイスをサポートするための show コマンドとその出力について説明します。

show pgw-service statistics all

スタンドアロン P-GW での S2b インターフェイスサポートの場合：このコマンドは、次の S2b インターフェイス機能の試行、失敗、および成功の回数に関する統計を提供します。

- S2bGTP から LTE へのハンドオーバー
- LTE から S2bGTP へのハンドオーバー

show subscribers epdg-address

このコマンドは、S2b インターフェイスを介して ePDG に接続されている S2b P-GW サブスクライバに関する情報を提供します。

show subscribers saegw-only epdg-address

このコマンドは、S2b インターフェイスを介して特定の ePDG に接続されている SAEGW の P-GW のサブスクライバに関連する情報を表示します。

show subscribers saegw-only interface-type S2bGTP

このコマンドは、S2b インターフェイスを介して接続された SAEGW の GTP P-GW サブスクライバに関連する情報を表示します。

show subscribers summary pgw-address

このコマンドにより、アクティブおよび休止中の GTP S2b IPv4 および IPv6 サブスクライバの数に関する情報が提供されます。

show subscribers pgw-only full all

スタンドアロン P-GW での S2b インターフェイスサポートの場合：このコマンドを使用して、P-GW サブスクライバの S2b コール関連情報を表示します。出力には、次の S2b 固有の情報が表示されます。

- インターフェイスタイプ（S2b PGW GTP-C インターフェイス）
- MAC アドレス
- ePDG c-teid（ePDG 制御トンネルエンドポイント識別子）
- ePDG u-teid（ePDG ベアラー トンネル エンドポイント識別子）
- ePDG c-addr（ePDG 制御 IP アドレス）
- ePDG u-addr（ePDG ベアラー IP アドレス）

show subscribers pgw-only epdg-address

スタンドアロン P-GW での S2b インターフェイスをサポートする場合：このコマンドを使用して、特定の ePDG の P-GW に存在するすべてのサブスクライバセッションの S2b 情報すべてを表示します。ePDG は ePDG アドレス（IPv4 または IPv6 アドレス形式）によって指定されます。

show subscribers summary epdg-address

スタンドアロンP-GWでのS2bインターフェイスサポートの場合：このコマンドを使用して、特定の ePDG の S2b インターフェイスに属する P-GW に存在するすべてのサブスクライバセッションの統計を表示します。ePDG は epdg-address によって指定されます。

show subscribers summary interface-type S2bGTP

スタンドアロン P-GW での S2b インターフェイスサポートの場合：S2b インターフェイスに属する P-GW 上のアクティブおよび休止中サブスクライバセッションの数が表示されます。

show subscribers saegw-only full all

SAEGW での S2b インターフェイスサポートの場合：このコマンドは、次のような P-GW サブスクライバの S2b コール関連情報を提供します。

- アクセステクノロジー
- インターフェイス タイプ
- アクセスポイントの MAC アドレス
- sgw c-teid
- ePDG c-teid
- sgw c-addr
- ePDG c-addr
- sgw u-teid
- ePDG u-teid
- sgw u-addr
- ePDG u-addr

show saegw-service statistics all function pgw

SAEGW での S2b インターフェイスサポートの場合：このコマンドは、以下を含むすべての P-GW SAEGW サービスのさまざまな S2bGTP ハンドオーバーの成功、失敗、および試行に関連する統計を提供します。

- S2bGTP から LTE へのハンドオーバー
  - 試行（Attempted）
  - 成功
  - 失敗しました（Failed）
- LTE から S2bGTP へのハンドオーバー
  - 試行（Attempted）

- 成功
- 失敗しました（Failed）

GTP ベースの S2a インターフェイス機能のモニタリング

ここでは、GTPベースのS2aインターフェイス機能をモニターする方法について説明します。

GTP ベースの S2a インターフェイスの show コマンド

ここでは、GTP ベースの S2a インターフェイスをサポートするための show コマンドとその出力について説明します。

show pgw-service statistics all

このコマンドの出力が拡張され、S2aGTP から LTE および LTE から S2aGTP のハンドオーバーに関する統計情報が提供されるようになりました。ハンドオーバー試行の合計回数のほかに、試行の成功回数と失敗回数が記録されます。

show saegw-service statistics all

このコマンドの出力には、S2aインターフェイス上のサブスクライバ、ベアラー、およびPDNに関連する情報が表示されます。

show saegw-service statistics all function-pgw

このコマンドの出力には、S2a インターフェイス上の SAEGW の P-GW 機能に関する、サブスクライバ、PDN、およびハンドオーバーの統計が表示されます。

show session-subsystem facility sessmgr service-type pgw-ingress

このコマンドの出力が拡張され、サブスクライバセッションの問題のトラブルシューティングと孤立したセッションの全般的なモニタリングのために、S2a インターフェイスのセッション情報が提供されるようになりました。キーワードを指定せずにこのコマンドを入力すると、表示される情報は、システムによって確立されたすべてのセッションの累積情報になります。

show subscribers pgw-only full all

このコマンドの出力が拡張され、アクセステクノロジー、TWAN、TEID 情報などの S2a コール関連情報が表示されるようになりました。

show subscribers saegw-only full all

このコマンドの出力には、S2a インターフェイスに関連するサブスクライバ情報（サブスクライバID情報、TEIDおよびアドレス情報、記録およびドロップされた入出力パケットなど）が含まれます。

show subscribers saegw-only interface-type S2aGTP

S2aGTP キーワードがこのコマンドに追加され、通信事業者がコールコード、コール ID、IMSI/IMEI、APN、アイドル時間など、S2a サブスクライバセッションの詳細情報を表示できるようになりました。

show subscribers summary interface-type S2aGTP

出力には、S2a インターフェイスを介して接続されたサブスクライバのインターフェイスタイプの詳細が示されます。出力には、S2a インターフェイスを介して接続されたサブスクライバのインターフェイスタイプの詳細が示されます。IPv4 インターフェイス、IPv6 インターフェイス、および IPv4v6 インターフェイスについて情報が提供されます。

show subscribers summary pgw-address

このコマンドの出力には、指定された P-GW の S2a サブスクライバ情報が含まれます。IPv4、IPv6、および IPv4v6 インターフェイスについてのインターフェイス情報が含まれます。



第 40 章

S6b インターフェイスの GTPv2 原因コードの変更

- 機能の概要と変更履歴 （703 ページ）
- 機能説明 （704 ページ）
- S6b 再試行コードの設定 （704 ページ）
- モニタリングおよびトラブルシューティング （704 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.24

機能説明

セッション作成応答の送信中に、S6b サービスが到達不能であるか、接続が不安定である場合、S6b インターフェイスは、既存の GTPv2 原因コード 92/0x5C（ユーザー認証の失敗）を原因コード 73/0x49（使用可能なリソースがない）に変更します。

S6b 再試行コードの設定

Diameter から S6b 再試行コードを適用するには、次の設定を使用します。

```
configure
   context context_name
      pgw-service service_name
         egtp { reject-cause { no-resource [ s6b-link-failure ] {
s6b-retry-code } }
         [ no | default ] egtp reject-cause no-resource
         end
```

注：

- **reject-cause**：reject-cause で応答を処理するオプションを設定します。
- **no-resource**：原因コード no-resource によるセッション作成応答の処理を設定します。
- **s6b-link-failure**：認証中に S6b サーバーの到達不能性に対して no-resource で応答します。
- **s6b-retry-code**：S6b Diameter 結果コードの 3002、3004、3005、および 5198 に対して no-resource で応答します。

モニタリングおよびトラブルシューティング

ここでは、各種 show コマンドとそれらの出力に関する情報を示します。

show コマンドと出力

show pgw-service name <pgw_service_name>

このコマンドの出力が強化され、以下のフィールドが追加されました。これらのフィールドは、S6b リンク障害および S6b 再試行コードに対する EGTP-C 原因コードマッピングが有効か無効かを示します。

- EGTP-C 原因コードのマッピング（S6b リンク障害）：有効または無効
- EGTP-C 原因コードマッピング（S6b 再試行コード）：有効または無効



第 41 章

P-GW、SAEGW、および S-GW における 3GPP R12 の GTP-C 負荷および過負荷制御のサポート

この章では、P-GW、SAEGW、および S-GW における 3GPP リリース 12 の GTP-C 負荷および過負荷制御機能について説明します。

- 機能説明 （707 ページ）
- 機能の仕組み （709 ページ）
- 3GPP R12 GTP-C 負荷制御プロファイルの作成と設定 （709 ページ）
- 3GPP R12 GTP-C 過負荷制御プロファイルの作成と設定 （715 ページ）
- 3GPP R12 GTP-C 負荷および過負荷制御機能のモニタリングと障害対応 （724 ページ）

機能説明

ここでは、3GPP R12 の GTP-C 負荷および過負荷制御機能について説明します。

重要 3GPP R12 の負荷および過負荷制御機能を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

3GPP R12 の GTP-C 負荷および過負荷制御機能はライセンス方式のオプション機能です。この機能により、GTP コントロールプレーンノードはピアの GTP コントロールプレーンノードに負荷情報を送信できます。受信側の GTP コントロールプレーン ピア ノードは、この情報を使用して P-GW と S-GW の既存の GW 選択プロシージャを強化します。負荷情報には、発信元の GTP コントロールプレーンノードのリソースの動作ステータスが反映されます。

GTP コントロールプレーンのシグナリングを使用するノードは、ピアノードで実行されるアクションを通じてノードの過負荷状態を軽減するために、過負荷制御情報の通信をサポートする場合があります。この機能は、GTPv2 コントロール プレーン プロトコルを介して S4、S11、S5、S8 インターフェイスでサポートされます。

GTP-C ノードが公称容量を超えて動作している場合に、そのノードは過負荷状態になっていると見なされ、結果としてパフォーマンスが低下します（着信トラフィックや発信トラフィック処理への影響もあります）。過負荷制御情報には、発信元ノードがそのような状況に達した日時が示されます。この情報が GTP-C ノード間で送信されると、これらのノード間の GTP-C シグナリングトラフィック量を削減またはスロットリングするために使用できます。このように過負荷制御情報によって、受信ノードが適切なアクションを決定するためのガイダンスが提供されるため、情報の送信側の負荷軽減につながります。

負荷制御と過負荷制御の概要は、次のように説明されます。

- **負荷制御**：負荷制御により、GTP-Cエンティティ（P-GW、SAEGW、S-GWなど）は負荷情報を GTP-C ピア（MME、SGSN、ePDG、TWAN など）に送信できます。これにより、同じ機能をサポートするエンティティ（S-GW クラスタなど）間で、有効な負荷に応じてセッション負荷を適宜分散させることができます。負荷情報には、GTP-Cエンティティリソースの動作ステータスが反映されます。
- **過負荷制御**：過負荷制御により、過負荷状態または過負荷状態になりつつある GTP-C エンティティで着信シグナリングの負荷を軽減できます。トラフィックを正常に処理するために使用できるシグナリング容量に従って、送信トラフィックを減らすように GTP-C ピアに指示します。GTP-Cエンティティがそのシグナリング容量を超えて動作すると過負荷状態になり、パフォーマンスが低下します（着信トラフィックや発信トラフィック処理への影響もあります）。

負荷および過負荷係数の計算機能の拡張

キャパシティテストおよびお客様のご利用環境において、sessmgr カードの CPU 使用率が高い場合でも、3GPP R12 の負荷および過負荷サポート機能が誤ったシャーシの負荷係数値を提供することが確認されました。根本原因は、sessmgr カードと demux カードの CPU 使用率の平均を取得して負荷係数が計算される際、demux カードの CPU 使用率が sessmgr カードの CPU 使用率を上回らないためです。そのため、sessmgr カードの CPU 使用率が高くても、システムは過負荷状態に移行しませんでした。

3GPP R12 負荷/過負荷制御プロファイル機能が強化され、CPU 負荷とメモリでは、同タイプのカードの大きいほうの値に基づいて負荷係数が計算されるようになりました。demux カードの CPU 使用率の値が sessmgr カードの CPU 使用率の値よりも高い場合、負荷係数の計算には demux カードの CPU 使用率の値が使用されます。

リソースマネージャに複数のポーリング間隔を設定するための新しい CLI コマンド **gtpc-system-param-poll interval** が導入されました。これにより、demuxmgr はさまざまなシステム要件に基づいて負荷係数を計算できます。

他の機能との関係

GTPP R12 GTP-C 負荷および過負荷制御機能を設定する前に、次の点に注意してください。

- GTP-C 負荷および過負荷制御を設定する前に、次のいずれかのサービスをノードで設定する必要があります。
  - P-GW
  - SAEGW

- S-GW

- 設定が完了したら、ネットワークで正しく機能するように、GTP-C 負荷および過負荷制御プロファイルを P-GW、SAEGW、または S-GW サービスに関連付ける必要があります。

機能の仕組み

ノードは、ノードレベルの負荷制御情報に必要なさまざまなパラメータ（ライセンスセッション使用率、システム CPU 使用率、システムメモリー使用率など）を定期的に取得します。取得後、ノードは、ユーザーが指定する重み係数に基づいて、またはデフォルトの重み係数を使用して、負荷および過負荷の制御情報それ自体を計算します。

ノードレベルの負荷制御情報は 30 秒ごとに計算されます。リソースマネージャは、システムレベルでシステム CPU 使用率とシステムメモリー使用率を計算します。

設定されているサービスごとに、負荷制御情報が異なる場合があります。これは、サービスライセンスごとにアクティブセッション数に重みを付けることで実現できます。たとえば、[（サービスごとのアクティブセッション数/サービスライセンスに許可された最大セッション数）* 100] とします。

ノードのリソースマネージャは、すべてのカードの CPU とメモリーの使用率を平均することにより、システムレベルでのシステム CPU 使用率とシステムメモリー使用率を計算します。この値は、個々のカードレベルで計算された値とは異なる場合があります。

3GPP R12 GTP-C 負荷制御プロファイルの作成と設定

この項では、3GPP R12 GTP-C 負荷制御プロファイルを作成および設定する方法について説明します。

コンフィギュレーションの概要

3GPP R12 GTP-C 負荷制御プロファイルの作成および設定手順は、以下のとおりです。

手順

ステップ 1 負荷制御プロファイルを作成します。GTPP R12 負荷制御プロファイルの作成（710 ページ） を参照してください。

ステップ 2 負荷制御の重み付けを設定します。3GPP R12 負荷制御プロファイルの重み付け設定の構成（710 ページ） を参照してください。

ステップ 3 負荷制御の包含頻度を設定します。3GPP R12 負荷制御プロファイルの包含頻度の設定（711 ページ） を参照してください。

ステップ 4 P-GW のみ。負荷制御しきい値を設定します。3GPP R12 負荷制御しきい値の設定（712 ページ） を参照してください。

ステップ 5 負荷制御情報の処理を設定します。3GPP R12 負荷制御情報の処理の設定 （712 ページ） を参照してください。

ステップ 6 負荷制御情報の公開を設定します。3GPP R12 過負荷制御情報のパブリッシングの設定 （712 ページ） を参照してください。

ステップ 7 3GPP R12 GTP-C ポーリングパラメータ間隔を設定します。3GPP R12 GTP-C パラメータポーリング間隔の設定 （713 ページ）を参照してください。

ステップ 8 負荷制御プロファイルを P-GW、SAEGW、または S-GW サービスと関連付けます。3GPP R12 負荷制御プロファイルと P-GW、SAEGW、または S-GW サービスとの関連付け。 （713 ページ） を参照してください。

ステップ 9 構成設定を確認します。3GPP R12 負荷制御設定の確認 （714 ページ） を参照してください。

ステップ 10 設定を保存します。「設定の保存 （715 ページ）」を参照してください。

GTPP R12 負荷制御プロファイルの作成

次の例を使用して、P-GW/SAEGW/S-GW で負荷制御プロファイルを作成します。

```
config
   gtpc-load-control-profile  profile_name
   end
```

注：

- プロファイル名前は、1 ～ 64 文字の英数字文字列である必要があります。
- 負荷制御プロファイルを作成したら、*GTP-C* 負荷制御プロファイル コンフィギュレーション モードが開始されます。

3GPP R12 負荷制御プロファイルの重み付け設定の構成

ここでは、GTP-C 負荷制御プロファイル設定の一部として、システム CPU、メモリ、およびライセンスセッションの使用率の重み付けパーセンテージを設定する方法について説明します。これらの設定は、このネットワーク要素の基本的な負荷制御プロファイルを構成します。これらのパラメータにより、P-GW/S-GW/SAEGW は、ピアの GTP コントロールプレーンノードに負荷情報を送信できます。受信側の GTP コントロールプレーンノードは、この情報を使用して GW と S-GW で既存の GW 選択プロシージャを強化します。負荷情報には、発信元の GTP コントロールプレーンノードのリソースの動作ステータスが反映されます。

P-GW/SAEGW/S-GW で負荷制御プロファイルの重み付けを設定するには、次の例を使用します。

```
config
   gtpc-load-control-profile  profile_name
  weightage  system-cpu-utilization percentage  system-memory-utilization
 percentage  license-session-utilization  percentage
   end
```

注：

- **system-cpu-utilization** *percentage*：システムの CPU 使用率の重みを 100 のパーセンテージとして設定します。

  percentage は 0 ー 100 の整数である必要があります。デフォルト値は 40 です。

- **system-memory-utilization** *percentage*：システムのメモリ使用率の重みを 100 のパーセンテージとして設定します。*percentage* は 0 ー 100 の整数である必要があります。デフォルトは 30 です。

- **license-session-utilization** *percentage*：ライセンスセッション使用率の重みを 100 のパーセンテージとして設定します。*percentage* は 0 ー 100 の整数である必要があります。デフォルトは 30 です。



重要 すべてのパラメータを指定する必要があります。3 つのパラメータ設定の合計は 100 である（100 を超えない）必要があります。

3GPP R12 負荷制御プロファイルの包含頻度の設定

ここでは、GTP-C 負荷制御プロファイル設定の負荷制御情報要素（LCI）の包含頻度を決定するパラメータの設定方法について説明します。LCI は、設定されたしきい値に達したときにピアに送信される 3GPP 固有の情報要素です。このパラメータは、通信事業者がノードのピアにこの情報を送信する頻度を指定します。

次の例を使用して、P-GW、SAEGW、および S-GW での負荷制御プロファイルの包含頻度を設定します。

```
config
   gtpc-load-control-profile  profile_name
      inclusion-frequency { advertisement-interval interval_in_seconds |
change-factor change_factor  }
      end
```

注：

- **inclusion frequency**：LCI の包含頻度を決定するパラメータを設定します。
- **advertisement-interval** *interval_in_seconds*：LCI のアドバタイズメント間隔を秒単位で設定します。これは、負荷制御情報をピアに送信する頻度を指定します。0 に設定した場合、ノードはピアに、すべての発信メッセージで負荷制御情報を送信します。*interval_in_seconds* は、0 ～ 3600 の整数にする必要があります。デフォルトは 300 です。

- **change-factor** *change_factor*：負荷制御プロファイルの変更係数を設定します。設定した係数によって負荷制御の変更係数が変わると、負荷の増減にかかわらず、負荷制御情報がピアに送信されます。この情報は、設定された係数により負荷係数が変更された場合にのみピアに送信されます。*change_factor* は、1 ～ 20 の整数である必要があります。デフォルトは 5 です。

3GPP R12 負荷制御しきい値の設定

ここでは、最初のノード選択時にP-GW実効重みを計算するためにP-GWが提供する負荷制御情報を使用する必要がある最小しきい値を設定する方法について説明します。

P-GW で負荷制御プロファイルしきい値を設定するには、次の例を使用します。

```
config
   gtpc-load-control-profile profile_name
      threshold time_in_seconds
      end
```

注：

- デフォルトのしきい値は 50 です。

3GPP R12 負荷制御情報の処理の設定

ホームまたは訪問先の PLMN の負荷制御情報の処理は、次の手順で有効または無効にできます。

SAEGW、S-GW、およびP-GWでの負荷制御プロファイル情報の処理を有効または無効にするには、次の例を使用します。

```
config
   gtpc-load-control-profile  profile_name
      load-control-handling { home | visited }
      no load-control-handling { home | visited }
      end
```

注：

- **no** により、指定されたオプションの負荷制御処理が無効になります。

3GPP R12 過負荷制御情報のパブリッシングの設定

ホームまたは訪問先の PLMN に対して、負荷制御情報のパブリッシングを有効または無効にすることができます。

P-GW/SAEGW/S-GW での負荷制御プロファイル情報のパブリッシングを有効または無効にするには、次の例を使用します。

```
config
   gtpc-load-control-profile  profile_name
      load-control-publishing { home | visited }
      no load-control-publishing { home | visited }
      end
```

注：

- **no** は、指定されたオプションの負荷制御プロファイル情報のパブリッシングを無効にします。

3GPP R12 GTP-C パラメータポーリング間隔の設定

キャパシティテストおよびお客様のご利用環境において、sessmgr カードの CPU 使用率が高い場合でも、3GPP R12 の負荷および過負荷サポート機能が誤ったシャーシの負荷係数値を提供することが確認されました。根本原因は、sessmgr カードと demux カードの CPU 使用率の平均を取得して負荷係数が計算される際、demux カードの CPU 使用率が sessmgr カードの CPU 使用率を上回らないためです。そのため、sessmgr カードの CPU 使用率が高くても、システムは過負荷状態に移行しませんでした。

3GPP R12 負荷/過負荷制御プロファイル機能が強化され、CPU 負荷とメモリでは、同タイプのカードの大きいほうの値に基づいて負荷係数が計算されるようになりました。demux カードの CPU 使用率の値が sessmgr カードの CPU 使用率の値よりも高い場合、負荷係数の計算には demux カードの CPU 使用率の値が使用されます。

StarOS リリース 21 以降、リソースマネージャに複数のポーリング間隔を設定するための新しい CLI コマンド **gtpc-system-param-poll interval** が、コンテキスト コンフィギュレーション モードに導入されました。これにより、demuxmgr はさまざまなシステム要件に基づいて負荷係数を計算できます。このコマンドは、リソースマネージャからシャーシレベルの CPU、メモリ、およびセッション数の情報をモニターする期間を設定します。

GTP-C ポーリング パラメータ間隔を設定するには、次の手順を実行します。

```
config
  context context_name
    gtpc-system-param-poll interval seconds
    default gtpc-system-param-poll interval
    end
```

- ここで、*seconds* は、リソースマネージャからシャーシレベルの CPU、メモリ、およびセッション数の情報をモニターする期間です。有効なエントリは、15 ～ 300 秒です。デフォルト設定は 30 秒です。
- **default** は、設定をデフォルト値の 30 秒に戻します。

⚠

注意 時間間隔を低い値に設定すると、システムパフォーマンスに影響を与える可能性があります。

3GPP R12 負荷制御プロファイルと P-GW、SAEGW、または S-GW サービスとの関連付け。

3GPP R12 GTP-C 負荷制御プロファイルが作成されたら、既存の P-GW、SAEGW、または S-GW サービスに関連付ける必要があります。

GTP-C 負荷制御プロファイルを既存の P-GW、SAEGW、または S-GW サービスに関連付けるには、次の例を使用します。

P-GW サービスの関連付け

```
configure
   context  context_name
      pgw-service pgw_service_name
         associate gtpc-load-control-profile profile_name
         no associate gtpc-load-control-profile
         end
```

注：

- **no** により、GTP-C 負荷制御プロファイルのサービス関係が無効になります。

S-GW サービスの関連付け

```
configure
   context  context_name
      sgw-service sgw_service_name
         associate gtpc-load-control-profile profile_name
         no associate gtpc-load-control-profile
         end
```

注：

- **no** により、GTP-C 負荷制御プロファイルのサービス関係が無効になります。

SAEGW サービスの関連付け

```
configure
   context context_name
      sgw-service sgw_service_name
         associate gtpc-load-control-profile profile_name
         exit
      pgw-service pgw_service_name
         associate gtpc-load-control-profile profile_name
         exit
      saegw-service saegw_service_name
         associate sgw-service sgw_service_name
         associate pgw-service pgw_service_name
         exit
```

3GPP R12 負荷制御設定の確認

負荷制御プロファイル構成設定を表示するには、次のコマンドを使用します。

show gtpc-overload-control-profile full name *load_control_profile_name*

このコマンドの出力には、以下を含むすべての負荷制御パラメータの構成設定が表示されます。

- 重み付け
- 包含頻度
- 負荷制御情報の処理
- 負荷制御情報の公開
- 負荷しきい値

設定の保存

EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

3GPP R12 GTP-C 過負荷制御プロファイルの作成と設定

この項では、P-GW/SAEGW/S-GW で 3GPP R12 GTP-C 過負荷制御プロファイルを作成および設定する方法について説明します。

コンフィギュレーションの概要

手順

ステップ 1 GTP-C 過負荷制御プロファイルを作成します。GTPP R12 過負荷制御プロファイルの作成 （716 ページ）を参照してください。

ステップ 2 重み付けを設定します。3GPP R12 過負荷制御重み付け設定の構成 （716 ページ） を参照してください。

ステップ 3 包含頻度を設定します。3GPP R12 過負荷制御の包含頻度の設定 （717 ページ） を参照してください。

ステップ 4 有効期間を設定します。3GPP R12 過負荷制御の有効期間の設定 （717 ページ） を参照してください。

ステップ 5 トレランスを設定します。3GPP R12 過負荷制御の許容限度の設定 （718 ページ） を参照してください。

ステップ 6 ノードのスロットリング動作を設定します。3GPP R12 過負荷制御スロットリング動作の設定 （718 ページ） を参照してください。

ステップ 7 メッセージの優先順位付けを設定します。3GPP R12 過負荷制御メッセージ優先順位付けの設定 （719 ページ） を参照してください。

ステップ 8 ノードの自己保護動作を設定します。3GPP R12 過負荷制御の自己保護動作の設定 （720 ページ） を参照してください。

ステップ 9 過負荷制御情報の処理を設定します。3GPP R12 過負荷制御情報の処理の設定 （720 ページ） を参照してください。

ステップ 10 過負荷制御情報の公開を設定します。3GPP R12 過負荷制御情報のパブリッシング （721 ページ） を参照してください。

ステップ 11 GTP-C ポーリングパラメータ間隔を設定します。3GPP R12 GTP-C パラメータポーリング間隔の設定 （713 ページ） を参照してください。

ステップ 12 過負荷制御設定を既存の P-GW/SAEGW/S-GW サービスに関連付けます。3GPP R12 過負荷制御設定と P-GW、SAEGW、または S-GW サービスとの関連付け （722 ページ） を参照してください。

ステップ 13 過負荷制御の設定を確認します。3GPP R12 過負荷制御設定の確認 （723 ページ） を参照してください。

ステップ 14　設定を保存します。「3GPP R12 過負荷制御の設定の保存 （723 ページ）」を参照してください。

GTPP R12 過負荷制御プロファイルの作成

GTP-C 過負荷制御プロファイルを作成するには、次の例を使用します。

```
configure
   gtpc-overload-control-profile  profile_name
   no gtpc-overload-control-profile  profile_name
   end
```

注：

- **no**：指定された GTP-C 過負荷制御プロファイルを削除します。
- *profile_name* は、1 ～ 64 文字の英数字文字列である必要があります。

3GPP R12 過負荷制御重み付け設定の構成

ここでは、GTP-C過負荷制御重み付けパラメータを設定する方法について説明します。これらのパラメータは、この GTP-C 過負荷制御プロファイルの基本設定を構成します。これらのパラメータの通信により、このネットワーク要素がいつ過負荷になりつつあるか、またはなっているかがピアに示されます。これが発生すると、NE は、トラフィックを正常に処理するために使用できるシグナリング容量に従って送信トラフィックを減らすようにピアに指示することで、着信シグナリングの負荷をグレースフルに軽減するようにピアに指示できるようになります。GTP-C エンティティがそのシグナリング容量を超えて動作すると過負荷状態になり、パフォーマンスが低下します（着信トラフィックや発信トラフィック処理への影響もあります）。

P-GW/SAEGW/S-GW で GTP-C 過負荷制御重み付け設定を構成するには、次の例を使用します。

```
configure
   gtpc-overload-control-profile  profile_name
     weightage system-cpu-utilization percentage system-memory-utilization
 percentage license-session-utilization percentage.
      default weightage
      end
```

注：

- 全パラメータの重みの合計は 100 である必要があります。
- **system-cpu-utilization** *percentage*：システムの CPU 使用率の重みを 100 のパーセンテージとして設定します。*percentage* は 0 ー 100 の整数である必要があります。デフォルト値は 40 です。
- **system-memory-utilization** *percentage*：システムのメモリ使用率の重みを 100 のパーセンテージとして設定します。*percentage* は 0 ー 100 の整数である必要があります。デフォルトは 30 です。

- **license-session utilization** *percentage*：ライセンスセッション使用率の重みを 100 のパーセンテージとして設定します。*percentage* は 0 ー 100 の整数である必要があります。デフォルトは 30 です。

3GPP R12 過負荷制御の包含頻度の設定

ここでは、GTP-C 負荷制御プロファイル設定の過負荷制御情報要素（OCI）の包含頻度を決定するパラメータの設定方法について説明します。OCI は、設定されたしきい値に達したときにピアに送信される 3GPP 固有の IE です。このパラメータは、通信事業者がピアにこの情報を送信する頻度を指定します。

次の例を使用して、P-GW、SAEGW、および S-GW での過負荷制御プロファイルの包含頻度を設定します。

```
configure
   gtpc-overload-control-profile  profile_name
      inclusion-frequency { advertisement-interval interval_in_seconds |
change-factor change_factor }
      default inclusion-frequency { advertisement-interval |
change-factor }
      end
```

注：

- **inclusion frequency**：OCI 情報要素の包含頻度を決定するパラメータを設定します。
- **advertisement-interval** *interval_in_seconds*：過負荷制御のアドバタイズメント間隔を秒単位で設定します。過負荷制御情報をピアに送信する頻度を指定します。0 に設定した場合、ノードはすべての発信メッセージでピアに過負荷制御情報を送信します。*interval_in_seconds* は 0 ～ 3600 の整数である必要があります。デフォルトは 300 です。
- **change-factor** *change_factor*：P-GW のみ。過負荷制御の変動係数を設定します。設定した係数によって過負荷制御の係数が変わると、その増減にかかわらず、過負荷制御情報がピアに送信される必要があります。この情報は、設定された係数により過負荷係数が変更された場合にのみピアに送信されます。*change_factor* は 1 ～ 20 の整数である必要があります。デフォルトは 5 です。

3GPP R12 過負荷制御の有効期間の設定

ここでは、過負荷制御の有効期間の設定方法について説明します。この有効期間は、後続の新しい過負荷制御情報によって上書きされない限り、過負荷制御の情報要素によって指定された過負荷条件が有効であると見なされる時間の長さです。

P-GW/SAEGW/S-GW で GTP-C 過負荷制御の有効期間を設定するには、次の例に示すコマンドを使用します。

```
configure
   gtpc-overload-control-profile profile_name
      validity-period seconds
```

```
      default validity-period
      end
```

注：

- **validity-period** *seconds*：過負荷制御情報の妥当性を設定します。*seconds* は、1 ～ 3600 の整数にする必要があります。デフォルトは 600 秒です。

3GPP R12 過負荷制御の許容限度の設定

GTP-C 過負荷制御の許容限度を設定するには、この例を使用します。

```
configure
   gtpc-overlaod-control-profile  profile_name
      tolerance { initial-reduction-metric percentage | threshold
report-reduction-metric percentage self-protection-limit percentage  }
      default tolerance { initial-reduction-metric | threshold }
      end
```

注：

- **initial-reduction-metric** *percentage*：過負荷許容下限に達したときにアドバタイズされる初期過負荷削減メトリック値を設定します。このパラメータでは、設定済みの最小しきい値に達した場合に、ノードがピアに着信トラフィックをどれだけ減らすことを求めるかを指定します。*percentage* は 1 ～ 100 の整数である必要があります。デフォルトは 10 です。
- **threshold report-reduction-metric** *percentage*：過負荷削減メトリックをピアにアドバタイズする最小過負荷許容しきい値を設定します。最小しきい値に達すると、ノードはこの情報をピアに報告します。上限に達すると、ノードは自己保護モードになります。*percentage* は 1 ー 100 の整数である必要があります。デフォルトは 80 です。
- **threshold report-reduction-metric** は常に **self-protection-limit** よりも小さくする必要があります。
- **self-protection-limit** *percentage*：ノードが自己保護モードに移行する過負荷許容しきい値を設定します。上限に達すると、ノードは、削除メッセージを除くすべての受信メッセージを拒否し始めます。ノードはピアへの新しいメッセージを一切発信しません。過負荷状態を軽減するためです。*percentage* は 1 ～ 100 の整数である必要があります。デフォルトは 95 です。

3GPP R12 過負荷制御スロットリング動作の設定

このコマンドを使用して、設定されたEARPを含む緊急イベントやメッセージの一部またはすべてを除外することにより、ピアの過負荷削減メトリックに基づくスロットリング動作を設定します。メッセージのスロットリングは初期メッセージにのみ適用されます。トリガーされた要求メッセージまたは応答メッセージはスロットリングしないでください。スロットリングすると、送信者によって対応する要求メッセージが再送信されることになるためです。

throttling-behavior が設定されている場合、プロファイルを S-GW サービスまたは P-GW サービスに関連付けることができます。P-GW 固有のキーワードが設定され、プロファイルが S-GW サービスに関連付けられている場合、S-GW は P-GW 固有の設定を無視します。S-GW または P-GW に固有のパラメータのみが使用されます。

P-GW/SAEGW/S-GW での GTP-C 過負荷制御スロットリング動作を設定するには、この例を使用します。

```
configure
   gtpc-overlaod-control-profile  profile_name
      throttling-behavior { earp [ 1 | 2 | 3 | 4 | 5 | 6 | 7 |8 | 9 |
10 | 11 | 12 | 13 | 14 | 15 ]* exclude } | emergency-events exclude }

      no throttling-behavior [ earp [ 1 |2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
 | 10 | 11 | 12 | 13 | 14 | 15 ]* exclude | emergency-events exclude ]

      end
```

注：

- **throttling-behavior**：ピアの過負荷削減メトリックに基づいてスロットリング動作を設定します。
- **earp**：ピアの過負荷削減メトリックによるスロットリングから、EARP が設定された特定のメッセージを除外します。EARP が設定されたベアラーが作成または更新された場合は、スロットリングから除外されます。
- *****：1 つのコマンド内で 1 つ以上のキーワードを入力できることを示します。
- **emergency-events exclude**：P-GW のみ。ピアの過負荷削減メトリックによるすべての緊急イベントをスロットリングから除外します。P-GW は、ピアから受信した過負荷情報に基づいてピアへのメッセージを減らす際に、緊急セッションのために送信されるイベントを除外します。

3GPP R12 過負荷制御メッセージ優先順位付けの設定

R12GTP-C過負荷制御機能では、メッセージの優先度に基づいて、（ピアが過負荷であることを示している場合）メッセージスロットリングを適用することができます。メッセージの優先順位付けを適用するには、各ノード（P-GW または ePDG）が生成することが想定される 2 つのグループのメッセージの割合を設定する必要があります。通信事業者は、各メッセージグループの予想されるメッセージ数をパーセンテージとして定義できます。

メッセージの優先順位付けを設定するには、次の例を使用します。

```
configure
   gtpc-overload-control-profile profile_name
      message-prioritization  group1 percentage group2 percentage
      no message-prioritization
      default message-prioritization
      end
```

注：

- **group1** は、次のメッセージのメッセージ優先度パーセンテージを指定します。
  - P-GW 入力から生成されるデフォルトベアラーのベアラー更新要求メッセージ
  - P-GW 入力から生成される専用ベアラーのベアラー更新要求メッセージ
  - ePDG 出力から生成されセッション作成ハンドオフ要求メッセージ
- **group2** は、次のメッセージのメッセージ優先度パーセンテージを指定します。
  - P-GW 入力から生成されるデフォルトベアラーのベアラー作成要求メッセージ
  - PDN 接続で要求される、ePDG 出力からのセッション作成要求メッセージ
- メッセージグループの合計パーセンテージは 100 と等しくなる必要があります。
- **group1** メッセージは最高の優先順位（1）を持ち、最後にドロップされます。**group2** メッセージは最低の優先順位（2）を持ち、最初にドロップされます。
- **default** は、グループメッセージの優先度設定をデフォルト値に戻します。各グループのデフォルトは 50 です。
- このコマンドのデフォルト動作は有効です。コマンドを無効にするには、**no** オプションを使用します。

3GPP R12 過負荷制御の自己保護動作の設定

通信事業者はこの機能を使用して、自己保護モードで APN 名と EARP 優先順位レベルの値を設定でき、システムが自己保護モードでも、緊急パケットデータノード（PDN）接続の着信要求メッセージや設定した EARP 優先順位値が拒否されないようにできます。

GTP-C 過負荷制御の自己保護動作を設定するには、次の例に示すコマンドを使用します。

```
configure
   gtpc-overload-control-profile profile_name
      self-protection-behavior { apn apn_name* exclude | earp { 1 | 2 |
3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15* } exclude } }

      no self-protection-behavior { apn apn_name* exclude | earp { 1 | 2
 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15* } exclude
} }
      end
```

注：

- **apn** は、自己保護動作で最大 3 つの APN 名を許可するように設定します。
- **earp** は、最大 3 つの EARP 優先順位レベル値を設定して、システムが自己保護モードの場合でも、設定された Evolved ARP の優先順位値の着信要求メッセージが拒否されないようにします。
- **no** は指定されたオプションを無効にします。

3GPP R12 過負荷制御情報の処理の設定

このコマンドを使用して、ホームまたは訪問先 PLMN の過負荷制御情報の処理を有効または無効にします。

```
configure
   gtpc-load-control-profile profile_name
      overload-control-handling { home | visited }
      no overload-control-handling { home | visited }
      default overload-control-handling
      end
```

注：

- **home**：ホーム PLMN の負荷制御情報の処理を有効にします。
- **visited** は、訪問先 PLMN の負荷制御情報の処理を有効にします。
- **default**：負荷制御の処理をデフォルトの動作（有効）に戻します。

3GPP R12 過負荷制御情報のパブリッシング

ホームまたは訪問先の PLMN に対する負荷制御情報のパブリッシングを有効または無効にします。

```
configure
   gtpc-overload-control-profile profile_name
      overload-control-publishing { home | visited }
      no overload-control-publishing { home | visited }
      default overload-control-publishing
      end
```

注：

- **home**：ホーム PLMN に対する負荷制御情報のパブリッシングを有効にします。
- **visited**：訪問先の PLMN に対する負荷制御情報のパブリッシングを有効にします。
- **default**：負荷制御の処理をデフォルトの動作（有効）に戻します。

3GPP R12 GTP-C パラメータポーリング間隔の設定

キャパシティテストおよびお客様のご利用環境において、sessmgr カードの CPU 使用率が高い場合でも、3GPP R12 の負荷および過負荷サポート機能が誤ったシャーシの負荷係数値を提供することが確認されました。根本原因は、sessmgr カードと demux カードの CPU 使用率の平均を取得して負荷係数が計算される際、demux カードの CPU 使用率が sessmgr カードの CPU 使用率を上回らないためです。そのため、sessmgr カードの CPU 使用率が高くても、システムは過負荷状態に移行しませんでした。

3GPP R12 負荷/過負荷制御プロファイル機能が強化され、CPU 負荷とメモリでは、同タイプのカードの大きいほうの値に基づいて負荷係数が計算されるようになりました。demux カードの CPU 使用率の値が sessmgr カードの CPU 使用率の値よりも高い場合、負荷係数の計算には demux カードの CPU 使用率の値が使用されます。

StarOS リリース 21 以降、リソースマネージャに複数のポーリング間隔を設定するための新しい CLI コマンド **gtpc-system-param-poll interval** が、コンテキスト コンフィギュレーション モードに導入されました。これにより、demuxmgr はさまざまなシステム要件に基づいて負荷

係数を計算できます。このコマンドは、リソースマネージャからシャーシレベルのCPU、メモリ、およびセッション数の情報をモニターする期間を設定します。

GTP-C ポーリング パラメータ間隔を設定するには、次の手順を実行します。

```
config
  context context_name
    gtpc-system-param-poll interval seconds
    default gtpc-system-param-poll interval
    end
```

- ここで、*seconds*は、リソースマネージャからシャーシレベルのCPU、メモリ、およびセッション数の情報をモニターする期間です。有効なエントリは、15～300秒です。デフォルト設定は 30 秒です。
- **default** は、設定をデフォルト値の 30 秒に戻します。

⚠

注意 時間間隔を低い値に設定すると、システムパフォーマンスに影響を与える可能性があります。

3GPP R12 過負荷制御設定と P-GW、SAEGW、または S-GW サービスとの関連付け

3GPP R12 過負荷制御プロファイルが設定されたら、既存の P-GW、SAEGW、または S-GW サービスに関連付ける必要があります。

過負荷制御設定を既存のサービスに関連付けるには、次の例を使用します。

P-GW サービスの関連付け

```
configure
   context context_name
      pgw-service pgw_service_name
         associate gtpc-overload-control-profile profile_name
         no associate gtpc-overload-control-profile
         end
```

注：

- **no** により、GTP-C 負荷制御プロファイルのサービス関係が無効になります。

S-GW サービスの関連付け

```
configure
   context context_name
      sgw-service sgw_service_name
         associate gtpc-overload-control-profile profile_name
         no associate gtpc-overload-control-profile
         end
```

注：

• **no** により、GTP-C 負荷制御プロファイルのサービス関係が無効になります。

SAEGW サービスの関連付け

```
configure
   context context_name
      sgw-service sgw_service_name
         associate gtpc-overload-control-profile profile_name
         exit
      pgw-service pgw_service_name
         associate gtpc-overload-control-profile profile_name
         exit
      saegw-service saegw_service_name
         associate sgw-service sgw_service_name
         associate pgw-service pgw_service_name
         exit
```

3GPP R12 過負荷制御設定の確認

過負荷制御設定の設定内容を表示するには、次のコマンドを使用します。

show gtpc-overload-control-profile full name *overload_control_profile_name*

このコマンドの出力には、以下を含む過負荷制御プロファイル設定のすべての設定内容が表示されます。

- 重み付け
- 許容値
- 包含頻度
- 有効期間
- スロットリングプロファイル
- 自己保護動作
- 過負荷制御情報の処理
- 過負荷制御情報の公開
- メッセージの優先順位付け

3GPP R12 過負荷制御の設定の保存

EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイスや、ネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

3GPP R12 GTP-C 負荷および過負荷制御機能のモニタリングと障害対応

ここでは、3GPP R12 GTP-C 負荷および過負荷制御機能をモニターする通信事業者を支援する情報を提供します。

3GPP R12 GTP-C 負荷および過負荷 Show コマンド

このセクションでは、3GPP R12 負荷および過負荷制御機能のサポートにおける show コマンドについて説明します。

show egtpc statistics egtp-service <egtp-service name>

このコマンドの出力では、送信（TX）および受信（RX）された 3GPP R12 の負荷および過負荷制御プロファイルの詳細な統計情報が提供されます。統計情報は EGTP サービスごとに提供されます。

show gtpc-load-control-profile full all

このコマンドの出力には、ノードに設定されているすべての 3GPP R12 負荷制御プロファイルのすべての設定が表示されます。このコマンドを使用して、負荷制御プロファイルが意図したとおりに設定されているかどうかを判定します。

show gtpc-load-control-profile full name <name>

このコマンドを使用して、指定された 3GPP R12 負荷制御プロファイルのすべての構成設定を表示します。

show gtpc-overload-control-profile full all

このコマンドの出力には、ノードに設定されているすべての 3GPP R12 過負荷制御プロファイルのすべての設定が表示されます。このコマンドを使用して、過負荷制御プロファイルが意図したとおりに設定されているかどうかを判定します。

show gtpc-overload-control full name <name>

このコマンドの出力には、ノードに設定されているすべての 3GPP R12 過負荷制御プロファイルのすべての設定が表示されます。このコマンドを使用して、過負荷制御プロファイルが意図したとおりに設定されているかどうかを判定します。

show pgw-service all

P-GW に設定されているすべての 3GPP R12 負荷制御プロファイルおよび 3GPP R12 過負荷制御プロファイルの名前を取得するには、このコマンドを使用します。

show sgw-service all

このコマンドを使用して、S-GW に設定されているすべての 3GPP R12 負荷制御プロファイルおよび過負荷制御プロファイルの名前を取得します。

eGTP-C バルク統計

3GPP R12 の負荷および過負荷制御機能をサポートするために、次の統計情報が eGTP-C スキーマに含まれています。

- load-overload-own-lci
- load-overload-own-oci
- load-overload-num-msg-throttled
- load-overload-num-ovrload-cond-reached

これらの変数の詳細については、『*Statistics and Counters Reference*』の「eGTP Schema Statistics」を参照してください。



第 42 章

Gx インターフェイスのサポート

この章では、サブスクライバのポリシーと課金制御をサポートする Gx インターフェイスの設定について説明します。

IMS サービスは、アクセスサポートとは無関係に、音声、ビデオ、およびデータの転送に関するアプリケーションサポートを提供します。ローミング IMS サブスクライバには、他の機能とは別に、必要十分で中断のない一貫性のあるシームレスなユーザーエクスペリエンスがアプリケーションセッション中に必要になります。また、使用されている特定の IMS アプリケーションによって消費されるリソースの料金のみがサブスクライバに請求されることも重要です。

この章に記載する手順を実行する前に、本アドミニストレーション ガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

この章の内容は、次のとおりです。

- Rel. 7 Gx インターフェイス （727 ページ）
- Rel. 8 Gx インターフェイス （756 ページ）
- Rel. 9 Gx インターフェイス （781 ページ）
- Rel. 10 Gx インターフェイス （791 ページ）
- サポートされる Gx 機能 （800 ページ）

Rel. 7 Gx インターフェイス

Rel. 7 Gx インターフェイスのサポートは、次の製品向けの Cisco ASR シャーシで利用できます。

- GGSN
- IPSG

ここでは、次の内容について説明します。

- はじめに （728 ページ）
- 用語および定義 （731 ページ）

• Rel. 7 Gx の動作 （747 ページ）
• Rel. 7 Gx インターフェイス （750 ページ）
• 統計情報の収集 （755 ページ）

はじめに

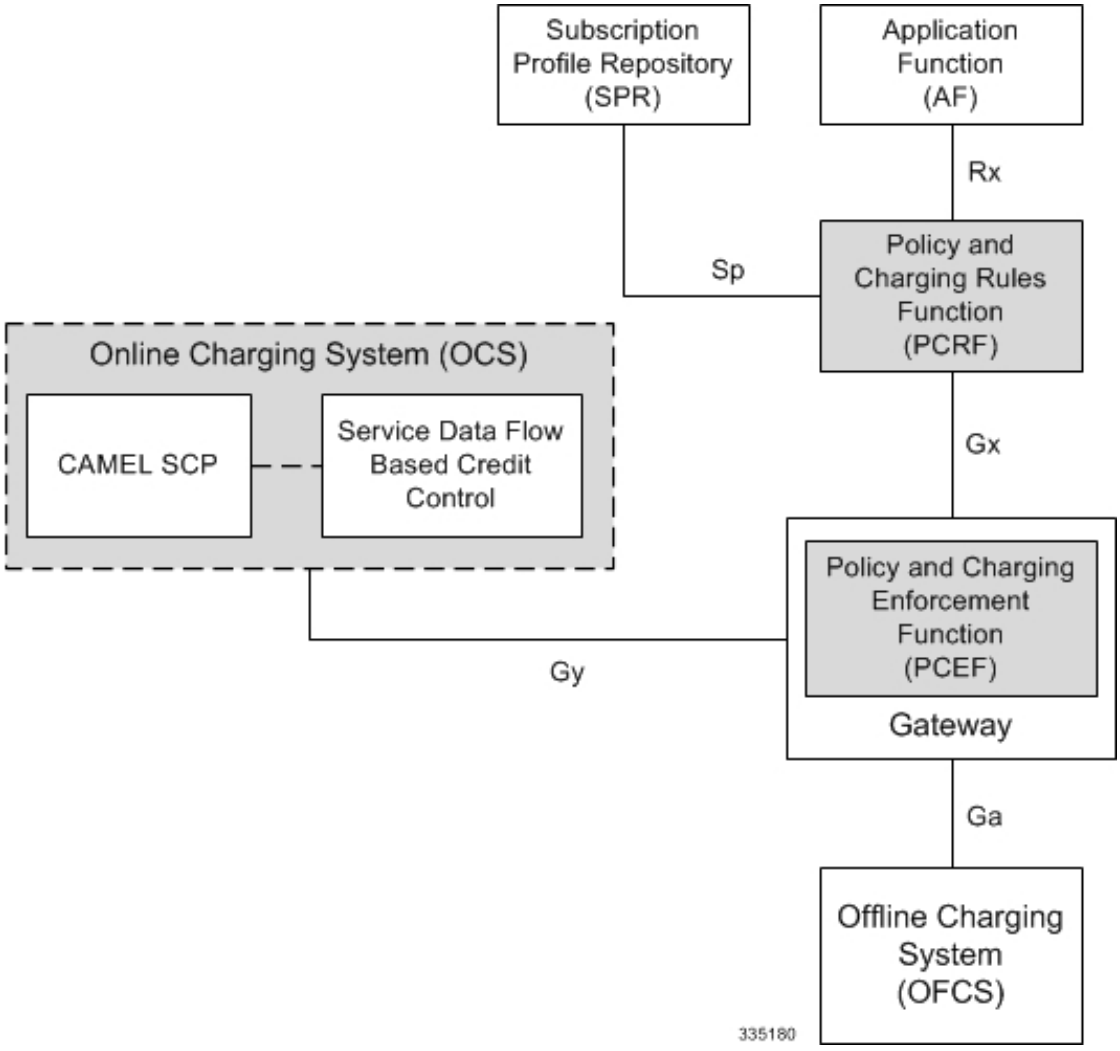
GPRS/UMTS ネットワークでの IMS 展開の場合、システムはポリシーベースのアドミッションコントロールのサポートおよびフローベース課金にリリース 7 Gx インターフェイスを使用します。Rel. 7 Gx インターフェイスは、ゲート設定、帯域幅制限などのポリシー制御適用機能をサポートし、フローベース課金もサポートします。これは、動的にプロビジョニングされたポリシー制御および課金（PCC）ルールによって実現されます。これらの PCC ルールは、サービスデータフロー（SDF）を識別し、課金を実行するために使用されます。ルールに関連付けられているその他のパラメータは、ポリシー制御を適用するために使用されます。

通信事業者は PCC アーキテクチャを利用することで、サービスベースの QoS ポリシーとフローベース課金制御を実行できます。PCC アーキテクチャでは、これは主にポリシーおよび課金適用機能（PCEF）/Cisco Systems GGSN とポリシーおよび課金ルール機能（PCRF）によって実現されます。

GPRS/UMTS ネットワークでは、クライアント機能は GGSNに付属しているため、IMS 承認のシナリオではゲートウェイとも呼ばれます。次の図では、ゲートウェイは Cisco Systems GGSN であり、PCEF 機能は Enhanced Charging Service（ECS）によって提供されます。Rel 7. Gx インターフェイスは、Diameter 接続として導入されます。Gx メッセージには、ほとんどの場合、ダイナミックルールのインストール/変更/削除と、事前定義されたルールのアクティブ化/非アクティブ化が含まれます。

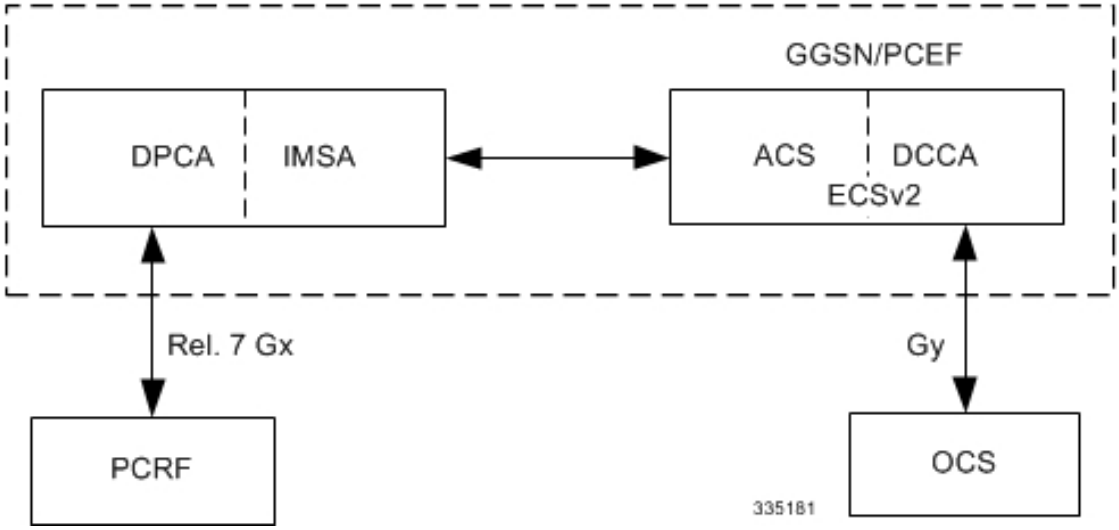
Rel. 7 Gx 参照ポイントは、ゲートウェイと PCRF の間にあります。この参照ポイントは、PCRF からゲートウェイへの PCC ルールのプロビジョニングと削除、およびゲートウェイから PCRF へのトラフィック プレーン イベントの送信に使用されます。Gx 参照ポイントは、アプリケーションに関連する AVP を適用することで、課金制御とポリシー制御のいずれかまたは両方に使用できます。次の図は、ポリシーおよび課金アーキテクチャに含まれるさまざまな要素間の参照ポイントを示します。

図 *59 : PCC* 論理アーキテクチャ



ゲートウェイ内では、IMSA モジュールと DPCA モジュールが（SessMgr で）Gx プロトコル関連の機能を処理し、ポリシーの適用と課金は ECS で行われます。Gy プロトコル関連の機能は、DCCA モジュール内（ECS）で処理されます。次の図は、ゲートウェイ内のコンポーネント間の連携動作を示しています。

図 *60 : Cisco PCEF* 内の *PCC* アーキテクチャ



サポート対象のネットワークとプラットフォーム

この機能は、コアネットワークサービスのGGSNサービスを実行しているすべてのシャーシでサポートされています。

ライセンス要件

Rel. 7 Gxインターフェイスのサポートは、ライセンス供与されたシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

サポートされる標準

Rel 7. Gx インターフェイスのサポートは、次の標準と RFC に基づいています。

- 3GPP TS 23.203 V7.6.0（2008-03）：3rd Generation Partnership Project、Technical Specification Group Services and System Aspects、Policy and charging control architecture（Release 7）
- 3GPP TS 29.212 V7.8.0（2009-03）：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control over Gx reference point（Release 7）
- 3GPP TS 29.213 V7.4.0（2008-03）：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control signalling flows and QoS parameter mapping（Release 7）
- RFC 3588、Diameter Base Protocol。2003 年 9 月
- RFC 4006、Diameter Credit-Control Application。2005 年 8 月

用語および定義

このセクションでは、Rel. 7 Gx に関連した機能と用語について説明します。

ポリシー制御

PCRF が IP-CAN ベアラーの制御方法を PCEF に指示するプロセス。

ポリシー制御は、次の機能で構成されます。

- **バインド**：バインドとは、サービスデータフロー（SDF）と、そのSDFを転送するIP CANベアラー（GPRS の場合は PDP コンテキスト）との間の関連付けの生成です。

  PCC ルールの QoS 要求と SDF テンプレートがベアラーバインドの入力になります。選択されたベアラーには、PCC ルールで示されているものと同じ QoS クラスが割り当てられます。

  IP-CANのタイプとベアラー制御モードに応じて、ベアラーバインドはPCRF、またはPCRFと PCEF の両方によって実行できます。

  - UE 専用 IP-CAN ベアラー確立モードの場合、PCRF がベアラーバインドを実行します。PCRFがベアラーバインドを実行する場合、ベアラーIDによってベアラー（PDPコンテキスト）が示されます。ベアラー ID で、PDP セッション内のベアラーが一意に識別されます。
  - UE/NW IP-CAN ベアラー確立モードの場合、PCRF はユーザー制御サービスの PCC ルールのバインドを実行し、PCEFはネットワーク制御サービスのPCCルールのバインドを実行します。

  PCEF ルールのバインドは、RAR や CCA-U などの PCRF メッセージで、「bearer-ID」なしで EPS IP-CAN ベアラーに対して BCM モードが UE のみに設定されている場合に成功します。

  3G から 4G へのハンドオーバーのシナリオでは、ルールバインドとルール削除はUE専用モードで正常に行われます。この変更/インストール/削除によるフィルタ（および関連情報）の変更は、UE専用モードでの更新としてUEに通知されず、UEに送信できません。これらのルールは課金のみに関して考慮されます。フィルタ（および関連情報）をUEに通知できるように、同じルールが 4G で再度変更されることが期待されます（ハンドオーバーが行われた場合）。

  GnGp HO シナリオ中にコリジョンが発生すると、CCR-U が生成され、ルール障害を報告するために PCRF に送信されます。

  この追加の Gx メッセージ（CCR-U）がトリガーされると、RAT_TYPE トリガーが有効になっている場合、複数のCCR-Uを設定する必要が生じます。設定しない場合、HO中にコリジョンが発生するたびにサブスクライバコールがドロップされます。

- **ゲート制御**：ゲート制御とは、SDFに属するパケットが目的のエンドポイントに向かってパススルーすることをブロックまたは許可することです。ゲートはPCCルール内で記述され、ゲート制御はSDFごとに適用されます。ゲートを開閉するコマンドを実行すると、対応するIPパケットの経路が有効または無効になります。ゲートが閉じられている場合、

関連する IP フローのすべてのパケットがドロップされます。ゲートが開いている場合、関連する IP フローのパケットの転送が許可されます。

- **イベントレポート**：イベントレポートは、ユーザープレーンでの新しい動作をトリガーするアプリケーションイベントの通知とこうしたイベントへの応答、およびゲートウェイ（PCEF）のリソースに関連したイベントのレポートです。
  - イベントトリガーを使用して、どの IP-CAN セッション変更や特定のイベントが発生すると、PCEF が PCC ルールを再要求するかを確認できます。PCEF から PCRF へのイベントトリガーレポートは、特定のイベントに応じて IP CAN セッションまたはベアラーに適用できますが、イベントトリガーのプロビジョニングはセッションレベルで行われます。

    イベントトリガーが不明なRARは動作を発生させずに無視され、DIAMETER_SUCCESSで応答されます。
  - イベントレポート機能（ERF）は、PCC ルールのプロビジョニング中に PCRF からイベントトリガーを受信し、イベントトリガー検出を実行します。受信したイベントトリガーに一致するイベントが発生すると、ERF は発生したイベントを PCRF に報告します。提示されたイベントトリガーが特定のパラメータ値に関連付けられている場合、ERF はそれらの値を PCRF への応答に含めます。イベントレポート機能を備えているのは PCEF です。

    SUCCESSFUL_RESOURCE_ALLOCATION (22) イベントトリガーは、次の条件で送信されます。
    - ルールが正常にインストールされた場合（およびイベントトリガーが PCRF によって導入され、resource-allocation-notification が有効になった場合）。
    - 部分的に失敗した場合、つまり、2 つ以上のルールがインストールされ、少なくとも 1 つのルールが正常にインストールされた場合。（およびイベントトリガーが PCRF によって導入され、resource-allocation-notification が有効になった場合）。

    完全に失敗した場合、つまり、ルールが 1 つもインストールされていない場合、イベントトリガー SUCCESSFUL_RESOURCE_ALLOCATION (22) は送信されません。

重要 このリリースでは、イベントトリガー「IP-CAN_CHANGE」および「MAX_NR_BEARERS_REACHED」はサポートされていません。

- **QoS 制御**：QoS 制御とは、SDF または IP-CAN ベアラーまたは QoS クラス識別子（QCI）に許可される最大 QoS の承認と適用のことです。複数の SDF の集約（GPRS の場合は PDP コンテキスト）の場合、個々の SDF の承認済み QoS 情報の組み合わせが、この集約の承認済み QoS として提供されます。
  - SDF ごとの QoS 制御により、PCC アーキテクチャは、特定の SDF ごとに適用される承認済み QoS を PCEF に提供できます。

- IP-CAN ベアラーの承認済み QoS の適用により、UE 開始 IP-CAN ベアラーの確立または変更の一環として、ゲートウェイ（PCEF）によって要求されたベアラー QoS のダウングレードまたはアップグレードが発生する可能性があります。また、オペレータのポリシーとネットワーク機能によっては、承認済み QoS の適用により、ネットワーク開始 IP-CAN ベアラーの確立または変更が発生する場合もあります。PCRF が IP-CAN ベアラーと PCC ルールの両方に承認済み QoS を提供する場合、個々の PCC ルールの承認済み QoS の適用が最初に実行されます。
- QoS 承認情報は、PCRF によって動的にプロビジョニングされる場合と、PCEF で事前定義された PCC ルールである場合があります。PCRF が PCC ルールを動的に提供する場合は、IP-CAN ベアラーに承認済み QoS 情報（統合された QoS）を提供できます。PCEF 内の事前定義された PCC ルールの場合、承認された QoS 情報は PCC ルールがアクティブになると有効になります。PCEF では、承認済み QoS 情報のさまざまなセット（PCRF から受信した情報と、事前定義された PCC ルールに対応する情報）が組み合わされます。PCRF は、事前定義された PCC ルールの承認済み QoS 情報を認識し、それらのルールをアクティブ化する際に、この情報を考慮します。これにより、PCRF によってアクティブ化される一連の PCC ルールの組み合わせによる承認済み QoS が、それらの PCC ルールが動的に提供されるか、事前定義されているか、またはその両方であるかに関係なく、サブスクリプションポリシーとオペレータポリシーによって指定された制限内に収まることが保証されます。



重要 このリリースでは、QoS リソース予約はサポートされていません。

サポートされる機能：

- 承認済み QoS のプロビジョニングとポリシー適用：PCRF は PCEF に承認済み QoS を提供する場合があります。承認済み QoS は、適用されるリソースの適切な値を提供します。
- IP CAN ベアラーごとの「承認済み QoS」のプロビジョニング：ベアラーバインドが PCRF によって実行される場合、IP-CAN ベアラーごとの承認済み QoS が使用されます。
- IP CAN ベアラーごとの「承認済み QoS」のポリシー適用：ポリシーベースの承認の適用を担当するのは PCEF です。結果として、要求された QoS が IP CAN ベアラーごとの「承認済み QoS」と一致することが保証されます。
- SDF ごとの承認済み QoS のポリシープロビジョニング：SDF ごとの承認済み QoS のプロビジョニングは、PCC ルールのプロビジョニング手順の一部です。
  - SDF ごとの承認済み QoS のポリシー適用：承認済み QoS が PCC ルールに対して定義されている場合、PCEF は、その PCC ルールに対応する SDF のデータレートを、PCC ルールに対して承認済みの最大帯域幅を超えないように制限します（制限を超えるパケットを破棄します）。
  - PCC ルールを非アクティブ化または削除すると、PCEF は、その PCC ルール用に予約されていたリソースを解放します。PCRF が IP-CAN ベアラーと PCC ルールの両方に

承認済み QoS を提供する場合、個々の PCC ルールの承認済み QoS の適用が最初に実行されます。

重要 このリリースでは、混合モード（BCM＝UE_NW）での承認済み QoS の範囲の調整はサポートされていません。

- • QCI ごとの承認済み QoS のプロビジョニング：PCEF がベアラーバインドを実行する場合、PCRF は非 GBR ベアラー QCI 値について QCI ごとの承認済み QoS をプロビジョニングできます。PCRF がベアラーバインドを実行する場合、PCRF は QCI ごとの承認済み QoS をプロビジョニングしません。PCRF は、GBR ベアラー QCI 値の QCI ごとの承認済み QoS をプロビジョニングしません。

重要 1 ー 9 の標準ベース QCI 値のみがサポートされます。QCI 値 1 ～ 9 は、3GPP Specification TS 23.203「Policy and charging control architecture」で定義されています。

- QCI ごとの承認済み QoS のポリシー適用：PCEF は、非 GBR ベアラー QCI 値の QCI ごとの承認済み QoS を受け取ることができます。

- その他の機能：
  - ベアラー制御モード選択：PCEF は、Gx 参照ポイントを介して、IP-CAN セッション確立時または（SGSN 変更の結果としての）IP-CAN セッション変更時に、ベアラー制御モード（BCM）選択の要求を通知する場合があります。この選択は「PCC ルール要求」の手順を使用して実行されます。

    Bearer-Control-Mode AVP が PCRF から受信されない場合、IP-CAN セッションは終了されません。UE/SGSN/GGSN 間でネゴシエートされた値は、BCM と見なされます。サービスタイプごとに、次の値が考慮されます。

    - GGSN：UE/SGSN/GGSN 間でネゴシエートされた値が考慮されます。

      次のシナリオでは、BCM として UE_ONLY が選択されています。

      シナリオ 1：

      - UE -> UE_ONLY
      - SGSN -> UE_ONLY
      - GGSN -> UE_ONLY
      - PCRF -> NO BCM

      シナリオ 2：

      - UE -> UE_ONLY

- SGSN -> UE_ONLY
- GGSN -> Mixed
- PCRF -> NO BCM

- GTP-PGW：UE_NW が BCM として考慮されます。
- IPSG：UE_ONLY が BCM として考慮されます。
- HSGW/SGW/PDIF/FA/PDSN/HA/MIPV6HA：NONE が BCM として考慮されます。

- PCC ルールのエラー処理：1 つ以上の PCC ルールのインストールまたはアクティブ化に失敗した場合、PCEF は、影響を受ける PCC ルールの CCR または RAA コマンドのいずれかに 1 つ以上の Charging-Rule-Report AVP を含めます。PCEF は、各 Charging-Rule-Report AVP 内に、1 つ以上の Charging-Rule-Name AVP または Charging-Rule-Base-Name AVP を追加することによってエラーの発生した PCC ルールを示し、Rule-Failure-Code AVP を追加することによってエラーの理由コードを示し、また PCC-Rule-Status AVP を追加します。

  1 つまたは複数の新しい PCC ルール（以前は正しくインストールされていなかったルール）のインストールまたはアクティブ化に失敗した場合、PCEF はプッシュモードとプルモードの両方で PCC-Rule-Status を INACTIVE に設定します。

  PCC ルールが正常にインストールまたはアクティブ化されたものの、PCEF によって適用できなくなった場合、PCEF は PCRF に新しい CCR コマンドを送信し、Charging-Rule-Report AVP を追加します。PCEF は、Charging-Rule-Report AVP 内に Rule-Failure-Code AVP を追加し、PCC-Rule-Status を INACTIVE に設定します。

  GnGp HO シナリオ中にコリジョンが発生すると、CCR-U が生成され、ルール障害を報告するために PCRF に送信されます。

  この追加の Gx メッセージ（CCR-U）がトリガーされると、RAT_TYPE トリガーが有効になっている場合、複数の CCR-U を設定する必要が生じます。設定しない場合、HO 中にコリジョンが発生するたびにサブスクライバコールがドロップされます。

- 時刻の手順：PCEF は、PCRF の指示に従って PCC ルール要求を実行します。再検証時間が PCRF によって設定されている場合、PCEF は、PCRF とのやり取りをトリガーし、確立された IP CAN セッションに関する PCC ルールを PCRF に要求します。PCEF が REVALIDATION_TIMEOUT イベントをトリガーすると、PCEF はタイマーを停止します。



重要 Rule-Activation-Time/Rule-Deactivation-Time/Revalidation-Time AVP は、その値が現在時刻または現在の IPSG 時刻より後の時刻に対応する場合にのみ正常に解析されます。それ以外の場合、AVP およびメッセージ全体が拒否されます。

CCA/RAR で Rule-Deactivation-Time AVP が省略されている場合、この AVP の以前の値は無効になります。新しい動作は、Gx の 3GPP 仕様、バージョン 12.1.0 に準拠しています。

PCRF が Rule-Deactivation-Time AVP なしで RAR/CCA-U で同じ事前定義済みルールを再度有効にすると、このルールの deactivation-time は削除されます。

以前の動作に切り替える場合、PCRF は PCRF メッセージ（RAR、CCA-U）で、predef-rule 名と一緒に Rule-Deactivation-Time AVP と同じ値を再送信する必要があります。

重要 この動作変更は、事前に定義したルールにのみ適用されます。

Gx でのファイアウォールポリシーのサポート：Diameter AVP「SN-Firewall-Policy」が Diameter ダイナミックディクショナリに追加され、Gx インターフェイスでファイアウォールポリシーをサポートできるようになりました。この AVP は CCA-I メッセージにエンコードされ、APN 設定を介して PDP コンテキストに静的に割り当てられた、またはRADIUS の Access-Accept を介して動的に割り当てられた fw-and-nat ポリシーを適用/上書きできます。この AVP は、任意の CCA-U または RAR メッセージ内で解析することも可能です。これにより、現在 PDP コンテキストに割り当てられている fw-and-nat ポリシーを変更できます。

課金制御

課金制御は、SDF に属するパケットを課金キーに関連付け、必要に応じてオンライン課金やオフライン課金を適用するプロセスです。フローベースの課金は、SDF のリアルタイム分析に基づいて、ベアラー使用量の差別化された課金を処理します。課金制御を可能にするために、PCC ルールの情報によって SDF が識別され、課金制御のパラメータが指定されます。PCC ルール情報は、サブスクリプションデータに依存する場合があります。

オンライン課金の場合、PCEF イベント時にオンライン課金アクションを適用できます（たとえば、QoS 変更時の再承認など）。

PCC ルールでは課金システムとの連携が不要であること、つまりこの SDF のアカウンティングもクレジット制御も実行せず、その後にオフライン課金情報が生成されないことを PCEF に示すことができます。

サポートされる機能：

- IP-CAN セッションの課金関連情報のプロビジョニング
- 課金アドレスのプロビジョニング：プライマリまたはセカンダリイベント課金機能名（オンライン課金サーバー（OCS）アドレスまたはピア名）

重要 このリリースでは、Gx を介したプライマリまたはセカンダリ課金収集機能名（オフライン課金サーバー（OFCS）アドレス）のプロビジョニングはサポートされていません。

- デフォルトの課金方法のプロビジョニング：このリリースでは、デフォルトの課金方法は CCR-I メッセージで送信されます。この場合、新しい AVP オンラインおよびオフラインが、設定に基づいて CCR-I メッセージで送信されます。コマンドレベルで受信した Online

または Offline AVP は、PCC ルールレベルで設定されていない場合、ダイナミックルールにのみ適用されます。

課金の相関

SDF レベルとアプリケーションレベル（IMS など）間の課金の相関、およびアプリケーションレベルでのオンライン課金サポートを目的として、該当する課金識別子と IP-CAN タイプ識別子が PCRF から AF に渡されます（これらの識別子が使用できる場合）。

IMS ベアラー課金の場合、IP マルチメディア コア ネットワーク（IM CN）サブシステムおよびパケット交換（PS）ドメインエンティティは、相関のある課金データを生成する必要があります。

これを実現するために、ゲートウェイは PDP コンテキストに関連付けられた GGSN 課金識別子（GCID）をそのアドレスとともに PCRF に提供します。次に PCRF は、P-CSCF によって提供される IMS 課金識別子（ICID）をゲートウェイに送信します。ゲートウェイは、課金データと課金システム間の相関を行えるように、GCID と ICID（PCRF から受信した場合）を含む課金レコードを生成します。

PCRF は、IMS セッションで IP フローを一意に識別するフロー識別子も提供します。

ポリシーおよび課金制御（PCC）ルール

PCC ルールにより、SDF の検出が可能になり、ポリシー制御や課金制御のパラメータが提供されます。PCC ルールの目的は次のとおりです。

- SDF に属するパケットを検出します。
  - PCC ルールの SDF フィルタに基づいてダウンリンク IP CAN ベアラーを選択します。
  - PCC ルール内の SDF フィルタを使用して、アップリンク IP フローが正しい IP CAN ベアラーで転送されるように強制します。
- SDF が提供するサービスを特定します。
- SDF に適用可能な課金パラメータを指定します。
- SDF のポリシー制御を提供します。

PCEF は PCC ルールの優先順位に従って、PCC ルールの SDF フィルタと照らし合わせて受信パケットを評価し、受信パケットごとに PCC ルールを選択します。パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。

PCC ルールには次の 2 種類があります。

- ダイナミック PCC ルール：Gx インターフェイスを介して PCEF に動的にプロビジョニングされるルール。この PCC ルールは事前に定義することも、PCRF で動的に生成することもできます。ダイナミック PCC ルールは任意のタイミングでインストール、変更、および削除できます。

- 定義済みPCCルール：通信事業者によってPCEFで事前設定されたルール。定義済みPCCルールは、PCRF が任意のタイミングでアクティブ化または非アクティブ化できます。PCEF 内の定義済み PCC ルールをグループ化すると、PCRF は Gx 参照ポイント上で一連の PCC ルールを動的にアクティブ化できます。



重要 3番目のルールであるスタティックPCCルールは、通信事業者によってシャーシに事前設定できます。スタティック PCC ルールは、PCRF で明示的に認識されておらず、PCRF の制御下にありません。スタティック PCC ルールは、Gx で制御されない汎用ベアラーにバインドされます。

PCC ルールの構成は次のとおりです。

- ルール名：PCEF と PCRF 間の通信で PCC ルールを参照するために使用されます。
- サービス識別子：SDFが関連するサービスやサービスコンポーネントを識別するために使用されます。
- サービス データ フロー フィルタ：サービスフローフィルタは、ルールを適用するトラフィックの選択に使用されます。
- 優先順位：SDF フィルタが重複しているさまざまな PCC ルールでは、ルールの優先順位によって、どのルールが適用されるかが決まります。ダイナミック PCC ルールと定義済み PCC ルールの優先順位が同じ場合は、ダイナミック PCC ルールが優先されます。
- ゲートステータス：SDF フィルタによって検出された SDF がアップリンク方向またはダウンリンク方向で通過するか（ゲートが開いている）、または破棄されるか（ゲートが閉じている）かを示します。
- QoS パラメータ：QoS 情報には、QoS クラス識別子（SDF の認定された QoS クラス）、割り当ておよび保持優先順位（ARP）、およびアップリンクとダウンリンクの認定ビットレートが含まれます。



重要 ECS は、ベアラーのバインドに ARP バイト全体を（QCI とともに）使用します。ダイナミックルールでは機能ビットと脆弱性ビットがオプションであるため、これらのフラグがないダイナミックルールを受信した場合、機能ビットが 1（無効）に設定され、脆弱性ビットが 0（有効）に設定されていると見なされます。事前定義済みルールでは、これらの 2 つのフラグはサポートされていないため、現時点では、すべての事前定義済みルールの機能ビットが 1（無効）に設定され、脆弱性ビットが 0（有効）に設定されていると見なされます。

- 課金キー（料金設定グループ）

- その他の課金パラメータ：課金パラメータは、オンライン課金インターフェイスとオフライン課金インターフェイスが使用されるかどうか、オフライン課金で計測される内容、どのレベルで PCEF がルールに関連する使用状況を報告するかなどを定義します。



重要 このリリースでは、ダイナミック PCC ルールの計測方式とレポートレベルの設定はサポートされていません。

アプリケーション機能（AF）が Rx インターフェイスを介してこの情報を提供した場合、PCC ルールにはアプリケーションとベアラーレイヤー間の課金相関を有効にするための AF レコード情報も含まれます。IMS の場合は、IMS 課金識別子（ICID）とフロー識別子が含まれます。



重要 ASR 5500 は、Gx メッセージのダイナミック課金ルールごとのフロー説明を含む 8 つのフロー情報のみをサポートします。

セッションマネージャがクラッシュした場合にベアラーごとに回復できる 24 の PCC ルールがあります。また、最大 24 の PCC ルールを ICSR 後に回復できます。

保留状態の PCC ルールの変更が受信されると、変更されたパラメータは P-GW でバッファに保存されます。保留中の要求に対する応答をアクセスネットワークから受信した後、P-GW はバッファされたパラメータの変更を処理し、必要に応じてネットワークに対する別の更新要求を生成します。

Gx 参照ポイントを介した PCC 手順

PCC ルールの要求

PCEF は、Gx 参照ポイントを使用して、次の場合に PCC ルールを要求します。

- IP-CAN セッションの確立時
- IP-CAN セッションの変更時

PCC ルールは、イベントトリガーを求めずに、PCC ルールのインストール/アクティブ化または適用の失敗の結果として要求することもできます。

PCC ルールのプロビジョニング

PCRF は、Rel. 8 Gx 参照ポイントを介して、PCEF で適用される PCC ルールを示します。これは、次のいずれかの手順で行われます。

- プル（PCEF により要請されたプロビジョニング）：PCEF による PCC ルールの要求に応じて、PCRF は CC-Answer で PCC ルールをプロビジョニングします。
- プッシュ（要請のないプロビジョニング）：PCRF は、PCEF からの要求を取得せずに PCC ルールのプロビジョニングを決定することがあります。たとえば、Rx 参照ポイントを介して PCRF に提供された情報への応答、または PCRF 内の内部トリガーへの応答。PCEF

からの要請なしにPCCルールをプロビジョニングするために、PCRFはこれらのPCCルールを RA 要求メッセージに含めます。この RA 要求によってトリガーされる CCR および CCA メッセージはありません。

PCEF からの要求ごとに、または要請のないプロビジョニング時に、PCRF は 0 個以上の PCC ルールをプロビジョニングします。PCRFは、次のいずれかの方法で単一のPCCルールに対する操作を実行できます。

- PCEFで事前定義されたPCCルールをアクティブ化または非アクティブ化する場合、PCRFは、Charging-Rule-Name AVP 内でこの PCC ルールへの参照をプロビジョニングし、Charging-Rule-Install AVP または Charging-Rule-Name AVP のいずれかを選択して必要なアクションを提示します。
- PCRF によりプロビジョニングされた PCC ルールをインストールまたは変更する場合、PCRF は、Charging-Rule-Install AVP 内で対応する Charging-Rule-Definition AVP をプロビジョニングします。
- 以前に PCRF によってプロビジョニングされた PCC ルールを削除する場合、PCRF は、このルールの名前を Charging-Rule-Remove AVP 内の Charging-Rule-Name AVP の値にしてプロビジョニングします。

重要 課金ルール名の最大長は 63 バイトです。課金ルール名の長さが 63 バイトを超える場合、Rule-Failure-Code が RESOURCES_LIMITATION の課金ルールレポートが送信されます。この課金ルールレポートは、ルール名の長さが 128 文字未満の場合にのみ送信されます。課金ルール名の長さが 128 文字以上の場合、課金ルールレポートは送信されません。

セッションの接続中、P-GW は、同じ CCR-U にルールの失敗とクレジットの不足を組み合わせて PCRF に送信します。

アップリンク IP パケットの PCC ルールの選択

PCC が有効になっている場合、PCEF は、PCC ルールの優先順位に従い、IP CAN ベアラーの PCRF が提供するアクティブな PCC ルールまたは事前定義済みのアクティブな PCC ルールのアップリンク SDF フィルタを使用してパケットを評価することで、IP CAN ベアラー内の受信アップリンク IP パケットそれぞれに適用する PCC ルールを選択します。

重要 PCRF が提供する PCC ルールと事前定義された PCC ルールが同じ優先順位を持つ場合、PCRF が提供する PCC ルールのアップリンク SDF フィルタが最初に適用されます。

重要 IMSA および ECS では、同じ優先順位の値を持つ 2 つ（以上）のダイナミックルールを PCRF にインストールできます。

パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。対応する IP CAN ベアラーのいずれの PCC ルールにも一致しないアップリンク IP パケットは廃棄されます。

ダウンリンク IP パケットの PCC ルールおよび IP CAN ベアラーの選択

PCC が有効になっている場合、PCEF は、PCC ルールの優先順位に従い、IP CAN セッションにおけるすべての IP CAN ベアラーの、PCRF が提供するアクティブな PCC ルールまたは事前定義済みのアクティブな PCC ルールのダウンリンク SDF フィルタを使用してパケットを評価することで、IP CAN セッション内の受信ダウンリンク IP パケットそれぞれに適用する PCC ルールを選択します。



重要 PCRF が提供する PCC ルールと事前定義された PCC ルールが同じ優先順位を持つ場合、PCRF が提供する PCC ルールのダウンリンク SDF フィルタが最初に適用されます。

パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。ダウンリンク IP パケットは、選択した PCC ルールがマッピングされている IP CAN ベアラー内で転送されます。IP CAN セッションのいずれの PCC ルールにも一致しないダウンリンク IP パケットは廃棄されます。

次の手順もサポートされています。

- IP-CAN ベアラー終了の表示の意味
- IP-CANセッション終了の表示：IP-CANセッションが終了している場合（たとえば、GPRSでIP-CANセッション内の最後のPDPコンテキストが終了している場合）、PCEFはPCRFに接続します。
- IP-CAN ベアラー終了の要求：IP CAN セッション内の最後の IP CAN ベアラーの終了が要求された場合、PCRF および PCEF は「IP-CAN セッション終了の要求」手順を適用します。
- IP-CAN セッション終了の要求：内部トリガーまたは SPR からのトリガーにより PCRF が IP CAN セッションの終了を決定した場合、PCRF は PCEF に通知します。PCEF は PCRF に確認応答し、その IP-CAN セッションで以前にインストールまたはアクティブ化されたすべての PCC ルールを即座に削除または非アクティブ化します。

PCEF は IP CAN セッションを終了するために、IP CAN 固有の手順を適用します。GPRS の場合、GGSNは、IP-CANセッション全体の終了が要求されたことを示すティアダウンインジケータを設定した PDP 非アクティブ化要求を送信します。さらに、PCEF は「IP CAN セッション終了の表示」の手順を適用します。

サブスクライバがダウンすると、PCRF から取得されたボリュームまたはルール情報は破棄されます。

Gx を介したボリュームレポート

ここでは、3GPP Rel. 9 の Gx を介したボリュームレポート機能について説明します。これは、Rel. 7 の Gx インターフェイスをサポートするすべての製品でサポートされます。

ライセンス要件

Gx を介したボリュームレポートは、シスコのライセンス供与された機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。



重要 Gx を介した課金機能または Gx を介したボリュームレポート機能に個別のライセンスは必要ありません。この機能は、「ポリシーインターフェイス」ライセンスの一部として有効にすることができます。

サポートされる標準

Gx を介したボリュームレポート機能は、次の標準規格に基づいています。

3GPP TS 29.212 V9.5.0 (2010-06)：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control over Gx reference point (Release 9)

機能の概要

Gx を介したボリュームレポート機能により、PCRF はサブスクライバのデータ使用量に基づいてリアルタイムの決定ができます。



重要 Volume Reporting over Gx は、ボリュームクォータにのみ適用されます。

PCEF は、最初からではなく、使用状況監視の最後のレポート以降の累積使用量のみを報告します。

使用量しきい値がゼロ（無限しきい値）に設定されている場合、PCEF によってそれ以上のしきい値イベントは生成されませんが、使用状況の監視は続行され、セッションの終了時に報告されます。

ベアラーの終了時の使用状況レポートと、アップリンク/ダウンリンクレベルのレポートがサポートされています。

次の手順を通じて、Gx を介したボリュームレポートの仕組みについて説明します。

1. PCEF は、PCRF からメッセージを受信した後、使用状況モニタリング関連の AVP を解析し、その情報を IMSA に送信します。
2. IMSA はこの情報で ECS を更新します。

3. PCRF からの使用状況モニタリング情報で ECS が更新されると、PCEF（ECS）はデータ使用状況の追跡を開始します。
4. セッションレベルのモニタリングの場合、ECS がデータ使用状況を保持します。
5. PCC ルールモニタリングの場合、モニタリングキーを一意の識別子として使用状況がモニタリングされます。各ノードがモニタリングキーごとの使用状況情報を保持します。データトラフィックが通過すると、使用量しきい値に照らして使用状況がチェックされ、「使用状況レポート」セクションに説明されているようにして報告されます。
6. PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況を追跡し続けます。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されません。

使用状況モニタリング

- セッションレベルでの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に使用量しきい値レベルを設定し、Usage-Monitoring-Level AVP を SESSION_LEVEL(0) に設定して、Usage-Monitoring-Information AVP を送信することで、Gx に関するセッションレベルのボリュームレポートにサブスクライブします。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。セッションレベルでのモニタリングキーがサポートされています。

  PCRF からの 1 つのメッセージでのセッション使用状況の有効化と無効化がサポートされています。この操作は、モニタリングキーがセッションレベルで関連付けられている場合にのみ可能です。

  入力/出力オクテットのしきい値レベルに基づく使用状況のモニタリングがサポートされています。有効になっているしきい値レベルに基づいて使用状況が報告されます。複数のレベルが有効になっている場合は、いずれか 1 つのレベルで侵害が発生しても、有効になっているすべてのレベルについて使用状況が報告されます。モニタリングは、PCRF からの使用状況レポートの応答で欠落しているしきい値レベルで停止されます（PCRF が以前に有効にされた複数のレベルでモニタリングを継続する場合、完全なセットを再度提供することが期待されます）。

  合計しきい値レベルと GSU AVP の UL/DL しきい値レベルの両方が提供された場合はエラーとして扱われ、合計しきい値レベルのみが受け入れられます。

  次の要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U が生成されます。

  - モニタリングキーを使用したルールレベルでの即時レポート要求
  - モニタリングキーを使用した、または使用しないセッションレベルでの即時レポート要求
  - ルールレベルでの明示的な無効化要求
  - セッションレベルでの明示的な無効化要求

上記のすべての要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U は生成されません。また、すべてのアクティブなモニタリングキーの使用状況を報告した CCR-U への応答で、ルールレベルのモニタリングキーのない即時レポート要求を受信した場合、追加の CCR-U は生成されません。

- フローレベルの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルと PCC_RULE_LEVEL(1) に設定された Usage-Monitoring-Level AVP とともに Usage-Monitoring-Information AVP を送信することで、Gx を介してフローレベルのボリュームレポートに登録します。フローレベルのモニタリングの場合、モニタリングキーは必須です。PCRF がルールとモニタリングキーを関連付ける際や、フローレベルで使用状況モニタリングを有効化または無効化する際に、モニタリングキーを使用して制御できるためです。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。

  使用状況モニタリングは、スタティックルール、定義済みルール、およびダイナミックルール定義に対応しています。

  - スタティックルールの使用状況モニタリング：スタティックルールの場合、モニタリングキーに関連付けられた最後のルール削除に関する使用状況はレポートの対象外になります。この場合、PCRF から使用状況モニタリング情報のみを受信します。
  - 定義済みルールの使用状況モニタリング：事前定義されたルールに対して使用状況モニタリングを有効にする必要がある場合、PCRF は、モニタリングキーと使用量しきい値を含むルールおよび使用状況モニタリング情報を送信します。モニタリングキーは、その事前定義済みルールの PCEF で事前設定されているものと同じである必要があります。同じモニタリングキーに複数のルールを関連付けることができます。そのため、特定のモニタリングキーを有効にすると、同じモニタリングキーを持つ複数のルールのデータが追跡されることになります。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。
  - ダイナミックルールの使用状況モニタリング：ダイナミックルール定義に対して使用状況モニタリングを有効にする必要がある場合、PCRF は課金ルールの定義や使用状況モニタリング情報（モニタリングキー、使用量しきい値など）とともにモニタリングキーを提供します。これにより、そのモニタリングキーに関連付けられているすべてのルールに対して使用状況モニタリングが実行されます。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。ダイナミックルール定義のモニタリングキーは、PCRF によって動的に割り当てられます。これが、使用状況モニタリングのケースにおいて定義済みルールとの唯一の違いです。

複数のモニタリングキーで同時にしきい値違反が発生した場合、最初に 1 つのモニタリングキーの使用状況のみが報告されます。PCRF から正常な応答を受信すると、残りのモニタリン

グキーの使用状況が PCRF に報告されます。Tx 期限切れ/TCP リンクエラーが発生すると、報告されていない使用状況が ECS に保存されます。セッションでその後 PCRF と正常なやり取りがあった場合、報告されていない UMI が PCRF に送信されます。

使用状況レポート

サブスクライバレベルやフローレベルでの使用状況は、次の条件で PCRF に報告されます。

- 使用量しきい値に達した：PCEF はサブスクライバデータの使用量を記録し、PCRF によって指定される使用量しきい値に達しているかどうかを確認します。これは、セッションレベルとルールレベルの両方のレポートで行われます。

  セッションレベルのレポートでは、実際の使用量が、使用量しきい値と比較されます。

  ルールレベルのレポートでは、データトラフィックにヒットするルールを使用して、モニタリングキーが関連付けられているかどうかが確認され、モニタリングキーに基づいてデータ使用量が確認されます。条件が満たされると、使用状況の情報を IMSA に報告し、モニタリングを続行します。IMSA は、「USAGE_REPORT」トリガーが PCRF によって有効になっている場合に、CCR-U をトリガーします。この CCR で、Usage-Monitoring-Information AVP と、サブスクライバのデータ使用量を設定した「Used-Service-Unit」が送信されます。

  使用量しきい値に達したときに、PCRF が使用状況モニタリング情報に PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、使用状況は報告されません。

  Gx を介した非標準ボリュームレポートの実装では、しきい値に違反すると使用状況モニタリングが停止します。それ以外の場合はモニタリングが続行されます。CCA が受信されるまで、以降の使用状況は報告されません。

- 使用状況モニタリングが無効：レポートの使用状況、その他の外部トリガー、または PCRF 内部トリガーに関連しない PCEF からの CCR の結果として PCRF により使用状況モニタリングが無効にされた場合には、PCRF が Usage-Monitoring-Support AVP を USAGE_MONITORING_DISABLED に設定して使用状況モニタリングを明示的に無効にすると、PCEF はモニタリングを停止し、（モニタリングが有効だったときの）使用状況情報を PCRF に報告します。使用量しきい値に達したときに、PCRF が PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、これ以降の使用状況は報告されません。

- IP CAN セッションの終了：IP CAN セッションが終了すると、サブスクライバの累積使用状況情報が PCEF からの CCR-T で PCRF に報告されます。PCC 使用量レベル情報が PCRF によって有効になっている場合、PCC 使用量も報告されます。

  PCRF は RAR メッセージを使用し、その中に Session-Release-Cause AVP を含めて、IP CAN セッション終了を開始します。ただし、PCRF が CCA メッセージで IP CAN セッションを終了する場合もあります。不要な追加メッセージを回避するために、PCRF は、CCA-U メッセージ自体で、サブスクライバを終了するように P-GW に通知できます。そのため、すべての Gx ディクショナリの CCA メッセージに Session Release Cause が追加されました。

- PCC ルールの削除：PCRF が使用量モニタリングキーに関連付けられている最後の PCC ルールを非アクティブ化すると、PCEF はそのモニタリングキーのデータ使用量を含む CCR を送信します。使用量モニタリングキーに関連付けられている最後の PCC ルールが非アクティブであると PCEF が報告する場合に、CCR コマンドに Charging-Rule-Report AVP が含まれていたなら、PCEF は同じ CCR コマンドでそのモニタリングキーの累積使用量を報告します。あるいは、Charging-Rule-Report AVP が RAA コマンドに含まれている場合、PCEF は新規に CCR コマンドを送信して、使用状況モニタリングキーの累積使用量を報告します。PCRF によって設定された、ルールの非アクティブ化時間を使用した最後のルールの非アクティブ化に関する使用状況レポートがサポートされています。

  PCRF からのメッセージを受信すると、削除対象のルールがマーク付けされ、アクセス側の手順が完了した後にルールが削除されます。

- PCRF 要求使用状況レポート：最後のレポートの送信以降の累積使用量（即時レポートの場合も同様）。即時レポート後に使用量はリセットされ、使用状況モニタリングが続行されます。後続の使用状況レポートには現在のレポート以降の使用量が含まれるようになります。

- ベアラー終了時の使用状況レポートを追加できます。ベアラーが何らかの理由で削除されると、そのベアラーに関連付けられているルールも削除されます。そのため、使用状況は、ベアラー終了が原因で削除された最後のルールが関連ルールであるモニタリングキーで報告されます。

- 再検証のタイムアウト：非標準の実装では、使用状況モニタリングとレポートが有効になっていて、再検証タイムアウトが発生した場合、PCEF は CCR を送信して PCC ルールを要求し、最後のレポート以降（または、使用状況がまだ報告されていない場合には、使用状況レポートが有効になった時点以降）の有効なすべてのモニタリングキーのすべての累積使用量を、IP-CAN セッションレベル（有効な場合）およびサービスデータフローレベル（有効な場合）の累積使用量を使用して報告します。これがデフォルトの動作です。

  標準実装の場合、これは CLI 設定によって有効にする必要があります。



重要 再検証タイムアウト時の使用状況レポート機能は、Gx を介したボリュームレポートの非標準実装ではデフォルトで使用できます。この機能は標準実装で設定可能です。

使用状況が報告されると、使用量カウンタはゼロにリセットされます。PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況の追跡を 0 から継続します。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されず、CCR-CCA 間の累積使用量は破棄されます。

サーバーの再試行でトリガーされた CCR-U は、サーバーによって付与されたクォータを考慮して、USU を報告します。新たに作成された MSCC の場合、USU を報告するために暫定クォータ設定が取得されます。

Gx を介したボリュームレポート機能を設定する方法については、Gx を介したボリュームレポートの設定 （755 ページ） を参照してください。

Gx を介したボリュームレポート（VoRoGx）のための ICSR サポート

ボリュームのしきい値とボリュームの使用状況はスタンバイシャーシに同期され、スイッチオーバー後の既存セッションの Gx を介したボリュームレポートをサポートします。

このサポートがないと、たとえば適切な使用を強制するためにボリュームレポートを使用した場合に、サブスクライバが想定以上に高い速度を使用する可能性はありません。通信事業者はこれをすでに収益の損失と見なしている可能性があります。また、EUのローミング規制によって設定された制限に達すると、通知を受け取り、ブロック/リダイレクトされるローミングサブスクライバに深刻な影響を及ぼします。セッションがブロックされずにこの時点でセッションが継続する場合、通信事業者は上限を超えたデータに課金することができず、実質的な収益の大幅な損失が発生します（ローミングパートナーはSGSNで使用されるデータに課金する場合があります）。

Rel. 7 Gx の動作

ここでは、GPRS/UMTS ネットワークでの Rel. 7 Gx インターフェイスのサポートにより、サブスクライバのダイナミックポリシーと課金制御がどのように動作するかについて説明します。

次の図と表は、UE により開始される、システムと IMS コンポーネント間の IMSA プロセスについて説明しています。

この例では、Diameter ポリシー制御アプリケーション（DPCA）が PCRF への Gx インターフェイスです。PCRF との IMSA 間のインターフェイスは Gx インターフェイスで、セッションマネージャ（SessMgr）とオンライン課金サービス（OCS）間のインターフェイスは Gy インターフェイスです。IMSA サービスと DPCA はシステムの SessMgr の一部であることに注意してください。分かりやすくするために、図では分離されています。



重要 DPCA と IMSA は、ポリシーサーバーインターフェイスアプリケーション内の 1 つのモジュールとして動作します。

図 *61 : Rel. 7 Gx IMS* 承認コールのフロー

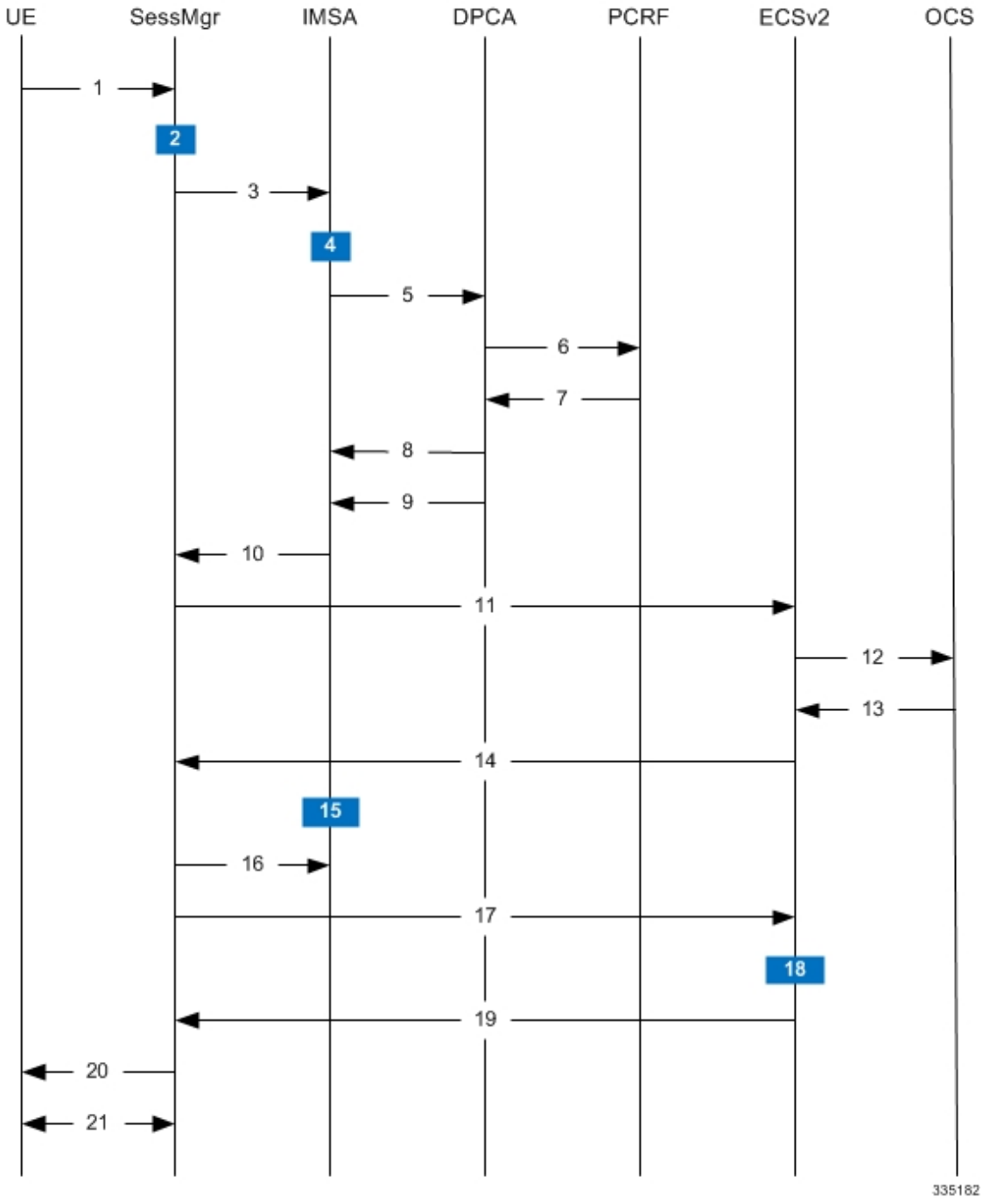


表 *71 : Rel. 7 Gx IMS* 承認コールのフローの説明

ステップ	説明
1	UE（IMS サブスクライバ）が、プライマリ PDP コンテキストのアクティブ化と作成を要求します。
2	SessMgr が UE に IP アドレスを割り当てます。
3	APN に対して IMSA が有効になっている場合、SessMgr は IMS 承認を要求します。
4	IMSA が、IP CAN セッションとベアラーにリソースを割り当て、ユーザーの選択キー（たとえば msisdn）に基づいて接続する PCRF を選択します。
5	IMSA が、DPCA モジュールに対して PCRF に承認要求を発行するよう要求します。
6	DPCA は、選択された PCRF に CCR 初期メッセージを送信します。このメッセージには、PRIMARY に設定された Context-Type AVP、および UE に割り当てられた IP アドレスが含まれます。このメッセージには、GENERAL に設定された Bearer-Usage AVP が含まれている場合があります。Bearer-Operation は Establishment に設定されています。PCRF がベアラーバインディングを行う場合、ベアラー ID が含まれます。
7	汎用 PDP コンテキスト用の事前設定済みルールセットが PCRF で提供されている場合、PCRF は CCA の事前設定済み課金ルールを送信することがあります。PCRF は、ダイナミックルールと承認された QoS パラメータも含める場合があります。
8	DPCA は、課金ルールの定義、課金ルールのインストール、PCRF から受信した QoS 情報、イベントトリガーなどを、PCRF から受信したルールに対応するベアラー ID とともに IMSA に渡します。IMSA が情報を保存します。ベアラー ID が存在せず、PCRF がベアラーバインディングを行う場合、ルールはスキップされます。一方、ベアラー ID が存在せず、PCEF がベアラーバインディングを行う場合、ルールが ECS に渡され、ベアラーバインディングが実行されます。
9	DPCA は、IMSA によって登録されたコールバック関数を呼び出します。
10	IMSA は、ベアラーが承認した QoS 情報を保存し、SessMgr に通知します。その他の PCRF によって提供される、PDP セッション全体に共通の情報（イベントトリガー、プライマリおよびセカンダリ OCS アドレスなど）は IMSA 内に保存されます。IMSA は、情報を処理した後、ポリシー承認が完了したことを SessMgr に通知します。
11	IMSA/DPCA でルールの検証が失敗した場合、Charging-Rule-Report AVP を含む PCRF に失敗が通知されます。それ以外の場合、IMSA が ECS セッションの作成を開始します。APN 名、プライマリおよびセカンダリ OCS サーバーアドレスなどが、SessMgr から ECS に送信されます。
12	ECS は、CC-Request-Type を INITIAL_REQUEST に設定した CCR(I) を OCS に送信してクレジット承認を実行し、クレジット制御セッションを開きます。この要求には、アクティブなルールベース ID（APN と AAA からのデフォルトのルールベース ID）と、GPRS 固有の属性（APN、UMTS QoS など）が含まれます。

ステップ	説明
13	OCS が CCA 初期メッセージを返します。これにより、静的に設定されたルールベースがアクティブ化されることがあります。また、プリエンプティブクォータが含まれていることがあります。
14	ECS が、応答メッセージで SessMgr に応答します。
15	SessMgr が、ダイナミックルールの IMSA を要求します。
16	IMSA がダイナミックルールを SessMgr に送信します。 RAR メッセージは、セッションが確立される前に許可されることに注意してください。 また、ダイナミックルール情報のリカバリとセッションマネージャの監査が進行中の場合は、RAR メッセージが拒否され、結果コード 3002 の RAA が送信されることに注意してください。
17	SessMgr が、ダイナミックルール情報を ECS に送信します。ゲートフローステータス情報およびフローごとの QoS（課金ルール）情報もメッセージで送信されます。
18	ECS は、受け取った事前定義済みルールをアクティブ化し、受け取ったダイナミックルールをインストールします。また、ゲートフローステータスと QoS パラメータが、ダイナミック課金ルールに従い ECS によって更新されます。Gx ルールベースは、ECS の group-of-ruledefs として扱われます。応答メッセージには、ECS でのルールプロビジョニングのステータスを伝達する課金ルールレポートが含まれます。ECS は、ベアラー ID のないルールに対して PCEF ベアラーバインディングを実行します。
19	ルールのプロビジョニングが部分的に失敗した場合、コンテキストセットアップが受け入れられ、失敗したルールの PCC ルールステータスを含む Charging-Rule-Report とともに、新しい CCR-U が PCRF に送信されます。ルールのプロビジョニングが完全に失敗すると、コンテキストセットアップが拒否されます。
20	PDP コンテキスト承認の応答に応じて、SessMgr は応答を UE に送信し、コールをアクティブにするか、拒否します。Charging-Rule-Report にいずれかのルールの部分的な失敗が含まれている場合、PCRF に通知され、コールがアクティブ化されます。Charging-Rule-Report に完全な失敗が含まれている場合、コールは拒否されます。
21	ステップ 18 での PCC ルールの PCEF ベアラーバインドに基づいて、UE を使用した 1 つ以上のネットワーク開始 PDP コンテキスト手順（Network Requested Update PDP Context（NRUPC）/Network Requested Secondary PDP Context Activation（NRSPCA））が行われます。

Rel. 7 Gx インターフェイス

Rel. 7 Gx インターフェイス機能を設定するには、コンテキストレベルで IMS 承認サービスを設定してから、IMS 承認サービスを使用するように APN を設定する必要があります。

Rel. 7 Gx インターフェイスの機能を設定するには、次の手順を実行します。

手順

ステップ 1 「コンテキストレベルでの IMS 承認サービスの設定 （751 ページ）」の説明に従って、GPRS/UMTS ネットワークの IMS サブスクライバの IMS 承認サービスをコンテキストレベルで設定します。

ステップ 2 「設定の確認 （753 ページ）」の説明に従って、設定内容を確認します。

ステップ 3 「APN への IMS 承認サービスの適用 （754 ページ）」の説明に従って、IMS サブスクライバの IMS 承認サービスを使用するように同じコンテキスト内の APN を設定します。

ステップ 4 「サブスクライバ設定の確認 （755 ページ）」の説明に従って、設定内容を確認します。

ステップ 5 オプション：「Gx を介したボリュームレポートの設定 （755 ページ）」の説明に従って、Gx を介したボリュームレポート機能を設定します。

ステップ 6 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

重要
この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンド、および/またはキーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

コンテキストレベルでの IMS 承認サービスの設定

次の例を使用して、GPRS や UMTS ネットワークの IMS サブスクライバの IMS 承認サービスをコンテキストレベルで設定します。

```
configure
     context <context_name>
          ims-auth-service <imsa_service_name>
               p-cscf discovery table { 1 | 2 } algorithm {
ip-address-modulus | msisdn-modulus | round-robin }
               p-cscf table { 1 | 2 } row-precedence <precedence_value> {
 address <ip_address> | ipv6-address <ipv6_address> } [ secondary { address
 <ip_address> | ipv6-address <ipv6_address> } ]
               policy-control
                    diameter origin endpoint <endpoint_name>
                    diameter dictionary <dictionary>
                    diameter request-timeout <timeout_duration>
                   diameter host-select table { { { 1 | 2 } algorithm
 { ip-address-modulus | msisdn-modulus | round-robin } } | prefix-table
 { 1 | 2 } }
                  diameter host-select row-precedence <precedence_value>
 table { { { 1 | 2 } host <host_name> [ realm <realm_id> ] [ secondary host
 <host_name> [ realm <realm_id> ] ] } | { prefix-table { 1 | 2 }
msisdn-prefix-from <msisdn_prefix_from> msisdn-prefix-to <msisdn_prefix_to>
```

```
host <host_name> [ realm <realm_id> ] [ secondary host <sec_host_name> [ realm
 <sec_realm_id> ] algorithm { active-standby | round-robin } ] } } [
-noconfirm ]
                    diameter host-select reselect subscriber-limit
<subscriber_limit> time-interval <duration>
                    failure-handling cc-request-type { any-request |
initial-request | terminate-request | update-request } {
diameter-result-code { any-error | <result_code> [ to <end_result_code> ] }
} { continue | retry-and-terminate | terminate }
                    end
```

注：

- <*context_name*> は、IMS 承認サービスを有効にするコンテキストの名前です。
- <*imsa_service_name*> は、Rel. 7 Gx インターフェイス承認用に設定する IMS 承認サービスの名前です。
- 最大 30 個の IMS 承認サービスプロファイルをシステムに設定できます。
- セカンダリ P-CSCF IP アドレスは、P-CSCF テーブルで設定できます。**p-cscf table** のコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

  p-cscf table 設定コマンドの構文は次のようになります。

  ```
  p-cscf table { 1 | 2 } row-precedence precedence_value { ipv4-address
  ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [
  ipv4-address ipv4_address ] } [ secondary { ipv4-address ipv4_address [
   ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address
   ipv4_address ] } [ weight value ]
  ```

- Rel. 7 Gx インターフェイスのサポートを有効にするには、関連する Diameter ディクショナリを設定する必要があります。使用する具体的な Diameter ディクショナリの詳細については、シスコのアカウント担当者にお問い合わせください。
- MSISDN プレフィックス範囲ベースの PCRF 選択メカニズムを設定する場合

  Gx インターフェイスが一定範囲のサブスクライバの特定の PCRF に接続できるようにするには、**msisdn-prefix-from** <*msisdn_prefix_from*> と **msisdn-prefix-to** <*msisdn_prefix_to*> に、それぞれ開始 MSISDN と終了 MSISDN を設定します。

  Gx インターフェイスが特定のサブスクライバの特定の PCRF に接続できるようにするには、**msisdn-prefix-from** <*msisdn_prefix_from*> と **msisdn-prefix-to** <*msisdn_prefix_to*> の両方に同じ MSISDN を設定します。

  MSISDN プレフィックス範囲テーブルには、最大 128 行まで追加できます。

  MSISDN の範囲は、各行間で重ならないようにする必要があります。
- PCRF 選択のためのラウンドロビンアルゴリズムは、多数の PCRF を選択する場合にのみ効果的であり、細かいレベルでの効果は薄いです。
- オプション：サブスクライバの Quality of Service（QoS）更新タイムアウトを設定するには、IMS 承認サービス コンフィギュレーション モードで次のコマンドを入力します。

- オプション：シグナリング制限を設定するには、IMS 承認サービス コンフィギュレーション モードで次のコマンドを入力します。

  signaling-flag { deny | permit }

  signaling-flow permit server-address <*ip_address*> **[server-port {** <*port_number*> **| range** <*start_number*> **to** <*end_number*> **}] [description** <*string*> **]**

- オプション：汎用 PDP コンテキストでどのポリシーゲートにも一致しないパケットに対するアクションを設定するには、IMS 承認サービス コンフィギュレーション モードで次のコマンドを入力します。

  traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink } { forward | discard }

- GGSN および PCEF で設定される PCRF ホスト宛先を設定するには、**diameter host-select** CLI コマンドを使用します。

- Gx が失敗したときに事前に定義されたルールを使用するように GGSN および PCEF を設定するには、**failure-handling cc-request-type** CLI を **continue** に設定します。使用可能または使用中のポリシーは引き続き使用され、PCRF とのそれ以上の連携はありません。

- デフォルトの課金方法のプロビジョニングには、次の設定を使用します。この場合、AVP のオンラインとオフラインは、設定に基づいてCCR-Iメッセージで送信されます。コマンドレベルで受信した Online または Offline AVP は、PCC ルールレベルで設定されていない場合、ダイナミックルールにのみ適用されます。

  - オンラインの有効化を送信するには、次の設定を使用します。

    configure

    active-charging service <*ecs_service_name*>

    charging-action <*charging_action_name*>

    cca charging credit

    exit

  - オフラインの有効化を送信するには、次の設定を使用します。

    configure

    active-charging service <*ecs_service_name*>

    rulebase <*rulebase_name*>

    billing-records rf

    exit

設定の確認

IMS 承認サービスの設定を確認するには、次の手順を実行します。

手順

ステップ 1 次のコマンドを入力して、IMS 承認サービスを有効にしたコンテキストに変更します。

```
context <context_name>
```

ステップ 2 次のコマンドを入力して、サブスクライバの IMS 承認サービスの設定を確認します。

```
show ims-authorization service name <imsa_service_name>
```

APN への IMS 承認サービスの適用

コンテキストレベルで IMS 承認サービスを設定したら、IMS サブスクライバに IMS 承認サービスを使用するように APN を設定する必要があります。

次の例を使用して、Rel. 7 Gx インターフェイス （750 ページ） で説明されているように設定されたコンテキスト内で、以前に設定された APN に IMS 承認サービス機能を適用します。

```
configure
   context <context_name>
      apn <apn_name>
         ims-auth-service <imsa_service_name>
         active-charging rulebase <rulebase_name>
         end
```

注：

- <*context_name*> は、IMS 承認サービスが設定されたコンテキストの名前です。
- <*imsa_service_name*> は、コンテキストで IMS 認証用に設定された IMS 承認サービスの名前です。
- Rel. 7 Gx の場合、ECS ルールベースは APN で設定する必要があります。
- ECS では、PCEF バインディングシナリオの場合に Gx を介してルールベースを変更できます。古いルールベースがなくなると、そのルールベースからインストールされていたすべてのルールが削除されます。これにより、ルールなしで残されたいくつかのベアラー（PDP コンテキスト）が終了する可能性があります。ルールベースを変更する Gx メッセージがあり、このメッセージにより事前定義済みの一部のルールもアクティブ化される場合、ルールベースの変更が最初に行われ、新しいルールベースのルールがアクティブ化されます。また、ルールベースはコール全体に適用されます。1 つのコール内のすべての PDP コンテキスト（ベアラー）で、同じ ECS ルールベースが使用されます。
- ECS で構成された事前定義済みルールの場合、ダイナミックまたは事前定義済みルールの MBR と GBR は、PCEF バインディングに使用される前にチェックされます。すべてのルール（ダイナミックおよび事前定義済み）には、MBR が関連付けられている必要があります。GBR QCI を含むすべてのルールには、GBR も設定されている必要があります。そのため、事前定義済みルールでは、QCI が GBR QCI または非 GBR QCI のいずれであるかに

応じて、適切なピークデータレート、認定データレートを設定する必要があります。詳細については、ACS課金アクション コンフィギュレーション モードで**flow limit-for-bandwidth** CLI コマンドを参照してください。

- PCRF からの Gx ルールベース（Charging-Rule-Base-Name AVP）を ECS の group-of-ruledefs として解釈するには、アクティブ課金サービス コンフィギュレーション モードで次のコマンドを設定します。

  policy-control charging-rule-base-name active-charging-group-of-ruledefs

サブスクライバ設定の確認

次のコマンドを入力して、サブスクライバの IMS 承認サーバーの設定を確認します。

show subscribers ims-auth-service <*imsa_service_name*>

<*imsa_service_name*> は、IMS 認証用に設定された IMS 承認サービスの名前です。

Gx を介したボリュームレポートの設定

ここでは、Gxを介したボリュームレポートを有効にするのに必要な設定について説明します。

Gx を介したボリュームレポートを有効にするには、次の設定コマンドを使用します。

```
configure
     active-charging service <ecs_service_name>
          rulebase <rulebase_name>
             action priority <priority> dynamic-only ruledef <ruledef_name>
 charging-action <charging_action_name> monitoring-key <monitoring_key>
                exit
          exit
     context <context_name>
          ims-auth-service <imsa_service_name>
               policy-control
                    event-update send-usage-report [ reset-usage ]
                    end
```

注：

- PCEF が受け入れる最大モニタリングキー値は 4294967295 です。PCEF がより大きい値を送信すると、値は符号なし整数値に変換されます。
- **event-update** CLI を使用すると、イベントの更新時にボリューム使用状況レポートを有効にできます。オプションキーワード **reset-usage** を使用すると、差分レポートをサポートできます。このレポートでは、使用状況が報告され、PCEF でリセットされます。このオプションが設定されていない場合、イベント更新の一部として使用状況の情報を送信しますが、PCEF でリセットすることはしません。

統計情報の収集

ここでは、Rel. 7 Gx の統計と設定情報を収集する方法について説明します。

次の表では、最初の列に、収集する統計が示されており、2 つ目の列に、実行するアクションが示されています。

表 *72 : Rel. 7 Gx* 統計と情報の収集

統計/情報	実行するアクション
IMS 承認サービスのポリシー制御に固有の情報と統計。	**show ims-authorization policy-control statistics**
IMS 承認サービスに使用される、承認サーバーに固有の情報と統計。	**show ims-authorization servers ims-auth-service**
すべての IMS 承認サービスの情報。	**show ims-authorization service all**
IMS 承認サービスの統計。	**show ims-authorization service statistics**
IMS 承認サービスでアクティブなセッションの情報、設定、統計。	**show ims-authorization sessions all**
IMS 承認サービスでアクティブなセッションの完全な情報、設定、統計。	**show ims-authorization sessions full**
IMS 承認サービスでアクティブなセッションの要約情報。	**show ims-authorization sessions summary**
アクティブな課金サービスセッションの完全な統計。	**show active-charging sessions full**
サービスに設定されているすべてのルール定義に関する情報。	**show active-charging ruledef all**
システムに設定されているすべてのルールベースに関する情報。	**show active-charging rulebase all**
システムに設定されているすべての ruledef グループに関する情報。	**show active-charging group-of-ruledefs all**

Rel. 8 Gx インターフェイス

Rel. 8 Gx インターフェイスのサポートは、Cisco ASR シャーシで使用できます。

ここでは、次の内容について説明します。

- HA/PDSN Rel. 8 Gx インターフェイスのサポート （757 ページ）
- P-GW Rel. 8 Gx インターフェイスのサポート （775 ページ）

HA/PDSN Rel. 8 Gx インターフェイスのサポート

ここでは、CDMA ネットワークのサブスクライバに対してポリシーおよび課金制御をサポートするための、HA および PDSN 用 Rel. 8 Gx インターフェイスの設定について説明します

IMS サービスは、アクセスサポートとは無関係に、音声、ビデオ、およびデータの転送に関するアプリケーションサポートを提供します。CDMA ネットワーク内のローミング IMS サブスクライバには、他の機能とは別に、必要十分で中断のない一貫性のあるシームレスなユーザーエクスペリエンスがアプリケーションセッション中に必要になります。また、使用されている特定の IMS アプリケーションによって消費されるリソースの料金のみがサブスクライバに請求されることも重要です。

ここに記載する手順を実行する前に、本アドミニストレーション ガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

ここでは、次の内容について説明します。

- はじめに （757 ページ）
- 用語および定義 （759 ページ）
- 機能の仕組み （768 ページ）
- HA/PDSN Rel. 8 Gx インターフェイスのサポート （771 ページ）
- 統計情報の収集 （774 ページ）

はじめに

CDMA ネットワークでの IMS 展開の場合、システムは、ポリシーベースのアドミッションコントロールのサポートおよびフローベース課金（FBC）に Rel. 8 Gx インターフェイスを使用します。Rel. 8 Gx インターフェイスは、ゲート設定、帯域幅制限などのポリシー制御適用機能をサポートし、FBC もサポートします。これは、動的にプロビジョニングされたポリシー制御および課金（PCC）ルールによって実現されます。これらの PCC ルールは、サービスデータフロー（SDF）を識別し、課金を実行するために使用されます。ルールに関連付けられているその他のパラメータは、ポリシー制御を適用するために使用されます。

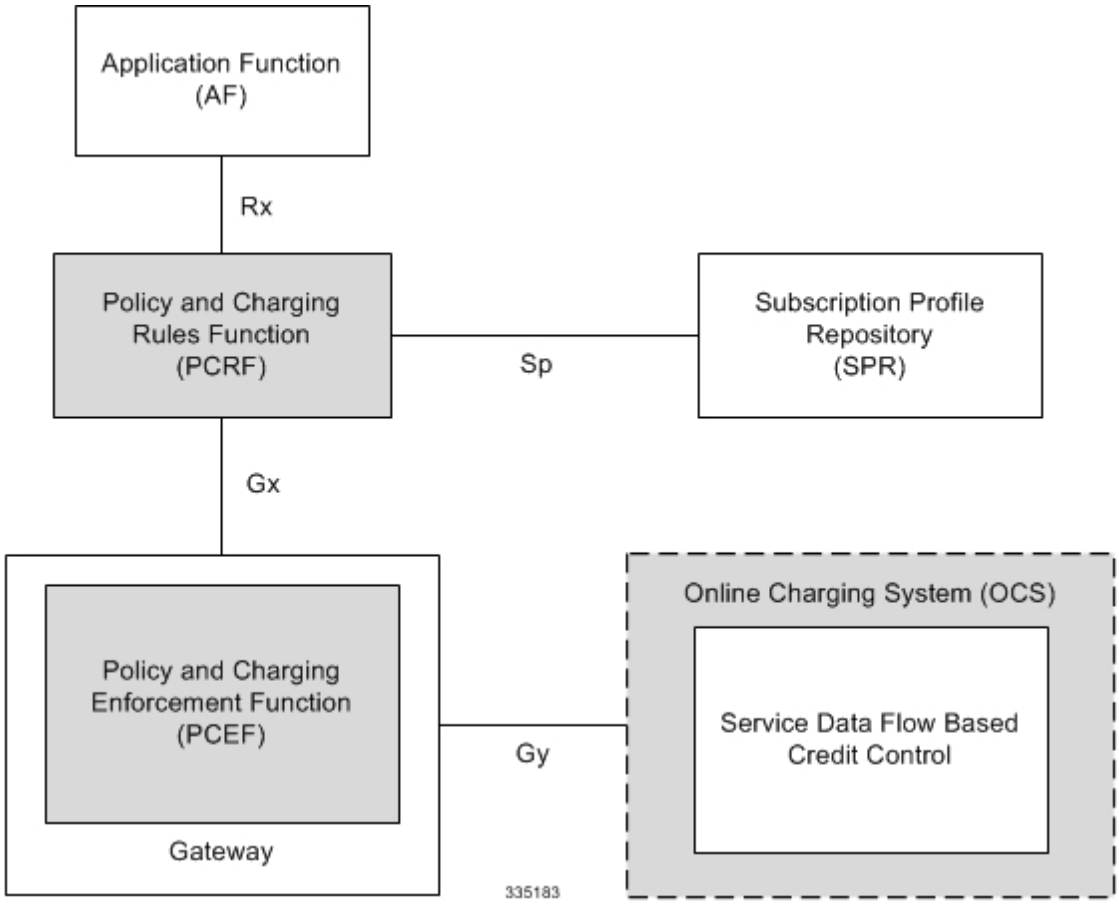
PCC アーキテクチャにより、オペレータは、サービスベースの QoS ポリシーと FBC 制御を実行できます。PCC アーキテクチャでは、これは主にポリシーおよび課金適用機能（PCEF）/HA/PDSN とポリシーおよび課金ルール機能（PCRF）によって実現されます。クライアント機能は HA/PDSN に付属しているため、IMS 承認（IMSA）シナリオではゲートウェイとも呼ばれます。PCEF 機能は、Enhanced Charging Service（ECS）により提供されます。Gx インターフェイスは、Diameter 接続として導入されます。Gx メッセージには、ほとんどの場合、ダイナミックルールのインストール/変更/削除と、事前定義されたルールのアクティブ化/非アクティブ化が含まれます。

Gx 参照ポイントは、ゲートウェイ/PCEF と PCRF の間にあります。この参照ポイントは、PCRF からゲートウェイ/PCEF への PCC ルールのプロビジョニングと削除、およびゲートウェイ/PCEF から PCRF へのトラフィック プレーン イベントの送信に使用されます。Gx 参照ポイントは、

アプリケーションに関連する AVP を適用することで、課金制御とポリシー制御のいずれかまたは両方に使用できます。

次の図は、ポリシーおよび課金アーキテクチャに含まれる要素間の参照ポイントを示します。

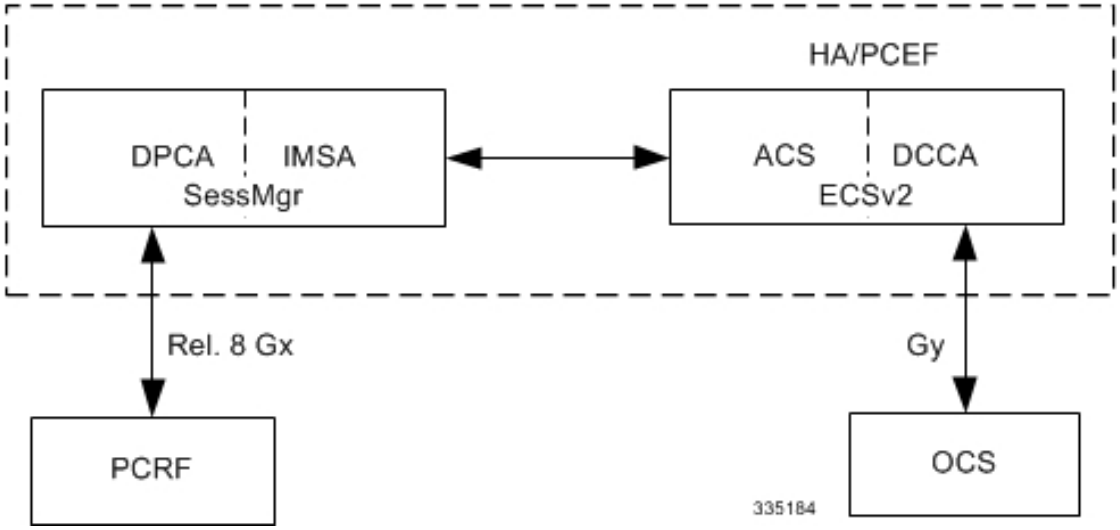
図 *62 : HA/PDSN Rel. 8 Gx PCC* 論理アーキテクチャ



ゲートウェイ内では、IMSA モジュールと DPCA モジュールが（SessMgr で）Gx プロトコル関連の機能を処理し、ポリシーの適用と課金は ECS で行われます。Gy プロトコル関連の機能は、DCCA モジュール内（ECS）で処理されます。

次の図は、ゲートウェイ内のコンポーネント間の連携動作を示しています。

図 *63 : HA/PDSN Rel. 8 Gx PCC* アーキテクチャ（*PCEF* 内）



ライセンス要件

HA/PDSN Rel. 8 Gx インターフェイスのサポートは、ライセンス供与されたシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

サポートされる標準

HA/PDSN Rel 8. Gx インターフェイスのサポートは、次の標準と RFC に基づいています。

- 3GPP TS 23.203 V8.3.0 (2008-09) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 8)
- 3GPP TS 29.212 V8.6.0 (2009-12) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 8)
- 3GPP TS 29.213 V8.1.1 (2008-10) 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 8)
- RFC 3588、Diameter Base Protocol。2003 年 9 月
- RFC 4006、Diameter Credit-Control Application。2005 年 8 月

用語および定義

このセクションでは、HA/PDSN Rel. 8 Gx に関連した機能と用語について説明します。

ポリシー制御

PCRF が IP-CAN セッションの制御方法を PCEF に指示するプロセスです。

ポリシー制御は、次の機能で構成されます。

- バインディング
- ゲート制御
- イベントレポート
- QoS 制御
- その他の機能

バインディング

HA/PDSN Rel. 8 Gx の実装では、MIP セッション内にベアラーがないため、IP-CAN ベアラーの概念が適用されません。承認済みの IP-CAN セッションのみが適用されます。

ゲート制御

ゲート制御とは、SDF に属するパケットが目的のエンドポイントに向かってパススルーすることをブロックまたは許可することです。ゲートは PCC ルール内で記述され、ゲート制御は SDF ごとに適用されます。ゲートを開閉するコマンドを実行すると、対応する IP パケットの経路が有効または無効になります。ゲートが閉じられている場合、関連する IP フローのすべてのパケットがドロップされます。ゲートが開いている場合、関連する IP フローのパケットの転送が許可されます。

イベントレポート

重要 PCEF が要求していない場合の PCRF から PCEF へのイベントトリガーの無条件レポートはサポートされていません。

重要 HA/PDSN Rel. 8 Gx の実装では、AN_GW_CHANGE (21) イベントトリガーのみサポートされます。

イベントレポートは、ユーザープレーンでの新しい動作をトリガーするアプリケーションイベントの通知とこうしたイベントへの応答、およびゲートウェイ（PCEF）のリソースに関連したイベントのレポートです。イベントトリガーを使用して、どの IP-CAN セッション変更や特定のイベントが発生すると、PCEF が PCC ルールを再要求するかを確認できます。PCEF から PCRF へのイベントトリガーレポート、およびイベントトリガーのプロビジョニングは、IP-CAN セッションレベルで行われます。

PCEF にあるイベントレポート機能（ERF）は、PCC ルールのプロビジョニング中に PCRF からイベントトリガーを受信し、イベントトリガー検出を実行します。受信したイベントトリガーに一致するイベントが発生すると、ERF は発生したイベントを PCRF に報告します。提示されたイベントトリガーが特定のパラメータ値に関連付けられている場合、ERF はそれらの値を PCRF への応答に含めます。

QoS 制御



重要 HA/PDSN Rel. 8 Gx の実装では、承認済みの IP-CAN セッションのみがサポートされます。IP-CAN ベアラーごとの承認済み QoS のプロビジョニング、QCI ごとの承認済み QoS のポリシー適用、および混合モードでの承認済み QoS の範囲の調整は、適用されません。

QoS 制御とは、SDF に許可される最大 QoS の承認と適用のことです。複数の SDF の集約の場合、個々の SDF の承認済み QoS 情報の組み合わせが、この集約の承認済み QoS として提供されます。SDF ごとの QoS 制御により、PCC アーキテクチャは、特定の SDF ごとに適用される承認済み QoS を PCEF に提供できます。

QoS 承認情報は、PCRF によって動的にプロビジョニングされる場合と、PCEF で事前定義された PCC ルールである場合があります。PCEF 内の事前定義された PCC ルールの場合、承認された QoS 情報は PCC ルールがアクティブになると有効になります。PCEF では、承認済み QoS 情報のさまざまなセット（PCRF から受信した情報と、事前定義された PCC ルールに対応する情報）が組み合わされます。PCRF は、事前定義された PCC ルールの承認済み QoS 情報を認識し、それらのルールをアクティブ化する際に、この情報を考慮します。これにより、PCRF によってアクティブ化される一連の PCC ルールの組み合わせによる承認済み QoS が、それらの PCC ルールが動的に提供されるか、事前定義されているか、またはその両方であるかに関係なく、サブスクリプションポリシーとオペレータポリシーによって指定された制限内に収まることが保証されます。

サポートする機能は次のとおりです。

- 承認済み QoS のプロビジョニングとポリシー適用：PCRF は PCEF に承認済み QoS を提供する場合があります。承認済み QoS は、適用されるリソースの適切な値を提供します。
- SDF ごとの承認済み QoS のポリシープロビジョニング：SDF ごとの承認済み QoS のプロビジョニングは、PCC ルールのプロビジョニング手順の一部です。
- SDF ごとの承認済み QoS のポリシー適用：承認済み QoS が PCC ルールに対して定義されている場合、PCEF は、その PCC ルールに対応する SDF のデータレートを、PCC ルールに対して承認済みの最大帯域幅を超えないように制限します（制限を超えるパケットを破棄します）。
- PCC ルールを非アクティブ化または削除すると、PCEF は、その PCC ルール用に予約されていたリソースを解放します。

その他の機能

ここでは、他のいくつかの機能について説明します。

PCC ルールエラーの処理

1 つ以上の PCC ルールのインストールまたはアクティブ化が失敗した場合、PCEF は、影響を受ける PCC ルールの CCR または RAA コマンドのいずれかに 1 つまたは複数の Charging-Rule-Report AVP を含めることで、PCRF にエラーを通知します。PCEF は、各 Charging-Rule-Report AVP 内に、1 つ以上の Charging-Rule-Name AVP または

Charging-Rule-Base-Name AVP を追加することによってエラーの発生した PCC ルールを示し、Rule-Failure-Code AVP を追加することによってエラーの理由コードを示し、また PCC-Rule-Status AVP を追加します。

1 つまたは複数の新しい PCC ルール（以前は正しくインストールされていなかったルール）のインストールまたはアクティブ化が失敗した場合、PCEF はプッシュモードとプルモードの両方で PCC-Rule-Status を INACTIVE に設定します。

PCC ルールが正常にインストールまたはアクティブ化されたが、PCEF によって適用できなくなった場合、PCEF は PCRF に新しい CCR コマンドを送信し、Charging-Rule-Report AVP を追加します。PCEF は、Charging-Rule-Report AVP 内に Rule-Failure-Code AVP を追加し、PCC-Rule-Status を INACTIVE に設定します。

GnGp HO シナリオ中にコリジョンが発生すると、CCR-U が生成され、ルールエラーを報告するために PCRF に送信されます。

この追加の Gx メッセージ（CCR-U）がトリガーされると、RAT_TYPE トリガーが有効になっている場合、複数の CCR-U を設定する必要が生じます。 設定しない場合、HO 中にコリジョンが発生するたびにサブスクライバコールがドロップされます。

HA/PDSN の Gx 実装では、以下のルール障害コードがサポートされています。

- RATING_GROUP_ERROR（2）
- SERVICE_IDENTIFIER_ERROR（3）
- GW/PCEF_MALFUNCTION（4）
- RESOURCES_LIMITATION（5）

RAR 手順において 1 つ以上の PCC ルールのインストールまたはアクティブ化が失敗した場合、Experimental-Result-Code AVP が DIAMETER_PCC_RULE_EVENT（5142）に設定された RAA コマンドが送信されます。

時刻プロシージャ

PCEF は、PCRF の指示に従って PCC ルール要求を実行します。再検証時間が PCRF によって設定されると、PCEF は PCRF との通信をトリガーし、確立された IP-CAN セッションに関する PCC ルールを PCRF に要求します。PCEF が REVALIDATION_TIMEOUT イベントをトリガーすると、PCEF はタイマーを停止します。

PCC ルールがインストールされている場合、非アクティブ状態です。Rule-Activation-Time / Rule-Deactivation-Time が指定されている場合、PCEF はその時間が経過した後にルールをアクティブまたは非アクティブに設定します。

CCA/RAR で Rule-Deactivation-Time AVP が省略されている場合、この AVP の以前の値は無効になります。新しい動作は、Gx の 3GPP 仕様、バージョン 12.1.0 に準拠しています。

PCRF が Rule-Deactivation-Time AVP なしで RAR/CCA-U で同じ事前定義済みルールを再度有効にすると、このルールの deactivation-time は削除されます。

以前の動作に切り替える場合、PCRF は PCRF メッセージ（RAR、CCA-U）で、predef-rule 名と一緒に Rule-Deactivation-Time AVP と同じ値を再送信する必要があります。

（注） この動作変更は、事前に定義したルールにのみ適用されます。

Gx 上のファイアウォールポリシーのサポート

Diameter AVP「SN-Firewall-Policy」が Diameter ダイナミックディクショナリに追加され、Gx インターフェイスでファイアウォールポリシーをサポートできるようになりました。この AVP は CCA-I メッセージにエンコードされ、APN 設定を介して PDP コンテキストに静的に割り当てられた、またはRADIUS の Access-Accept を介して動的に割り当てられた fw-and-nat ポリシーを適用/上書きできます。この AVP は、任意の CCA-U または RAR メッセージ内で解析することも可能です。これにより、現在 PDP コンテキストに割り当てられている fw-and-nat ポリシーを変更できます。

課金制御

重要 HA/PDSN Rel. 8 Gx の実装において、オフライン課金はサポートされていません。

課金制御は、SDF に属するパケットを課金キーに関連付け、必要に応じてオンライン課金を適用するプロセスです。FBC は、SDF のリアルタイム分析に基づいて、ベアラー使用量の差別化された課金を処理します。課金制御を可能にするために、PCC ルールの情報によって SDF が識別され、課金制御のパラメータが指定されます。PCC ルール情報は、サブスクリプションデータに依存する場合があります。

オンライン課金は Gy インターフェイスを介してサポートされます。オンライン課金の場合、PCEF イベント時にオンライン課金アクションを適用できます（たとえば、QoS 変更時の再承認など）。

PCC ルールでは課金システムとの連携が不要であること、つまりこの SDF のアカウンティングもクレジット制御も実行せず、その後オンライン課金もオフライン課金も実行されないことを PCEF に示すことができます。

サポートされる機能：

- IP-CAN セッションの課金関連情報のプロビジョニング
- 課金アドレスのプロビジョニング：プライマリまたはセカンダリイベント課金機能名（オンライン課金サーバー（OCS）アドレス）

重要 HA/PDSN Rel. 8 Gx の実装において、Gx を介したプライマリまたはセカンダリ課金収集機能名（オフライン課金サーバー（OFCS）アドレス）のプロビジョニングはサポートされていません。

- デフォルトの課金方法のプロビジョニング：このリリースでは、デフォルトの課金方法は CCR-I メッセージで送信されます。この場合、新しい AVP オンラインおよびオフラインが、設定に基づいて CCR-I メッセージで送信されます。コマンドレベルで受信した Online

または Offline AVP は、PCC ルールレベルで設定されていない場合、ダイナミックルールにのみ適用されます。

課金の相関

HA/PDSN Rel. 8 Gx の実装では、課金の相関はサポートされていません。PCRF は、IMS セッションで IP フローを一意に識別するフロー識別子を提供します。

ポリシーおよび課金制御（PCC）ルール

PCC ルールにより、SDF の検出が可能になり、ポリシー制御や課金制御のパラメータが提供されます。PCC ルールの目的は次のとおりです。

- PCC ルールの SDF フィルタ（パケットルールに一致）に基づいて、アップリンク IP フローとダウンリンク IP フローの両方のケースで、SDF に属するパケットを検出します。

  パケットと一致する PCC ルールがない場合、パケットはドロップされます。

- SDF が提供するサービスを特定します。
- SDF に適用可能な課金パラメータを指定します。
- SDF のポリシー制御を提供します。

PCEF は PCC ルールの優先順位に従って、PCC ルールの SDF フィルタと照らし合わせて受信パケットを評価し、受信パケットごとに PCC ルールを選択します。パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。

PCC ルールには次の 2 種類があります。

- ダイナミック PCC ルール：Gx インターフェイスを介して PCEF に動的にプロビジョニングされるルール。この PCC ルールは事前に定義することも、PCRF で動的に生成することもできます。ダイナミック PCC ルールは任意のタイミングでアクティブ化、変更、および非アクティブ化できます。
- 定義済み PCC ルール：通信事業者によって PCEF で事前設定されたルール。定義済み PCC ルールは、PCRF が任意のタイミングでアクティブ化または非アクティブ化できます。PCEF 内の定義済み PCC ルールをグループ化すると、PCRF は Gx 参照ポイント上で一連の PCC ルールを動的にアクティブ化できます。



重要 3 番目のルールであるスタティック PCC ルールは、通信事業者によってシャーシに事前設定できます。スタティック PCC ルールは、PCRF で明示的に認識されておらず、PCRF の制御下にありません。スタティック PCC ルールは、Gx で制御されない汎用ベアラーにバインドされます。

PCC ルールの構成は次のとおりです。

- ルール名：PCEF と PCRF 間の通信で PCC ルールを参照するために使用されます。

- サービス識別子：SDF が関連するサービスやサービスコンポーネントを識別するために使用されます。
- サービス データ フロー フィルタ：サービスフローフィルタは、ルールを適用するトラフィックの選択に使用されます。
- 優先順位：SDF フィルタが重複しているさまざまな PCC ルールでは、ルールの優先順位によって、どのルールが適用されるかが決まります。ダイナミック PCC ルールと定義済み PCC ルールの優先順位が同じ場合は、ダイナミック PCC ルールが優先されます。
- ゲートステータス：SDF フィルタによって検出された SDF がアップリンク方向またはダウンリンク方向で通過するか（ゲートが開いている）、または破棄されるか（ゲートが閉じている）かを示します。
- QoS パラメータ：QoS 情報には、QoS クラス識別子（SDF の認定された QoS クラス）と、アップリンクおよびダウンリンクの認定ビットレートが含まれます。
- 課金キー（料金設定グループ）
- その他の課金パラメータ：課金パラメータは、オンライン課金インターフェイスを使用するかどうか、どのレベルで PCEF がルールに関連する使用状況を報告するかなどを定義します。

重要 ダイナミック PCC ルールの計測方式とレポートレベルの設定はサポートされていません。

アプリケーション機能（AF）が Rx インターフェイスを介してこの情報を提供した場合、PCC ルールにはアプリケーションとベアラーレイヤー間の課金相関を有効にするための AF レコード情報も含まれます。IMS の場合は、IMS 課金識別子（ICID）とフロー識別子が含まれます。

重要 ASR 5500 は、Gx メッセージのダイナミック課金ルールごとのフロー説明を含む 8 つのフロー情報のみをサポートします。

セッションマネージャがクラッシュした場合、最大 24 の PCC ルールを ICSR 後に回復できます。

回復可能な PCC ルールの制限が増加しても、ルールが失われることはないため、エンドユーザーに適用される課金は影響を受けません。

保留状態の PCC ルールの変更が受信されると、変更されたパラメータは P-GW でバッファに保存されます。保留中の要求に対する応答をアクセスネットワークから受信した後、P-GW はバッファされたパラメータの変更を処理し、必要に応じてネットワークに対する別の更新要求を生成します。

Gx 参照ポイントを介した PCC 手順

PCC ルールの要求

PCEF は、Gx 参照ポイントを使用して、次の場合に PCC ルールを要求します。

- IP-CAN セッションの確立時
- IP-CAN セッションの変更時

PCC ルールは、イベントトリガーを求めずに、PCC ルールのインストール/アクティブ化または適用の失敗の結果として要求することもできます。

PCC ルールのプロビジョニング

PCRF は、Rel. 8 Gx 参照ポイントを介して、PCEF で適用される PCC ルールを示します。これは、次のいずれかの手順で行われます。

- プル（PCEF により要請されたプロビジョニング）：PCEF による PCC ルールの要求に応じて、PCRF は CC-Answer で PCC ルールをプロビジョニングします。
- プッシュ（要請のないプロビジョニング）：PCRF は、PCEF からの要求を取得せずに PCC ルールのプロビジョニングを決定することがあります。たとえば、Rx 参照ポイントを介して PCRF に提供された情報への応答、または PCRF 内の内部トリガーへの応答。PCEF からの要請なしに PCC ルールをプロビジョニングするために、PCRF はこれらの PCC ルールを RA 要求メッセージに含めます。この RA 要求によってトリガーされる CCR および CCA メッセージはありません。

PCEF からの要求ごとに、または要請のないプロビジョニング時に、PCRF は 0 個以上の PCC ルールをプロビジョニングします。PCRF は、次のいずれかの方法で単一の PCC ルールに対する操作を実行できます。

- PCEF で事前定義された PCC ルールをアクティブ化または非アクティブ化する場合、PCRF は、Charging-Rule-Name AVP 内でこの PCC ルールへの参照をプロビジョニングし、Charging-Rule-Install AVP または Charging-Rule-Name AVP のいずれかを選択して必要なアクションを提示します。
- PCRF によりプロビジョニングされた PCC ルールをインストールまたは変更する場合、PCRF は、Charging-Rule-Install AVP 内で対応する Charging-Rule-Definition AVP をプロビジョニングします。
- 以前に PCRF によってプロビジョニングされた PCC ルールを削除する場合、PCRF は、このルールの名前を Charging-Rule-Remove AVP 内の Charging-Rule-Name AVP の値にしてプロビジョニングします。



重要 課金ルール名の最大長は 63 バイトです。課金ルール名の長さが 63 バイトを超える場合、Rule-Failure-Code が RESOURCES_LIMITATION の課金ルールレポートが送信されます。この課金ルールレポートは、ルール名の長さが 128 文字未満の場合にのみ送信されます。課金ルール名の長さが 128 文字以上の場合、課金ルールレポートは送信されません。

セッションの接続中、P-GW は、同じ CCR-U にルールの失敗とクレジットの不足を組み合わせて PCRF に送信します。

アップリンク IP パケットの PCC ルールの選択

PCC が有効になっている場合、PCEF は、PCC ルールの優先順位に従い、IP CAN セッションの PCRF が提供するアクティブな PCC ルールまたは事前定義済みのアクティブな PCC ルールのアップリンク SDF フィルタを使用してパケットを評価することで、IP CAN セッション内の受信アップリンク IP パケットそれぞれに適用する PCC ルールを選択します。



重要 PCRF が提供する PCC ルールと事前定義された PCC ルールが同じ優先順位を持つ場合、PCRF が提供する PCC ルールのアップリンク SDF フィルタが最初に適用されます。

パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。対応する IP CAN セッションのいずれの PCC ルールにも一致しないアップリンク IP パケットは廃棄されます。

ダウンリンク IP パケットの PCC ルールの選択

PCC が有効になっている場合、PCEF は、PCC ルールの優先順位に従い、IP-CAN セッションの PCRF が提供するアクティブな PCC ルールまたは事前定義済みのアクティブな PCC ルールのダウンリンク SDF フィルタを使用してパケットを評価することで、IP-CAN セッション内の受信ダウンリンク IP パケットそれぞれに適用する PCC ルールを選択します。



重要 PCRF が提供する PCC ルールと事前定義された PCC ルールが同じ優先順位を持つ場合、PCRF が提供する PCC ルールのダウンリンク SDF フィルタが最初に適用されます。

パケットが SDF フィルタに一致すると、そのパケットの照合プロセスが完了し、そのフィルタの PCC ルールが適用されます。IP-CAN セッションのいずれの PCC ルールにも一致しないダウンリンク IP パケットは廃棄されます。

次の手順もサポートされています。

- IP-CAN セッション終了の表示：IP-CAN セッションが終了している場合、PCEF は PCRF に接続します。
- IP-CAN セッション終了の要求：内部トリガーまたは SPR からのトリガーにより PCRF が IP-CAN セッションの終了を決定した場合、PCRF は PCEF に通知します。PCEF は PCRF

に確認応答し、その IP-CAN セッションで以前にインストールまたはアクティブ化されたすべての PCC ルールを即座に削除または非アクティブ化します。

PCEF は IP-CAN セッションを終了するために、IP-CAN 固有の手順を適用します。HA または PDSN は、IP-CAN セッション全体の終了が要求されたことを示すティアダウンインジケータを設定した MIP 失効要求を送信します。さらに、PCEF は「IP-CAN セッション終了の表示」の手順を適用します。

- セッション確立中に Supported-Features AVP を使用して、送信元ホストがサポートする必須機能とオプション機能について宛先ホストに通知します。

機能の仕組み

このセクションでは、HA/PDSN Rel. 8 Gx インターフェイスサポートの仕組みについて説明します。

次の図と表は、UE により開始される、システムと IMS コンポーネント間の IMS 承認プロセスについて説明しています。

この例では、Diameter ポリシー制御アプリケーション（DPCA）が PCRF への Gx インターフェイスです。PCRF との IMSA 間のインターフェイスは Gx インターフェイスで、セッションマネージャ（SessMgr）とオンライン課金サービス（OCS）間のインターフェイスは Gy インターフェイスです。IMSA サービスと DPCA はシステムの SessMgr の一部であることに注意してください。分かりやすくするために、図では分離されています。

重要 DPCA と IMSA は、ポリシーサーバーインターフェイスアプリケーション内の 1 つのモジュールとして動作します。

図 *64 : HA/PDSN Rel. 8 Gx IMS* 承認コールのフロー

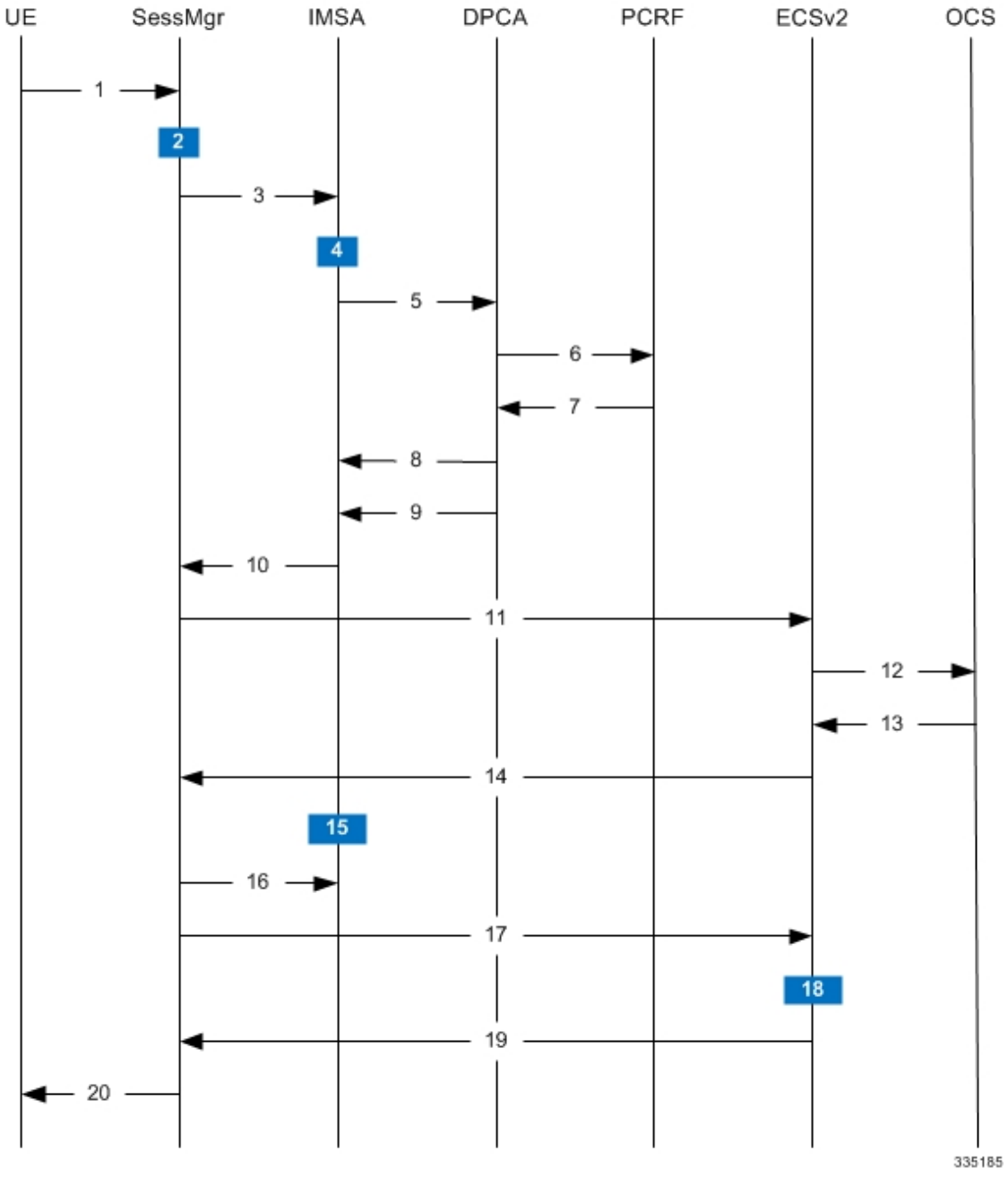


表 *73 : HA/PDSN Rel. 8 Gx IMS* 承認コールのフローの説明

ステップ	説明
1	UE（IMS サブスクライバ）が MIP 登録要求を要求します。
2	SessMgr が UE に IP アドレスを割り当てます。

ステップ	説明
3	サブスクライバに対して IMSA が有効になっている場合、SessMgr は IMS 承認を要求します。 IMSA サービスは、サブスクライバテンプレートで設定できます。または AAA から受け取ることもできます。
4	IMSA が、IP-CAN セッションにリソースを割り当て、ユーザーの選択キー（たとえば round-robin）に基づいて接続する PCRF を選択します。
5	IMSA が、DPCA モジュールに対して PCRF に承認要求を発行するよう要求します。
6	DPCA は、選択された PCRF に CCR 初期メッセージを送信します。
7	PCRF は、事前設定された課金ルールを CCA で送信できます。PCRF は、ダイナミックルールと承認された QoS パラメータも含める場合があります。
8	DPCA は、課金ルールの定義、課金ルールのインストール、PCRF から受信した QoS 情報、イベントトリガーなどを渡します。この情報は IMSA によって保存されます。
9	DPCA は、IMSA によって登録されたコールバック関数を呼び出します。
10	IP-CAN セッション全体に共通の PCRF 提供情報（イベントトリガー、プライマリ/セカンダリ OCS アドレスなど）は IMSA 内に保存されます。IMSA は、情報を処理した後、ポリシー承認が完了したことを SessMgr に通知します。
11	IMSA/DPCA でルールの検証が失敗した場合、Charging-Rule-Report AVP を含む PCRF に失敗が通知されます。それ以外の場合、IMSA が ECS セッションの作成を開始します。プライマリ/セカンダリ OCS サーバーアドレスなどが、SessMgr から ECS に送信されます。
12	ECS は、CC-Request-Type を INITIAL_REQUEST に設定した CCR(I) を OCS に送信してクレジット承認を実行し、クレジット制御セッションを開きます。この要求には、アクティブな Rulebase-Id（AAA からのデフォルトのルールベース ID）が含まれています。
13	OCS が CCA 初期メッセージを返します。これにより、静的に設定されたルールベースがアクティブ化されることがあります。また、プリエンプティブクォータが含まれていることがあります。
14	ECS が、応答メッセージで SessMgr に応答します。
15	SessMgr が、ダイナミックルールの IMSA を要求します。
16	IMSA がダイナミックルールを SessMgr に送信します。 RAR メッセージは、セッションが確立される前に許可されます。 また、ダイナミックルール情報のリカバリとセッションマネージャの監査が進行中の場合は、RAR メッセージが拒否され、結果コード 3002 の RAA が送信されることに注意してください。

ステップ	説明
17	SessMgr が、ダイナミックルール情報を ECS に送信します。ゲートフローステータス情報およびフローごとの QoS（課金ルール）情報もメッセージで送信されます。
18	ECS は、受け取った事前定義済みルールをアクティブ化し、受け取ったダイナミックルールをインストールします。また、ゲートフローステータスと QoS パラメータが、ダイナミック課金ルールに従い ECS によって更新されます。Gx ルールベースは、ECS の group-of-ruledefs として扱われます。応答メッセージには、ECS でのルールプロビジョニングのステータスを伝達する課金ルールレポートが含まれます。
19	ルールのプロビジョニングが部分的に失敗した場合、コンテキストセットアップが受け入れられ、失敗したルールの PCC ルールステータスを含む Charging-Rule-Report とともに、新しい CCR-U が PCRF に送信されます。ルールのプロビジョニングが完全に失敗すると、コンテキストセットアップが拒否されます。
20	MIP セッション承認の応答に応じて、SessMgr は応答を UE に送信し、コールをアクティブにするか、拒否します。Charging-Rule-Report にいずれかのルールの部分的な失敗が含まれている場合、PCRF に通知され、コールがアクティブ化されます。Charging-Rule-Report に完全な失敗が含まれている場合、コールは拒否されます。

HA/PDSN Rel. 8 Gx インターフェイスのサポート

HA/PDSN Rel. 8 Gx インターフェイスの機能を設定するには、次の手順を実行します。

1. コンテキストレベルでの IMS 承認サービスの設定 （772 ページ）の説明に従って、コンテキストレベルで IMS サブスクライバの IMSA サービスを設定します。
2. 同じコンテキスト内で、サブスクライバテンプレートへの IMS 承認サービスの適用 （773 ページ）の説明に従って、IMSA サービスを使用するためのサブスクライバテンプレートを設定します。
3. Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

重要 この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンド、および/またはキーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

コンテキストレベルでの IMS 承認サービスの設定

コンテキストレベルで IMS サブスクライバの IMSA サービスを設定するには、次の例に示すコマンドを使用します。

```
configure
     context <context_name>
          ims-auth-service <imsa_service_name>
               policy-control
                    diameter origin endpoint <endpoint_name>
                    diameter dictionary <dictionary>
                    diameter request-timeout <timeout_duration>
                    diameter host-select table { 1 | 2 } algorithm
round-robin
                   diameter host-select row-precedence <precedence_value>
 table { 1 | 2 } host <primary_host_name> [ realm <primary_realm_id> ] [
secondary host <secondary_host_name> [ realm <secondary_realm_id> ] ] [
-noconfirm ]
                    failure-handling cc-request-type { any-request |
initial-request | terminate-request | update-request } {
diameter-result-code { any-error | <result_code> [ to <end_result_code> ] }
} { continue | retry-and-terminate | terminate }
                    exit
               exit
          diameter endpoint <endpoint_name> [ -noconfirm ]
               origin realm <realm_name>
               use-proxy
               origin host <host_name> address <ip_address>
               no watchdog-timeout
               response-timeout <timeout_duration>
               connection timeout <timeout_duration>
               connection retry-timeout <timeout_duration>
              peer <primary_peer_name> [ realm <primary_realm_name> ] address
 <ip_address> [ port <port_number> ]
             peer <secondary_peer_name> [ realm <secondary_realm_name> ] address
 <ip_address> [ port <port_number> ]
               end
```

注：

- <*context_name*> は、IMSA サービスを有効にするコンテキストの名前です。
- <*imsa_service_name*> は、リリース8 Gx インターフェイス認証用に設定する IMSA サービスの名前です。
- 最大 30 個の IMS 承認サービスプロファイルをシステムに設定できます。
- Rel. 8 Gx インターフェイスのサポートを有効にするには、関連する Diameter ディクショナリを設定する必要があります。使用する具体的な Diameter ディクショナリの詳細については、シスコのアカウント担当者にお問い合わせください。
- PCRF 選択のためのラウンドロビンアルゴリズムは、多数の PCRF を選択する場合にのみ効果的であり、細かいレベルでの効果は薄いです。

- PCEF で設定される PCRF ホスト宛先を設定するには、**diameter host-select** CLI コマンドを使用します。
- Gx が失敗したときに事前に定義されたルールを使用するように PCEF を設定するには、**failure-handling cc-request-type** CLI を **continue** に設定します。使用可能または使用中のポリシーは引き続き使用され、PCRF とのそれ以上の連携はありません。

IMSA サービス設定の確認

IMSA サービスの設定を確認するには、次のコマンドを実行します。

1. IMSA サービスを有効にしたコンテキストに変更するには、次のコマンドを入力します。

   context <*context_name*>

2. 次のコマンドを入力して、IMSA サービスの設定を確認します。

   show ims-authorization service name <*imsa_service_name*>

サブスクライバテンプレートへの IMS 承認サービスの適用

コンテキストレベルで IMSA サービスを設定した後、同じコンテキスト内で、IMS サブスクライバに対して IMSA サービスを使用するようにサブスクライバテンプレートを設定する必要があります。

次の例を使用して、「コンテキストレベルでの IMS 承認サービスの設定（772 ページ）」で説明されているように設定されたコンテキスト内のサブスクライバテンプレートに IMSA サービス機能を適用します。

```
configure
   context <context_name>
      subscriber default
         encrypted password <encrypted_password>
         ims-auth-service <imsa_service_name>
         ip access-group <access_group_name> in
         ip access-group <access_group_name> out
         ip context-name <context_name>
         mobile-ip home-agent <ip_address>
         active-charging rulebase <rulebase_name>
         end
```

注：

- <*context_name*> は、IMSA サービスが設定されたコンテキストの名前である必要があります。
- <*imsa_service_name*> は、コンテキストで IMS 認証用に設定された IMSA サービスの名前である必要があります。
- サブスクライバテンプレートで ECS ルールベースを設定する必要があります。

- PCRF からの Gx ルールベース（Charging-Rule-Base-Name AVP）を ECS の group-of-ruledefs として解釈するには、アクティブ課金サービス コンフィギュレーション モードで次のコマンドを設定します。

  policy-control charging-rule-base-name active-charging-group-of- ruledefs

サブスクライバ設定の確認

Exec CLI コンフィギュレーション モードで次のコマンドを入力して、サブスクライバの IMSA サービスの設定を確認します。

show subscribers ims-auth-service <*imsa_service_name*>

注：

- <*imsa_service_name*> は、IMS 認証用に設定された IMSA サービスの名前にする必要があります。

統計情報の収集

ここでは、Rel. 8 Gx の統計と設定情報を収集する方法について説明します。

次の表では、最初の列に、収集する統計が示されており、2 つ目の列に、実行するアクションが示されています。

表 *74 : HA/PDSN* リリース *8 Gx* の統計と情報の収集

統計/情報	実行するアクション
IMS 承認サービスのポリシー制御に固有の情報と統計。	**show ims-authorization policy-control statistics**
IMS 承認サービスに使用される、承認サーバーに固有の情報と統計。	**show ims-authorization servers ims-auth-service**
すべての IMS 承認サービスの情報。	**show ims-authorization service all**
IMS 承認サービスの統計。	**show ims-authorization service statistics**
IMS 承認サービスでアクティブなセッションの情報、設定、統計。	**show ims-authorization sessions all**
IMS 承認サービスでアクティブなセッションの完全な情報、設定、統計。	**show ims-authorization sessions full**
IMS 承認サービスでアクティブなセッションの要約情報。	**show ims-authorization sessions summary**
アクティブな課金サービスセッションの完全な統計。	**show active-charging sessions full**

統計/情報	実行するアクション
サービスに設定されているすべてのルール定義に関する情報。	**show active-charging ruledef all**
システムに設定されているすべてのルールベースに関する情報。	**show active-charging rulebase all**
システムに設定されているすべての ruledef グループに関する情報。	**show active-charging group-of-ruledefs all**

P-GW Rel. 8 Gx インターフェイスのサポート

はじめに

Gx 参照ポイントは、パケットデータネットワーク（PDN）ゲートウェイ（P-GW）上のポリシーおよび課金ルール機能（PCRF）とポリシーおよび課金適用機能（PCEF）の間にあります。Gx 参照ポイントは、PCRF から PCEF への PCC ルールのプロビジョニングと削除、および PCEF から PCRF へのトラフィック プレーン イベントの送信に使用されます。Gx 参照ポイントは、アプリケーションに関連する AVP を適用することで、課金制御とポリシー制御のいずれかまたは両方に使用できます。

PCEF は、ポリシーの適用とフローベースの課金機能を包含する機能要素です。この機能エンティティは P-GW にあります。これには、以下の主要な機能があります。

- ゲートウェイでのユーザー プレーン トラフィックの処理とその QoS の制御。
- サービスデータフローの検出とカウント、およびオンラインとオフラインの課金操作。
- ポリシー制御されているサービスデータフローの場合、PCEF は、対応するゲートウェイが開いている場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- 課金制御されているサービスデータフローの場合、PCEF は、対応するアクティブな PCC ルールがあり、オンライン課金で OCS がその課金キーで該当するクレジットを承認した場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- PCRF から要求された場合、PCEF は関連するサービスデータフローのステータスが変わったときに PCRF に報告します。
- SDF が BBERF でトンネリングされている場合、PCEF は、IP-CAN セッションの確立時のサービスデータフローのモビリティ プロトコル トンネリング ヘッダーについて PCRF に通知します。

用語および定義

このセクションでは、Rel. 8 Gx に関連した機能と用語について説明します。

Gx を介したボリュームレポート

ここでは、3GPP Rel. 9 の Gx を介したボリュームレポート機能について説明します。

ライセンス要件

Gx を介したボリュームレポートは、シスコのライセンス供与された機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。



重要 Gxを介した課金機能またはGxを介したボリュームレポート機能に個別のライセンスは必要ありません。この機能は、「ポリシーインターフェイス」ライセンスの一部として有効にすることができます。

サポートされる標準

Gx を介したボリュームレポート機能は、次の標準規格に基づいています。

3GPP TS 29.212 V9.5.0 (2010-06)：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control over Gx reference point (Release 9)

機能の概要

Gxを介したボリュームレポート機能により、PCRFはサブスクライバのデータ使用量に基づいてリアルタイムの決定ができます。



重要 Volume Reporting over Gx は、ボリュームクォータにのみ適用されます。

ボリュームレポートは、合計データ使用量レポートとアップリンク/ダウンリンクレベルのレポートの両方をサポートします。

PCEF は、最初からではなく、使用状況監視の最後のレポート以降の累積使用量のみを報告します。

使用量しきい値がゼロ（無限しきい値）に設定されている場合、PCEF によってそれ以上のしきい値イベントは生成されませんが、使用状況の監視は続行され、セッションの終了時に報告されます。

ベアラーの終了時の使用状況レポートがサポートされています。

次の手順を通じて、Gx を介したボリュームレポートの仕組みについて説明します。

1. PCEF は、PCRF からメッセージを受信した後、使用状況モニタリング関連の AVP を解析し、その情報を IMSA に送信します。
2. IMSA はこの情報で ECS を更新します。

3. PCRF からの使用状況モニタリング情報で ECS が更新されると、PCEF（ECS）はデータ使用状況の追跡を開始します。
4. セッションレベルのモニタリングの場合、ECS がデータ使用状況を保持します。
5. PCC ルールモニタリングの場合、モニタリングキーを一意の識別子として使用状況がモニタリングされます。各ノードがモニタリングキーごとの使用状況情報を保持します。データトラフィックが通過すると、使用量しきい値に照らして使用状況がチェックされ、「使用状況レポート」セクションに説明されているようにして報告されます。
6. PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況を追跡し続けます。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されません。

使用状況モニタリング

- セッションレベルでの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に使用量しきい値レベルを設定し、Usage-Monitoring-Level AVP を SESSION_LEVEL(0) に設定して、Usage-Monitoring-Information AVP を送信することで、Gx に関するセッションレベルのボリュームレポートにサブスクライブします。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。PCRF は、セッションレベルでモニタリングキーをサポートしています。

  PCRF では、単一のメッセージでセッションの使用状況を有効または無効にすることができます。この操作は、モニタリングキーがセッションレベルで関連付けられている場合にのみ可能です。

  PCRF では、入力/出力オクテットのしきい値レベルに基づき使用状況をモニタリングできます。有効になっているしきい値レベルに基づいて使用状況が報告されます。複数のレベルが有効になっている場合は、いずれか1つのレベルで侵害が発生しても、有効になっているすべてのレベルについて使用状況が報告されます。モニタリングは、PCRF からの使用状況レポートの応答で欠落しているしきい値レベルで停止されます（PCRF が以前に有効にされた複数のレベルでモニタリングを継続する場合、完全なセットを再度提供することが期待されます）。

  合計しきい値レベルと GSU AVP の UL/DL しきい値レベルの両方が提供された場合はエラーとして扱われ、合計しきい値レベルのみが受け入れられます。

  次の要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U が生成されます。

  - モニタリングキーを使用したルールレベルでの即時レポート要求
  - モニタリングキーを使用した、または使用しないセッションレベルでの即時レポート要求
  - ルールレベルでの明示的な無効化要求
  - セッションレベルでの明示的な無効化要求

上記のすべての要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U は生成されません。また、すべてのアクティブなモニタリングキーの使用状況を報告した CCR-U への応答で、ルールレベルのモニタリングキーのない即時レポート要求を受信した場合、追加の CCR-U は生成されません。

- フローレベルの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルと PCC_RULE_LEVEL(1) に設定された Usage-Monitoring-Level AVP とともに Usage-Monitoring-Information AVP を送信することで、Gx を介してフローレベルのボリュームレポートに登録します。フローレベルのモニタリングの場合、モニタリングキーは必須です。PCRF がルールとモニタリングキーを関連付ける際や、フローレベルで使用状況モニタリングを有効化または無効化する際に、モニタリングキーを使用して制御できるためです。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。

  使用状況モニタリングは、スタティックルール、定義済みルール、およびダイナミックルール定義に対応しています。

  - スタティックルールの使用状況モニタリング：スタティックルールの場合、モニタリングキーに関連付けられた最後のルール削除に関する使用状況はレポートの対象外になります。この場合、PCRF から使用状況モニタリング情報のみを受信します。
  - 定義済みルールの使用状況モニタリング：事前定義されたルールに対して使用状況モニタリングを有効にする必要がある場合、PCRF は、モニタリングキーと使用量しきい値を含むルールおよび使用状況モニタリング情報を送信します。モニタリングキーは、その事前定義済みルールの PCEF で事前設定されているものと同じである必要があります。同じモニタリングキーに複数のルールを関連付けることができます。そのため、特定のモニタリングキーを有効にすると、同じモニタリングキーを持つ複数のルールのデータが追跡されることになります。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。
  - ダイナミックルールの使用状況モニタリング：ダイナミックルール定義に対して使用状況モニタリングを有効にする必要がある場合、PCRF は課金ルールの定義や使用状況モニタリング情報（モニタリングキー、使用量しきい値など）とともにモニタリングキーを提供します。これにより、そのモニタリングキーに関連付けられているすべてのルールに対して使用状況モニタリングが実行されます。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。ダイナミックルール定義のモニタリングキーは、PCRF によって動的に割り当てられます。これが、使用状況モニタリングのケースにおいて定義済みルールとの唯一の違いです。

モニタリングキーの 1 つの使用状況だけが最初に報告されます。PCRF から正常な応答を受信すると、残りのモニタリングキーの使用状況が PCRF に報告されます。Tx 期限切れ/TCP リン

クエラーが発生すると、報告されていない使用状況が ECS に保存されます。セッションでその後 PCRF と正常なやり取りがあった場合、報告されていない UMI が PCRF に送信されます。

使用状況レポート

サブスクライバレベルやフローレベルでの使用状況は、次の条件で PCRF に報告されます。

- 使用量しきい値に達した：PCEF はサブスクライバデータの使用量を記録し、PCRF によって指定される使用量しきい値に達しているかどうかを確認します。これは、セッションレベルとルールレベルの両方のレポートで行われます。

  セッションレベルのレポートでは、実際の使用量が、使用量しきい値と比較されます。

  ルールレベルのレポートでは、データトラフィックにヒットするルールを使用して、モニタリングキーが関連付けられているかどうかが確認され、モニタリングキーに基づいてデータ使用量が確認されます。条件が満たされると、使用状況の情報を IMSA に報告し、モニタリングを続行します。IMSA は、「USAGE_REPORT」トリガーが PCRF によって有効になっている場合に、CCR-U をトリガーします。この CCR で、Usage-Monitoring-Information AVP と、サブスクライバのデータ使用量を設定した「Used-Service-Unit」が送信されます。

  使用量しきい値に達したときに、PCRF が使用状況モニタリング情報に PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、使用状況は報告されません。

  Gx を介した非標準ボリュームレポートの実装では、しきい値に違反すると使用状況モニタリングが停止します。それ以外の場合はモニタリングが続行されます。CCA が受信されるまで、以降の使用状況は報告されません。

- 使用状況モニタリングが無効：レポートの使用状況、その他の外部トリガー、または PCRF 内部トリガーに関連しない PCEF からの CCR の結果として PCRF により使用状況モニタリングが無効にされた場合には、PCRF が Usage-Monitoring-Support AVP を USAGE_MONITORING_DISABLED に設定して使用状況モニタリングを明示的に無効にすると、PCEF はモニタリングを停止し、（モニタリングが有効だったときの）使用状況情報を PCRF に報告します。使用量しきい値に達したときに、PCRF が PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、これ以降の使用状況は報告されません。

- IP CAN セッションの終了：IP CAN セッションが終了すると、サブスクライバの累積使用状況情報が PCEF からの CCR-T で PCRF に報告されます。PCC 使用量レベル情報が PCRF によって有効になっている場合、PCC 使用量も報告されます。

  PCRF は RAR メッセージを使用し、その中に Session-Release-Cause AVP を含めて、IP CAN セッション終了を開始します。ただし、PCRF が CCA メッセージで IP CAN セッションを終了する場合もあります。不要な追加メッセージを回避するために、PCRF は、CCA-U メッセージ自体で、サブスクライバを終了するように P-GW に通知できます。そのため、すべての Gx ディクショナリの CCA メッセージに Session Release Cause が追加されました。

- PCC ルールの削除：PCRF が使用量モニタリングキーに関連付けられている最後の PCC ルールを非アクティブ化すると、PCEF はそのモニタリングキーのデータ使用量を含む CCR を送信します。使用量モニタリングキーに関連付けられている最後の PCC ルールが非アクティブであると PCEF が報告する場合に、CCR コマンドに Charging-Rule-Report AVP が含まれていたなら、PCEF は同じ CCR コマンドでそのモニタリングキーの累積使用量を報告します。あるいは、Charging-Rule-Report AVP が RAA コマンドに含まれている場合、PCEF は新規に CCR コマンドを送信して、使用状況モニタリングキーの累積使用量を報告します。PCRF によって設定された、ルールの非アクティブ化時間を使用した最後のルールの非アクティブ化に関する使用状況レポートがサポートされています。

  PCRF からのメッセージを受信すると、削除対象のルールがマーク付けされ、アクセス側の手順が完了した後にルールが削除されます。

- PCRF 要求使用状況レポート：最後のレポートの送信以降の累積使用量（即時レポートの場合も同様）。即時レポート後に使用量はリセットされ、使用状況モニタリングが続行されます。後続の使用状況レポートには現在のレポート以降の使用量が含まれるようになります。

- ベアラーの終了に関する使用状況レポートを追加できます。ベアラーが何らかの理由で削除されると、そのベアラーに関連付けられているルールも削除されます。そのため、使用状況は、ベアラー終了が原因で削除された最後のルールが関連ルールであるモニタリングキーで報告されます。

- 再検証のタイムアウト：非標準の実装では、使用状況モニタリングとレポートが有効になっていて、再検証タイムアウトが発生した場合、PCEF は CCR を送信して PCC ルールを要求し、最後のレポート以降（または、使用状況がまだ報告されていない場合には、使用状況レポートが有効になった時点以降）の有効なすべてのモニタリングキーのすべての累積使用量を、IP-CAN セッションレベル（有効な場合）およびサービスデータフローレベル（有効な場合）の累積使用量を使用して報告します。これがデフォルトの動作です。

  標準実装の場合、これは CLI 設定によって有効にする必要があります。



重要 再検証タイムアウト時の使用状況レポート機能は、Gx を介したボリュームレポートの非標準実装ではデフォルトで使用できます。この機能は標準実装で設定可能です。

使用状況が報告されると、使用量カウンタはゼロにリセットされます。PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況の追跡を 0 から継続します。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されず、CCR-CCA 間の累積使用量は破棄されます。

サーバーの再試行でトリガーされた CCR-U は、サーバーによって付与されたクォータを考慮して、USU を報告します。新たに作成された MSCC の場合、USU を報告するために暫定クォータ設定が取得されます。

Gx を介したボリュームレポート機能を設定する方法については、「Gx を介したボリュームレポートの設定 （755 ページ）」を参照してください。

Gx を介したボリュームレポート（*VoRoGx*）のための *ICSR* サポート

ボリュームのしきい値とボリュームの使用状況はスタンバイシャーシに同期され、ICSR スイッチオーバー後の既存のセッションの Gx を介したボリュームレポートをサポートします。

このサポートがないと、たとえば適切な使用を強制するためにボリュームレポートを使用した場合に、サブスクライバが想定以上に高い速度を使用する可能性はありません。通信事業者はこれをすでに収益の損失と見なしている可能性があります。また、EUのローミング規制によって設定された制限に達すると、通知を受け取り、ブロック/リダイレクトされるローミングサブスクライバに深刻な影響を及ぼします。セッションがブロックされずにこの時点でセッションが継続する場合、通信事業者は上限を超えたデータに課金することができず、実質的な収益の大幅な損失が発生します（ローミングパートナーはSGSNで使用されるデータに課金する場合があります）。

Rel. 9 Gx インターフェイス

Rel. 9 Gx インターフェイスのサポートは、Cisco ASR シャーシで使用できます。

P-GW Rel. 9 Gx インターフェイスのサポート

はじめに

Gx 参照ポイントは、パケットデータネットワーク（PDN）ゲートウェイ（P-GW）上のポリシーおよび課金ルール機能（PCRF）とポリシーおよび課金適用機能（PCEF）の間にあります。Gx 参照ポイントは、PCRF から PCEF への PCC ルールのプロビジョニングと削除、および PCEF から PCRF へのトラフィック プレーン イベントの送信に使用されます。Gx 参照ポイントは、アプリケーションに関連する AVP を適用することで、課金制御とポリシー制御のいずれかまたは両方に使用できます。

PCEF は、ポリシーの適用とフローベースの課金機能を包含する機能要素です。この機能エンティティは P-GW にあります。これには、以下の主要な機能があります。

- ゲートウェイでのユーザー プレーン トラフィックの処理とその QoS の制御。
- サービスデータフローの検出とカウント、およびオンラインとオフラインの課金操作。
- ポリシー制御されているサービスデータフローの場合、PCEF は、対応するゲートウェイが開いている場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- 課金制御されているサービスデータフローの場合、PCEF は、対応するアクティブな PCC ルールがあり、オンライン課金で OCS がその課金キーで該当するクレジットを承認した場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- PCRFから要求された場合、PCEFは関連するサービスデータフローのステータスが変わったときに PCRF に報告します。

- SDF が BBERF でトンネリングされている場合、PCEF は、IP-CAN セッションの確立時のサービスデータフローのモビリティ プロトコル トンネリング ヘッダーについて PCRF に通知します。



重要 ASR 5500 は、Gx メッセージのダイナミック課金ルールごとのフロー説明を含む 8 つのフロー情報のみをサポートします。

用語および定義

このセクションでは、Rel. 9 Gx に関連する機能と用語について説明します。.

Gx を介したボリュームレポート

ここでは、3GPP Rel. 9 の Gx を介したボリュームレポート機能について説明します。

ライセンス要件

Gx を介したボリュームレポートは、シスコのライセンス供与された機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。



重要 Gx を介した課金機能または Gx を介したボリュームレポート機能に個別のライセンスは必要ありません。この機能は、「ポリシーインターフェイス」ライセンスの一部として有効にすることができます。

サポートされる標準

Gx を介したボリュームレポート機能は、次の標準規格に基づいています。

3GPP TS 29.212 V9.5.0 (2011-01)：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control over Gx reference point (Release 9)

機能の概要

Volume Reporting over Gx 機能により、PCRF はサブスクライバのデータ使用量に基づいてリアルタイムの決定ができます。



重要 Volume Reporting over Gx は、ボリュームクォータにのみ適用されます。

Gx を介したボリュームレポートは、合計データ使用量レポートとアップリンク/ダウンリンクレベルのレポートの両方をサポートします。

PCEF は、最初からではなく、使用状況監視の最後のレポート以降の累積使用量のみを報告します。

使用量しきい値がゼロ（無限しきい値）に設定されている場合、PCEF によってそれ以上のしきい値イベントは生成されませんが、使用状況の監視は続行され、セッションの終了時に報告されます。

ベアラーの終了時の使用状況レポートがサポートされています。

次の手順を通じて、Gx を介したボリュームレポートの仕組みについて説明します。

1. PCEF は、PCRF からメッセージを受信した後、使用状況モニタリング関連の AVP を解析し、その情報を IMSA に送信します。
2. IMSA はこの情報で ECS を更新します。
3. PCRF からの使用状況モニタリング情報で ECS が更新されると、PCEF（ECS）はデータ使用状況の追跡を開始します。
4. セッションレベルのモニタリングの場合、ECS がデータ使用状況を保持します。
5. PCC ルールモニタリングの場合、モニタリングキーを一意の識別子として使用状況がモニタリングされます。各ノードがモニタリングキーごとの使用状況情報を保持します。データトラフィックが通過すると、使用量しきい値に照らして使用状況がチェックされ、「使用状況レポート」セクションに説明されているようにして報告されます。
6. PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況を追跡し続けます。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されません。

使用状況モニタリング

- セッションレベルでの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に使用量しきい値レベルを設定し、Usage-Monitoring-Level AVP をSESSION_LEVEL(0) に設定して、Usage-Monitoring-Information AVP を送信することで、Gx に関するセッションレベルのボリュームレポートにサブスクライブします。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。PCRF は、セッションレベルでモニタリングキーをサポートしています。

  PCRF では、単一のメッセージでセッションの使用状況を有効または無効にすることができます。この操作は、モニタリングキーがセッションレベルで関連付けられている場合にのみ可能です。

PCRF では、入力/出力オクテットのしきい値レベルに基づき使用状況をモニタリングできます。有効になっているしきい値レベルに基づいて使用状況が報告されます。複数のレベルが有効になっている場合は、いずれか1つのレベルで侵害が発生しても、有効になっているすべてのレベルについて使用状況が報告されます。モニタリングは、PCRF からの使用状況レポートの応答で欠落しているしきい値レベルで停止されます（PCRF が以前に有効にされた複数のレベルでモニタリングを継続する場合、完全なセットを再度提供することが期待されます）。

合計しきい値レベルと GSU AVP の UL/DL しきい値レベルの両方が提供された場合はエラーとして扱われ、合計しきい値レベルのみが受け入れられます。

次の要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U が生成されます。

- モニタリングキーを使用したルールレベルでの即時レポート要求
- モニタリングキーを使用した、または使用しないセッションレベルでの即時レポート要求
- ルールレベルでの明示的な無効化要求
- セッションレベルでの明示的な無効化要求

上記のすべての要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U は生成されません。また、すべてのアクティブなモニタリングキーの使用状況を報告した CCR-U への応答で、ルールレベルのモニタリングキーのない即時レポート要求を受信した場合、追加の CCR-U は生成されません。

- フローレベルの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルと PCC_RULE_LEVEL(1) に設定された Usage-Monitoring-Level AVP とともに Usage-Monitoring-Information AVP を送信することで、Gx を介してフローレベルのボリュームレポートに登録します。フローレベルのモニタリングの場合、モニタリングキーは必須です。PCRF がルールとモニタリングキーを関連付ける際や、フローレベルで使用状況モニタリングを有効化または無効化する際に、モニタリングキーを使用して制御できるためです。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。

  使用状況モニタリングは、スタティックルール、定義済みルール、およびダイナミックルール定義に対応しています。

  - スタティックルールの使用状況モニタリング：スタティックルールの場合、モニタリングキーに関連付けられた最後のルール削除に関する使用状況はレポートの対象外になります。この場合、PCRF から使用状況モニタリング情報のみを受信します。
  - 定義済みルールの使用状況モニタリング：事前定義されたルールに対して使用状況モニタリングを有効にする必要がある場合、PCRF は、モニタリングキーと使用量しきい値を含むルールおよび使用状況モニタリング情報を送信します。モニタリングキーは、その事前定義済みルールの PCEF で事前設定されているものと同じである必要があります。同じモニタリングキーに複数のルールを関連付けることができます。そのため、特定のモニタリングキーを有効にすると、同じモニタリングキーを持つ複数の

ルールのデータが追跡されることになります。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。

- ダイナミックルールの使用状況モニタリング：ダイナミックルール定義に対して使用状況モニタリングを有効にする必要がある場合、PCRF は課金ルールの定義や使用状況モニタリング情報（モニタリングキー、使用量しきい値など）とともにモニタリングキーを提供します。これにより、そのモニタリングキーに関連付けられているすべてのルールに対して使用状況モニタリングが実行されます。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。ダイナミックルール定義のモニタリングキーは、PCRF によって動的に割り当てられます。これが、使用状況モニタリングのケースにおいて定義済みルールとの唯一の違いです。

モニタリングキーの 1 つの使用状況だけが最初に報告されます。PCRF から正常な応答を受信すると、残りのモニタリングキーの使用状況が PCRF に報告されます。Tx 期限切れ/TCP リンクエラーが発生すると、報告されていない使用状況が ECS に保存されます。セッションでその後 PCRF と正常なやり取りがあった場合、報告されていない UMI が PCRF に送信されます。

使用状況レポート

サブスクライバレベルやフローレベルでの使用状況は、次の条件で PCRF に報告されます。

- 使用量しきい値に達した：PCEF はサブスクライバデータの使用量を記録し、PCRF によって指定される使用量しきい値に達しているかどうかを確認します。これは、セッションレベルとルールレベルの両方のレポートで行われます。

  セッションレベルのレポートでは、実際の使用量が、使用量しきい値と比較されます。

  ルールレベルのレポートでは、データトラフィックにヒットするルールを使用して、モニタリングキーが関連付けられているかどうかが確認され、モニタリングキーに基づいてデータ使用量が確認されます。条件が満たされると、使用状況の情報を IMSA に報告し、モニタリングを続行します。IMSA は、「USAGE_REPORT」トリガーが PCRF によって有効になっている場合に、CCR-U をトリガーします。この CCR で、Usage-Monitoring-Information AVP と、サブスクライバのデータ使用量を設定した「Used-Service-Unit」が送信されます。

  使用量しきい値に達したときに、PCRF が使用状況モニタリング情報に PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、使用状況は報告されません。

  Gx を介した非標準ボリュームレポートの実装では、しきい値に違反すると使用状況モニタリングが停止します。それ以外の場合はモニタリングが続行されます。CCA が受信されるまで、以降の使用状況は報告されません。

- 使用状況モニタリングが無効：レポートの使用状況、その他の外部トリガー、または PCRF 内部トリガーに関連しない PCEF からの CCR の結果として PCRF により使用状況モニタ

リングが無効にされた場合には、PCRF が Usage-Monitoring-Support AVP を USAGE_MONITORING_DISABLED に設定して使用状況モニタリングを明示的に無効にすると、PCEF はモニタリングを停止し、（モニタリングが有効だったときの）使用状況情報を PCRF に報告します。使用量しきい値に達したときに、PCRF が PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、これ以降の使用状況は報告されません。

- IP CAN セッションの終了：IP CAN セッションが終了すると、サブスクライバの累積使用状況情報が PCEF からの CCR-T で PCRF に報告されます。PCC 使用量レベル情報が PCRF によって有効になっている場合、PCC 使用量も報告されます。

  PCRF は RAR メッセージを使用し、その中に Session-Release-Cause AVP を含めて、IP CAN セッション終了を開始します。ただし、PCRF が CCA メッセージで IP CAN セッションを終了する場合もあります。不要な追加メッセージを回避するために、PCRF は、CCA-U メッセージ自体で、サブスクライバを終了するように P-GW に通知できます。そのため、すべての Gx ディクショナリの CCA メッセージに Session Release Cause が追加されました。

- PCC ルールの削除：PCRF が使用量モニタリングキーに関連付けられている最後の PCC ルールを非アクティブ化すると、PCEF はそのモニタリングキーのデータ使用量を含む CCR を送信します。使用量モニタリングキーに関連付けられている最後の PCC ルールが非アクティブであると PCEF が報告する場合に、CCR コマンドに Charging-Rule-Report AVP が含まれていたなら、PCEF は同じ CCR コマンドでそのモニタリングキーの累積使用量を報告します。あるいは、Charging-Rule-Report AVP が RAA コマンドに含まれている場合、PCEF は新規に CCR コマンドを送信して、使用状況モニタリングキーの累積使用量を報告します。PCRF によって設定された、ルールの非アクティブ化時間を使用した最後のルールの非アクティブ化に関する使用状況レポートがサポートされています。

  PCRF からのメッセージを受信すると、削除対象のルールがマーク付けされ、アクセス側の手順が完了した後にルールが削除されます。

- PCRF 要求使用状況レポート：最後のレポートの送信以降の累積使用量（即時レポートの場合も同様）。即時レポート後に使用量はリセットされ、使用状況モニタリングが続行されます。後続の使用状況レポートには現在のレポート以降の使用量が含まれるようになります。

- ベアラーの終了に関する使用状況レポートを追加できます。ベアラーが何らかの理由で削除されると、そのベアラーに関連付けられているルールも削除されます。そのため、使用状況は、ベアラー終了が原因で削除された最後のルールが関連ルールであるモニタリングキーで報告されます。

- 再検証のタイムアウト：非標準の実装では、使用状況モニタリングとレポートが有効になっていて、再検証タイムアウトが発生した場合、PCEF は CCR を送信して PCC ルールを要求し、最後のレポート以降（または、使用状況がまだ報告されていない場合には、使用状況レポートが有効になった時点以降）の有効なすべてのモニタリングキーのすべての累積使用量を、IP-CAN セッションレベル（有効な場合）およびサービスデータフローレベル（有効な場合）の累積使用量を使用して報告します。これがデフォルトの動作です。

  標準実装の場合、これは CLI 設定によって有効にする必要があります。



重要 再検証タイムアウト時の使用状況レポート機能は、Gx を介したボリュームレポートの非標準実装ではデフォルトで使用できます。この機能は標準実装で設定可能です。

使用状況が報告されると、使用量カウンタはゼロにリセットされます。PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況の追跡を 0 から継続します。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されず、CCR-CCA 間の累積使用量は破棄されます。

サーバーの再試行でトリガーされた CCR-U は、サーバーによって付与されたクォータを考慮して、USU を報告します。新たに作成された MSCC の場合、USU を報告するために暫定クォータ設定が取得されます。

Gx を介したボリュームレポート機能を設定する方法については、「Gx を介したボリュームレポートの設定 （755 ページ）」を参照してください。

Gx を介したボリュームレポート（*VoRoGx*）のための *ICSR* サポート

ボリュームのしきい値とボリュームの使用状況はスタンバイシャーシに同期され、ICSR スイッチオーバー後の既存のセッションの Gx を介したボリュームレポートをサポートします。

このサポートがないと、たとえば適切な使用を強制するためにボリュームレポートを使用した場合に、サブスクライバが想定以上に高い速度を使用する可能性はありません。通信事業者はこれをすでに収益の損失と見なしている可能性があります。また、EU のローミング規制によって設定された制限に達すると、通知を受け取り、ブロック/リダイレクトされるローミングサブスクライバに深刻な影響を及ぼします。セッションがブロックされずにこの時点でセッションが継続する場合、通信事業者は上限を超えたデータに課金することができず、実質的な収益の大幅な損失が発生します（ローミングパートナーは SGSN で使用されるデータに課金する場合があります）。

IPFilterRule の 3GPP Rel. 9 コンプライアンス

このセクションでは、IPFilterRule 機能の 3GPP Rel. 9 コンプライアンスの概要と実装について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

- 機能説明 （787 ページ）
- Rel. 9 準拠 AVP の設定 （789 ページ）
- IPFilterRule の 3GPP Rel. 9 コンプライアンスのモニタリングと障害対応 （790 ページ）

機能説明

現在 PCEF は、Flow-Description AVP、TFT-Filter、および Packet-Filter-Content AVP の IPFilterRule に関して、3GPP Rel. 8 に準拠しています。ネットワークによって開始された専用ベアラーの作成または変更中、PCRF が Rel. 9 形式の Flow-Description AVP を使用して CCA-U または RAR

を送信するときに、PCEF が送信元および宛先 IP アドレスを誤って解釈し、UE に誤った TFT を送信していました。

PCRF が 3GPP Rel. 9 にアップグレードされても、PCEF は、UE によって開始されたセカンダリベアラーの作成または変更中、Flow-Description、TFT-Filter、および Packet-Filter-Content AVP を Rel. 8 形式で CCR-U に送信し続けます。

Flow-Description AVP、TFT-Filter、および Packet-Filter-Content AVP を PCEF 3GPP Rel. 9 に準拠させるため、次の変更が導入されます。

- Flow-Description AVP の IPFilterRule の送信元および宛先 IP アドレスの解釈は、3GPP Rel. 9 に準拠するように変更されます。つまり、ネットワークによって開始されたベアラー作成または変更中に UPLINK の Rel. 9 フロー説明が受信され、送信元 IP アドレスがリモートとして解釈され、宛先がローカル IP アドレスとして解釈されます。
- トラフィックフローの方向は、新しい Diameter AVP「Flow-Direction」から解釈されます。この新しい AVP で、フィルタが適用される 1 つまたは複数の方向、ダウンリンクのみ、アップリンクのみ、またはダウンリンクとアップリンクの両方（双方向）が示されます。
- IMSA モジュールは、TFT-Packet-Filter-Information および Packet-Filter-Information AVP を Rel. 9 形式でエンコードするように変更されました（ネゴシエートされたサポート対象機能が Rel. 9 以上の場合）。
- CCR-U の PCEF によって送信される Flow-Description、TFT-Filter、および Packet-Filter-Content AVP に対する Rel. 9 の変更を有効にするための設定サポートが提供されています。**diameter 3gpp-r9-flow-direction** CLI コマンドは、Rel. 9 の変更を有効にするために使用されます。この CLI コマンドが設定およびネゴシエートされた場合、サポートされる機能は、Rel. 9 以上（ゲートウェイと PCRF の両方が Rel. 9 以降に準拠）で、P-GW は Flow-Description、TFT-Filter、および Packet-Filter-Content AVP を Rel. 9 形式で送信します。

後方互換性は維持されています。つまり、Rel. 8（入出力を許可）および Rel. 9（フロー方向を含む出力を許可）形式が PCEF で受け入れられます。

3GPP Rel. 8 標準規格に従って、Flow-Description、TFT-Filter、および Packet-Filter-Content AVP の IPFilterRule が、UPLINK 方向の「入力許可」、DOWNLINK 方向の「出力許可」として送信されます。3GPP Rel. 9 以降、Flow-Information AVP 内の Flow-Description AVP には「出力許可」のみが含まれ、トラフィックフローの方向は Flow-Direction AVP で示されます。3GPP Rel. 9 形式では、UPLINK と DOWNLINK の両方が常に「出力許可」として送信されるため、「入力許可」の使用は廃止されます。



重要 この機能は、CCA-I でネゴシエートされたサポート対象の機能が Rel. 9 以上の場合にのみ、**diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** CLI コマンドを使用して、3GPP Rel. 9 準拠の PCEF および PCRF のみに適用されます。

他の機能との関係

この機能は、**diameter update-dictionary-avps** CLI コマンドが 3gpp-r9 または 3gpp-r10 として設定されている場合にのみ機能します。つまり、PCEF は、**diameter 3gpp-r9-flow-direction** CLI コマンドが有効で、サポートされている機能が Rel. 9 以上である場合にのみ、3GPP Rel. 9 形式で Flow-Description、TFT-Filter、および Packet-Filter-Content AVP を送信します。この機能をアクティブ化する **diameter 3gpp-r9-flow-direction** CLI コマンドは、PCRF が Rel. 9 にアップグレードされた後にしか使用できません。9.

Rel. 9 準拠 AVP の設定

以下では、Flow-Description、TFT-Filter、および Packet-Filter-Content AVP の Rel. 9 の変更を有効にする設定コマンドについて説明します。

3GPP 準拠のための AVP のエンコーディング

次の設定コマンドを使用して、Rel. 9 形式の Flow-Description、TFT-Filter、および Packet-Filter-Content AVP から PCEF を制御します。

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter 3gpp-r9-flow-direction
end
```

- **3gpp-r9-flow-direction**：3GPP Rel. 9 仕様に基づいて、Flow-Description、TFT-Filter、および Packet-Filter-Content AVP をエンコードします。デフォルトでは、この機能は無効になっています。
- この CLI 設定は、PCEF によって CCR-U で送信された TFT-Filter、Packet-Filter-Content、および Flow-Description AVP にのみ適用されます。
- この CLI コマンドは、PCRF が次にアップグレードされた後にしか使用できません：Rel. 9.
- この CLI コマンドは **diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** と連携して動作します。**diameter 3gpp-r9-flow-direction** が設定され、サポート対象機能が 3gpp-r9 以上にネゴシエートされた場合、PCEF は、Flow-Description、TFT-Filter、および Packet-Filter-Content AVP を 3GPP Rel. 9 形式で送信します。

AVP コンプライアンスの設定の確認

次のコマンドを使用して、この機能の設定ステータスを確認します。

```
show ims-authorization service name service_name
```

service_name は、IMS 認証用に設定された IMS 承認サービスの名前にする必要があります。

「3GPP R9 Flow Direction Compliance」フィールドを使用して、この機能を有効にするか無効にするかを決定できます。

```
[local]st40# show ims-authorization service name gngp-gx
  Context: gngp
  IMS Authorization Service name: gngp-gx
  Service State: Enabled
  Service Mode: Single Interface Policy and Charging
...
  Diameter Policy Control:
   Endpoint: gx
   Origin-Realm: xyz.com
   Dictionary: r8-gx-standard
   Supported Features:
      3gpp-r9
...
   Host Selection: Table: 1 Algorithm: Round-Robin
   Host Reselection Subscriber Limit: Not Enabled
   Host Reselection Interval: Not Enabled
   Sgsn Change Reporting: Not Enabled
    3GPP R9 Flow Direction Compliance: Enabled
  Host Selection Table[1]: 1 Row(s)
   Precedence: 1
...
```

IPFilterRule の 3GPP Rel. 9 コンプライアンスのモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

この機能に関連した障害については、次の操作を実行する必要があります。

- **show ims-authorization service name** <*service_name*> CLI コマンドを使用して、この機能が有効であるかどうかを確認します。有効になっていない場合は、**diameter 3gpp-r9-flow-direction** CLI コマンドを設定して、この機能が動作するかどうかを確認します。
- **monitor protocol** コマンドを実行し、CCA-I でネゴシエーションされたサポート機能が Rel. 9 以上であるかどうか確認します。そうでない場合、この機能は動作しません。**diameter update-dictionary-avps { 3gpp-r9 | 3gpp-r10 }** CLI コマンドを使用して、サポートされる機能を設定します。
- それでも問題が解決しない場合は、次の情報を入手して、シスコのアカウント担当者に詳細な分析を依頼してください。
  - オプション 24（GTPC）と 75-3（App Specific Diameter - DIAMETER Gx/Ty/Gxx）がオンになっているモニタープロトコルログ
  - acsmgr を有効にしたログ
  - **show active-charging sessions full all** および show ims-authorization sessions CLI コマンドの出力

show ims-authorization service name

Rel. 9 フロー方向変更が有効または無効になっているかどうかを示すために、この show コマンドの出力に新しいフィールド「3GPP R9 Flow Direction Compliance」が追加されました。

Rel. 10 Gx インターフェイス

Rel. 10 Gx インターフェイスのサポートは Cisco ASR シャーシで使用できます。

ここでは、次の内容について説明します。

• P-GW Rel. 10 Gx インターフェイスのサポート （791 ページ）

P-GW Rel. 10 Gx インターフェイスのサポート

はじめに

Gx 参照ポイントは、パケットデータネットワーク（PDN）ゲートウェイ（P-GW）上のポリシーおよび課金ルール機能（PCRF）とポリシーおよび課金適用機能（PCEF）の間にあります。Gx 参照ポイントは、PCRF から PCEF への PCC ルールのプロビジョニングと削除、および PCEF から PCRF へのトラフィック プレーン イベントの送信に使用されます。Gx 参照ポイントは、アプリケーションに関連する AVP を適用することで、課金制御とポリシー制御のいずれかまたは両方に使用できます。

PCEF は、ポリシーの適用とフローベースの課金機能を包含する機能要素です。この機能エンティティは P-GW にあります。これには、以下の主要な機能があります。

- ゲートウェイでのユーザー プレーン トラフィックの処理とその QoS の制御。
- サービスデータフローの検出とカウント、およびオンラインとオフラインの課金操作。
- ポリシー制御されているサービスデータフローの場合、PCEF は、対応するゲートウェイが開いている場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- 課金制御されているサービスデータフローの場合、PCEF は、対応するアクティブな PCC ルールがあり、オンライン課金で OCS がその課金キーで該当するクレジットを承認した場合にのみ、サービスデータフローがゲートウェイを通過するのを許可します。
- PCRF から要求された場合、PCEF は関連するサービスデータフローのステータスが変わったときに PCRF に報告します。
- SDF が BBERF でトンネリングされている場合、PCEF は、IP-CAN セッションの確立時のサービスデータフローのモビリティ プロトコル トンネリング ヘッダーについて PCRF に通知します。



重要 ASR 5500 は、Gx メッセージのダイナミック課金ルールごとのフロー説明を含む 8 つのフロー情報のみをサポートします。

用語および定義

このセクションでは、Rel. 10 Gx に関連する機能と用語について説明します。.

Gx を介したボリュームレポート

ここでは、3GPP Rel. 10 の Gx を介したボリュームレポートについて説明します。

ライセンス要件

Gx を介したボリュームレポートは、シスコのライセンス供与された機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

重要 Gxを介した課金機能またはGxを介したボリュームレポート機能に個別のライセンスは必要ありません。この機能は、「ポリシーインターフェイス」ライセンスの一部として有効にすることができます。

サポートされる標準

Gx を介したボリュームレポート機能は、次の標準規格に基づいています。

3GPP TS 29.212 V10.5.0（2012-01）：3rd Generation Partnership Project、Technical Specification Group Core Network and Terminals、Policy and Charging Control over Gx reference point (Release 10)

機能の概要

Gxを介したボリュームレポート機能により、PCRFはサブスクライバのデータ使用量に基づいてリアルタイムの決定ができます。

重要 Volume Reporting over Gx は、ボリュームクォータにのみ適用されます。

PCEF は、最初からではなく、使用状況監視の最後のレポート以降の累積使用量のみを報告します。

使用量しきい値がゼロ（無限しきい値）に設定されている場合、PCEF によってそれ以上のしきい値イベントは生成されませんが、使用状況の監視は続行され、セッションの終了時に報告されます。

ベアラーの終了時の使用状況レポートがサポートされています。

次の手順を通じて、Gx を介したボリュームレポートの仕組みについて説明します。

1. PCEF は、PCRF からメッセージを受信した後、使用状況モニタリング関連の AVP を解析し、その情報を IMSA に送信します。

2. IMSA はこの情報で ECS を更新します。
3. PCRF からの使用状況モニタリング情報で ECS が更新されると、PCEF（ECS）はデータ使用状況の追跡を開始します。
4. セッションレベルのモニタリングの場合、ECS がデータ使用状況を保持します。
5. PCC ルールモニタリングの場合、モニタリングキーを一意の識別子として使用状況がモニタリングされます。各ノードがモニタリングキーごとの使用状況情報を保持します。データトラフィックが通過すると、使用量しきい値に照らして使用状況がチェックされ、「使用状況レポート」セクションに説明されているようにして報告されます。
6. PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況を追跡し続けます。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されません。

使用状況モニタリング

- セッションレベルでの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に使用量しきい値レベルを設定し、Usage-Monitoring-Level AVP を SESSION_LEVEL(0) に設定して、Usage-Monitoring-Information AVP を送信することで、Gx に関するセッションレベルのボリュームレポートにサブスクライブします。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。PCRF は、セッションレベルでモニタリングキーをサポートしています。

  PCRF では、単一のメッセージでセッションの使用状況を有効または無効にすることができます。この操作は、モニタリングキーがセッションレベルで関連付けられている場合にのみ可能です。

  PCRF では、入力/出力オクテットのしきい値レベルに基づき使用状況をモニタリングできます。有効になっているしきい値レベルに基づいて使用状況が報告されます。複数のレベルが有効になっている場合は、いずれか1つのレベルで侵害が発生しても、有効になっているすべてのレベルについて使用状況が報告されます。モニタリングは、PCRF からの使用状況レポートの応答で欠落しているしきい値レベルで停止されます（PCRF が以前に有効にされた複数のレベルでモニタリングを継続する場合、完全なセットを再度提供することが期待されます）。

  合計しきい値レベルと GSU AVP の UL/DL しきい値レベルの両方が提供された場合はエラーとして扱われ、合計しきい値レベルのみが受け入れられます。

  次の要求がモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、同じモニタリングキーの追加の CCR-U が生成されます。

  - モニタリングキーを使用したルールレベルでの即時レポート要求
  - モニタリングキーを使用した、または使用しないセッションレベルでの即時レポート要求
  - ルールレベルでの明示的な無効化要求
  - セッションレベルでの明示的な無効化要求

上記のすべての要求が同じモニタリングキーの使用状況を報告した CCR-U への応答で受信された場合、モニタリングキーの追加の CCR-U は生成されません。また、すべてのアクティブなモニタリングキーの使用状況を報告した CCR-U への応答で、ルールレベルのモニタリングキーのない即時レポート要求を受信した場合、追加の CCR-U は生成されません。

- フローレベルの使用状況モニタリング：PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルと PCC_RULE_LEVEL(1) に設定された Usage-Monitoring-Level AVP とともに Usage-Monitoring-Information AVP を送信することで、Gx を介してフローレベルのボリュームレポートに登録します。フローレベルのモニタリングの場合、モニタリングキーは必須です。PCRF がルールとモニタリングキーを関連付ける際や、フローレベルで使用状況モニタリングを有効化または無効化する際に、モニタリングキーを使用して制御できるためです。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。

  使用状況モニタリングは、スタティックルール、定義済みルール、およびダイナミックルール定義に対応しています。

  - スタティックルールの使用状況モニタリング：スタティックルールの場合、モニタリングキーに関連付けられた最後のルール削除に関する使用状況はレポートの対象外になります。この場合、PCRF から使用状況モニタリング情報のみを受信します。
  - 定義済みルールの使用状況モニタリング：事前定義されたルールに対して使用状況モニタリングを有効にする必要がある場合、PCRF は、モニタリングキーと使用量しきい値を含むルールおよび使用状況モニタリング情報を送信します。モニタリングキーは、その事前定義済みルールの PCEF で事前設定されているものと同じである必要があります。同じモニタリングキーに複数のルールを関連付けることができます。そのため、特定のモニタリングキーを有効にすると、同じモニタリングキーを持つ複数のルールのデータが追跡されることになります。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。
  - ダイナミックルールの使用状況モニタリング：ダイナミックルール定義に対して使用状況モニタリングを有効にする必要がある場合、PCRF は課金ルールの定義や使用状況モニタリング情報（モニタリングキー、使用量しきい値など）とともにモニタリングキーを提供します。これにより、そのモニタリングキーに関連付けられているすべてのルールに対して使用状況モニタリングが実行されます。AVP が DPCA によって解析された後、IMSA は情報を ECS に対して更新します。ECS が更新されると、使用状況モニタリングが開始され、データトラフィックが発生するたびに使用量しきい値がチェックされます。ダイナミックルール定義のモニタリングキーは、PCRF によって動的に割り当てられます。これが、使用状況モニタリングのケースにおいて定義済みルールとの唯一の違いです。

複数のモニタリングキーで同時にしきい値違反が発生した場合、最初に 1 つのモニタリングキーの使用状況のみが報告されます。PCRF から正常な応答を受信すると、残りのモニタリン

グキーの使用状況が PCRF に報告されます。Tx 期限切れ/TCP リンクエラーが発生すると、報告されていない使用状況が ECS に保存されます。セッションでその後 PCRF と正常なやり取りがあった場合、報告されていない UMI が PCRF に送信されます。

使用状況レポート

サブスクライバレベルやフローレベルでの使用状況は、次の条件で PCRF に報告されます。

- 使用量しきい値に達した：PCEF はサブスクライバデータの使用量を記録し、PCRF によって指定される使用量しきい値に達しているかどうかを確認します。これは、セッションレベルとルールレベルの両方のレポートで行われます。

  セッションレベルのレポートでは、実際の使用量が、使用量しきい値と比較されます。

  ルールレベルのレポートでは、データトラフィックにヒットするルールを使用して、モニタリングキーが関連付けられているかどうかが確認され、モニタリングキーに基づいてデータ使用量が確認されます。条件が満たされると、使用状況の情報を IMSA に報告し、モニタリングを続行します。IMSA は、「USAGE_REPORT」トリガーが PCRF によって有効になっている場合に、CCR-U をトリガーします。この CCR で、Usage-Monitoring-Information AVP と、サブスクライバのデータ使用量を設定した「Used-Service-Unit」が送信されます。

  使用量しきい値に達したときに、PCRF が使用状況モニタリング情報に PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、使用状況は報告されません。

  Gx を介した非標準ボリュームレポートの実装では、しきい値に違反すると使用状況モニタリングが停止します。それ以外の場合はモニタリングが続行されます。CCA が受信されるまで、以降の使用状況は報告されません。

- 使用状況モニタリングが無効：レポートの使用状況、その他の外部トリガー、または PCRF 内部トリガーに関連しない PCEF からの CCR の結果として PCRF により使用状況モニタリングが無効にされた場合には、PCRF が Usage-Monitoring-Support AVP を USAGE_MONITORING_DISABLED に設定して使用状況モニタリングを明示的に無効にすると、PCEF はモニタリングを停止し、（モニタリングが有効だったときの）使用状況情報を PCRF に報告します。使用量しきい値に達したときに、PCRF が PCEF からの CCR による新しい使用量しきい値を提供しない場合、使用状況モニタリングは PCEF で停止し、これ以降の使用状況は報告されません。

- IP CAN セッションの終了：IP CAN セッションが終了すると、サブスクライバの累積使用状況情報が PCEF からの CCR-T で PCRF に報告されます。PCC 使用量レベル情報が PCRF によって有効になっている場合、PCC 使用量も報告されます。

  PCRF は RAR メッセージを使用し、その中に Session-Release-Cause AVP を含めて、IP CAN セッション終了を開始します。ただし、PCRF が CCA メッセージで IP CAN セッションを終了する場合もあります。不要な追加メッセージを回避するために、PCRF は、CCA-U メッセージ自体で、サブスクライバを終了するように P-GW に通知できます。そのため、すべての Gx ディクショナリの CCA メッセージに Session Release Cause が追加されました。

- PCC ルールの削除：PCRF が使用量モニタリングキーに関連付けられている最後の PCC ルールを非アクティブ化すると、PCEF はそのモニタリングキーのデータ使用量を含む CCR を送信します。使用量モニタリングキーに関連付けられている最後の PCC ルールが非アクティブであると PCEF が報告する場合に、CCR コマンドに Charging-Rule-Report AVP が含まれていたなら、PCEF は同じ CCR コマンドでそのモニタリングキーの累積使用量を報告します。あるいは、Charging-Rule-Report AVP が RAA コマンドに含まれている場合、PCEF は新規に CCR コマンドを送信して、使用状況モニタリングキーの累積使用量を報告します。PCRF によって設定された、ルールの非アクティブ化時間を使用した最後のルールの非アクティブ化に関する使用状況レポートがサポートされています。

  PCRF からのメッセージを受信すると、削除対象のルールがマーク付けされ、アクセス側の手順が完了した後にルールが削除されます。

- PCRF 要求使用状況レポート：最後のレポートの送信以降の累積使用量（即時レポートの場合も同様）。即時レポート後に使用量はリセットされ、使用状況モニタリングが続行されます。後続の使用状況レポートには現在のレポート以降の使用量が含まれるようになります。

- ベアラーの終了に関する使用状況レポートを追加できます。ベアラーが何らかの理由で削除されると、そのベアラーに関連付けられているルールも削除されます。そのため、使用状況は、ベアラー終了が原因で削除された最後のルールが関連ルールであるモニタリングキーで報告されます。

- 再検証のタイムアウト：非標準の実装では、使用状況モニタリングとレポートが有効になっていて、再検証タイムアウトが発生した場合、PCEF は CCR を送信して PCC ルールを要求し、最後のレポート以降（または、使用状況がまだ報告されていない場合には、使用状況レポートが有効になった時点以降）の有効なすべてのモニタリングキーのすべての累積使用量を、IP-CAN セッションレベル（有効な場合）およびサービスデータフローレベル（有効な場合）の累積使用量を使用して報告します。これがデフォルトの動作です。

  標準実装の場合、これは CLI 設定によって有効にする必要があります。



重要 再検証タイムアウト時の使用状況レポート機能は、Gx を介したボリュームレポートの非標準実装ではデフォルトで使用できます。この機能は標準実装で設定可能です。

使用状況が報告されると、使用量カウンタはゼロにリセットされます。PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況の追跡を 0 から継続します。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されず、CCR-CCA 間の累積使用量は破棄されます。

サーバーの再試行でトリガーされた CCR-U は、サーバーによって付与されたクォータを考慮して、USU を報告します。新たに作成された MSCC の場合、USU を報告するために暫定クォータ設定が取得されます。

Gx を介したボリュームレポート機能を設定する方法については、「Gx を介したボリュームレポートの設定 （755 ページ）」を参照してください。

Gx を介したボリュームレポート（*VoRoGx*）のための *ICSR* サポート

ボリュームのしきい値とボリュームの使用状況はスタンバイシャーシに同期され、スイッチオーバー後の既存セッションの Gx を介したボリュームレポートをサポートします。

このサポートがないと、たとえば適切な使用を強制するためにボリュームレポートを使用した場合に、サブスクライバが想定以上に高い速度を使用する可能性はありません。通信事業者はこれをすでに収益の損失と見なしている可能性があります。また、EUのローミング規制によって設定された制限に達すると、通知を受け取り、ブロック/リダイレクトされるローミングサブスクライバに深刻な影響を及ぼします。セッションがブロックされずにこの時点でセッションが継続する場合、通信事業者は上限を超えたデータに課金することができず、実質的な収益の大幅な損失が発生します（ローミングパートナーはSGSNで使用されるデータに課金する場合があります）。

Gx インターフェイスでの Supported-Features AVP の使用

Supported-Features AVP はセッションの確立中に使用され、送信元ホストがサポートする必須機能とオプション機能について宛先ホストに通知します。クライアントは、Diameterセッションの最初の要求で、セッションの正常な処理に必要な一連の機能を指定します。クライアントによってサポートされており、必要な機能セットの一部としてアドバタイズされていない機能がある場合、クライアントは、セッションを正常に処理するためのオプションであるこのオプション機能のセットを同じ要求で提供します。サーバーは、Diameterセッション内の最初の応答で、クライアントと共通する機能のセットと、同じ Diameter セッション内でサーバーがサポートする機能のセットを示します。以降のコマンドメッセージは、セッション確立中に、Supported-Features AVP に示されているサポート対象機能のリスト、および Supported-Features AVP に示されていない機能に常に準拠します。サポート対象としてアドバタイズされていない機能は、そのDiameterセッションのコマンドメッセージの作成に使用されません。特に明記されていない限り、Gx 参照ポイントでの Supported-Features AVP の使用は、サポートされている機能の動的な検出および関連するエラー処理の要件に準拠します。

Gx 参照ポイントの基本的役割は 3GPP Rel. 7 標準であり、機能はその役割の拡張です。元のホストが基本的な役割を超える機能をサポートしていない場合、Supported-Features AVP が Gx コマンドに存在しない場合があります。3GPP TS 29.229 に定義されているように、機能の新しい AVP を追加してアプリケーションを拡張する場合、新しい AVP は M ビットがクリアされ、AVP はコマンド ABNF で必須として定義されません。

Supported-Features AVP はある種グループ化されており、Vendor-Id、Feature-List-ID、および Feature-List の各 AVP が含まれています。Gx 参照ポイントでは、3GPP によって定義された機能を識別するために Supported-Features AVP を使用するため、Vendor-Id AVP には 3GPP のベンダーID（10415）が含まれます。Gx参照ポイントに複数の機能リストが定義されている場合、Feature-List-ID AVP はそれらのリストを互いに区別します。

機能ビット	機能	M/O	説明
0	Rel8	M	この機能は、3GPP Rel-8 の基本的な Gx の役割のサポートを示します。これには、基本の 3GPP Rel-7 Gx 標準でサポートされる AVP および対応するプロシージャが含まれますが、個別の機能ビットで表される機能は除外されます。

機能ビット	機能	M/O	説明
1	Rel9	M	この機能は、3GPP Rel-9 の基本的な Gx の役割のサポートを示します。これには、Rel8 機能ビットでサポートされる AVP および対応するプロシージャが含まれますが、個別の機能ビットで表される機能は除外されます。
3	Rel10	M	この機能は、3GPP Rel-10 の基本的な Gx の役割のサポートを示します。これには、Rel8 および Rel9 機能ビットでサポートされる AVP および対応するプロシージャが含まれますが、個別の機能ビットで表される機能は除外されます。
4	SponsoredConnectivity	O	この機能は、スポンサーデータ接続機能に対するサポートを示しています。PCEF がこの機能をサポートしている場合、PCRF はサブスクライバへのスポンサーデータ接続を承認できます。

PCEF が Diameter ディクショナリをリリース 8、9、または 10 として設定すると、PCRF は Supported-Features AVP を送信して、PCEF は PCRF がサポートする機能を認識できるようにします。PCEF が、要求された機能よりも少ない、または要求された機能よりも多いサポート対象の機能を受信した場合、サポート対象機能は、少ない方の機能にマッピングされます。

カスタムディクショナリ「dpca-custom24」が構成されている場合は、Vendor-Id AVP を含む Supported-Features AVP がすべての CCR メッセージで送信されます。

Rule-Failure-Code AVP

Rule-Failure-Code AVP は、QoS/PCC ルールのインストール、アクティブ化、適用を正常に実行できない理由を示します。Rule-Failure-Code AVP のタイプは列挙されます。PCC ルールが報告されている理由を特定するために、この情報が PCEF から Charging-Rule-Report AVP 内の PCRF に送られます。

2 つの新しいルール障害コード INCORRECT_FLOW_INFORMATION (12) と NO_BEARER_BOUND (15) が追加されています。既存のルール障害コード 9 の名前が MISSING_FLOW_INFORMATION に変更されます。3GPP リリース 10 の場合、ルール障害コード 9 は GW/PCEF_MALFUNCTION にマッピングされます。

スポンサーデータ接続

スポンサーはスポンサーデータ接続機能により通信事業者と取引関係を結びます。スポンサーはユーザーが関連するアプリケーション サービス プロバイダー（ASP）のサービスにアクセスできるようにするために、ユーザーのデータ接続料を通信事業者に支払います。または、ユーザーが基本使用料とは別に、トランザクションを使用した接続に対して料金を支払います。これは、ユーザーが通信事業者とサブスクリプション契約を締結していることが前提です。

スポンサーデータ接続機能は、 3GPP TS 29.212 仕様のリリース 10 で導入されました。スポンサードデータ接続機能がサポートされている場合、PCC ルールのスポンサー ID によって、エ

ンドユーザーへのサービス提供に必要な接続料金を通信事業者に支払うサードパーティ組織（スポンサー）が識別されます。

この機能の目的は、特定のフローセットのデータ使用量を個別に識別し、スポンサーに請求することです。これに対応するために、新しいレポートレベル「SPONSORED_CONNECTIVITY_LEVEL」がスポンサー接続レベルでのレポート用に追加され、ルールレベルで 2 つの新しい AVP「Sponsor-Identity」と「Application-Service-Provider-Identity」が導入されました。

スポンサーやアプリケーションサービスプロバイダーに関する情報やしきい値（オプション）がアプリケーション機能（AF）によって提供されると、1 つ以上の PCC ルールに関連付けられたサービスデータフローに対してスポンサーデータ接続が実行されます。

PCC ルールに基づくスポンサーデータ接続のプロビジョニングは、PCC ルールのプロビジョニング手順に従って実行されます。スポンサー ID は、PCC ルールの Charging-Rule-Definition AVP 内にある Sponsor-Identity AVP を使用して設定されます。アプリケーション サービス プロバイダーの ID は、PCC ルールの Charging-Rule-Definition AVP 内にある Application-Service-Provider-Identity AVP を使用して設定されます。Reporting-Level AVP の値が SPONSORED_CONNECTIVITY_LEVEL に設定されている場合は、Sponsor-Identity AVP および Application-Service-Provider-Identity AVP が含まれています。

AF からフローベースの使用量しきい値を受信すると、PCRF はスポンサー ID を使用してモニタリングキーを生成します。PCRF は使用量のモニタリング制御を要求することもあります。この場合、フローベースの使用量のみがスポンサーデータ接続に適用されます。PCEF は要求に応じて PCRF に使用量を報告する場合もあります。

新しい CLI コマンド「**diameter encode-supported-features**」がポリシー制御設定モードに追加され、サポートされる機能をスポンサー ID で送信できるようになりました。コマンドの詳細については、『*Command Line Interface Reference*』[英語] を参照してください。

スポンサー接続機能は、P-GW と PCRF の両方が 3GPP リリース10 に対応している場合にのみサポートされます。P-GW は、CCR-I でサポートされている機能の一部としてリリースを PCRF にアドバタイズします。P-GW がリリース 10 とスポンサー接続機能をサポートしているが、PCRF が（CCA-I でサポートされている機能の一部として）スポンサー接続機能をサポートしていない場合、この機能はオフになります。

スポンサー接続機能は、「dpca-custom8」Gx ディクショナリと連携します。セッションが PCRF からのスポンサー接続に対して有効になっており、オフライン課金が aaa-custom4 ディクショナリを使用して有効になっている場合、スポンサー接続の AVP が ACR 中間パケットと ACR 停止パケットで CDF サーバーに報告されます。Sponsor-Identity AVP と Application-Service-Provider-Identity AVP は、ACR パケット内でグループ化された Service-Data-Container AVP で送信されます。

この機能は、ダイナミックルールと Gx ディクショナリ（dpca-custom 15 および dpca-custom8）をサポートしています。

使用量のレポート

Gx を介したボリュームレポートの場合、PCRF はスポンサー ID に基づいて一意のモニタリングキーを生成します。異なるモニタリングキーを持つフローは個別に扱われるため、スポンサー ID を持つフローは個別に課金されます。

サポートされる Gx 機能

Gx でのポジティブ想定

プライマリとセカンダリ両方の PCRF サーバーが過負荷になっているシナリオでは、PCRF は P-GW と HSGW にエラーを返します。P-GW と HSGW の現在の動作は、プライマリとセカンダリの両方が失敗またはタイムアウトを返した場合にセッションを終了することです。

この機能は、ゲートウェイにローカルポリシーを適用してサブスクライバセッションが継続されるようにすることで、上述の動作を拡張するために開発されました。P-GW/HSGW は、エラーを処理し、イベントタイプに基づいて特定のルールを適用するため、ポジティブ想定機能を導入する必要があります。



重要 Gx ポジティブ想定を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

障害処理の動作が強化され、PCRF が使用できない場合に、サブスクライバサービスが確実に維持されるようになりました。また GW は、Diameter ビジー状態（3004）を受信したときに、設定可能な時間の間、PCRF との Diameter メッセージ（CCR および RAR）の送受信を停止することによって、PCRF へのトラフィックを削減することが必要です。

PCRF で次のいずれかの障害が発生した場合、GW は、障害処理を適用してサブスクライバを終了させるか、それ以上ポリシーを適用せずにブラウジングを許可するかを選択します。

- TCP リンク障害
- アプリケーションタイマー（Tx）の期限切れ
- 結果コードベースの障害

PCRF は、すべての接続レベルの障害、結果コード/実験結果コードの障害が発生した場合、ローカルポリシーにフォールバックできます。ローカルポリシーは、設定された時間の間、サブスクライバを許可する選択を下す場合があります。この間、コールのサブスクライバ/内部イベントはローカルポリシーから処理されます。タイマーの期限が切れた後、サブスクライバセッションを終了するか、PCRF を再試行できます。PCRF の再試行は、**timer-expiry event** が **reconnect-to-server** として設定されている場合にのみ行われることに注意してください。

フォールバックのサポートが障害処理テンプレートに追加されました。また、ローカルポリシーサービスは IMS 承認サービスに関連付けられている必要があります。

ローカルポリシーが適用されると、PCRF が有効になっているすべてのイベントトリガーが無効になります。サブスクライバセッションでローカルポリシーが使用されている場合、GW は、CCR-T の送信をスキップし、ローカルでセッションをクリーンアップします。

アクティブな Gx セッションで作成されたセッションの場合、GW は CCR-T をプライマリ PCRF に送信し、障害が発生すると、CCR-T をセカンダリ PCRF に送信します。CCR-T がプライマリとセカンダリの両方から失敗を返した場合、またはタイムアウトした場合、GW はセッションをローカルでクリーンアップします。

ローカルポリシーへのフォールバックは、次のシナリオで行われます。

- Tx タイマーの期限切れ
- Diabase エラー
- 結果コードエラー（持続的/一時的）
- 実験結果コード
- 応答タイムアウト

次のポイントは、PCRF への再接続が試行されるシナリオにのみ適用されます。

- サブスクライバが CCR-I 障害が原因でローカルポリシーにフォールバックした場合、タイマーの期限切れ後に CCR-I が PCRF に送信されます。成功した CCA-I コールは PCRF で続行されます。成功しなかった場合、コールはローカルポリシーで続行され、再試行カウントが増分されます。
- サブスクライバが CCR-U 障害のためにローカルポリシーにフォールバックした場合、IMS 承認アプリケーションは、イベントの変更が発生するまで、または PCRF から RAR を受信するまで待機します。
- タイマーの期限切れ後にイベントが変更された場合、CCR-U が PCRF に送信されます。CCA-U メッセージが成功すると、コールは PCRF で続行されます。成功しなかった場合は、ローカルポリシーでコールが実行され、再試行カウントが増分されます。
- タイマーの期限切れ後に RAR を受信した場合、コールは PCRF で続行されます。PCRF への接続の再試行期限が切れると、コールは切断されます。

CCR-I エラーに関するデフォルトポリシー

P-GW のローカル設定では、次のパラメータがサポートされています。設定パラメータは、APN ごとおよび RAT タイプごとに設定できます。

デフォルトベアラー課金ルールの次のフィールドは、APN ごとおよび RAT タイプごとに設定できます。

- ルール名
- 料金設定グループ
- Service ID
- オンライン課金
- オフライン課金
- QCI

- ARP
  - 優先度
  - QCI
  - QVI
- 最大要求帯域幅
  - UL
  - DL

フローの説明とフローステータスは設定できませんが、デフォルト値は Any to Any に設定され、フローステータスは Enabled に設定されます。

次のコマンドレベルのフィールドは、APN ごとおよび RAT タイプごとに設定できます。

- AMBR
  - UL
  - DL
- QCI
- ARP
  - 優先度
  - QCI
  - QVI

Gx バックオフ機能

このシナリオは、プライマリ PCRF クラスタが使用できないものの、新しい CCR-I メッセージを処理できるセカンダリ PCRF が使用可能な場合に適用されます。

シャーシが 3004 結果コードを受信すると、ピアのバックオフタイマーが開始され、タイマーが実行されている間、そのピアにメッセージは送信されません。

タイマーは、値がエンドポイント設定で設定されている場合にのみ開始されます。

P-GW/GGSN は、CCR が失敗した場合、サブスクライバに PCRF に再接続する優れた機会を提供します。この機能をサポートするために、設定可能な有効性タイマーとピアバックオフタイマーが、ローカルポリシーサービスおよびDiameterエンドポイント設定コマンドに導入されています。また、ローカルポリシータイマーの実行中に受信した RAR は、「DIAMETER_UNABLE_TO_DELIVER」が原因で拒否されます。

CLI コマンド **diameter encodeevent-avps local-fallback** がポリシー制御コンフィギュレーションモードで設定されている場合、再接続中にルールレポートが PCRF に送信されます。

ローカルポリシーでのボリュームレポートのサポート

この機能により、CCR-U障害シナリオでの、イベントベースではなく時間ベースの PCRF への再接続がサポートされます。

ローカルポリシーのボリュームレポートに関して、次の動作が見られました。

- CCR-U 障害の発生時、CCR-U は、サブスクライバイベントの受信時にのみ PCRF にトリガーされていました。
- CCR-U障害が発生し、コールがGxなしで続行された場合、しきい値が無限に設定されているため、報告されていないボリュームは失われました。次のCCR-UがPCRFにトリガーされると、累積ボリュームが PCRF に送信されました。
- 有効性タイマーの実行中に、RARは、原因コードdiameter_unable_to_comply（3002）で拒否されました。

タイマーベースの実装後、この機能により、既存の動作に次の変更が導入されます。

- send-usage-reportが設定されている場合、使用状況レポートを含むCCR-Uが、ローカルポリシータイマーの有効期限が切れた直後に送信されます。
- 報告されていない使用状況は、ECS に返されません。そのため、最後に CCR-U を試行してからの使用状況が PCRF に送信されます。
- タイマーが実行されている場合でも、RAR は受け入れられ、RAR で受信されたルールがインストールされます。

サブスクライバイベントを待つ代わりに、セッションをPCRFにすぐに接続し、更新された使用状況レポートを送信することができます。

セッションリカバリとセッション同期のサポート

現在、通常のシナリオで Gx のポジティブ想定機能が適用されていない場合、PCRF ノードとASR 5500 ゲートウェイノードは同期しています。ただし、PCRFがローカルで削除されたり、Gx セッション情報が損失しているシナリオが考えられます。また、メッセージの損失が原因で、ゲートウェイノードと PCRF のセッション状態が同期していない可能性もあります。

ネットワークがこのような状態になるのはまれですが、セッションの損失時にPCRFがGxセッションを復元し、またPCRFとゲートウェイ間でルールとセッション情報を同期させるのが、望ましい動作です。この機能を使用すると、PCRFとゲートウェイがセッション情報を同期し、失われた Gx セッションを復元できます。セッションリカバリ機能とセッション同期機能を有効にするための設定がサポートされるようになりました。

ゲートウェイ（GW）ノードとPCRFはセッション情報を交換する機能をサポートしています。GW は完全なサブスクライバセッション情報を提供して PCRF がセッション状態を確立できるようにします。これにより、上記のシナリオの発生を回避し、GW と PCRF が常に同期されるようになります。キーワード **session-recovery** および **session-sync** は、Gx 同期をサポートするために、ポリシー制御コンフィギュレーション モードで **diameter encode-supported-features** CLI コマンドと一緒に使用されます。

Gx のポジティブ想定機能の設定

Gx のポジティブ想定機能を設定するには、次の手順を実行します。

手順

ステップ 1 グローバル コンフィギュレーション レベルでのローカルポリシーサービスの設定 （804 ページ）の説明に従って、グローバル コンフィギュレーション レベルでサブスクライバのローカルポリシーサービスを設定します。

ステップ 2 グローバル コンフィギュレーション レベルでの障害処理テンプレートの設定 （805 ページ）の説明に従って、グローバル コンフィギュレーション レベルでローカルポリシーサービスを使用して、障害処理テンプレートを設定します。

ステップ 3 ローカルポリシーサービスと障害処理テンプレートの関連付け （805 ページ）の説明に従って、IMS 承認サービス内でローカルポリシーサービスと障害処理テンプレートを関連付けます。

ステップ 4 ローカルポリシーサービス設定の確認 （806 ページ）の説明に従って、設定内容を確認します。

ステップ 5 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

重要
この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンド、および/またはキーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

グローバル コンフィギュレーション レベルでのローカルポリシーサービスの設定

サブスクライバ向けのローカルポリシーサービスをグローバル コンフィギュレーション レベルで設定するには、次の例を使用します。

```
configure
    local-policy-service  LOCAL_PCC
         ruledef 2G_RULE
              condition priority 1 apn match .*
              exit
         ruledef all-plmn
              condition priority 1 serving-plmn match .*
              exit
         actiondef 2G_UPDATE
             action priority 1 activate-ambr uplink 18000 downlink 18000

              action priority 2 reject-requested-qos
              exit
         actiondef action1
              action priority 2 allow-requested-qos
              exit
         actiondef allow
              action priority 1 allow-session
```

```
            exit
        actiondef delete
            action priority 1 terminate-session
            exit
        actiondef lp_fall
            action priority 1 reconnect-to-server
            exit
        actiondef time
            action priority 1 start-timer timer duration 10
        exit
        eventbase default
            rule priority 1 event fallback ruledef 2G_RULE actiondef
time continue
            rule priority 2 event new-call ruledef 2G_RULE actiondef
action1
            rule priority 3 event location-change ruledef 2G_RULE
actiondef action1
          rule priority 5 event timer-expiry ruledef 2G_RULE actiondef
 lp_fall
            rule priority 6 event request-qos default-qos-change
ruledef 2G_RULE actiondef allow
            end
```

注：

- 一部のイベントが発生すると、イベントは、イベントベースのデフォルトの優先順位に基づいて最初に照合されます。一致したルールについて、対応する ruledef が満たされている場合、特定のアクションが実行されます。

グローバル コンフィギュレーション レベルでの障害処理テンプレートの設定

次の例を使用して、グローバル コンフィギュレーション レベルで障害処理テンプレートを設定します。

```
configure
   failure-handling-template <template_name>
      msg-type any failure-type any action continue local-fallback
      end
```

注：

- TCP リンク障害、アプリケーションタイマー（Tx）期限切れ、または結果コードベース障害が発生すると、関連する failure-handling が考慮され、failure-handling アクションが local-fallback として設定されている場合、コールは local-fallback モードにフォールバックします。

ローカルポリシーサービスと障害処理テンプレートの関連付け

ローカルポリシーサービスと障害処理テンプレートを関連付けるには、次の例を使用します。

```
configure
   context <context_name>
      ims-auth-service <service_name>
         associate local-policy-service <lp_service_name>
```

```
associate failure-handling <failure-handling-template-name>
end
```

ローカルポリシーサービス設定の確認

ローカルポリシーサービスの設定を確認するには、次のコマンドを使用します。

show local-policy statistics service *service_name*

Gx を介した時間レポート

ここでは、このリリースの GGSN でサポートされている Gx を介した時間レポートの機能について説明します。

ライセンス要件

Gx を介した時間レポート機能に個別のライセンスは必要ありません。この機能は、「ポリシーインターフェイス」ライセンスの一部として有効にすることができます。

特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

機能の概要

この非標準の Gx を介した時間使用状況レポート機能は、Gx を介したボリューム使用状況レポートに似ています。PCRF は、CCA または RAR で、セッション全体または特定のモニタリングキーの時間使用量しきい値を提供します。指定されたしきい値を超えると、使用状況レポートが CCR で PCRF に送信されます。この時間しきい値は、データトラフィックとは無関係です。使用量しきい値違反とは別に、使用状況レポートが PCRF に送信される他のシナリオがあります。



重要 Gx を介した時間レポートは、時間クォータにのみ適用されます。

PCEF は、最初からではなく、時間モニタリングの最後のレポート以降の累積時間使用状況のみを報告します。

時間使用量しきい値がゼロ（無限しきい値）に設定されている場合、PCEF によってそれ以上のしきい値イベントは生成されませんが、使用状況の監視は続行され、セッションの終了時に報告されます。

ベアラーの終了時の時間使用状況レポートがサポートされています。ベアラーが何らかの理由で削除されると、そのベアラーに関連付けられているルールも削除されます。そのため、使用状況は、ベアラー終了が原因で削除された最後のルールが関連ルールであるモニタリングキーで報告されます。

次の手順を通じて、Gx を介した時間レポートの仕組みについて説明します。

1. PCEF は、PCRF からメッセージを受信した後、時間モニタリング関連の AVP を解析し、その情報を IMSA に送信します。
2. IMSA はこの情報で ECS を更新します。
3. PCRF からの時間モニタリング情報で ECS が更新されると、PCEF（ECS）は時間使用状況の追跡を開始します。
4. セッションレベルのモニタリングの場合、ECS が時間使用状況を保持します。
5. PCC ルールモニタリングの場合、モニタリングキーを一意の識別子として使用状況がモニタリングされます。各ノードがモニタリングキーごとの時間使用状況情報を保持します。
6. PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、時間使用状況を追跡し続けます。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での時間モニタリングは続行されません。

制限事項

このセクションでは、このリリースの Gx を介した時間レポートの制限事項を示します。

- Gx を介したボリュームレポートのように、整数のモニタリングキーのみがサポートされます。
- 時間とデータボリューム両方のモニタリングに同じモニタリングキーが使用されている場合、モニタリングキーを無効にすると、時間とデータ使用状況の両方のモニタリングが無効になります。
- 同じモニタリングキーが時間とデータ使用状況両方のモニタリングに使用されている場合、即時レポート要求が受信されると、そのモニタリングキーの時間とボリューム両方のレポートが送信されます。

使用状況モニタリング

次の 2 つのレベルの時間使用状況レポートがサポートされています。

- セッションレベルでの使用量のモニタリング
- フローレベルでの使用量のモニタリング

セッションレベルでの使用量のモニタリング

PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルおよび SESSION_LEVEL（0）に設定された Usage-Monitoring-Level AVP と共に Usage-Monitoring-Information AVP を送信することで、Gx を介してセッションレベル時間レポートにサブスクライブします。

フローレベルでの使用量のモニタリング

PCRF は、Granted-Service-Unit AVP に設定された使用量しきい値レベルおよび PCC_RULE_LEVEL(1) に設定された Usage-Monitoring-Level AVP とともに Usage-Monitoring-Information AVP を送信することで、Gx を介してフローレベル時間レポートをサブスクライブします。フローレベルのモニタリングの場合、モニタリングキーは必須で

す。PCRF がルールとモニタリングキーを関連付ける際や、フローレベルで使用状況モニタリングを有効化または無効化する際に、モニタリングキーを使用して制御できるためです。使用状況モニタリングは、定義済みルールとダイナミックルール定義の両方に対応しています。

事前定義されたスタティックルールの使用状況モニタリング

事前定義されたルールに対して使用状況モニタリングを有効にする必要がある場合、PCRFは、モニタリングキーと使用量しきい値を含むルールおよび使用状況モニタリング情報を送信します。モニタリングキーは、その事前定義済みルールの PCEF で事前設定されているものと同じである必要があります。同じモニタリングキーに複数のルールを関連付けることができます。そのため、特定のモニタリングキーを有効にすると、同じモニタリングキーを持つ複数のルールの時間が追跡されることになります。同様に、スタティックルールの使用状況モニタリング情報も PCRF から送信されます。

ダイナミックルール定義の使用状況モニタリング

ダイナミックルール定義に対して使用状況モニタリングを有効にする必要がある場合、PCRFは課金ルールの定義や使用状況モニタリング情報（モニタリングキー、使用量しきい値など）とともにモニタリングキーを提供します。これにより、そのモニタリングキーに関連付けられているすべてのルールに対して使用状況モニタリングが実行されます。

使用状況レポート

サブスクライバレベルやフローレベルでの時間の使用状況は、次の条件でPCRFに報告されます。

- 使用量しきい値に達した：PCEF はサブスクライバの使用量を記録し、PCRF によって指定される使用量しきい値に達しているかどうかを確認します。条件が満たされると、使用状況の情報をIMSAに報告し、モニタリングを続行します。IMSAは、「USAGE_REPORT」トリガーがPCRFによって有効になっている場合に、CCR-Uをトリガーします。設定された「Used-Service-Unit」の「CC-Time」とともに、Usage-Monitoring-Information AVP がこの CCR で送信され、サブスクライバの時間使用量を追跡します。
- 使用状況モニタリングが無効：レポートの使用状況、その他の外部トリガー、またはPCRF内部トリガーに関連しない PCEF からの CCR の結果として PCRF により使用状況モニタリングが無効にされた場合には、PCRF が Usage-Monitoring-Support AVP を USAGE_MONITORING_DISABLEDに設定して使用状況モニタリングを明示的に無効にすると、PCEF はモニタリングを停止し、（モニタリングが有効だったときの）使用状況情報を PCRF に報告します。
- IP CAN セッションの終了：IP CAN セッションが終了すると、サブスクライバの累積使用状況情報が PCEF からの CCR-T で PCRF に報告されます。

  PCRF はRAR メッセージを使用し、その中に Session-Release-Cause AVP を含めて、IP CAN セッション終了を開始します。ただし、PCRF が CCA メッセージで IP CAN セッションを終了する場合もあります。不要な追加メッセージを回避するために、PCRF は、CCA-U メッセージ自体で、サブスクライバを終了するようにP-GWに通知できます。そのため、すべての Gx ディクショナリの CCA メッセージに Session Release Cause が追加されました。

- PCC ルールの削除：PCRF が使用量モニタリングキーに関連付けられている最後の PCC ルールを非アクティブ化すると、PCEF はそのモニタリングキーの使用時間を含む CCR を送信します。使用量モニタリングキーに関連付けられている最後の PCC ルールが非アクティブであると PCEF が報告する場合に、CCR コマンドに Charging-Rule-Report AVP が含まれていたなら、PCEF は同じ CCR コマンドでそのモニタリングキーの累積使用量を報告します。あるいは、Charging-Rule-Report AVP が RAA コマンドに含まれている場合、PCEF は新規に CCR コマンドを送信して、使用状況モニタリングキーの累積使用量を報告します。
- PCRF が要求した使用状況レポート：PCRF が Usage-Monitoring-Report を USAGE_MONITORING_REPORT_REQUIRED に設定して Usage-Monitoring-Information を提供すると、PCEF は時間使用状況情報を送信します。モニタリングキーが PCRF によって提供される場合、そのモニタリングキーの時間使用状況は、使用量しきい値に関係なく PCRF に通知されます。モニタリングキーが PCRF によって提供されない場合、有効なすべてのモニタリングキーの時間使用状況が PCRF に通知されます。
- イベントベースのレポート：イベントベースのレポートは、CLI コマンド **event-update send-usage-report events** を使用して有効化できます。SGSN 変更、QoS 変更、再検証タイムアウトなどのイベントがこの CLI で設定されると、そのイベントが発生するたびに時間使用状況レポートが生成されます。

使用状況が報告されると、使用量カウンタはゼロにリセットされます。PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、時間使用状況の追跡を 0 から継続します。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用量しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での時間使用状況モニタリングは続行されません。

Gx を介した時間レポート機能を設定する方法については、「Gx を介した時間レポートの設定（809 ページ）」を参照してください。

Gx を介した時間レポートの設定

ここでは、Gx を介した時間レポートを有効にするのに必要な設定について説明します。

Gx を介した時間レポートを有効にするには、次の設定を使用します。

```
configure
     active-charging service <ecs_service_name>
          rulebase <rulebase_name>
             action priority <priority> dynamic-only ruledef <ruledef_name>
 charging-action <charging_action_name> monitoring-key <monitoring_key>
                exit
          exit
     context <context_name>
          ims-auth-service <imsa_service_name>
               policy-control
                    event-update send-usage-report [ reset-usage ]
                    end
```

注：

- Gx を介した時間レポートを有効にするための設定は、Gx を介したボリュームレポートの設定と同じです。PCRF から時間しきい値を受信すると時間モニタリングが実行され、ボリュームしきい値を受信するとボリュームモニタリングが実行されます。
- PCEF が受け入れる最大モニタリングキー値は 4294967295 です。PCEF がより大きい値を送信すると、値は符号なし整数値に変換されます。
- **event-update** CLI を使用すると、イベントの更新時に時間使用状況レポートを送信できます。オプションキーワード **reset-usage** を使用すると、差分レポートをサポートできます。このレポートでは、使用状況が報告され、PCEF でリセットされます。このオプションが設定されていない場合、イベント更新の一部として時間使用状況の情報を送信しますが、PCEF でリセットすることはしません。

PCRF への複数のアクティブおよびスタンバイ Gx インターフェイスのサポート

以前の Gx の実装では、Diameter ポリシー制御アプリケーションに、IMS 認証サービスの一部としてホストを強制的に設定するか、ホストテンプレートを関連付けて、サブスクライバセッションごとに通信するホストを選択するという制限がありました。ピアの選択は diabase で実行でき、アプリケーションはホストを選択する必要がないため、この機能は、アプリケーションに課されていた制限を取り除き、diabase がラウンドロビン方式でピアを選択できるようにするために開発されました。さらに、この機能により、アプリケーションによって選択されたホストがアクティブでない場合でも、diabase でのピアの選択が処理されます。デフォルトの動作では、アプリケーションでのサーバー検出が失敗した場合にコールがドロップされるため、この動作の変更は、CLI コマンドの「**endpoint-peer-select**」によって制御されます。

コールが確立されると、IMSA モジュールは、接続されるプライマリピアとセカンダリピアを選択するために、IMSA サービスに関連付けられたホスト選択テーブル/プレフィックステーブル/ホストテンプレートをチェックします。ホストテーブル/プレフィックステーブル/ホストテンプレートが設定されていない場合、プレフィックステーブル内のどの行も一致しない場合、または IMSA によって選択されたホストが非アクティブである場合、CLI 設定に基づいて diabase モジュールに制御が渡され、ラウンドロビン方式でピアが選択されるか、CLI 設定に基づいてコールが終了します。

CCR メッセージが diabase エラー/Tx 期限切れ/応答タイムアウトになった場合、IMSA は、障害が発生したピアを除外することで diabase に代替ルートを選択させ、ルックアップが成功した場合はそのピアに切り替えます。

CCR/CCA メッセージが、diabase によって選択された直接接続ホストと交換され、新しいホストから RAR メッセージが受信されると、IMSA は、ホスト設定チェックをスキップし、新しいホストとのさらなる通信を許可します。コールの確立中に直接接続ホストがアプリケーションによって選択された場合、IMSA は、アプリケーションごとに新しいホストがセカンダリサーバーかどうかをチェックします。CCR/CCA メッセージが、diabase によって選択された DRA を介して間接的に接続されたホストと交換され、別の DRA を介して同じホストから RAR メッセージが受信されると、IMSA は、ホスト設定チェックをスキップし、新しい DRA を介した同じホストとのさらなる通信を許可します。コールの確立中に DRA がアプリケーションによって選択された場合、IMSA は、アプリケーションごとに新しい DRA がセカンダリサーバーか

どうかをチェックします。別の DRA を介して異なるホストから RAR メッセージを受信した場合でも、IMSA は、ホスト設定チェックをスキップし、新しい DRA を介した新しいホストとのさらなる通信を許可します。

障害シナリオにおける diabase での Diameter ピア選択の設定

次の設定により、IMSA で障害が発生した場合に diabase が Diameter ピアを選択できるようになります。

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            endpoint-peer-select [ on-host-select-failure |
on-inactive-host ]
            { default | no } endpoint-peer-select
            end
```

注：

- このコマンドは、IMS 承認アプリケーションによってホストを選択できなかった場合、または IMS 承認アプリケーションによって選択されたホストが非アクティブの場合に、データベースでサーバー選択を実行するために使用されます。たとえば、ホストテーブルが IMSA サービスで設定されていない場合、ホストテーブルは設定されているがアクティブ化されていない場合、プレフィックステーブルのどの行もサブスクライバと一致しない場合、ホストテンプレートが IMSA サービスに関連付けられていない場合、ホストテンプレートがホストを選択できなかった場合などです。
- **on-host-select-failure**：IMS 承認アプリケーションがホストを選択できなかった場合に diabase でサーバー選択を実行するように指定します。
- **on-inactive-host**：アプリケーションによって選択されたホストが非アクティブである場合に、diabase でサーバー選択を実行するように指定します。
- この CLI コマンドは、IMS 承認アプリケーションでサーバー選択が失敗した場合にコールを終了する以前の動作との下位互換性を維持するために、ポリシー制御設定モードで追加されます。

Gx インターフェイスにおける複数 CCR-U のサポート

ASR 5500 は、IMS 承認サービス コンフィギュレーション モードで設定可能な CLI コマンド「**max-outstanding-ccr-u**」を使用して、セッションごとに同時に複数の CCR-U メッセージをサポートします。よって、この CLI では、セッションあたりの CCR-U メッセージの最大数として、最大 12 の値を設定できます。

CLI ベースの実装では、要求メッセージがトリガーされたときにそのまま送信し、受信時に応答を処理できます。応答メッセージが順不同で受信された場合、ゲートウェイは順序の変更を行います。

PCRF に対する複数の未処理メッセージをサポートするには、次の項目がサポートされている必要があります。

- IMSA が複数の CCR-U メッセージを送信できる：これは、IMS 承認サービス コンフィギュレーション モードで **max-outstanding-ccr-u** コマンドを使用することで実現できます。
- 順序付けのための応答メッセージのキューイング：DPCA は、受信順序に関係なく、受信メッセージを解析する必要があります。IMSA は、応答をセッションマネージャに転送するか、ローカルでキューに入れるかを判定します。
- ピアスイッチ：複数の CCR-U がトリガーされると、IMSA は送信される各要求に対して Tx タイマーを開始します。Tx の最初の期限切れ時に、IMSA/DPCA はピアの切り替えを行います。つまり、IMSA は他のすべての要求の Tx タイマーを停止し、セカンダリピアに切り替えるか（可能な場合）、適切な障害処理アクションを実行します。
- 障害処理：Tx 期限切れによるピアスイッチ障害が発生した場合、DPCA は、ims-auth-service にある設定に基づいて障害処理アクションを実行します。
- バックプレッシャの処理：プライマリ PCRF に対して複数の CCR-U がトリガーされた場合、Tx タイムアウトによりすべてのメッセージがセカンダリ PCRF に切り替えられます。セカンダリサーバーがすでにバックプレッシャ状態にある場合、IMSA は最初のメッセージをバックプレッシャキューに入れ、メッセージが処理されると、次の保留中の要求が BP キューに入れられます。
- ボリュームレポート：使用状況レポートの複数の CCR-U が（別々のモニタリングキーに対して）トリガーされ、障害処理が「**continue send-ccrt-on-call-termination**」として設定されている場合、最初の Tx タイムアウトまたは応答タイムアウト時に、すべての CCR-U の使用状況レポートが ECS に送信されます。サブスクライバがダウンすると、未報告のすべての使用状況が CCR-T メッセージで送信されます。「**event-update send-usage-report**」CLI が存在する場合、複数の CCR-U の同じモニタリングキーの使用状況がレポートされる可能性があります。

max-outstanding-ccr-u CLI コマンドは複数 CCR-U の設定をサポートしますが、一度に送信されるアクセス側更新用の未処理の CCR-U は 1 つだけであり、内部更新用には複数の CCR-U が送信されます。

CCR-U がトリガーされる可能性があるアクセス側更新は次のとおりです。

- ベアラーリソースコマンド
- ベアラー要求の変更（S-GW の変更、RAT の変更、ULI の変更）
- ベアラー変更コマンド

CCR-U がトリガーされる内部更新は次のとおりです。

- S-GW の復元
- ベアラーのダウン（GGSN、BCM UE_Only）
- ULI/タイムゾーンの通知
- デフォルト EPS ベアラー QoS の障害
- APN AMBR の障害
- Charging-Rule-Report
- クレジットの不足/クレジットの再割り当て
- 使用状況レポート
- テザリングフロー検出
- アクセスネットワーク課金識別子

バックツーバック CCR-U をサポートするためのゲートウェイノードの設定

次の設定コマンドを使用すると、ゲートウェイによるPCRFへの複数のバックツーバックCCR-Uの送信が有効または無効になります。

```
configure
   context  context_name
      ims-auth-service   service_name
         policy-control
            [ default ] max-outstanding-ccr-u value
            end
```

注：

- *value* は、1 から 12 までの整数値にする必要があります。デフォルト値は 1 です。

Gx インターフェイスにおける RAN/NAS 原因 IE のサポート

3GPP TS 29.212 のリリース 12 仕様に準拠するために、新規サポート機能として「Netloc-RAN-NAS-Cause」が導入されました。この機能は、アクセスネットワークからPCRFにRANやNASの詳細なリリース原因コード情報を送信するために使用されます。利用するには、NetLoc 機能もサポートされている必要があります。

重要 この機能は、NetLoc機能のライセンスがインストールされている場合にのみ有効にできます。

NetLoc-RAN-NAS-Causeをサポートする機能が有効になっている場合には、Charging-Rule-Report AVP と、ベアラーおよびセッション削除イベントの CCR-T にそれぞれ、新しい Diameter AVP「RAN-NAS-Release-Cause」が含まれます。このAVPは、サブスクライバまたはベアラーの終了の原因コードを示します。

サポートされる機能「Netloc-RAN-NAS-Cause」の設定

次の設定では、サポートされている機能「Netloc-RAN-NAS-Cause」が有効になります。

```
configure
    context  context_name
         ims-auth-service  service_name
              policy-control
                   diameter encode-supported-features
netloc-ran-nas-cause
                   end
```

注：

- **netloc-ran-nas-cause**：Netloc-RAN-NAS-Cause 機能を有効にします。この機能はサポートされますが、デフォルトでは無効になっています。
- サポートされている機能である [netloc-ran-nas-code] と [netloc] を有効にすると、netloc-ran-nas-cause コードが PCRF に送信されます。

このサポートされている機能を無効にするには、次のコマンドを使用します。

[default | no] diameter encode-supported-features

Gx インターフェイスを介した ADC ルールのサポート

このリリースでは、P-GW は、3GPP 標準規格のリリース 11 仕様で定義されているように、Gx を介してアプリケーションの検出と制御（ADC）機能を使用します。

Gx を介した ADC 拡張は、特定のプロトコルまたはプロトコルのグループの開始と停止に関して PCRF に通知する機能を提供し、PCRF がこの情報を認識して、ユーザーがアプリケーションの使用を開始して、それが終了するまでの間、ユーザーの QoS を変更できるようにします。

ADC 情報のプロビジョニングは ADC ルールを介して行われ、PCRF によって開始されるアクションは PCC ルールを介して行われます。

ADC ルールは、アプリケーションフローの指定、検出、およびレポートをサポートするための動的な事前定義されたいくつかの PCC ルールを拡張したものです。これらのルールは、CCA-I/CCA-U/RAR イベントを介して PCRF によってインストール（変更/削除）されます。ADC ルールは、動的な PCC ルールまたは事前定義された PCC ルールのいずれかにすることができ、動的ルールおよび事前定義ルールの既存の属性が適用されます。

動的な PCC ルールには、トラフィックフローフィルタまたはアプリケーション ID のいずれかが含まれます。アプリケーション ID が存在する場合、ルールは ADC ルールとして扱われます。アプリケーション ID は、Boxer の設定で事前に定義されている ruledef の名前です。この ruledef には、P2P プロトコルによってサポートされているアプリケーションを定義するアプリケーションフィルタが含まれています。

PCEF は、PCRF インターフェイスから受信した ADC ルールを処理およびインストールし、指定されたアプリケーションを検出し、アプリケーショントラフィックの検出を PCRF に報告します。次に、PCRF はアプリケーショントラフィックのレポートを制御します。

PCEF は、PCRF によって有効になっている指定のアプリケーションをモニターし、アプリケーション ID を含む開始/停止イベントを生成します。このようなアプリケーション検出は、ADC PCC ルールがバインドされるベアラーとは無関係に実行されます。たとえば、ADC ルールが専用ベアラーにインストールされている一方で ADC トラフィックがデフォルトのベアラーで受信された場合でも、アプリケーション検出ユニットは PCRF に開始イベントを報告します。

重要 ADC ルールのサポートは、ライセンスで制御される機能です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

この機能をサポートするため、次の Diameter AVP が Charging-Rule-Definition AVP に新たに追加されました。この AVP は、PCEF が PCRF から受信します。

- TDF アプリケーション識別子：PCEF 内のアプリケーションの検出と制御 PCC ルールが適用されるアプリケーション検出フィルタを参照します。TDF アプリケーション識別子 AVP は、PCRF へのレポート内のアプリケーションも参照します。

- Redirect-Information：検出されたアプリケーショントラフィックを別の制御対象アドレスにリダイレクトする必要があるかどうかを示します。
- Mute-Notification：この AVP は、PCEF からの特定の ADC/PCC ルールについて、検出されたアプリケーションの開始/停止の PCRF への通知をミュートするために使用されます。
- Application Detection Information：Mute-Notification AVP が課金ルールレポートに含まれておらず、APPLICATION_START/APPLICATION_STOP イベントトリガーが有効になっている場合、PCEF は TDF アプリケーション識別子に対応する PCRF に Application-Detection-Information を送信します。

さらに、2 つの新しいイベントトリガー「APPLICATION_START」および「APPLICATION_STOP」が、レポート目的で生成されます。

制限事項

ADC over Gx 機能の制限事項は以下のとおりです。

- ADC は ruledef のグループをサポートしていません。
- 重複するアプリケーション ID の登録はサポートされません。
- P2P フローの再アドレス付け/リダイレクションはサポートされません。
- リダイレクションは、GET/Response のトランザクションでのみ発生します。
- ポートベース、IP プロトコルベース、および URL ベースのアプリケーションはサポートされていません。
- ダイナミック ADC ルールの事前設定オプション（precedence、redirect-server-ip）はサポートされていません。
- 同じサブスクライバのアプリケーションの同時インスタンスは区別されません。
- アプリケーションフローでは、フローリカバリがサポートされていません。

Gx を介した ADC ルールの設定

次の設定により、Gx インターフェイスを介した ADC ルールが有効になります。

```
configure
   context  context_name
      ims-auth-service   service_name
         policy-control
            diameter encode-supported-features adc-rules
            end
```

注：

- キーワード「**adc-rules**」は、機能固有のライセンスが設定されている場合にのみ使用できます。
- ADC の場合、サポートされている機能の第 6 ビットが設定されます。

Gx を介した ADC ルールのサポートを無効にするには、次のコマンドを使用します。

```
[ default | no ] diameter encode-supported-features
```

TDF アプリケーション識別子での GoR 名のサポート

ASR 5500 では、TDF アプリケーション識別子として GoR 名を使用してインストールするダイナミックルールがサポートされています。ADC ルールが PCRF からダイナミックルールとしてインストールされている場合、TDF アプリケーション識別子には、P-GW で事前設定された GoR 名を含めることができます。

ADC 機能が有効になっている場合、PCRF は、P-GW 設定で事前定義された GoR の名前として、TDF アプリケーション識別子を送信できます。

- Charging-Rule-Definition AVP を使用したダイナミック課金ルールが PCRF からアクティブ化されると、PCRF は、ECS で TDF アプリケーション識別子として設定された GoR 名を指定できます。
- Charging-Rule-Definition AVP を含むダイナミック課金ルールがアクティブ化されると、PCRF は、RAR を使用して、Charging-Rule-Definition を介してルールを削除または変更できます。ルールの有効化または変更の際に、PCRF は、ルールの課金ルール属性を追加、変更、または削除できます。

PCRF からの TDF アプリケーション識別子の設定の変更を以下に示します。

- 非 ADC ダイナミックルールは、関連する ruledef または GoR 名とともに TDF アプリケーション識別子 AVP を送信することで、ADC ダイナミックルールに変更できます。

  ADC ダイナミックルールを非 ADC ダイナミックルールに変更することはできません。
- PCRF からの受信後に、次の AVP が変更され、適用されます。
  - 優先順位（Precedence）
  - Rating-Group/Service-Identifier/Sponsor-Identity（レポートレベルに応じて必須）
  - Metering-Method
  - Online/Offline
  - QoS-Information
  - Monitoring-Key
  - Redirect-Information
- ダイナミックルートは、TDF アプリケーション識別子 GoR の一部であるルールの全プロトコルに対して更新されます。
- ダイナミックルールの優先順位または TDF アプリケーション識別子の値が変更されると、新しいルール照合として APP-START および APP-STOP イベント通知が送信されます。ルール変更の前に APP-START 通知が送信されている場合、対応する APP-STOP 通知は送信されません。
- 関連付けられた GoR のランタイム削除はすぐに有効になり、APP-START がすでに送信されている場合、APP-STOP 通知は送信されません。サービスレベルでの GoR の追加では、

ダイナミック ADC ルールと事前定義された ADC ルールの両方で新しい追加を有効にするために、ルールを再インストールする必要があります。

ADC ミュートのカスタマイズ

以前は、3GPP ADC over Gx はアプリケーションのミュートステータスの変更をサポートしていませんでした。アプリケーションがミュートされると、ミュートを解除できませんでした。リリース 21.1 から、この機能にカスタム MUTE およびカスタム UNMUTE の機能が導入されました。ASR 5500 PCEF では、アプリケーション検出情報 CCRU のレポートを制御するためのカスタマイズをサポートするようになりました。このために、カスタム MUTE とカスタム UNMUTE という 2 つの可能な値を持つ AVP が導入されました。

- Gx メッセージには、標準ベースの MUTE とカスタム MUTE の両方が含まれている場合があります。
- 標準ベースの MUTE は、カスタムの MUTE および UNMUTE よりも優先されます。
- ダイナミック ADC ルールは、カスタム MUTE を使用してインストールおよび変更できます。
- Custom-Mute-Notification AVP は、CCA-I および RAR の PCRF によって送信できます。
- ダイナミック ADC ルールは、カスタム UNMUTE を使用して変更できます。
- 特定のダイナミック ADC ルールのカスタム MUTE では、PCEF はフローごとに APPLICATION_START/APPLICATION_STOP 応答を送信するのではなく、アプリケーション トラフィック全体に対して 1 つの APPLICATION_START/APPLICATION_STOP 応答を送信します。
- 特定のダイナミック ADC ルールのカスタム MUTE では、カスタム MUTE の前に APPLICATION_START が送信されていない場合、ダイナミックルールにヒットする次のフローパケットで 1 つの APPLICATION_START が送信されます。
- 特定のダイナミックルールのカスタム MUTE では、APPLICATION_START 応答がフローの 5 タプル情報とともに送信されます。
- 特定のダイナミックルールのカスタム MUTE では、APPLICATION_START 応答が TDF-Application-Instance-Identifier = 0 で送信されます。
- 特定のダイナミックルールのカスタム MUTE では、特定のダイナミックルールに関連付けられた最後のフローが終了すると、1 つの APPLICATION_STOP が送信されます。このような APPLICATION_STOP には、最後のフローの 5 タプル情報は含まれず、TDF-Application-Instance-Identifier = 0 で送信されます。
- 特定のダイナミックルールのカスタム UNMUTE では、APPLICATION START 応答が特定のダイナミックルールと照合された後、その後のすべてのフローに送信されます。
- カスタム UNMUTE の動作に変更はありません。これは、UNMUTING 以前はカスタム MUTED でも標準 MUTED でもありませんでした。APPLICATION_START および APPLICATION_STOP は、以前と同様に、フローごとに引き続き送信されます。
- カスタム UNMUTE では、PCEF は、終了するすべてのフローに対して APPLICATION_STOP を送信し、次に進みます。
- 特定のダイナミックルールは、カスタム MUTE または UNMUTE ステータスを含む SR と ICSR の両方で回復されます。特定のダイナミックルールの APPLICATION_START ステー

タスがチェックポイント化され、回復されます。これにより、リカバリ後に余分な APPLICATION_START が PCRF に送信されなくなります。

ADC カスタムミュート/ミュート解除機能の強化

機能情報

要約データ

[ステータス（Status）]	変更された機能
導入されたリリース	21.1
変更されたリリース	21.2
対象製品	SAEGW
該当プラットフォーム	ASR 5500
デフォルト設定	無効
関連する CDETS ID	CSCvd00699
このリリースでの関連する変更点	N/A
関連資料	Command Line Interface Reference SAEGW Administration Guide

マニュアルの変更履歴

重要 リリース 21.2 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース	リリース日
このリリースで変更。	21.2	2017 年 4 月 27 日

変更された機能

「ADC ミュートのカスタマイズ」機能により、アプリケーション検出情報 CCRU のレポートを制御するカスタム MUTE/UNMUTE 機能が導入されました。PCRF はカスタム MUTE PCRF AVP を使用して、ADC アプリケーション通知を無効または有効にするタイミングを P-GW に通知するようになりました。

この機能は「ADC ミュートのカスタマイズ」機能をさらに強化し、カスタムミュートとミュート解除イベント間のフローアクティビティを報告します。P-GW はカスタムミュートイベント間のフローアクティビティを学習し、ADC ルールでカスタムミュート解除イベントが発生し

た後に PCRF に報告します。これにより、標準の ADC のミュートおよびミュート解除ケースで、ADC アプリケーションの開始および停止メカニズムが最小限となります。

新しい CLI コマンドが設定に応じてルールベースで実装されるようになりました。ルールごとに 1 回のみ、ADC アプリケーションの開始と停止が報告されます。これは、PCRF へのメッセージングフローを削減するのに役立ちます。

制限事項

この機能には次の制限があります。

- P-GW では、ADC ルールごとに最大 12 の学習済みフローが保存されます。上限の 12 に達すると、P-GW は最も古いフローの学習データを削除し、最新のフローについて学習します。P-GW がカスタムミュート解除イベントを受信すると、学習した通知内容を PCRF に伝えます。フローのアプリケーション開始通知が送信された場合、P-GW はアプリケーション停止通知を送信します。
- カスタムミュート解除のイベントが回復されない場合、アプリケーション開始通知を PCRF に送信するためにフロー情報が保存されます。
- LTE から Wi-Fi へのハンドオーバーでは、ADC ダイナミックルールごとのカスタムミュートまたはカスタムミュート解除で PCRF から受信した値が新しい RAT に適用されます。ハンドオーバーコンテキストで値が受信されない場合、存在するすべての ADC ダイナミックルールについて、RAT 変更前の以前の値が保持されます。
- CLI コマンド **adc notify** が有効になっている場合は、単一の ADC アプリケーションの開始と停止の通知が PCRF に送られます。同じ ADC ダイナミックルールに一致する複数のフローがある場合、1 つのアプリケーション開始通知と停止通知のみが PCRF に送信されます。
- この機能はダイナミックルールにのみ実装されます。

機能の仕組み

P-GW がパケットを受信し、ADC ルールイベントが PCRF から発生したときのイベントシーケンスは次のとおりです。

1. パケットが ECS ルールマッチングエンジンに到達します。
2. ルールマッチングエンジンは、ADC ダイナミックルールが一致するかどうかを確認します。また、PCRF やルールベースレベルの CLI を介してカスタムミュートが適用されているかどうかも確認します。単一のアプリケーション開始通知が以前に送信されていない場合は、送信されます。
3. 同じ ADC ルールに一致するすべての後続フローについて、アプリケーション開始通知が保存されます。これらの通知は、カスタムミュート解除イベントの受信後に CCRU で送信されます。

重要なポイントは次のとおりです。

- PCRF から受信した値の優先順位が最も高くなります。したがって、標準ミュートはカスタムミュートやカスタムミュート解除よりも優先されます。CLI *adc notify one* の優先順位が最も低くなります。
- CLI **adc notify one** がルールベースで設定されている場合、その逆の **no adc notify** が影響することはありません。CLI の影響を回避するには、次のタスクのいずれかを実行します。
  - CLI **adc notify once** が設定されていないルールベースに切り替えます。
  - その特定のダイナミックルールの「カスタムミュート解除」を送信します。

ADC 通知の設定

新しい CLI コマンド **adc notify**が、アクティブ課金サービスモードに追加されました。

この CLI が設定されると、ルールごとの ADC フローの一致に対して単一のアプリケーション開始通知またはアプリケーション停止通知が PCRF に送信されます。この CLI が設定され、PCRF がカスタムミュート通知を送信した場合、PCRF 通知は、通知をレポートするための標準的な動作よりも優先されます。

このキーワードのデフォルト値は false です。この CLI が設定されていない場合、ADC 通知の送信時にアクションは実行されません。

この機能を有効または無効にするには、以下のコマンドを入力します。

```
configure
  active-charging service <service_name>
    rulebase <rulebase_name>
      [no] adc notify [once]
      end
```

1 つの通知を設定するには、次のコマンドを使用します。

```
adc notify once
```

注：

- **no:** ADC 通知を無効にします。ADC 通知はデフォルトの動作に従って送信されます。
- **adc:** ADC 通知を設定します。
- **notify:** アプリケーション通知を設定します。このキーワードが設定されていない場合、ADC 通知はデフォルトの動作に従って送信されます。
- **once:** アプリケーション通知を 1 回だけ設定します。PCRF が優先されます。

TAI および ECGI 変更レポートのサポート

このセクションでは、TAI および ECGI 変更レポート機能の概要と導入について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

- 機能説明 （821 ページ）

• 機能の仕組み （822 ページ）
• TAI および ECGI 変更レポート機能のモニタリングと障害対応 （823 ページ）

機能説明

Gx を介した UE のユーザーロケーションレポートをアクティブ化する場合、PCRF は「USER_LOCATION_CHANGE（13）」イベントトリガーを使用して RAR と CCA を送信します。このイベントトリガーを受信すると、P-GW は通常、変更レポートアクション（CRA）情報要素（IE）を「レポート開始」とともに MME に送信し、MME 内の UE のロケーション変更レポートを有効にします。

現在のアーキテクチャでは、「USER_LOCATION_CHANGE（13）」トリガーを使用して、ユーザーロケーション情報（ULI）、トラッキング領域 ID（TAI）、および E-UTRAN セルグローバル ID（ECGI）の変更が報告されます。show configuration コマンドで新しいイベントトリガーを表示するために、CLI が変更されました。



重要 TAI レポートを機能させるには、値 33 を使用するように、ポリシー制御コンフィギュレーション モードで **diameter map usage-report** CLI コマンドを設定する必要があります。

PCRF は、TAI と ECGI の変更を報告するための CRA イベントをサブスクライブします。P-GW は、PCRF によってサブスクライブされた場合にのみ CCR-U でイベントトリガーを送信します。PCRF が ECGI の変更や TAI の変更のイベントトリガーをインストールすると、ECGI と TAI の変更（インストールされているトリガーに基づく）が報告されます。

TAI および ECGI 変更レポート機能は、3GPP TS 29.212 v9.7.0 に準拠しています。この機能は Gx インターフェイスでサポートされているため、ECGI や TAI の変更時に UE が追跡され、PCRF に報告できます。ユーザーロケーション情報に関するレポート機能の詳細については、展開している製品のアドミニストレーション ガイドを参照してください。

CRA 値は、PCRF から受信したイベントトリガーによって異なります。

Change Reporting Support Indication（CRSI）と ULI も、ベアラーリソースコマンドでサポートされています。

P-GW は、対応するベアラー削除応答を受信すると、ベアラー削除コマンドで MME からの受信した ULI を PCRF に送信します。ULI がベアラー削除コマンドとベアラー削除応答の両方に含まれている場合、ベアラー削除応答の ULI が PCRF に送信されます。ベアラー削除応答に ULI がない場合、ベアラー削除コマンドで受信した ULI が PCRF に送信されます。

他の機能との関係

この機能は、Event-Trigger AVP の USAGE_REPORT 値に依存しています。この機能は、USAGE_REPORT の値が 33 に設定されている場合にのみ機能します。これは、ポリシー制御コンフィギュレーション モードで **diameter map usage-report** CLI コマンドを使用して実現できます。

機能の仕組み

P-GW は、P-GW によって検出されたイベントトリガーに基づいて、イベントトリガー値を CCR-U で送信します。P-GW は、次の表に従って、イベントトリガーと ULI タイプを CCR-U で PCRF に送信します。

PCRF からのイベントトリガー	**CRA** 値	**P-GW** で検出されたイベント	**PCRF** への通知内容
ULI_CHANGE	6	TAI_CHANGE または ECGI_CHANGE	イベントトリガー：ULI_CHANGE ULI タイプ：TAI + ECGI
TAI_CHANGE	3	TAI_CHANGE	イベントトリガー：TAI_CHANGE ULI タイプ：TAI
ECGI_CHANGE	4	ECGI_CHANGE	イベントトリガー：ECGI_CHANGE ULI タイプ：ECGI
ULI_CHANGE + TAI_CHANGE	6	TAI_CHANGE	イベントトリガー：ULI_CHANGE+ TAI_CHANGE ULI タイプ：TAI+ECGI
ULI_CHANGE + ECGI_CHANGE	6	ECGI_CHANGE	イベントトリガー：ULI_CHANGE + ECGI_CHANGE ULI タイプ：TAI+ECGI
ULI_CHANGE + TAI_CHANGE + ECGI_CHANGE	6	TAI/ECGI が変更された	イベントトリガー：ULI_CHANGE + TAI/ECGI CHANGE ULI タイプ：TAI+ECGI
TAI_CHANGE + ECGI_CHANGE	6	TAI/ECGI が変更された	イベントトリガー：TAI_CHANGE/ECGI_CHANGE ULI タイプ：TAI+ECGI

PCRF からのイベントトリガー	CRA 値	P-GW で検出されたイベント	PCRF への通知内容
特に上記に記載されていない組み合わせについては、	6		イベントトリガー：ULI_CHANGE ULI タイプ：TAI+ECGI

制限事項

TAI および ECGI 変更レポート機能は、**diameter map usage-report** CLI コマンドが 33 に設定されている場合にのみサポートされます。

TAI および ECGI 変更レポート機能のモニタリングと障害対応

ここでは、TAI および ECGI 変更レポート機能のサポートにおける show コマンドとその出力について説明します。

show ims-authorization sessions full all

この機能をサポートするこの show コマンドの出力に、以下のフィールドが追加されました。

- TAI-Change：サブスクライバセッションの TAI が変更された場合に、このイベントトリガーを表示します。
- ECGI-Change：サブスクライバセッションの ECGI が変更された場合に、このイベントトリガーを表示します。

show ims-authorization service statistics all

この機能をサポートするこの show コマンドの出力に、以下の統計が追加されました。

- TAI 変更：P-GW が PCRF に TAI_CHANGE（26）イベントトリガーを報告した合計回数を表示します。
- ECGI 変更：P-GW が PCRF に ECGI_CHANGE（27）イベントトリガーを報告した合計回数を表示します。

ロケーションベースのローカルポリシールール適用

このセクションでは、ロケーションベースのローカルポリシー（LP）ルール適用機能の概要と実装について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

- 機能説明 （824 ページ）
- 機能の仕組み （824 ページ）

- ロケーションベースのローカルポリシールール適用機能の設定 （826 ページ）
- ロケーションベースのローカルポリシールール適用機能のモニタリングと障害対応 （828 ページ）

機能説明

この機能は、サブスクライバが企業APNに接続したときに、さまざまなE-UTRANセルグローバル識別子（ECGI）に対して事前定義されたさまざまなルールをアクティブにするために導入されました。サブスクライバは、企業エリア外にいる場合は、企業 APN との接続を明示的にダウンし、インターネット APN とのセッションを再確立する必要があります。企業 APN は PCRF を使用せず、ローカルポリシーのみを使用することを前提としています。この場合、APN に一致するすべてのコールがローカルポリシーに転送されます。



重要 この機能を動作させるには、ローカルポリシーを有効にするライセンスを設定する必要があります。ライセンス要件の詳細については、最寄りのシスコのアカウント担当者にお問い合わせください。

ECGIに対して事前定義されたさまざまなルールをアクティブ化するために、ローカルポリシーの設定は以下をサポートするように拡張されています。

- 一連の ECGI の設定と検証
- 変更レポートアクション（CRA）イベントによる ECGI_CHANGE イベントトリガーのインストール
- ECGI_CHANGE イベントの検出

この機能は、ローカルポリシー ruledef 条件との ECGI 一致に基づいて適用される次のアクションをサポートしています。

- ECGI が特定のグループに属した場合の ECGI_CHANGE イベント通知のリダイレクトルールを有効にする
- 他の ECGI に対するワイルドカードルールを有効にする

他の機能との関係

この機能は、TAI および ECGI 変更レポート機能に依存しています。これにより、セッションマネージャ モジュールから IMSA/ローカルポリシーモジュールへの ECGI 変更をレポートするためのフレームワークが提供されます。

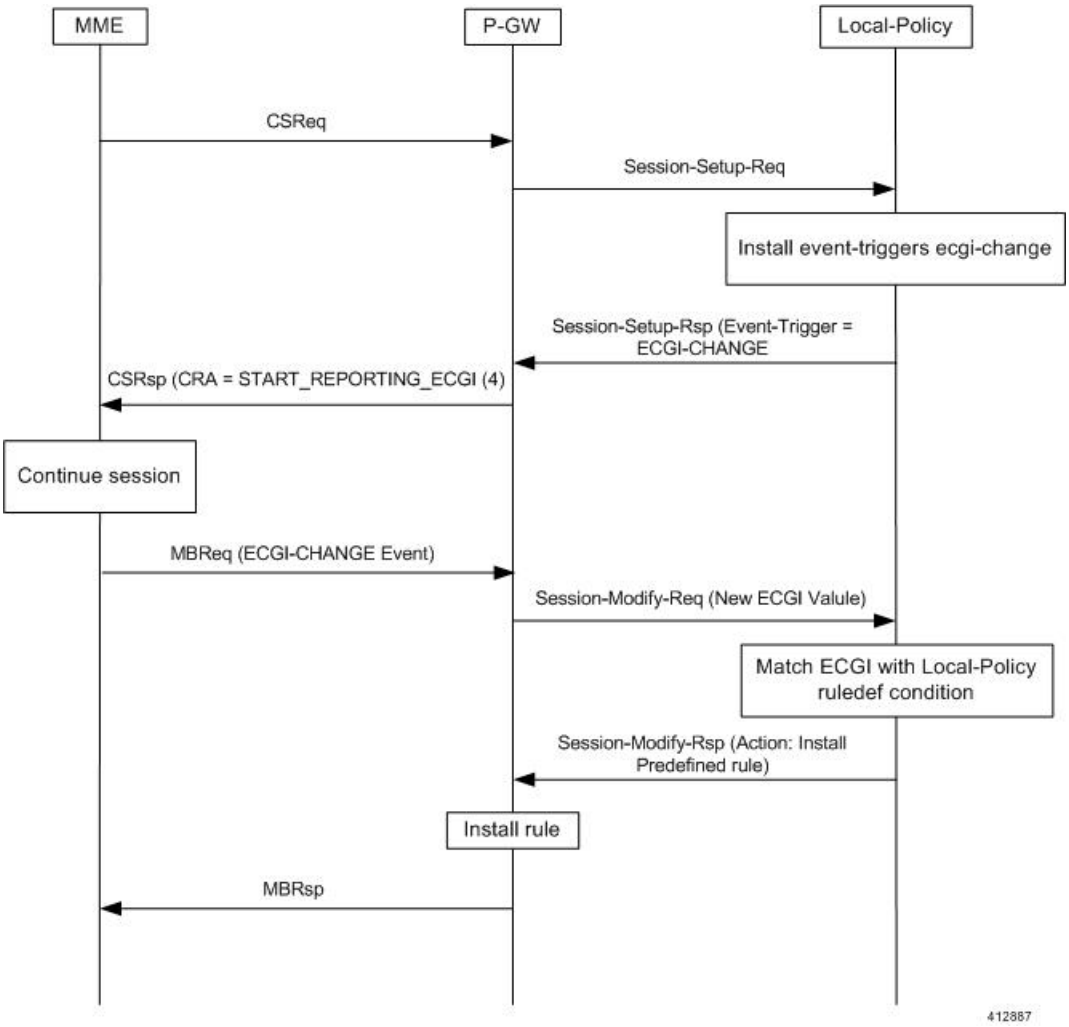
機能の仕組み

この項では、ECGI-CHANGE イベントトリガーに基づいて、ローカルポリシールールの選択と適用がどのように行われるかについて説明します。

Flows

次の図は、ECGI-CHANGE イベントがローカルポリシー、MME、および P-GW でどのように処理されるかを示しています。

図 *65 : ECGI* 変更イベントの処理



新しいコールが確立されると、ECGI 変更イベントトリガーがローカルポリシーから送信されます。P-GW は、セッション作成応答（CSRsp）で CRA 値 4 を送信して ECGI レポートを MME に要求します。MME は、変更通知要求/ベアラー変更要求（MBReq）を介して ECGI の変更を P-GW に通知します。P-GW でのローカルポリシー設定により ECGI 変更イベントが処理され、新しい ECGI が属する ECGI グループに基づいて適切なアクションが実行されます。1 つのアクションとして、ECGI が特定のグループに属する場合に特定のリダイレクトルールをアクティブ化することが考えられます。別のアクションとして、その他のすべての ECGI に対してワイルドカードルールを有効にすることが考えられます。

制限事項

ここでは、この機能の既知の制限について説明します。

- ECGI 変更の検出とトリガリングは、この機能の前提条件です。
- この機能は、特定の APN 内のすべての要求と応答が PCRF に接続せずにローカルポリシーに直接送信されるローカルポリシーのみ（lp のみ）モードでサポートされます。つまり、この機能は、ローカルポリシーフォールバックモードや、PCRF とローカルポリシーの両方が共存するデュアルモードでは機能しません。

ロケーションベースのローカルポリシールール適用機能の設定

このセクションでは、ECGI-Change イベント通知に基づいてルールの適用を有効にするための、local-policy 内パラメータの設定について説明します。

ECGI 変更トリガーの設定

次の設定を使用して、local-policy から ECGI-Change トリガーをインストールします。

```
configure
   local-policy-service service_name
      actiondef actiondef_name
         action priority priority event-triggers ecgi-change
         exit
      eventbase default
        rule priority priority event new-call ruledef ruledef_name actiondef
 actiondef_name [ continue ]
         end
```

注：

- **priority** *priority*：指定されたアクションの優先順位を指定します。*priority* は一意で、1 ～ 2048 の整数である必要があります。
- **ecgi-change**：このキーワードは、ECGI-CHANGE イベントトリガーをインストールするように指定します。有効にすると、ECGI-CHANGE イベントトリガーが local-policy から送信されます。
- 通信事業者が CRA 値を送信して MME で ECGI-Change 通知を有効にする場合は、この CLI コマンドを local-policy で設定します。

ECGI 変更イベントのルールの適用

次の設定を使用して、ECGI の変更の検出を有効にし、MME によって報告された ECGI-CHANGE イベントに対して特定のアクションを実行します。

```
configure
   local-policy-service service_name
      eventbase eventbase_name
         rule priority priority event ecgi-change ruledef ruledef_name
```

```
actiondef actiondef_name [ continue ]
         end
```

注：

- **priority** *priority*：指定されたルールの優先順位を指定します。*priority* は一意で、1 ～ 2048 の整数である必要があります。
- **ruledef** *ruledef_name*：ルールを特定の ruledef に関連付けます。*ruledef_name* は、このローカル QoS ポリシーサービス内にある既存の ruledef にする必要があります。
- **actiondef** *actiondef_name*：ルールを特定の actiondef に関連付けます。*actiondef_name* は、1 ～ 63 文字の英数字の文字列で表される、このローカル QoS ポリシーサービス内にある既存の actiondef である必要があります。
- **ecgi-change**：ECGI-CHANGE を検出する新しいイベントを有効にし、actiondef 設定で定義されているようにして ECGI-CHANGE イベントに特定のアクションを適用します。
- **continue**：後続のルールも照合されます。指定しない場合、ルールの評価は最初の一致の時点で終了します。

ECGI 値に基づくローカルポリシールールの適用

MME による ECGI-Change イベント通知で受信した ECGI 値に基づいてルールを適用するには、次の設定を使用します。

```
configure
   local-policy-service service_name
      ruledef ruledef_name
         condition priority priority ecgi mcc mcc_num mnc mnc_num eci { eq
| ge | gt | le | lt | match | ne | nomatch } regex | string_value | int_value
 | set }
         end
```

注：

- **priority** *priority*：指定された条件の優先順位を指定します。*priority* は一意で、1 ～ 2048 の整数である必要があります。
- **ecgi mcc** *mcc_num* **mnc** *mnc_num* **eci**：MCC、MNC、および ECI の値を使用して ECGI を設定します。
  - **mcc** *mcc_num* ：MCC は 001 ～ 999 の 3 桁の数字です。これは、サイズ 3 の文字列です。
  - **mnc** *mnc_num* ：MNC は 01 ～ 999 の 2 または 3 桁の数字です。これは、サイズ 2 ～ 3 の文字列です。
  - **eci**：ECI は 0x1 ～ 0xffffffff の 16 進数です。これは、サイズ 1 ～ 7 の文字列です。
- この CLI コマンドは、MME による ECGI-Change イベント通知で受信した特定の ECGI 値に基づいて通信事業者が特定のアクションを実行する場合に、local-policy で設定されます。

ロケーションベースの LP ルール適用設定の確認

次のコマンドを使用して、この機能の設定を確認します。

show configuration context



重要　この機能は、特定の APN 内のすべての要求と応答が PCRF に接続せずにローカルポリシーに直接送信されるローカルポリシーのみのモードでサポートされます。

この機能の設定例を次に示します。

```
configure
   context source
      apn corporate-apn
         ims-auth-service LocalPolicy_1
      exit
   exit
end

configure
   local-policy-service LocalPolicy_1
      ruledef any-imsi
         condition priority 1 imsi match *
      exit
      ruledef ecgi-group
         condition priority 1 ecgi mcc 123 mnc 456 eci eq ffff
      exit
      actiondef ecgi-trigger
         action priority 1 event-triggers ecgi-change
      exit
      actiondef ecgi-redirect-rule
         action priority 1 activate-rule namerule-1
      exit
      eventbase default
         rule priority 1 event new-call ruledef any-imsi actiondef
ecgi-trigger
         rule priority 2 event ecgi-change ruledef ecgi-group actiondef
ecgi-redirect-rule
        rule priority 3 event location-change ruledef ecgi-group actiondef
 ecgi-redirect-rule
      exit
   exit
end
```

ロケーションベースのローカルポリシールール適用機能のモニタリングと障害対応

この項では、ロケーションベースのローカルポリシールール適用機能のサポートに使用できる show コマンドとその出力について説明します。

この機能で問題が発生した場合、トラブルシューティングを行うには次の CLI コマンドを使用します。

```
show configuration context
logging filter active facility local-policy level debug
show local-policy statistics
show active-charging sessions full
```

show local-policy statistics summary

ECGI-CHANGE イベントトリガーのインストールをサポートするために、この show コマンドの出力に次の統計が追加されています。

- イベント統計：
  - ECGI Change：ローカルポリシーが受信した ECGI-CHANGE イベントトリガーの数を表示します。
- 変数一致統計
  - ECGI：ECGI が一致して、このイベントに基づいて特定のアクションが適用された回数を表示します。

GTP ベースの S2a/S2b の Gx サポート

GTP ベースの S2a/S2 インターフェイスの Gx サポートは、P-GW での Wi-Fi 統合のためにすべての顧客に拡張されました。この実装は、29.212 の標準 Rel. 8 Non-3GPP 仕様部分に準拠しており、加えて Rel. 10/Rel. 11 の C3-101419 C3-110338 C3-110225 C3-120852 C3-130321 C3-131222 CR に準拠しています。

この機能拡張の一部として、次の変更が導入されました。

- TWAN ID の AVP サポートが提供されました
- TWAN-ID が r8-gx-standard ディクショナリに追加されました

Gx ベースの仮想 APN の選択

このセクションでは、Gx ベースの仮想 APN 選択機能の概要と実装について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

- 機能説明 （830 ページ）
- Gx ベース仮想 APN 選択機能 （831 ページ）
- Gx ベース仮想 APN 選択のモニタリングと障害対応 （831 ページ）

機能説明

概要

現在の実装では、RADIUS またはローカル設定による仮想 APN（VAPN）の選択がサポートされています。ASR 5500 では、仮想 APN の選択に PCRF と Gx インターフェイスを使用してシグナリングの削減を実現しています。

機能ビットを 4 に設定する、新規のサポート機能「**virtual-apn**」が IMSA 設定に追加されました。この設定により、特定の IMS 承認サービスに対して Gx ベースの仮想 APN 選択機能が有効になります。この設定が P-GW や GGSN で有効になっている場合、P-GW または GGSN は、CCR-I の Supported-Features AVP を介してこの機能を PCRF にアドバタイズします。 VAPN が選択されている場合、PCRF は Experimental-Result-Code AVP が 5999（DIAMETER_GX_APN_CHANGE）に設定された CCR-I メッセージを拒否し、CCA-I の Called-Station-Id AVP メッセージを介して新しい APN を送信します。その後、既存のコールが切断され、新しい仮想 APN で再確立されます。Experimental Result Code 5999 にはシスコのベンダー ID が設定されていることに注意してください。

重要 この機能を有効にすると、（この機能を使用するコールの数に応じて）CPU に影響が出る可能性があります。

ライセンス要件

この機能を使用するには、有効なライセンスをインストールしてこの機能を設定する必要があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

制限事項

この機能には次の制限があります。

- 新しい仮想 APN とのコールを確立するには、仮想 APN がサポートする機能のネゴシエーション、 実験結果コード（5999）、Called-Station-Id AVP を受信する必要があります。いずれかの条件が満たされていない場合、コールは終了します。
- また、CCA-I メッセージで受信した場合、障害処理は 5999 結果コードでは考慮されません。
- 実験結果コード 5999 が CCA-U で受信されると、障害処理アクションが実行されます。
- Called-Station-Id AVP を CCA-U または CCA-T で受信した場合、AVP は無視されます。
- ローカルポリシーによって開始された最初のメッセージで仮想 APN を受信すると、コールは終了します。
- PCRF が同じ仮想 APN を繰り返し送信すると、コールは終了します。

Gx ベース仮想 APN 選択機能

次のセクションでは、Gx ベース仮想 APN 選択を有効にするための設定コマンドについて説明します。

```
configure
    context  context_name
         ims-auth-service  service_name
              policy-control
                   diameter encode-supported-features virtual-apn
                   end
```

注：

- **virtual-apn**：このキーワードで、Gx ベース仮想 APN 選択機能の設定が有効になります。デフォルトでは、この機能は無効になっています。
- このキーワードはライセンスによって異なります。詳細については、シスコのアカウント担当者にお問い合わせください。

Gx ベース仮想 APN 設定の確認

Gx ベース仮想 APN 選択機能が Supported-Features AVP の一部として設定されているかどうかを表示するには、Exec モードで次のコマンドを使用します。

```
show ims-authorization sessions full all
```

この show コマンドの出力にある「Negotiated Supported Features」フィールドに、設定ステータスが表示されます。このサポートされている機能は、機能ライセンスが設定されている場合にのみ表示されます。

Gx ベース仮想 APN 選択のモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show ims-authorization policy-control statistics

新しい仮想 APN が選択された場合に PCRF が Diameter Experimental Result Code（5999）を送信する回数を追跡するために、この show コマンドの出力に次のフィールドが追加されました。

- **Gx APN Change**

この統計の詳細については、『*Statistics and Counters Reference*』を参照してください。

統計のデバッグ

Gx ベースの仮想 APN コールをデバッグするには、次のコマンドを使用します。

```
show session subsystem facility sessmgr debug-info
```

このコマンドは、Gx ベースの VAPN 機能に関連する詳細な統計を表示します。たとえば、受信した Gx VAPN の数、Gx VAPN を有効にした後の AAAMGR/SGX/DHCP メッセージの数、および Gx VAPN コールのセットアップ時間などを表示します。

Gx ベース仮想 APN 選択機能のバルク統計

IMSA スキーマ

次の新しいバルク統計変数が IMSA スキーマに追加され、新しい仮想 APN が選択された場合に PCRF が Diameter Experimental Result Code（5999）を送信する回数が追跡されるようになりました。

- dpca-expres-gx-apn-change

この変数の詳細については、『*Statistics and Counters Reference*』を参照してください。

システムスキーマ

PCRF から受信した仮想 APN の検証失敗が原因で P-GW、GGSN、または SAEGW セッションが切断された回数を追跡するために、次の新しい切断理由がシステムスキーマに追加されました。

- gx-vapn-selection-failed（618）

この変数の詳細については、『*Statistics and Counters Reference*』を参照してください。

異なるピアからの RAR の適切な処理

StarOS Gx アーキテクチャでは、ホストの選択が IMSA サービスで設定されている場合、すべての Diameter セッションがプライマリおよびセカンダリピアに関連付けられます。

PCRF と PCEF が複数の DRA を介して接続されているようなネットワークでは、PCRF がラウンドロビン方式で DRA を選択し、セッションの RAR がプライマリまたはセカンダリのいずれでもないピアから送信されることがあります。このようなシナリオを処理するために、プライマリでもセカンダリでもないピアから受信した RAR に応答する機能が追加されました。この場合、RAR への応答は、RAR の送信元であるピアを介して行われます。ただし、以降のセッションのシグナリングは以前に通信していたピアを介して行われます。セカンダリピアを介して RAR が受信されると、ホストスイッチが発生し、動作は変更されません。3 番目のピアからの RAR を処理できるようにするために、そのピアを Diameter エンドポイント設定で設定する必要があります。さらに言えば、この問題は、ホスト選択が IMSA サービスに設定されている場合にのみ発生します。ホスト選択がエンドポイントレベルで行われる場合、この問題は発生しません。

3 つの DRA があり、次の例に示すように設定されているとします。

```
configure
   context test
      diameter endpoint Gx
         ...
         peer DRA1 realm realmName address 192.168.23.3
         peer DRA2 realm realmName address 192.168.23.3 port 3869
         peer DRA3 realm realmName address 192.168.23.3 port 3870
         exit
      ims-auth-service imsa-Gx
```

```
        policy-control
           diameter host-select row-precedence 1 table 1 host DRA1
secondary host DRA2
end
```

この機能がない場合、DRA3 から RAR を受信すると、拒否されます。この機能を有効にすると、DRA3 からの RAR は DRA3 のみを介して応答されます。この場合、ピアの切り替えは発生せず、以前にピアの切り替えが発生していれば、後続のメッセージは DRA1 または DRA2 を介して送信されます。

制限事項

ここでは、この機能の制限について説明します。

- 異なる送信元ホストから受信された RAR は拒否されます。
- Diameter エンドポイントに設定されていない DRA から受信した RAR は拒否されます。

NetLoc の機能強化

この機能により、既存の NetLoc 機能に、3GPP 標準 R13 バージョンへの準拠が追加されます。

機能説明



重要 これはライセンスで制御される機能です。有効にするには、NetLoc 機能ライセンスキーが必要です。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

この機能により、既存の NetLoc 機能に、3GPP 標準 R13 バージョンへの準拠が追加されます。この NetLoc 機能を使用して、IMS ネットワークは、WLAN アクセスネットワークから UE の位置情報を取得できます。これにより、位置関連の機能と、位置情報に基づく課金が強化されます。

この機能により、次の動作が変更されます。

- NetLoc 機能がシャーシで有効になっており、アクセスネットワーク情報（ANI-45）イベントトリガーがインストールされている場合、次の動作が変更されています。

表 *75 : PCRF* に対する *Gx* インターフェイスの動作の変更

PCRF Gx インターフェイスの相互作用	アクセス側の相互作用	リリース **21.1** より前の **ULI** および **MS TZ** の動作（標準 **Gx-R8/Custom15**（**AT&T**））	**ULI** および **MS TZ** の動作の変更（標準 **Gx-R8/Custom15**（**AT&T**））
課金ルールインストール要求で「0 - ULI」を含む RAI AVP を受信します。	**新しい ULI パラメータのみ**を含むベアラー作成応答を受信します。	**新しい ULI パラメータのみ**を含むベアラー作成応答を受信します。	動作の変更はありません。
課金ルールインストール要求で「0 - ULI」を含む RAI AVP を受信します。	**ULI パラメータを含まない**ベアラー作成応答を受信します。	古い ULI パラメータが、CCR-U メッセージで PCRF に送信されます。	3GPP-SGSN-MCC-MNC AVP に含まれる PLMN-id が PCRF に送信されます。
課金ルール変更要求で「0 - ULI」を含む RAI AVP を受信します。	**新しい ULI パラメータのみ**を含むベアラー更新応答を受信します。	新しい ULI パラメータが、CCR-U メッセージで PCRF に送信されます。	動作の変更はありません。
課金ルール変更要求で「0 - ULI」を含む RAI AVP を受信します。	**ULI パラメータを含まない**ベアラー更新応答を受信します。	古い ULI パラメータが、CCR-U メッセージで PCRF に送信されます。	3GPP-SGSN-MCC-MNC AVP に含まれる PLMN-id が PCRF に送信されます。
課金ルール変更要求で「0 - ULI」を含む RAI AVP を受信します。	**新しい ULI パラメータのみ**を含み、MS TZ パラメータを含まないベアラー削除応答を受信します。	新しい ULI パラメータと古い MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	新しい ULI のみが、CCR-U メッセージで PCRF に送信されます。
課金ルール変更要求で「0 - ULI」を含む RAI AVP を受信します。	**ULI パラメータを含まず**、MS TZ パラメータも含まないベアラー削除応答を受信します。	古い ULI パラメータと古い MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	3GPP-SGSN-MCC-MNC AVP に含まれる PLMN-id が PCRF に送信されます。
課金ルールインストール要求で「1 -MSTZ」を含む RAI AVP を受信します。	**新しい MS TZ パラメータのみ**を含むベアラー作成応答を受信します。	新しい MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	動作の変更はありません。

PCRF Gx インターフェイスの相互作用	アクセス側の相互作用	リリース 21.1 より前の ULI および MS TZ の動作（標準 Gx-R8/Custom15（AT&T））	ULI および MS TZ の動作の変更（標準 Gx-R8/Custom15（AT&T））
課金ルールインストール要求で「1 -MSTZ」を含む RAI AVP を受信します。	**MS TZ パラメータを含まない**ベアラー作成応答を受信します。	古い MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	動作の変更はありません。
課金ルール変更要求で「1-MSTZ」を含む RAI AVP を受信します。	**新しい MS TZ パラメータのみ**を含むベアラー更新応答を受信します。	新しい MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	動作の変更はありません。
課金ルール変更要求で「1-MSTZ」を含む RAI AVP を受信します。	**MS TZ パラメータを含まない**ベアラー更新応答を受信します。	古い MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	動作の変更はありません。
課金ルール変更要求で「1-MSTZ」を含む RAI AVP を受信します。	**新しい MS TZ パラメータのみ**を含むベアラー削除応答を受信します。	古い ULI パラメータと新しい MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	新しい MS TZ のみが、CCR-U メッセージで PCRF に送信されます。
課金ルール変更要求で「1-MSTZ」を含む RAI AVP を受信します。	**MS TZ パラメータを含まない**ベアラー削除応答を受信します。	新しい ULI パラメータと古い MS TZ パラメータが、CCR-U メッセージで PCRF に送信されます。	古い MS TZ のみが PCRF に送信されます。
何も受信しません。	新しい ULI パラメータと新しい MS TZ パラメータを含むセッション削除要求を受信します。	新しい ULI パラメータと新しい MS TZ パラメータが、CCR-T メッセージで PCRF に送信されます。	動作の変更はありません。
何も受信しません。	新しい ULI パラメータを含み、MS TZ パラメータを含まないセッション削除要求を受信します。	新しい ULI パラメータと古い MS TZ パラメータが、CCR-T メッセージで PCRF に送信されます。	動作の変更はありません。

PCRF Gx インターフェイスの相互作用	アクセス側の相互作用	リリース 21.1 より前の ULI および MS TZ の動作（標準 Gx-R8/Custom15（AT&T））	ULI および MS TZ の動作の変更（標準 Gx-R8/Custom15（AT&T））
何も受信しません。	新しい ULI パラメータを含まず、MS TZ パラメータも含まないセッション削除要求を受信します。	古い ULI パラメータと古い MS TZ パラメータが、CCR-T メッセージで PCRF に送信されます。	動作の変更はありません。

重要 ULI と ULI タイムスタンプはペアになっていると見なされます。ULI タイムスタンプが転送される場合は、その ULI とともに転送および受信されます。ULI が受信され、ULI タイムスタンプが受信されない場合、その P-GW は、古いタイムスタンプを転送しません。

- Gx インターフェイスでは NETLOC-ACCESS-NOT-SUPPORTED に AVP を含めることができます。AVP をこのように含めることは、次の条件に基づきます。
  - RAT タイプが、E-UTRAN、UTRAN、WCDMA、GPRS、GERAN、W-LAN 以外である。
  - IP CAN タイプが、3GPP EPS、GPRS、非 3GPP EPS 以外である。
  - Required-Access-Info AVP を含む再承認要求が受信される。
  - シャーシで NetLoc 機能が有効になっている。
  - イベントトリガー ACCESS_NETWORK_INFO_REPORT (45) がインストールされている。

リリース 21.1 より前の動作（標準 Gx-R8/Custom15（AT&T））	新しい動作（標準 Gx-R8/Custom15（AT&T））
以前は、IP-CAN タイプまたは RAT タイプが NETLOC をサポートしていない場合、P-GW（PCEF）は、PCRF から受信した RAI を無視していました。	R8-Gx 標準および Custom15 Gx ディクショナリの再承認応答メッセージに新しい AVP である NetLoc-Access-Support が追加されました。

- 表 *76 : LastUserLocationInformation AVP* および *LastMSTimeZone AVP* に関する動作の変更

P-GW CDR の動作	21.1 リリース以降の、Custom 35/Custom 24/Custom 48 ディクショナリでの動作	Custom52 ディクショナリ（標準準拠の新しいディクショナリ）/Custom 35 ディクショナリ（顧客固有）

ベアラー削除コマンド/ベアラー削除要求/セッション削除要求で ULI を受信します。	ULI は P-GW CDR 生成の一部ではありませんでした。	ULI は、P-GW CDR 生成で **LastUserLocationInformation** AVP として記録されます（AVP は CLI コマンドを使用して制御されません）。
ベアラー削除コマンド/ベアラー削除要求/セッション削除要求で MS TZ を受信します。	MS TZ は P-GW CDR 生成の一部ではありませんでした。	MS TZ は、P-GW CDR 生成で **LastMSTimeZone** AVP として記録されます。 CDR は、通常リリースとしてリリースされます。この場合、MS TZ は完全なトリガーとして検出されず、MS TZ の変更を原因として追加の CDR がリリースされません。 AVP は CLI コマンドを使用して制御されません。

S-GW CDR の動作	**21.1 リリース以降の、Custom 35/Custom 24 ディクショナリでの動作**	**Custom24 ディクショナリ（標準ディクショナリ）/Custom 35 ディクショナリ（AT&T）**
ベアラー削除コマンド/ベアラー削除要求/セッション削除要求で ULI を受信します。	ULI は CDR 生成の一部ではありませんでした。	ULI は、S-GW CDR 生成で **LastUserLocationInformation** AVP として記録されます属性は CLI コマンドを使用して制御されます。
ベアラー削除コマンド/ベアラー削除要求/セッション削除要求で MS TZ を受信します。	MS TZ は CDR 生成の一部ではありませんでした。	MS TZ は、S-GW CDR 生成で **LastMSTimeZone** AVP として記録されます。属性は CLI コマンドを使用して制御されます。 CDR は、通常リリースとしてリリースされます。この場合、MS TZ は完全なトリガーとして検出されず、MS TZ の変更を原因として追加の CDR がリリースされません。

制限事項

1. この機能拡張は、S-GW、P-GW、および SAEGW にのみ適用されます。GGSN と SGSN では、NetLoc 機能の動作に変更はありません。

2. **Last-MS-Timezone** 属性と **Last ULI** 属性は、S-GW CDR 生成専用に custom24 および custom35 ディクショナリに追加されています。
3. CLI コマンド **gtpp attribute** に追加されたキーワード **last-ms-timezone** と **last-uli** は S-GW CDR の生成にのみ適用されます。
4. ディクショナリ custom35（お客様固有のディクショナリ）および custom52（3GPP R13 標準規格を遵守）に追加された **Last-MS-Timezone** 属性と **Last ULI** 属性は、P-GW CDR の生成にのみ適用されます。これらの属性は CLI で制御されません。

コマンドの変更

gtpp-attribute

このCLIコマンドは、オプション属性の指定を、GPRS/PDN/UMTSアクセスゲートウェイが生成するコール詳細レコード（CDR）に表示できるようにします。また、属性フィールド値をエンコードすることによって、情報がCDRにどのように表示されるかを定義します。CDR生成中に属性を制御するために、キーワード **last-ms-timezone** と **last-uri** がこのCLIコマンドに追加されました。

重要 キーワードの追加は、S-GW CDR にのみ適用されます。P-GW CDR には適用されません。

```
configure
  context <context_name>
     gtpp group group_name
       gtpp attribute { last-ms-timezone | last-uli | .. }
       [no | default ] gtpp attribute { last-ms-timezone | last-uli
| .. }
  end
```

注：

- **no:** CDR から設定された GTPP 属性を削除します。
- **default:** 生成されたCDRのデフォルトのGTPP属性を設定します。また、生成されたCDRの属性値のデフォルトの表示も設定します。
- **last-ms-timezone:** CDR フィールドに「Last MS-Timezone」を設定します。デフォルトのオプションが使用されている場合、このオプションは無効になります。
- **last-uli:** CDR フィールドに「Last ULI」を設定します。デフォルトのオプションが使用されている場合、このオプションは無効になります。

パフォーマンス指標の変更

show configuration

このコマンドは、以下の出力を表示するように変更されました。

- Last-MS-Timezone の有無

- 最後のユーザーロケーション情報の有無

show gtpp group name *group_name*

このコマンドは、以下の出力を表示するように変更されました。

```
    Last-MS-Timezone present: yes
    Last-User Location Information present:
yes
```

RAN-NAS 原因コードの機能強化

この章では、RAN-NAS 原因コードの機能強化について説明します。

機能説明

重要 これはライセンスで制御される機能です。NPLI の既存のライセンスを有効にする必要があります。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

この機能により、Gx インターフェイス、P-GW、および S-GW CDR での「ベアラー作成失敗応答」、「ベアラー更新失敗応答」、および「ベアラー削除応答」に対する 3GPP RAN/NAS 原因コード IE のサポートが導入されています。これにより、通信事業者はアクセスネットワークから詳細な RAN/NAS リリース原因コード情報を取得できます。RAN/NAS 原因は、次のいずれかのメッセージでアクセス側から取得できます。

- ベアラー作成失敗応答
- ベアラー更新失敗応答
- セッション削除要求
- ベアラー削除応答
- ベアラー削除コマンド

顧客固有のディクショナリ Gx- dpca-custom15 および Gz-Custom35 の標準 IE に加え、S4、S11、S5、および S8 インターフェイス上の 3GPP リリース 12 RAN/NAS 原因 IE のこのサポートが、「セッション削除要求」および「ベアラー削除」コマンドのために存在し、プライベート拡張を介して提供されています。

ただし、「ERAB creation Failure」、「ERAB modification Failure」、および「ERAB release indication」メッセージで受信した RAN/NAS 原因は、S-GW と P-GW で処理されませんでした。したがって、P-GW によって PCRF に転送されず、P-GW および S-GW の CDR にも入力されませんでした。この機能強化により、S-GW（S4、S11 インターフェイス）および P-GW（S5、S8 インターフェイス）で、「ベアラー作成応答」、「ベアラー更新応答」、および「ベアラー削除応答」の RAN/NAS 原因コードを処理するためのサポートが追加されました。また、

RAN/NAS 原因コードは、P-GW によって PCRF に転送され、P-GW と S-GW の CDR に入力されます。

「ベアラー作成応答」、「ベアラー更新応答」、および「ベアラー削除応答」について、プライベート拡張に 3GPP リリース 12 RAN/NAS 原因 IE のサポートを追加する必要はありません。「セッション削除要求」と「ベアラー削除コマンド」内の 3GPP リリース 12 原因コード IE のプライベート拡張サポートは、引き続きサポートされます。

この機能強化により、dpca-custom15 ディクショナリの Gx インターフェイスと custom35 ディクショナリの Gz インターフェイスで、次の RAN/NAS 原因 IE の動作の変更が導入されます。

表 *77 : RAN/NAS* 原因の *Gx* インターフェイス要件

Message	GTP 原因	RAN-NAS 原因情報を伝送する Gx メッセージ
ベアラー作成応答	Accepted	29.274 の表 7.2.4-2 に従い、RAN/NAS の原因は予期されません。そのため、受信しても無視され、PCRF に転送されません。
	Temporarily rejected due to HO in progress.	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。そのため、受信しても無視され、PCRF に転送されません。
	Other GTP Causes	CCR-U
ベアラー更新応答	Accepted	29.274 の表 7.2.16-2 に従い、RAN/NAS 原因は予期されていません。そのため、受信しても無視され、PCRF に転送されません。
	No Resources	CCR-U
	Available	**重要** UE によって開始された（MBC）ベアラーの変更が GTP 原因「NO RESOURCES AVAILABLE」で失敗した場合、P-GW は PDN セッション全体を削除します。この場合、RAN-NAS 原因情報は CCR-T メッセージの一部として転送されます。
	Context Not Found	ベアラー更新応答をメッセージレベルの原因「CONTEXT NOT FOUND」とともに受信した場合、これは PDN の削除につながり、RAN-NAS 原因情報は CCR-T メッセージの一部として転送されます。
	Temporarily rejected due to HO in progress.	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。そのため、この原因は受信しても無視され、PCRF に転送されません。
	Other GTP Causes	CCR-U

Message	GTP 原因	RAN-NAS 原因情報を伝送する Gx メッセージ
ベアラー削除応答	Temporarily rejected due to HO in progress	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。そのため、この原因は受信しても無視され、PCRF に転送されません。 **重要** S-GW の既存の設計に従い、「ベアラー削除応答」を GTP 原因「Temporarily rejected due to handover/ TAU/ RAU procedure in progress」で受信した場合、GTP 原因が「Request Accepted」に変更され、P-GW に転送されます。この場合、RAN/NAS の原因を「ベアラー削除応答」で受信すると、S-GW はそれを P-GW に転送します。P-GW では、「ベアラー削除応答」を GTP 原因「Request Accepted」で受信しているため、RAN/NAS 原因が PCRF に転送され、P-GW の CDR に入力されます。この動作は、SAEGW および S-GW + P-GW の組み合わせのコールで見られます。
	Accepted / Other GTP CCR-UCauses	**重要** ネットワークで RAR/CCA-U を介して開始されたベアラー削除応答で RAN/NAS 原因を受信した場合、P-GW は、RAN/NAS 原因をレポートするために CCR-U を PCRF に送信しません。 このサポートは、29.212 リリース 13.5 の「RAN/NAS 機能の強化」により導入されました。

表 *78 : RAN/NAS* 原因の *Gz* インターフェイス要件

Message	S-GW CDR	P-GW CDR
セッション削除要求	対応	対応
ベアラー削除コマンド	対応	対応 注：RAN/NAS 原因をベアラー削除応答で受信した場合、これによりベアラー削除コマンドで受信した RAN/NAS 原因が上書きされます。
ベアラー作成失敗応答	非対応	非対応
ベアラー更新失敗応答	非対応	非対応
ベアラー削除応答	非対応	はい

制限事項

この機能には次の制限があります。

- S2a および S2b インターフェイスを介した RAN/NAS 原因のサポートは未サポートです。
- RAN/NAS 原因情報のサポートは、標準 Gx および Gz ディクショナリに追加されていません。
- P-GW は、GTP インターフェイスから受信した最初の 2 つの RAN/NAS 原因 IE（最大 1 つの RAN と最大 1 つの NAS）情報を処理します。たとえば、アクセスネットワークが不正な動作をし、2 つの NAS と 1 つの RAN の RAN/NAS 原因リストを送信した場合、最初の 2 つの原因のみが考慮され、検証されます。この場合、2 つの NAS 原因があり、許可される NAS は 1 つだけであるため、最初の NAS 原因だけが Gx インターフェイスと CDR で入力されます。
- 仕様 32.251 の表 5.2.3.4.1.1 および 表 5.2.3.4.2.1 に従い、失敗したベアラー作成応答と失敗したベアラー更新応答に対して S-GW CDR および P-GW CDR を生成するトリガーはありません。したがって、「ベアラー作成失敗」応答および「ベアラー更新失敗」応答で受信した RAN/NAS 原因は、Gz インターフェイスに送信されません。
- 「ベアラー削除」シナリオでは、「ベアラー削除」要求を受信した直後に S-GW CDR が生成されます。したがって、「ベアラー削除」応答で受信した RAN/NAS 原因は S-GW CDR に入力されません。
- ネットワークで RAR/CCA-U を介して開始された「ベアラー削除」応答で RAN/NAS 原因を受信した場合、P-GW は、RAN/NAS 原因をレポートするために CCR-U を PCRF に送信しません。このサポートは、仕様 29.212 リリース 13.5 の「RAN/NAS 機能の強化」により導入されました。
- RAN-NAS-Cause 機能がサポートされている場合、RAN/NAS 原因のみが PCRF に転送されます。ANI 情報は、NetLoc 機能が有効になっている場合にのみ転送されます。以下の表は、さまざまなシナリオを示しています。

シナリオ	RAN/NAS 原因の動作	ANI の動作
IP-CAN ベアラーターの終了	RAN-NAS-Cause 機能がサポートされている場合（Netloc-ran-nas-cause CLI が設定されており、Supported-Features = RAN-NAS-CAUSE が Gx CCR-I/CCA-I でアサートされた場合）、PCEF はベアラー終了により受信した RAN 原因および/または NAS 原因を、Charging-Rule-Report AVP に含まれている RAN-NAS-Release-Cause AVP に含めます。	1 つ以上の失敗した課金ルールインストール要求が CCA-U/RAR で受信されたときに Required-Access-Info がアサートされた場合（Netloc CLI が設定され、Supported-Features = Netloc が Gx CCR-I/CCA-I でアサートされた場合）、ベアラーの終了中に受信した ANI 情報が CCR-U に入力されます。

シナリオ	RAN/NAS 原因の動作	ANI の動作
IP-CAN セッションの終了	RAN-NAS-Cause 機能がサポートされている場合（Netloc-ran-nas-cause CLI が設定されており、Supported-Features = RAN-NAS-CAUSE が Gx CCR-I/CCA-I でアサートされた場合）、PCEF はセッション終了により受信した RAN 原因および/または NAS 原因を、RAN-NAS-Release-Cause AVP にコマンドレベルで含めます。	1 つ以上の失敗した課金ルールインストール要求が CCA-U/RAR で受信されたときに Required-Access-Info がアサートされた場合（Netloc CLI が設定され、Supported-Features = Netloc が Gx CCR-I/CCA-I でアサートされた場合）、セッションの終了中に受信した ANI 情報が CCR-T に入力されます。
PCC ルールエラーの処理	RAN-NAS-Cause 機能がサポートされている場合（Netloc-ran-nas-cause CLI が設定されており、Supported-Features = RAN-NAS-CAUSE が Gx CCR-I/CCA-I でアサートされた場合）、PCEF はルールのインストール/アクティブ化/変更の失敗により受信した RAN 原因および/または NAS 原因を、Charging-Rule-Report AVP に含まれている RAN-NAS-Release-Cause AVP に含めます。	1 つ以上の失敗した課金ルールインストール要求が CCA-U/RAR で受信されたときに Required-Access-Info がアサートされた場合（Netloc CLI が設定され、Supported-Features = Netloc が Gx CCR-I/CCA-I でアサートされた場合）、ルールのインストール/アクティブ化/変更の失敗により受信した ANI 情報が CCR-U に入力されます。

コマンドの変更

diameter encode-supported-features netloc netloc-ran-nas-cause

この機能拡張では、この CLI コマンドの動作が変更されています。

以前の動作：RAN/NAS 原因機能を有効にするには、NetLoc 機能を有効にする必要がありました。この場合、CLI コマンド **diameter encode-supported-features netloc netloc-ran-nas-cause** で **netloc** キーワードを設定することが必須でした。

新しい動作：NetLoc 機能を設定しなくても、RAN/NAS 機能を有効にできるようになりました。これは、CLI コマンド **diameter encode-supported-features netloc netloc-ran-nas-cause** で **netloc** キーワードを設定する必要がないことを意味します。

```
configure > context context_name > ims-auth-service service_name > policy-control
 diameter encode-supported-features netloc netloc-ran-nas-cause
```

Diamproxy セッション ID 不一致の場合のセッションの切断

このセクションでは、Diamproxy グループ化情報とセッション ID の不一致の影響を受けるサブスクライバセッションをクリアする方法について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

- 機能説明 （844 ページ）
- Diamproxy セッション ID が一致しないセッションを削除するようシステムを設定する （844 ページ）
- 不一致セッション削除機能のモニタリングと障害対応 （845 ページ）

機能説明

高速バックツーバック ICSR スイッチオーバーまたは広範囲にわたる複数のプロセス障害の間、Diameter プロキシセッションマネージャのマッピング情報は ICSR ペア間で保持されません。この Diameter プロキシセッション ID の不一致の結果、原因コード 5002（DIAMETER_UNKNOWN_SESSION_ID）で RAR が拒否されます。この動作は、VoLTE コールのセットアップ手順に影響します。そのため、Diameter プロキシセッションマネージャ マッピングの不一致が原因で影響を受けるサブスクライバセッションをクリアするためにこの機能が導入されました。動作を制御するために新しい CLI 設定が用意され、Diamproxy セッション ID の不一致を報告する新しいバルク統計カウンタがサポートされています。

バルク統計カウンタは、結果コードが 5002 の RAR メッセージが受信され、セッション ID Diampproxy マッピングの不一致が検出されて、セッションがクリアされた場合にのみ増分されます。CCR-T が PCRF に送信されるのを抑制し、原因コードとしての「Reactivation Requested」を使用してベアラー削除要求が S-GW に送信されます。そのため、サブスクライバは後続の VoLTE コールに影響を与えることなくすぐに再アタッチします。手動での介入は必要にならず、エラー 1 つのみが発生することになります。

重要 この機能拡張は IMS PDN にのみ適用されるため、この状況が発生した場合、手動での介入の必要がないエラーは 1 つに限定されます。これは Gx RAR にのみ適用されます。

Diamproxy セッション ID が一致しないセッションを削除するようシステムを設定する

続くセクションでは、Diamproxy グループ化情報とセッション ID の不一致が原因で影響を受けるサブスクライバセッションをシステムでクリアできるようにするための設定コマンドについて説明します。

一致しないサブスクライバセッションのクリア

セッション ID と Diamproxy の不一致が識別されたときに、シグナリングトリガーに基づいてサブスクライバセッションを切断するようにシステムを設定するには、次の設定コマンドを使用します。

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
             diameter clear-session sessid-mismatch
end
```

- **sessid-mismatch**：セッション ID が一致しないセッションをクリアします。この CLI 設定はオプションです。
- デフォルトの設定は、**no diameter clear-session** です。デフォルトでは、セッションはクリアされません。

一致しないセッションを削除する設定の確認

次のコマンドを使用して、この機能の設定ステータスを確認します。

show ims-authorization service name *service_name*

service_name は、IMS 認証用に設定された IMS 承認サービスの名前にする必要があります。

このコマンドを実行すると、指定された IMS 承認サービス内で有効になっているすべての設定が表示されます。「セッション ID が一致しないセッションのクリア」フィールドを使用して、この機能を有効にするか無効にするかを決定できます。

```
[local]st40# show ims-authorization service name service1
  Context: test
  IMS Authorization Service name: service1
  Service State: Enabled
  Service Mode: Single Interface Policy and Charging
...
  Diameter Policy Control:
   Endpoint: gx
   Origin-Realm: xyz.com
   Dictionary: standard
   Supported Features:
      3gpp-r9
...
   Host Selection: Table: 1 Algorithm: Round-Robin
   Host Reselection Subscriber Limit: Not Enabled
   Host Reselection Interval: Not Enabled
   Sgsn Change Reporting: Not Enabled
     Session-Id Mismatch Clear Session: Enabled
   3GPP R9 Flow Direction Compliance: Not Enabled
  Host Selection Table[1]: 1 Row(s)
   Precedence: 1
...
```

不一致セッション削除機能のモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

この機能に関連した障害については、次の操作を実行する必要があります。

- **show ims-authorization service name** <*service_name*> CLI コマンドを使用して、この機能が有効であるかどうかを確認します。有効になっていない場合は、**diameter clear-session sessid-mismatch** CLI コマンドを設定して、この機能が動作するかどうかを確認します。

- **show ims-authorization policy-control statistics debug-info** および **show diameter statistics proxy debug-info** CLI コマンドの出力を収集し、デバッグ統計を分析します。
- 影響を受けるセッションの削除中に報告されたシステムログを確認します。詳細な分析が必要な場合は、シスコのアカウント担当者にご連絡ください。

show ims-authorization service name

指定した IMS 承認サービス内でこの機能が有効になっているか無効になっているかを示すために、この show コマンドの出力に新しいフィールド「Session-Id Mismatch Clear Session」が追加されました。

IMSA スキーマ

次のバルク統計変数がこのスキーマに追加され、Diamproxy-Session ID の不一致が報告されるようになりました。

- dpca-rar-dp-mismatch：このカウンタは、セッション ID Diamproxy マッピングの不一致が原因で RAR の受信中にクリアされたセッションの合計数を表示します。

ミッションクリティカル QCI のネゴシエーションのサポート

このセクションでは、ミッションクリティカル QCI ネゴシエーション機能の概要と導入について説明します。

この項では、次のトピックについて取り上げます。

- 機能説明 （846 ページ）
- ミッションクリティカル QCI のネゴシエーションにおける DPCA の設定 （847 ページ）
- ミッションクリティカル QCI のモニタリングと障害対応 （848 ページ）

機能説明

ミッションクリティカル（MC）プッシュツートーク（PTT）サービスをサポートするために、一連の標準化された新しい QoS クラス識別子（QCI）（65、66、69、70）が導入されました。これらは、3GPP TS 23.203 v13.6.0 および 3GPP TS 23.401 v13.5.0 仕様で定義されている 65 ～ 66（GBR）および 69 ～ 70（非 GBR）のネットワーク開始型 QCI です。これらの QCI は、プレミアム モバイル ブロードバンド（PMB）/公安ソリューションに使用されます。

重要 MC-PTT QCI 機能を使用するには、ワイヤレス プライオリティ サービス（WPS）ライセンスを設定する必要があります。詳細については、シスコのアカウント担当者にお問い合わせください。

以前の動作：ゲートウェイは、標準 QCI（1 ～ 9）と通信事業者定義 QCI（128 ～ 254）のみを受け入れていました。PCRF が 10 ～ 127 の値を持つ QCI を送信する場合、ゲートウェイは要求を拒否します。MC QCI サポートは PCRF とネゴシエートされませんでした。

新しい動作：PCRF は、デフォルトベアラーの作成について新しい標準化された QCI の値である 69 と 70 を受け入れ、専用ベアラーの作成について 65、66、69、および 70 を受け入れます。

この機能を動作させるために、新しい設定可能な属性である **mission-critical-qcis**が、**diameter encode-supported-features** CLI コマンドに導入されました。この CLI オプションを有効にすると、ゲートウェイは、MC-QCI をサポートされる機能として設定することを許可し、その後、Supported-Features AVP を介して MC-PTT QCI 機能を PCRF とネゴシエートします。

WPS ライセンスが有効になっておらず、Diameter が MC-PTT QCI 機能（サポートされている機能のビットの一部）をネゴシエートするように設定されていない場合、ゲートウェイは、MC-PTT QCI を使用したセッション作成要求を拒否します。

この機能および関連する設定の詳細については、『*Release Change Reference*』ガイドの「*P-GW Enhancements for 21.0*」を参照してください。

ミッションクリティカル QCI のネゴシエーションにおける DPCA の設定

以下では、MC-PTT QCI 機能のサポートを有効にするための設定コマンドについて説明します。

ミッションクリティカル QCI 機能の有効化

MC-PTT QCI 機能を有効にするには、次の設定コマンドを使用します。

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features mission-critical-qcis
            end
```

注：

- **mission-critical-qcis**：このキーワードにより MC-PTT QCI 機能が有効になります。デフォルトでは、この機能は有効になりません。
- このキーワードは、WPS ライセンスが設定されている場合にのみ有効にできます。詳細については、シスコのアカウント担当者にお問い合わせください。
- この機能のネゴシエーションを無効にするには、既存の **no diameter encode-supported-features** コマンドを設定する必要があります。このコマンドを実行すると、サポートされている設定済み機能のいずれも PCRF とネゴシエーションされません。

ミッションクリティカル QCI 機能の設定の確認

show ims-authorization sessions full all コマンドにより、この機能の設定ステータスを示す表示が生成されます。

次の表示例は、ネゴシエートされたサポート対象機能の中で *mission-critical-qcis* なものを示す出力の一部のみを示しています。

```
show ims-authorization sessions full all

 CallId: 00004e29            Service Name:  ims-ggsn-auth
   IMSI: 123456789012341
   ....

 Negotiated Supported Features:
   3gpp-r8
   mission-critical-qcis
 Bound PCRF Server: 209.165.200.233
 Primary PCRF Server: 209.165.200.233
 Secondary PCRF Server: NA
 ....
```

ミッションクリティカル QCI のモニタリングと障害対応

以下では、ミッションクリティカルQCI機能をモニターするために使用できるコマンドについて説明します。

ミッションクリティカル QCI の show コマンドと出力

show ims-authorization sessions full all

上記のshowコマンドを実行すると、次のような統計が表示され、ミッションクリティカルQCI機能が有効かどうかが示されます。

```
show ims-authorization sessions full all

 CallId: 00004e29            Service Name:  ims-ggsn-auth
   IMSI: 123456789012341
   ....

 Negotiated Supported Features:
   3gpp-r8
   mission-critical-qcis
   ....
```

WLAN 向けの HSS および PCRF ベース P-CSCF 復元のサポート

ここでは、WLAN および EPC ネットワーク向けの HSS ベースおよび PCRF ベース P-CSCF 復元機能の概要と実装について説明します。

この項では、次のトピックについて取り上げます。

- 機能説明 （849 ページ）
- HSS/PCRF ベースの P-CSCF 復元の設定 （850 ページ）
- HSS および PCRF ベースの P-CSCF 復元のモニタリングと障害対応 （852 ページ）

機能説明

P-CSCF の復元手順が標準化され、P-CSCF 障害後のコール終了により UE と通信できなくなる時間が最小限に抑えられました。3GPP 標準規格リリース 13 に準拠して、この機能は、次の P-CSCF 復元メカニズムを含むように開発されています。

- 信頼できるまたは信頼できない WLAN アクセス（S2a/S2b）のための HSS ベース P-CSCF 復元
- LTE（S5/S8）および信頼できるまたは信頼できない WLAN アクセス（S2a/S2b）のための PCRF ベース P-CSCF 復元



重要 HSS ベースの P-CSCF 復元は、StarOS リリース 21.0 より前の LTE（S5 または S8）向けの P-GW でサポートされていました。

この機能は、基本と拡張の両方の P-CSCF 復元手順をサポートします。



重要 P-CSCF 復元は、ライセンスで制御される機能です。この機能を設定する前に、有効な機能ライセンスをインストールする必要があります。詳細については、シスコのアカウント担当者にお問い合わせください。

- **WLAN での HSS ベースの P-CSCF 復元**：

  P-CSCF 復元メカニズムがサポートされている場合、ゲートウェイは、S6b インターフェイスを介して送信される承認認証要求（AAR）メッセージ内の Feature-List AVP を介して AAA サーバーに復元サポートを示します。Feature-List AVP は、Supported-Features grouped AVP の一部です。Feature-List AVP のビット 0 は、WLAN での P-CSCF 復元サポートを示すために使用されます。

  P-CSCF 復元中に、3GPP AAA サーバーは、PGW が WLAN で HSS ベースの P-CSCF 復元をサポートしていることを確認した後、Re-authorization Request（RAR）コマンドで S6b を介して P-GW に P-CSCF 復元指示を送信します。 新しい Diameter AVP 「**RAR-Flags**」は、ビット 1 が設定された RAR メッセージ内にエンコードされ、AAA サーバーが WLAN で HSS ベースの P-CSCF 復元手順の実行を要求していることをゲートウェイに示します。

  AAA グループ設定の既存の CLI コマンド **diameter authentication** が拡張され、AAR メッセージ内の Supported-Features AVP の一部として P-CSCF 復元機能をエンコードするようになりました。



重要 Supported-Features は、RAT タイプ WLAN のすべての AAR メッセージで送信されます。すべての AAR で機能のネゴシエーションが必要です。再認証 AAR は、機能の再ネゴシエーションも行います。

- **PCRF ベースの P-CSCF 復元**：

  P-CSCF 復元メカニズムをサポートする PCEF は、Supported-Features AVP を介して CCR-I メッセージで復元サポートを示します。Supported-Feature-List AVP の 24 番目のビットは、このメカニズムがサポートされているかどうかを示します。

  ポリシー制御設定の既存の CLI コマンド **diameter encode-supported-features** が拡張され、PCRF による P-CSCF 復元機能サポートのネゴシエーションを許可するようになりました。P-CSCF 復元が要求されたことを PCEF に示すために、新しい Diameter AVP 「**PCSCF-Restoration-Indication**」が導入されました。これを行うには、AVP 値を 0 に設定します。

  Supported-Features AVP は、すべてのアクセスタイプ（eHRPD、P-GW、GGSN）の CCR-I でネゴシエートされます。ただし、復元トリガーを受信した場合、このトリガーは eHRPD および GGSN では無視されます。

制限事項

- 3GPP 標準仕様に従って、S6b 再承認要求が WLAN の P-CSCF 復元に使用される場合、拡張 P-CSCF 復元のために、ゲートウェイは、必須の AVP のみを含む承認要求を送信できます。ただし、現在の実装では、拡張 P-CSCF 復元に使用される再承認は、通常の再承認の一般的な承認要求です。これには、再承認 AAR のすべての AVP が含まれます。

この機能および関連する設定の詳細については、『*Release Change Reference*』ガイドの「*P-GW Enhancements for 21.0*」および「*SAEGW Enhancements for 21.0*」の項を参照してください。

HSS/PCRF ベースの P-CSCF 復元の設定

次の項では、HSS ベースおよび PCRF ベースの P-CSCF 復元機能のサポートを有効にするための設定コマンドについて説明します。

S6b AAA インターフェイスでの P-CSCF 復元通知の有効化

S6b インターフェイスを介して AAA サーバーに送信される AAR メッセージ内の Supported-Features AVP をエンコードするには、次の設定コマンドを使用します。

```
configure
   context context_name
      aaa group group_name
         diameter authentication encode-supported-features
pcscf-restoration-indication
         end
```

注：

- **encode-supported-features**：Supported-Features AVP をエンコードします。
- **pcscf-restoration-indication**：P-CSCF 復元の通知機能を有効にします。
- **default encode-supported-features**：AAR メッセージで Supported-Features AVP を送信しないデフォルト設定を指定します。

- **no encode-supported-features**：Supported-Features AVP を送信しないように、CLI コマンドを無効にします。
- **pcscf-restoration-indication** キーワードはライセンスによって異なります。詳細については、シスコのアカウント担当者にお問い合わせください。

Gx インターフェイスでの P-CSCF 復元通知の有効化

Gx インターフェイスで P-CSCF 復元通知機能を有効にするには、次の設定を使用します。

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features pcscf-restoration-ind
            end
```

注：

- **pcscf-restoration-ind**：P-CSCF 復元の通知機能を有効にします。このキーワードはライセンスによって異なります。詳細については、シスコのアカウント担当者にお問い合わせください。デフォルトでは、この機能は無効になっています。
- **default encode-supported-features**：デフォルト設定では、サポートされている機能が削除/リセットされます。
- **no encode-supported-features**：以前に設定されたサポート対象機能を削除します。

HSS/PCRF ベースの P-CSCF 復元の確認

show ims-authorization sessions full all

このコマンドにより、この機能のネゴシエーションステータスを示す表示が生成されます。

次の表示例は、ネゴシエートされたサポート対象機能の中で **pcscf-restoration-ind** を示す出力の一部のみを示しています。

```
show ims-authorization sessions full all

CallId: 00004e22            Service Name:  imsa-Gx
  IMSI: 123456789012341
  ....
Negotiated Supported Features:
  3gpp-r8
  pcscf-restoration-ind
....
```

show aaa group all

この機能が AAA グループで設定されている場合、この show コマンドは、サポート対象機能の一部として **pccf-restoration-ind** を表示します。

```
show aaa group all
 Group name:    default
 Context:   local
```

```
 Diameter config:
  Authentication:
....
Supported-Features:   pcscf-restoration-ind
....
```

HSS および PCRF ベースの P-CSCF 復元のモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

次の操作を実行して、この機能に関連する障害をトラブルシュートできます。

- **show ims-authorization sessions full all** および **show aaa group all** CLI コマンドを使用して、機能が有効になっているかどうかを確認します。有効になっていない場合は、ポリシー制御と AAA グループ設定の両方で必要な CLI コマンドを設定し、動作するかどうかを確認します。
- **monitor protocol** コマンドを実行し、P-CSCF 復元機能のサポートが CCR-I および AAR メッセージでネゴシエートされているかどうかを確認します。ネゴシエートされていない場合は、この機能のそれぞれの CLI コマンドを有効にします。
- それでも問題が解決しない場合は、次の情報を入手して、シスコのアカウント担当者に詳細な分析を依頼してください。
  - オプション 74（EGTPC）および 75（App Specific Diameter -Gx/S6b）をオンにした状態でのプロトコルのモニターのログ
  - sessmgr、imsa、および diameter-auth が有効な状態でのログ
  - **show session disconnect reason** CLI コマンドの出力とサービスレベルの関連統計

show コマンドと出力

show ims-authorization sessions full all

この show コマンド出力の **Negotiated Supported Features** フィールドには、P-CSCF 復元機能が PCRF とネゴシエートされているかどうかが表示されます。

このサポートされている機能は、機能ライセンスが設定されている場合にのみ表示されます。

show aaa group all

この show コマンド出力の **Supported Features** フィールドには、P-CSCF 復元機能が Supported-Features AVP の一部として設定されているかどうかが表示されます。

このサポートされている機能は、機能ライセンスが設定されている場合にのみ表示されます。

show license information コマンドを実行します。

P-CSCF 復元機能を有効にするライセンスが設定されている場合、**show license information** コマンドにより、関連するライセンス情報が表示されます。

ログのモニタリング

ここでは、HSS および PCRF ベースの P-CSCF 復元機能に関連して生成されるログのモニター方法について説明します。

S6b Diameter プロトコルログ

Supported-Features フィールドは、AAR および AAA セクションで使用できます。生成されるログの出力は次のように表示されます。

```
<<<<OUTBOUND  15:37:23:561 Eventid:92870(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
   [V] Feature-List: 1
....
INBOUND>>>>>  15:37:23:562 Eventid:92871(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
   [V] Feature-List: 1
....
```

RAR-Flags フィールドは、RAR セクションで使用できます。生成されるログの出力は次のように表示されます。

```
INBOUND>>>>>  15:37:43:562 Eventid:92871(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
[V] RAR-Flags: 2
....
```

Gx Diameter プロトコルログ

Supported-Features で、CCR-I/CCA-I セクションの P-CSCF 復元の **Feature-List** が使用できます。生成される出力は次のように表示されます。

```
<<<<OUTBOUND  13:52:06:117 Eventid:92820(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
    [V] Feature-List: 16777217
....
INBOUND>>>>>  13:52:06:118 Eventid:92821(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
    [V] Feature-List: 16777216
....
```

PCSCF-Restoration-Indication AVP は RAR で使用できます。生成される出力は次のように表示されます。

```
INBOUND>>>>>  13:52:26:119 Eventid:92821(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
```

```
[V] PCSCF-Restoration-Indication: 0
....
```

ダイナミックルールのループ防止

機能情報

要約データ

[ステータス（Status）]	新しい機能
導入されたリリース	21.2
変更されたリリース	該当なし
対象製品	P-GW
該当プラットフォーム	ASR 5500
デフォルト設定	無効
関連する CDETS ID	CSCvc97345、CSCvd02249
このリリースでの関連する変更点	N/A
関連資料	P-GW Administration Guide Command Line Interface Reference

マニュアルの変更履歴

重要 リリース 21.2 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

機能説明

PCC（動的または事前定義）ルールのインストールに失敗すると、PCEF は、失敗したルールを報告するために、PCRF に対する CCR-U を開始します。PCRF が同じルール定義で応答すると、ルール障害 CCR-U が再度開始されます。この動作により、ルール障害のループが発生します。

この機能により、ゲートウェイは、ルールインストールの失敗を PCRF に 1 回だけ、正常にインストールされるまで報告することにより、ループを防止できます。

機能の仕組み

この機能は、CLI コマンドを使用して設定できます。サブスクライバの障害が報告されると、CLI コマンドを使用して、同じルールの障害は、正常にインストールされるまでそのサブスクライバに対して抑制されます。ルール名は、障害が報告されたサブスクライバ用に保持されます。ただし、ルールの障害の状態がエラーに修正された場合（たとえば、ルール定義が設定に追加され、ルールが正常にインストールされた場合）、ゲートウェイは、機能不全のルールのリストからルール名を削除します。そのため、特定のルールの障害が再発すると、PCRF に報告されます。

機能不全のルール名はチェックポイントの対象とならないため、セッションリカバリや ICSR などのリカバリイベントが発生した場合、これらのルールの障害は再度報告されます。

ダイナミックルールのループ防止の設定

ここでは、機能を有効にするのに必要な設定手順について説明します。

ループ防止の制御のための **ACS** ポリシーの有効化

ACS 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て、PCRF と PCEF 間のルール障害ループを防止する機能を有効または無効にします。

```
configure
  active-charging service<service_name>
      policy-control report-rule-failure-once
      end
```

注：

- 設定すると、同じルールの失敗に対して CCR-U が 1 回だけ送信されます。
- デフォルトでは、この機能は無効です。
- 以前に設定済みの場合は、**no policy-control report-rule-failure-once** を使用して機能を無効にします。

モニタリングおよびトラブルシューティング

以下では、機能をモニターするために使用できるコマンドを説明します。

コマンドと出力の表示

ここでは、ダイナミックルールのループ防止機能のための show コマンドとそれらの出力について説明します。

show active-charging service all

上記のコマンドの出力が強化され、機能のステータス（有効または無効）が表示されるようになりました。次に例を示します。

```
show active-charging service all
```

```
.
.
.
Report Rule Failure Once: Enabled
```

show active-charging subscribers full all

上記のコマンドの出力が拡張され、報告されなかったルール失敗の合計数を示す新しいパラメータが表示されるようになりました。次に例を示します。

```
Callid:                          4e21        ACSMgr Card/Cpu:            15/0
Active Charging Service name:                                            acs
Active charging service scheme:
ACSMgr Instance:                  1          Number of Sub sessions:     1
Data Sessions Active:             0          Dynamic Routes created:     0
Uplink Bytes:                     0          Downlink Bytes:             0
Uplink Packets:                   0          Downlink Packets:           0
Accel Packets:                    0
FastPath Packets:                 0
Total NRSPCA Requests:            0          NRSPCA Req. Succeeded:      0
NRSPCA Req. Failed:               0
Total NRUPC Requests:             0          NRUPC Req. Succeeded:       0
NRUPC Req. Failed:                0
Pending NRSPCA Requests:          0          Pending NRUPC Requests:     0
Total Bound Dynamic Rules:        0          Total Bound Predef. Rules:  0
Data Sessions moved:              0
Bearers Terminated for no rules:                                         0
Failed Rulebase Install (unknown bearer-id):                             0
Failed Rule Install (unknown bearer-id):                                 0
Total number of rule failures not reported:                              1
```

show active-charging subsystem all

上記のコマンドの出力が拡張され、報告されなかったルール失敗の合計数を示す新しいパラメータが表示されるようになりました。次に例を示します。

```
Total ACS Managers:            2
Session Creation Succ:         1      Session Creation Fail:      0
.
.
.
Total Number of Unsolicited Downlink packets received : 0
Total Number of ICMP-HU packets sent :                   0

RADIUS Prepaid Statistics:
Total prepaid sess:            0      Current prepaid sess:       0
Total prepaid auth req:        0      Total prepaid auth success: 0
Total prepaid auth fail:       0      Total prepaid errors:       0
Total number of rule failures not reported :           4

Content Filtering URL Cache Statistics:
Total cached entries:          0
Total hits:                    0      Total misses:               0
.
.
.
```

RADIUS および Diameter Rf の中間アカウンティング インターバル タイマーの分離

機能情報

要約データ

[ステータス（Status）]	新しい機能
導入されたリリース	21.2
変更されたリリース	該当なし
対象製品	eHRPD、GGSN、P-GW
該当プラットフォーム	ASR 5500
デフォルト設定	無効
関連する CDETS ID	CSCvc97616
このリリースでの関連する変更点	N/A
関連資料	AAA Interface Administration and Reference Command Line Interface Reference

マニュアルの変更履歴



重要 リリース 21.2 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

機能説明

リリース 21.2 よりも前の Cisco StarOS プラットフォームには、アカウンティング中間レコードを RADIUS サーバーと Diameter Rf サーバーに送信する単一の設定パラメータがありました。そのため、使用可能な CLI オプションを使用して、さまざまな間隔でアカウンティング中間レコードを RADIUS サーバーと Diameter Rf サーバーに送信することができませんでした。この機能により、Diameter Rf および RADIUS アカウンティング アプリケーションにさまざまな中間間隔を設定するための CLI 制御メカニズムが提供されます。RADIUS サーバーおよび Diameter Rf サーバーに個別に設定可能な CLI および中間間隔タイマーの値を設定すると、使いやすさが向上します。

機能の仕組み

現在、Diameterアカウンティングは、RADIUSアカウンティングの暫定間隔に設定された値を使用します。CLI コマンドで設定可能なこの機能では、 Rf インターフェイスの Diameter アカウンティングの暫定間隔を個別に設定するためのオプションが提供されます。Diameter interim CLI が「**no**」オプションまたは特定のタイマー値を使用して設定されるまでは、RADIUS 暫定間隔値が互換性の尺度として Diameter 暫定間隔に使用されます。Diameter 設定が有効になると、RADIUS設定を変更しても Diameter設定に影響を与えることはなく、その逆も同様です。さまざまなシナリオで使用される Diameter の暫定間隔値を以下の表に示します。

RADIUS 設定	Diameter 設定	Diameter の暫定的な動作
設定なし または 暫定間隔：X または 暫定無効	暫定間隔：Y	暫定間隔：Y 注：X は Y と同じ場合と違う場合があります
設定なし または 暫定間隔：X または 暫定無効	「No」オプションを使用した暫定の無効化	暫定無効
設定なし または 暫定間隔：X または 暫定無効	設定なし	RADIUS 設定へのフォールバック

- リカバリ/ICSR の動作：PDN の作成時に使用された暫定的な間隔の設定は、PDN のライフタイム全体に適用されます。リカバリ/ICSRは、Diameterの暫定間隔に関する既存の PDN の動作に影響を与えません。
- ICSR アップグレード/ダウングレードの動作：
  - 既存のセッションは、古いシャーシに存在する RADIUS 設定に基づいて回復されます。
  - 新しいセッションの動作は、新たにアクティブになったシャーシで利用可能な設定に従います。

制限事項

この機能には次の既知の制限事項があります。

1. Diameter 中間インターバル CLI が設定されていない場合、P-GW は以前の動作を維持するため、Diameter アカウンティングでは RADIUS アカウンティングで設定されたものと同じ中間インターバル値が使用されます。
2. Diameter アカウンティングの設定が完了すると、以前の動作に戻すことはできません。

Diameter 中間アカウンティング インターバルの設定

RADIUS 中間アカウンティングインターバルとは別に Diameter 中間アカウンティングインターバルを設定するには、AAA サーバー グループ 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。

```
configure
    context context_name
      aaa group group_name
         diameter accounting interim interval interval_in_seconds
         end
```

注：

- *interval_in_seconds*：中間インターバルを指定します。50 ～ 40000000 の範囲にする必要があります。
- 以前に設定されている場合は、**no diameter accounting interim interval** を使用して Rf インターフェイスの中間アカウンティングメッセージを無効にします。
- デフォルトの Diameter 中間インターバル値はありません。
- Diameter 中間インターバル CLI が設定されていない場合、P-GW は以前の動作を維持するため、Diameter アカウンティングでは AAA サーバーグループの構成ブロックで使用可能な RADIUS 中間インターバルの設定が使用されます。

モニタリングおよびトラブルシューティング

以下では、機能をモニターするために使用できるコマンドについて説明します。

コマンドと出力の表示

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show aaa group { name <group_name> | all }

上記のコマンドの出力が変更されて、今後の Diameter Rf アカウンティングセッションに使用される暫定間隔の現在の設定を示す次の新しいフィールドが表示されます。

- Interim-timeout: <50-40000000> または <None>

次に、Diameter の暫定間隔が設定されていない場合の出力例を示します。

```
show aaa group name default
Group name:                    default
Context:                       pgw

Diameter config:
  Accounting:
    Request-timeout:           20
    Interim-timeout:           None
```

次に、Diameter の暫定間隔の値を 900 に設定した場合の出力例を示します。

```
show aaa group name default
Group name:                    default
Context:                       pgw

Diameter config:
  Accounting:
    Request-timeout:           20
    Interim-timeout:           900
```

show configuration [verbose]

上記のコマンドの出力が変更され、中間メッセージの間隔を秒単位で示す次の新しいフィールドが表示されるようになりました。

- diameter accounting interim interval <*value_in_seconds*>

次に、Diameter の中間間隔値を 60 に設定した場合の出力例を示します。

```
show configuration context isp verbose
config
    context isp
        aaa group default
            diameter accounting interim interval 60
```

Gy の OCS 障害レポートの強化

機能情報

要約データ

[ステータス（Status）]	変更された機能
導入されたリリース	21.1
変更されたリリース	21.2
対象製品	P-GW、SAEGW
該当プラットフォーム	ASR 5500
デフォルト設定	有効

関連する CDETS ID	CSCvc93904
このリリースでの関連する変更点	N/A
関連資料	AAA Interface Administration and Reference P-GW Administration Guide SAEGW Administration Guide

マニュアルの変更履歴

重要 リリース 21.2 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

機能説明

Cisco-Event-Trigger-Type AVP が CCA-I、CCA-U、または値が CREDIT_CONTROL_FAILURE（5）の RAR メッセージの PCRF によってインストールされる場合、シスコイベントグループ化 AVP が P-GW によって、OCS 障害コードの正確な値を含む CCR-U メッセージで PCRF に送信されます。このトリガーは、Gy で障害が発生した場合にのみ送信され、設定（クレジット制御障害の処理）に基づいて「続行」アクションが実行され、Gy セッションがオフライン状態に移行します。

この機能強化により、範囲ではなく正確な障害コードが PCRF に報告されます。たとえば、シスコ イベント トリガー タイプが CREDIT_CONTROL_FAILURE（5）で、CCA-U の OCS 障害コードが 3002 の場合、PCRF に送信される CCR-U では、シスコ CC 障害タイプ（グループ化された AVP シスコイベントの一部）が値 3002 で送信されます。

S5/S8 および S2b インターフェイスの RAN/NAS 原因コードに追加されたサポート

機能情報

要約データ

[ステータス（Status）]	変更された機能
導入されたリリース	21.1
変更されたリリース	21.2

対象製品	P-GW、S-GW、SAEGW
該当プラットフォーム	ASR 5500
デフォルト設定	無効
関連する CDETS ID	CSCuy93748/CSCvc97356
このリリースでの関連する変更点	N/A
関連資料	*P-GW Administration Guide* *S-GW Administration Guide* *SAEGW Administration Guide* *Command Line Interface Reference*

マニュアルの変更履歴

重要 リリース 21.2 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

変更された機能

重要 これはライセンスで制御される機能です。この機能用に別のライセンスがあります。NPLI の既存のライセンスを有効にする必要があります。または、シスコのアカウント担当者に、カスタムライセンスの取得方法をお問い合わせください。

IMS ドメインと VoWiFi の展開で課金を調整する場合、通信事業者は P-CSCF で入手可能な RAN または NAS（または両方）のリリース原因コード情報にアクセスする必要がある場合があります。P-GW は、アクセスネットワークから受信した ANI 情報とともに詳細な RAN/NAS 原因情報を提供し、さらに次のイベントに基づいて PCRF に提供します。

- ベアラーの非アクティブ化（ベアラー作成応答/ベアラー削除コマンド）
- セッションの非アクティブ化（セッション削除要求）
- ベアラーの作成/変更の失敗（原因が FAILURE の ベアラー作成/更新応答）

IMS ネットワークはアクセスネットワークから詳細な RAN または NAS（またはその両方）のリリース原因コード情報を取得できます。この情報は、コールパフォーマンス分析、ユーザー

QoE 分析、および適切な課金調整に使用されます。この機能は、S5、S8、Gx、および S2b インターフェイスでサポートされています。

この機能には、ベアラー作成応答、ベアラー更新応答、ベアラー削除応答、ベアラー削除コマンド、およびセッション削除要求での RAN/NAS 原因 IE のサポートが含まれています。次の表は、RAN/NAS 原因 IE でサポートされているプロトコルタイプを示しています。

表 *79 : RAN/NAS IE* のプロトコルタイプ

Interface	RAN/NAS IE でサポートされているプロトコルタイプ
S5/S8	S1AP Cause（1）/EMM Cause（2）/ESM Cause（3）
S2b	Diameter Cause（4）/IKEv2 Cause （5）

（注） 表にリストされているサポート対象プロトコルタイプの値以外の受信されたプロトコルタイプ値は、無視され、PCRF に転送されません。

RAN/NAS 原因の GTP インターフェイス要件

S5/S8 インターフェイスの場合、RAN/NAS 原因は、dpca-custom8 ディクショナリの次のメッセージでサポートされます。

- ベアラー作成失敗応答
- ベアラー更新失敗応答
- セッション削除要求
- ベアラー削除応答
- ベアラー削除コマンド

S2bインターフェイスでは、カスタムdpca-custom8ディクショナリの次のメッセージでRAN/NASの原因がサポートされています。

- ベアラー作成失敗応答
- ベアラー更新失敗応答
- セッション削除要求

RAN/NAS 原因の Gx インターフェイス要件

RAN/NAS 原因がカスタム dpca-custom8 ディクショナリに追加され、RAN/NAS の原因が確実に表示されるようになりました。RAN/NAS 原因を処理するための Gx インターフェイスの動作は次のとおりです。

表 *80 : RAN/NAS* 原因の *Gx* インターフェイス要件

Message	GTP 原因	RAN-NAS 原因情報を伝送する Gx メッセージ
ベアラー作成応答	Accepted	29.274 の表 7.2.4-2 に従い、RAN/NAS の原因は予期されません。したがって、受信しても無視され、PCRF に転送されません。
	Temporarily rejected due to HO in progress.	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。したがって、受信しても無視され、PCRF に転送されません。
	Other GTP Causes	CCR-U
ベアラー更新応答	Accepted	29.274 の表 7.2.16-2 に従い、RAN/NAS 原因は予期されていません。したがって、受信しても無視され、PCRF に転送されません。
	No Resources Available	CCR-U （注） UE によって開始された（MBC）ベアラーの変更が GTP 原因「NO RESOURCES AVAILABLE」で失敗した場合、P-GW は PDN セッション全体を削除します。この場合、RAN-NAS 原因情報は CCR-T メッセージの一部として転送されます。
	Context Not Found	CCR-U （注） ベアラー更新応答をメッセージレベルの原因「CONTEXT NOT FOUND」とともに受信した場合、これは PDN の削除につながり、RAN-NAS 原因情報は CCR-T メッセージの一部として転送されます。
	Temporarily rejected due to HO in progress.	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。したがって、受信しても無視され、PCRF に転送されません。
	Other GTP Causes	CCR-U

Message	GTP 原因	RAN-NAS 原因情報を伝送する Gx メッセージ
ベアラー削除応答	Temporarily rejected due to HO in progress	この GTP 原因による RAN/NAS 原因は、29.274 の表 C.4 に従って適用されません。したがって、受信しても無視され、PCRF に転送されません。 （注） • ベアラー削除コマンドの一部としてトリガーされるベアラー作成応答内で RAN/NAS 原因が受信され、原因が「Request Accepted」の場合、P-GW は（ベアラー作成応答で受信した）RAN/NAS 原因をPCRF に転送します。 • ベアラー削除コマンドで RAN/NAS 原因を受信し、ベアラー削除応答が「HO in progress」である場合、ベアラー削除コマンドで受信した RAN/NAS 原因は PCRF に転送されます。 • ベアラー削除コマンドで RAN/NAS 原因を受信し、ベアラー削除応答が「Accepted」または「Other Cause」である場合、新しい RAN/NAS 原因が PCRF に転送されます。
	Accepted / Other GTP CCR-UCauses	CCR-U （注） RAR/CCA-U を介して開始されたベアラー削除応答で RAN/NAS 原因を受信した場合、P-GW は、RAN/NAS 原因をレポートするために CCR-U を PCRF に送信しません。 このサポートは、29.212 リリース 13.5 の「RAN/NAS 機能の強化」により導入されました。
セッション削除要求	Accepted	CCR-T

PCRF に対する ANI の動作

3GPP 29.212 v13.4.0 のセクション 4.5.6、4.5.7、4.5.12 には、RAN-NAS-Cause 機能がサポートされている場合、PCEF は 3GPP-User-Location-Info AVP（利用可能な場合）、TWAN-Identifier（利用可能な場合で Trusted-WLAN 機能がサポートされている場合）、User-Location-Info-Time AVP（利用可能な場合）、および 3GPP-MS-TimeZone AVP（利用可能な場合）で、使用可能なアクセスネットワーク情報を提供する必要があると記載されています。

USER-LOCATION-INFO-TIME AVP が dpca-custom8 ディクショナリに追加され、ANI の一部として PCRF（使用可能な場合）に送信されます。また、RAN/NAS に対して新しい PROTOCOL-TYPE（1 ～ 5）がサポートされています。この AVP は、CCR-U と CCR-T（該当する場合）で確認できます。また、新しい PROTOCOL-TYPE（S1AP Cause、EMM Cause、ESM

Cause、IKEv2, DIAMETER）が Gx インターフェイスに表示されます（同じものが S5/S8/S2b インターフェイスを介して受信されている場合）。

S5/S8 インターフェイスの ANI の動作

P-GW は、RAN/NAS 原因とともに、dpca-custom8 ディクショナリの次の情報（存在する場合）も PCRF に送信します。

表 *81 : Gx* インターフェイスでの *GTP IE* から *ANI AVP* へのマッピング

GTP IE	Gx AVP
UE Time Zone	3GPP-MS-TimeZone
ULI Timestamp	User-Location-Info-Time
ユーザーロケーション情報	3GPP-User-Location-Info

RAN/NAS 機能が有効になっている場合、設定されたイベントトリガーに関係なく、ANI 情報が PCRF に送信されます。

S2b インターフェイスの ANI の動作

dpca-custom8 ディクショナリの場合、ANI 情報は PCRF に送信されません。また、dpca-custom8 ディクショナリの場合、TWAN-Identifier は ANI の一部としてはサポートされていません。

制限事項

この機能には次の制限があります。

- RAN/NAS 原因情報のサポートは、dpca-custom8 ディクショナリについてのみ追加されます。
- PGW は、GTP インターフェイスから受信した最初の 2 つの RAN/NAS 原因 IE（最大 1 つの RAN と最大 1 つの NAS）情報を処理します。たとえば、アクセスネットワークが不正な動作をし、2 つの NAS と 1 つの RAN の RAN/NAS 原因リストを送信した場合、最初の 2 つの原因のみが考慮され、検証されます。この場合、2 つの NAS 原因があり、最初の NAS 原因だけが Gx インターフェイスで入力されます。
- RAN/NAS 情報は Gx インターフェイスでのみ入力され、他のインターフェイスは影響を受けません。

コマンドの変更

diameter encode-supported-features netloc-ran-nas-cause

既存の CLI コマンドである **diameter encode-supported-features netloc-ran-nas-cause** を使用して、S5/S8 および S2b インターフェイスの各々で RAN/NAS 原因を有効にします。

この機能はデフォルトで無効に設定されています。

この機能を有効にするには、以下のコマンドを入力します。

```
configure
   context ISP1
      ims-auth-service IMSGx
        policy-control
        diameter encode-supported-features netloc-ran-nas-cause
        end
```



第 43 章

eMPS の Gx サポート

- 機能の概要と変更履歴 （869 ページ）
- 機能説明 （870 ページ）
- 機能の仕組み （871 ページ）
- eMPS の Gx サポートの設定 （872 ページ）
- eMPS の Gx サポートのモニタリングと障害対応 （875 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	ASR 5500
機能のデフォルト	• eMPS セッションの GTP および Gx の優先順位付け：無効 - 設定が必要 • DRMP AVP の解析：有効 - 常時オン
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.3

機能説明

National Security/Emergency Preparedness（NS/EP）Next Generation Network（NGN）Priority Services（NGN-PS）（旧称 NGN Government Emergency Telecommunications Service（GETS））とは、パブリックパケット交換サービスプロバイダーから利用可能なサービスに基づく一連の音声、動画、およびデータのサービスであり、National Security and Emergency Preparedness（NS/EP）の通信をサポートする優先処理を提供します。サービスプロバイダーとは、GETS（レガシー GETS を含む）、ワイヤレス プライオリティ サービス（WPS）、または NS/EP NGN プライオリティサービス（NS/EP NGN-PS）を提供することが NCS によって許可されている公衆電気通信サービスプロバイダーです。NS/EP NGN-PS は、サービスユーザーの NS/EP 通信に関する優先処理を提供するものであり、サービスプロバイダーのネットワークで、輻輳を原因とする障害が発生したり、自然災害（洪水、地震、ハリケーンなど）による損傷が発生したり、人為的な災害（物理攻撃、サイバー攻撃、または他の形態のテロ攻撃など）が発生したりした場合に必要です。

この機能を使用すると、ネットワークでの NS/EP NGN プライオリティサービスのサポートが追加されます。これにより、P-GW ノードはまず、（設定された Enhanced Multimedia Priority Service（eMPS）により進化した割り当ておよび保持プライオリティ（eARP）に基づいて）eMPS ベアラーまたはセッションを識別し、その後にネットワーク上の GTP および Gx シグナリングを優先処理します。

重要 eMPS プロファイルの設定（eMPS ベアラーまたはセッションとしてベアラーまたはセッションを識別するために使用される eMPS ARP の設定）、および eMPS 統計に関連する補足情報については、『*P-GW Administration Guide*』または『*SAEGW Administration Guide*』の「*VoLTE/*緊急コールの拡張優先順位付け」の章を参照してください。

GTP および Gx シグナリングの優先順位付け

1. eMPS セッションにおける GTP シグナリングの優先順位付けは、次のことを意味します。
   - 負荷および過負荷制御により、eMPS セッションの GTP 制御トラフィックがスロットリングから除外されます（負荷および過負荷制御に関する補足情報については、『*P-GW Administration Guide*』または『*SAEGW Administration Guide*』の「*P-GW*、*SAEGW*、および *S-GW* での *3GPP R12 GTP-C* 負荷および過負荷制御のサポート」の章を参照してください）。
2. eMPS セッションにおける Gx シグナリングの優先順位付けは、次のことを意味します。

- eMPS セッションの Gx トラフィックが発信 RLF スロットリングから除外されます（RLF スロットリングは Gx 発信メッセージにのみ適用されます）。
- eMPS セッションの Gx トラフィックが最大未処理キューの判定から除外されます。

RAR メッセージからの DRMP AVP の解析

Gx インターフェイスでの RAR メッセージからの DRMP AVP を解析するためのサポートも拡張されています。また、DRMP 値が 0 として受信された場合は、対応する応答（RAA）メッセージが優先されます。つまり、Gx RLF スロットリングおよび最大未処理キューの判定からは除外されます。

他の機能との関係

この機能は、eMPS プロファイル、負荷/過負荷制御、Gx RLF スロットリング、および最大未処理設定機能に関連しています。これらの機能のうち、1 つ以上を使用するには、追加のライセンスキーをインストールする必要があります。

機能の仕組み

この機能の動作の概要を以下で説明します。

- 新しく導入された CLI コマンド **diameter session-prioritization** は、eMPS セッションの Gx シグナリングの優先順位付けを有効または無効にするために使用します。この CLI コマンドは、ims-authorization サービスの policy-control 設定にあり、以下の動作のために必要となります。
  - eMPS セッションの Gx トラフィックを RLF スロットリングから除外する。
  - eMPS セッションの Gx トラフィックを最大未処理キューの判定から除外する。

  次の Gx シグナリングは、RLF スロットリングおよび最大未処理キューの判定から除外されます。
  - eMPS セッションのすべての Gx シグナリング。
  - eMPS アップグレード/ダウングレード切り替えに関連する Gx シグナリング。これにはアクセステクノロジー間ハンドオーバーも含まれます。
  - eMPS アップグレードの失敗（アクセス側からの UBRsp/CBRsp の失敗）の一部として開始される Gx シグナリング。
- RAR からの DRMP AVP を解析し、DRMP 値が 0 として受信した場合、対応する RAA を優先させるサポートが追加されました。この動作はデフォルトで有効になっており、eMPS セッションと非 eMPS セッションの両方に適用でき、diameter session-prioritization CLI コマンドとは無関係です。

- **GTP 負荷過負荷スロットリングの動作**：Cisco P-GW は、自己過負荷シナリオとピア過負荷シナリオの両方で GTP 負荷過負荷スロットリングをサポートしています。ただし、これらの条件下でも、eMPS セッションの GTP シグナリングはスロットリングから除外する必要があります。この優先順位付けを機能させるには、eMPS プロファイルで設定されているすべての eARP 値を、負荷過負荷プロファイル構成で（自己過負荷とピア過負荷の両方について）設定する必要があります。負荷過負荷プロファイル構成（自己過負荷およびピア過負荷）で設定された追加の eARP 値については、自己過負荷とピア過負荷の従来の動作が続行されます。

  eMPS プロファイル構成で設定された eARP 値に変更がある場合：

  1. 既存のセッションの場合：
     1. そのセッションの既存のベアラーの eARP 値に変更がある場合、またはそのセッションのベアラーの作成時に、eMPS アップグレード/ダウングレード切り替え用の新しい設定が考慮されます。
     2. セッションが eMPS とマークされるまで、自己過負荷とピア過負荷の従来の動作が、新しく設定された eARP 値について続行されます。
  2. 新しいセッションの場合：
     1. 新しい設定はシームレスに反映されます。

- セッションリカバリと ICSR により、セッションの eMPS 状態が回復されます。
- Government Industry Requirements（GIR）ドキュメントに従って、eMPS マーキングは P-GW EUTRAN および S4-SGSN PDN に対してのみ行われます。

制限事項

この機能には次の既知の制限事項があります。

- セッションが eMPS とマークされている場合、そのセッションは非 eMPS セッションにダウングレードされた後も、GTP 自己過負荷の状況下で GTP スロットリングから除外されたままになります。
- セッションで、内部障害によりセッションを非 eMPS から eMPS にアップグレードできるベアラー更新要求またはベアラー作成要求に失敗すると、対応する CCR-U が優先されない場合があります。

eMPS の Gx サポートの設定

ここでは、この機能をサポートするために使用可能な CLI コマンドについて説明します。

eMPS プロファイルの設定

次のコマンドを使用して eMPS プロファイルを設定します。この eMPS プロファイルは、eMPS ベアラーまたはセッションとしてベアラーまたはセッションを識別およびマークするために使用されます。

```
configure
  emps-profile emps_profile
    earp earp_value earp_value
    end
```



重要 eMPS プロファイルの設定（eMPS ベアラーまたはセッションとしてベアラーまたはセッションを識別するために使用される eMPS ARP の設定）、および eMPS 統計に関連する補足情報については、『*P-GW Administration Guide*』または『*SAEGW Administration Guide*』の「*VoLTE/*緊急コールの拡張優先順位付け」の章を参照してください。

eMPS セッションの Gx 優先順位付けの有効化

セッションの eMPS 状態に基づく Gx メッセージの優先順位付けを有効にするには、ポリシー制御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。

```
configure
  context context_name
    ims-auth-service service_name
     policy-control
       [ no ] diameter session-prioritization
       end
```

注：

- デフォルトでは、**diameter session-prioritization** CLI コマンドは無効になっており、Gx メッセージは eMPS 値に基づいて優先順位付けされません。
- 以前に設定されている場合は、**no diameter session-prioritization** CLI コマンドを使用してデフォルトの動作を設定します。
- **diameter session-prioritization** CLI は、eMPS プロファイルとともに、Gx が設定で有効になっている場合に有効になります。

GTP 負荷の過負荷スロットリングにおける eMPS セッションの GTP 優先順位付けの有効化

GTP ピア過負荷制御や自己保護の設定がシステムで有効になっている場合は、次の設定を使用して、GTP シグナリングに関連する eMPS セッションの優先付けを行います。これらの設定では、ピア過負荷または自己保護の条件下でのスロットリングから eMPS セッションの GTP トラフィックを除外するオプションが提供されます。

```
configure
  emps-profile emps_profile_name
    earp earp_value earp_value
    end
```

```
configure
  gtpc-overload-control-profile overload_profile
    throttling-behavior earp earp_value earp_value exclude
    self-protection-behavior earp earp_value earp_value exclude
    end
```

注：

- **emps-profile** *emps_profile_name*：eMPS セッションの属性を定義するための eMPS プロファイルを設定します。*emps_profile_name* は、1 ～ 63 文字の文字列です。
- **earp**：最大 3 つの eARP プライオリティレベル（PL）値を設定して、設定された eARP プライオリティ値を持つセッションを eMPS セッションとしてマークできるようにします。eMPS プロファイルでは、最大 3 つの eARP 値を設定できます。
- 上記の設定に従って、いずれかの eARP 値を持ついずれか 1 つのベアラーとのセッションが負荷の過負荷 GTP スロットリングから除外されます。



重要 GTP-C 過負荷制御スロットリングと自己保護の動作および設定の詳細に関する補足情報については、『*P-GW Administration Guide*』または『*SAEGW Administration Guide*』の「*P-GW*、*SAEGW*、および *S-GW* における *3GPP R12* の *GTP-C* 負荷および過負荷制御のサポート」の章を参照してください。

eMPS プロファイルの設定（eMPS ベアラーまたはセッションとしてベアラーまたはセッションを識別するために使用される eMPS ARP の設定）、および eMPS 統計に関連する補足情報については、『*P-GW Administration Guide*』または『*SAEGW Administration Guide*』の「*VoLTE/*緊急コールの拡張優先順位付け」の章を参照してください。

Gx RLF スロットリングおよび Gx の最大未処理キューの設定の詳細については、『*CLI* コンフィギュレーション ガイド』を参照してください。

eMPS の Gx サポートの設定の確認

ここでは、eMPS の Gx サポート設定を確認するための情報を提供します。

show configuration

この CLI コマンドの出力範囲が拡張され、次の新しいフィールドが表示されるようになりました。

- diameter session-prioritization

ユーザーが [support record] セクションを指定していない場合は、show configuration verbose

このCLIコマンドの出力範囲が拡張され、次の新しいフィールドが表示されるようになりました。

- diameter session-prioritization

eMPS の Gx サポートのモニタリングと障害対応

ここでは、機能のモニタリングと障害対応に使用できる CLI コマンドについて説明します。

show ims-authorization policy-control statistics

このCLIコマンドを使用して、優先されるDRMPメッセージの数に関する統計を表示します。出力例の一部を以下に示します。

```
show ims-authorization policy-control statistics

Rule Installation Failure:
  Resource Limitation:           0             Unknown Bearer ID:             0
  Invalid QCI:                   0             Invalid ARP:                   0
  Bearer-Id in QoS:              0             Parse Error:                   0
  Invalid Redirect Address:      0             ADC Absent:                    0
  Incorrect Metering Method:     0             Incorrect Rating Group:        0
  Incorrect Online AVP:          0             Incorrect Offline AVP:         0
  Incorrect Flow Status:         0             Incorrect Usage Monitoring AVP:0
  Incorrect Required Access Info:0             Incorrect Flow Description:     0
  Incorrect Reporting Level:     0

DRMP Statistics:
  RAR with P0 priority:          0             RAR with other priority:       2
```



第 44 章

Gy インターフェイスのサポート

この章では、Gyインターフェイスの概要と、Gyインターフェイスの設定方法について説明します。

次の製品のシスコシステムで Gy インターフェイスがサポートされています。

- GGSN
- HA
- IPSG
- PDSN
- P-GW

この章に記載する手順を実行する前に、展開する製品のアドミニストレーションガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

- 機能の概要と変更履歴 （877 ページ）
- はじめに （878 ページ）
- 機能と用語 （880 ページ）
- Gy インターフェイスのサポートの設定 （925 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	PGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
このリリースでの関連する変更点	N/A

関連資料	• *Command Line Interface Reference* • *PGW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

重要　リリース 21.2 および N5.1 よりも前に導入された機能の改訂履歴の詳細は示していません。

改訂の詳細	リリース
CDR のサーバー到達不能フィールドを追加するためのサポートが追加されました。	21.27
最初の導入。	21.22

はじめに

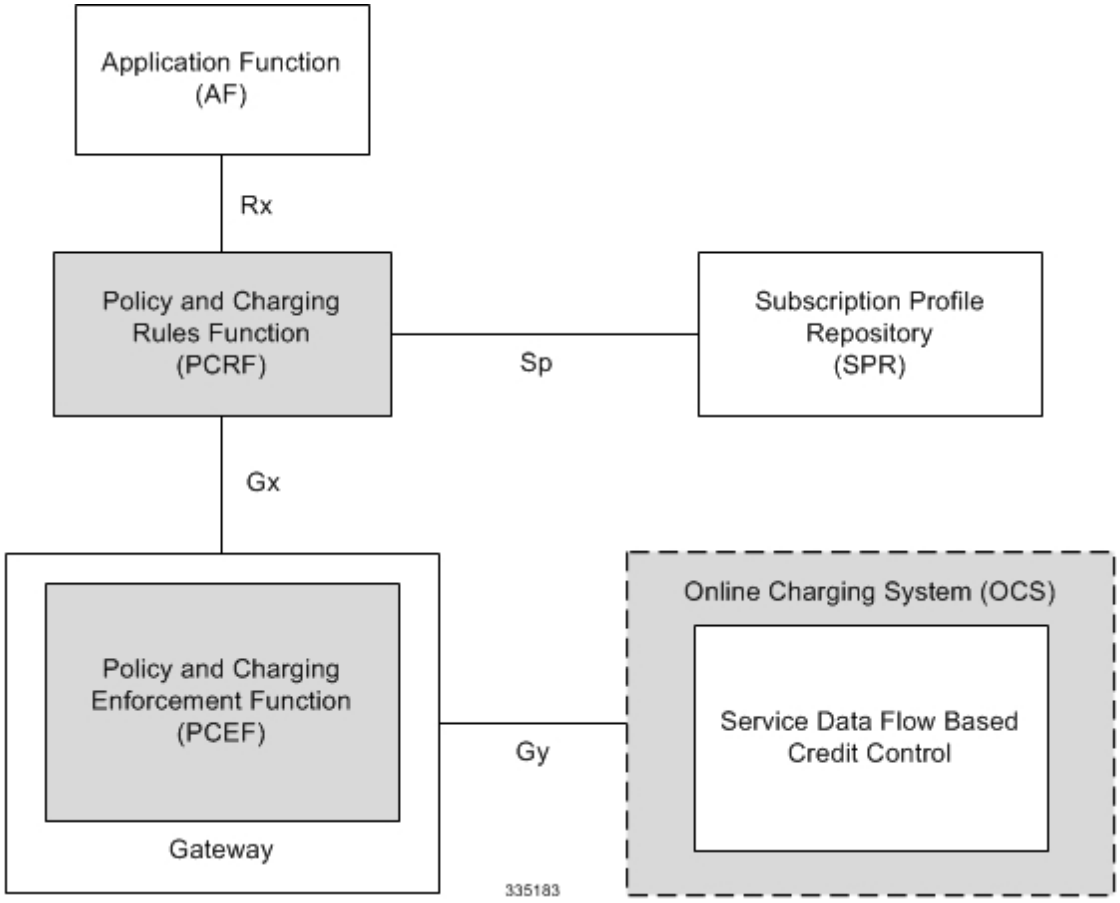
Gy インターフェイスは、PCEF/GW（課金トリガー機能（CTF））とオンライン課金システム（課金データ機能（CDF））間のオンライン課金インターフェイスです。

Gy インターフェイスは、アクティブ課金サービス（ACS）や Enhanced Charging Service（ECS）を利用して、データサービスのコンテンツベースの課金にリアルタイムで対応します。これは 3GPP 標準規格に基づいており、クォータ割り当てに依存しています。オンライン課金システム（OCS）は、オンライン課金データを PCEF/GW に提供する Diameter クレジット制御サーバーです。Gy を使用すると、カスタマートラフィックをゲートウェイに送り、オンラインまたは前払いの形式で課金できます。時間ベースと使用量ベースの課金モデルがサポートされています。これらのモデルでは、ECS のシャローパケット インスペクションまたはディープパケット インスペクションに基づいて、各種サービスに異なるレートを適用できます。

最も単純なインストールでは、システムは Diameter TCP リンクを介して、システム自体と 1 台の前払いサーバーとの間で、Gy Diameter メッセージを交換します。インストールを堅牢化するには、複数のサーバーを使用します。これらのサーバーは、必要に応じて単一のクォータ データベースを共有またはミラーリングして、あるサーバーから別のサーバーへの Gy セッションのフェールオーバーに対応します。拡張性の高いインストールでは、プロキシまたは他の Diameter エージェントのレイヤを導入して、マルチパス メッセージ ルーティング、メッセージやセッションのリダイレクト機能などを提供できます。

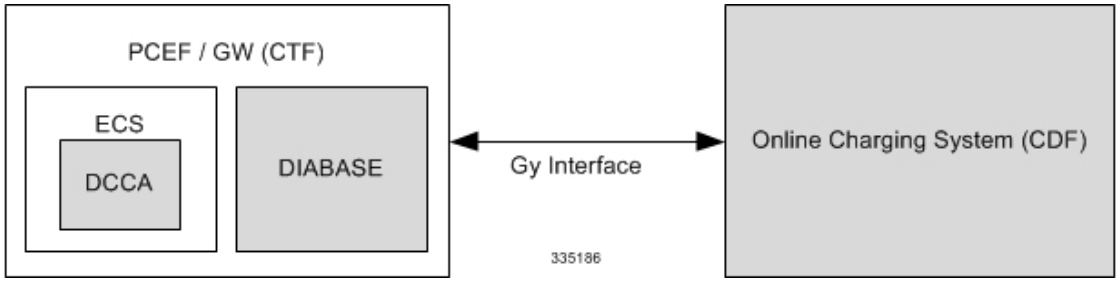
次の図は、ポリシーと課金アーキテクチャの Gy 参照ポイントを示しています。

図 *66 : PCC* 論理アーキテクチャ



次の図は、ECS と OCS（CDF/サーバー）を実行している CTF/ゲートウェイ/PCEF/クライアント間の Gy インターフェイスを示しています。PCEF/GW 内では、Gy プロトコル機能は、DCCA モジュール内（ECS）で処理されます。

図 *67 : Gy* アーキテクチャ



ライセンス要件

Gy インターフェイスのサポートは、ライセンス供与されたシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカ

ウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

サポートされる標準

Gy インターフェイスのサポートは、次の標準に基づいています。

- IETF RFC 4006：Diameter Credit Control Application（2005 年 8 月）
- 3GPP TS 32.299 V9.6.0 (2010-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 9)

機能と用語

ここでは、Gy 機能に関連する機能と用語について説明します。

課金シナリオ



重要 イベントのオンライン課金（「即時イベント課金」および「予約によるイベント課金」）はサポートされていません。「予約によるセッション課金」のみがサポートされます。

予約によるセッション課金

ユニット予約によるセッション課金は、セッションのクレジット制御に使用されます。

分散型ユニット決定と集中型レート設定

このシナリオでは、CTF はセッションの指揮の前にユニットの予約を要求します。セッションの終了処理が終わると、口座引き落とし操作が実行されます。

集中型ユニット決定と集中型レート設定

このシナリオでは、CTF が、OCS に、CTF によって指定されるセッション識別子に基づいてユニットを予約するように要求します。セッションの終了後に、口座引き落とし操作が実行されます。

分散型ユニット決定と分散型レート設定



重要 分散型レート設定は、このリリースではサポートされていません。分散型ユニットの決定は、CLI 設定コマンドを使用して行われます。

このシナリオでは、CTF は OCS に対して、指定された単位の金額の支払い予約をサブスクライバのアカウントで保証するよう要求します。サブスクライバのアカウントからの支払いをトリガーするアカウントのデビット操作は、セッションの確立の終了後に実行されます。

基本操作

重要 即時イベント課金は、このリリースではサポートされていません。「予約ユニット要求」と「予約ユニット応答」は、イベント課金ではなく、セッション課金に対して実行されます。

オンラインクレジット制御では、基本的な論理演算「デビットユニット」と「予約ユニット」を使用します。

- デビットユニット要求（CTF から OCS に送信）：CTF は、サブスクライバからサービス要求を受信した後、デビットユニット要求を OCS に送信します。CTF では、サービス識別子（集中型ユニット決定）または要求されるユニット数（分散型ユニット決定）のいずれかを指定できます。返金を目的として、CTF はデビットユニット要求も OCS に送信します。
- デビットユニット応答（OCS から CTF に送信）：OCS はデビットユニット応答で応答します。この応答は、デビットユニット要求の結果として付与されたユニット数を CTF に通知します。これには、付与されたユニット数が、要求されたサービスをレンダリングする権限を示す場合も含まれます。返金を目的として、OCS はデビットユニット応答で応答します。
- 予約ユニット要求（CTF から OCS に送信）：CTF によって提供されるサービスのためにユニット数を予約するよう要求します。集中型ユニット決定の場合、CTF は予約ユニット要求でサービス識別子を指定し、OCS は要求されるユニット数を決定します。分散型ユニット決定の場合、要求されるユニット数は CTF によって指定されます。
- 予約ユニット応答（OCS から CTF に送信）：「予約ユニット要求」の結果として予約されたユニット数を CTF に通知する OCS からの応答。

ユニット予約（SCUR）によるセッション課金では、「デビットユニット」と「予約ユニット」の両方の操作が使用されます。SCUR では、RFC 4006 で指定されているセッションベースのクレジット制御手順が使用されます。ユニット予約によるセッション課金では、「デビットユニット」操作と「予約ユニット」操作の両方が必要な場合、これらの操作は 1 つのメッセージに統合されます。

重要 コスト情報、残高、および残高減少を示す AVP はサポートされていません。

消費されたユニットは、サービスの提供後にサブスクライバのアカウントから差し引かれます。そのため、予約済みユニットと消費済みユニットは必ずしも同一ではありません。この操作を使用して、CTF は、以前に予約されたユニットの返戻分を含めて、現在の予約を変更することもできます。

再承認

サーバーは、付与されたクォータに関連付けられたアイドルタイムアウトを指定できます。または、クライアントに設定可能なデフォルト値を指定することもできます。このタイマーが切れると、再承認要求がトリガーされます。

セッション中のサービスイベント（再承認トリガー）によって、現在のサービス使用状況のレーティングが影響を受ける場合があります。サーバーは、レーティング条件に影響を与える可能性のあるさまざまなセッション関連のトリガーが発生した場合に、クォータを再承認するようにクレジット制御クライアントに指示する場合があります。

再承認がトリガーされると、クライアントはクォータの使用状況を報告します。クォータが報告されている理由がサーバーに通知されます。

しきい値ベースの再承認トリガー

サーバーはオプションで、クォータの再承認をトリガーする残りのクォータしきい値のクライアントへの指示を追加することができます。

終了アクション

サーバーは、最後に許可されたユニットの消費時の動作をクライアントに対して指定できます。これは終了アクションと呼ばれます。

Diameter 基本プロトコル

Diameter 基本プロトコルは、Diameter クライアントと Diameter サーバー間の基礎となる接続を維持します。クライアントとサーバー間の接続は TCP ベースです。接続と機能のステータスを確認するために、一連のメッセージが交換されます。

- 機能交換メッセージ：機能交換メッセージは、互いの機能と互いのアイデンティティを認識するために、Diameter ピア間で交換されます。
  - 機能交換要求（CER）：このメッセージは、サーバーの機能を認識するためにクライアントからサーバーに送信されます。
  - 機能交換応答（CEA）：このメッセージは、CER メッセージへの応答としてサーバーからクライアントに送信されます。



重要 Acct-Application-Id は解析されず、送信された場合は PCEF/GW によって無視されます。Result-Code が DIAMETER_SUCCESS でない場合、ピアとの接続は閉じられます。

- デバイスウォッチドッグ要求（DWR）：CER/CEA メッセージが交換された後、しばらくの間ピア間のトラフィックがなくなった場合、接続の正常性をモニターするために、DWR メッセージがクライアントから送信されます。デバイス ウォッチドッグ タイマー（Tw）は PCEF/GW で設定可能で、6 ～ 30 秒の範囲で設定できます。値を小さくすると、メッ

セージの重複が発生します。デフォルト値は 30 秒です。DWA がない状態で Tw が 2 回連続して期限切れになると、ピアはダウンしていると見なされます。

重要 DWR は、サーバーから最後のメッセージ受信した後、Tw の期限切れ後にのみ送信されます。たとえば、ピア間で継続的にメッセージが交換される場合、サーバーからの最後のメッセージ受信時刻から現在時刻までの経過時間が Tw よりも小さい場合、DWR は送信されない可能性があります。

- デバイスウォッチドッグ応答（DWA）：これは、サーバーからの DWR メッセージに対する応答です。接続状態のモニタリングに使用されます。
- ピア切断要求（DPR）：このメッセージは、接続をシャットダウンするように通知するためにピアに送信されます。PCEF/GW はこのメッセージの受信のみを行います。現在、Diameter サーバーにメッセージを送信する機能はありません。
- ピア切断応答（DPA）：このメッセージは、ピアからの DPR 要求に対する応答です。DPR を受信すると、ピアは DPA を送信し、接続状態を「DO NOT WANT TO TALK TO YOU」状態にします。ピアを再度設定する以外、接続を元に戻す方法はありません。

  切断されたピアを再試行するためのタイムアウト値を指定する必要があります。
- Tw タイマー期限切れ動作：クライアントとサーバー間の接続は、DIABASE アプリケーションによって管理されます。Tw タイマーが 2 回連続で期限切れになると、ピア状態はアイドルに設定され、接続の確立が再試行されます。その後、その接続上のすべてのアクティブセッションは、セカンダリ接続に転送されます（セカンダリ接続が設定されている場合）。すべての新しいセッションのアクティブ化も、セカンダリ接続で試行されます。

  Tw タイマーとも同等である接続タイムアウト間隔があります。その期間中、CER がサーバーに送信された後、接続の再確立の試行中に応答を受信しない場合、接続は閉じられ、状態はアイドルに設定されます。

Diameter クレジット制御アプリケーション

Diameter クレジット制御アプリケーション（DCCA）は、ECS サブシステムの一部です。Diameter クレジット制御が有効になっているすべてのプリペイドのお客様について、セッションが開始されるたびに、Diameter サーバーに接続され、サブスクライバのクォータが取得されます。

クォータの動作

さまざまな形式のクォータが存在し、これを使用して効率的な方法でサブスクライバに課金できます。さまざまなクォータメカニズムにより、エンドユーザーには選択可能な多様なオプションが提供されます。また、サービスプロバイダーはクォータをより効果的に扱えるようになります。

時間クォータ

クレジット制御サーバーは、クライアントとの任意の問い合わせ中に、サブスクライバの CC-Time クォータを送信できます。また、以下で説明するさまざまなメカニズムもあり、これらを時間クォータと組み合わせて使用して、顧客満足度を高めるさまざまな方法を派生させることができます。

- Quota-Consumption-Time：サーバーはオプションで、パケットが受信されない「Quota-Consumption-Time」と等しい期間が経過するか、セッションの終了時かのどちらか早い方で、クォータ消費を停止する必要があることをクライアントに示すことができます。Quota-Consumption-Time に等しいアイドル期間は、報告される使用量に含まれます。クォータは通常、Quota-Consumption-Time 以下の期間のトラフィックギャップ中に消費されます。クォータの消費は、サービスデータフローに属するパケットをさらに受信すると再開されます。

  CCR（Update）/CCA 交換時のパケットフローが許可されており、提供されたクォータの Quota-Consumption-Time AVP 値が以前に提供されたクォータと同じである場合、Quota-Consumption-Time は、この手順で正常に実行されます。たとえば、CCR（U）がトリガーされたときに 10 秒の QCT タイマーのうち 5 秒が経過しており、CCA（U）が 2 秒後に返された場合、QCT タイマーは CCA の受信から 3 秒後に期限切れとなり、新しいクォータでパケットが送信されなかった場合でも、算入されていない残りの 5 秒分の使用量が新しいクォータに対して記録されます。

  サーバーが CCA で QCT を送信しない場合は、クライアントで、ローカルに設定可能なデフォルト値を使用できます。

- 組み合わせクォータ：Discrete-Time-Period（DTP）と Continuous-Time-Period（CTP）は、時間クォータを消費するための Quota-Consumption-Time を拡張および一般化するメカニズムを定義します。
  - DTP と CTP はどちらも、使用されるクォータの時間エンベロープを作成するために使用される「Base-Time-Interval」を使用します。
  - DTP と CTP は、クォータを直線的に消費するのではなく、付与されたクォータを、各 Base-Time-Interval の開始時に、Base-Time-Interval のチャンク単位で段階的に消費します。
  - このアルゴリズムのいずれかが、CCA のサーバーから送信された「Time-Quota-Mechanism」AVP に基づいて選択されます。
  - 使用量のレポートは、クォータの付与中に CCA のサーバーによって送信される Envelope-Reporting AVP によって制御することもできます。この AVP の値に基づいて、使用量を、エンベロープごとの使用量またはその付与の通常の累積使用量として報告できます。

- Discrete-Time-Period：Discrete-Time-Period の長さは Base-Time-Interval によって定義されます。そのため、各時間エンベロープは、1 つの Discrete-Time-Period に正確に対応します。そのため、トラフィックが検出されると、Base-Time-Interval に等しいサイズのエンベロープが作成されます。トラフィックは時間エンベロープを通過できます。トラフィックが Base-Time-Interval を超えると、Base-Time-Interval に等しい別の新しいエンベロープが作成

されます。これは、使用されているクォータがクォータ付与を超えるか、そのクォータのしきい値制限に達するまで続きます。

- Continuous-Time-Period：Continuous-Time-Period メカニズムは、トラフィックを含まない Base-Time-Interval までの（この Base-Time-Interval を含む）時間エンベロープを、トラフィックが発生した連続した Base-Time-Interval から構築します。そのため、前の Base-Time-Interval にトラフィックがあった場合、クォータ消費が時間エンベロープ内で継続されます。エンベロープが閉じられた後のクォータ消費は、エンベロープが閉じられた後の最初のトラフィックでのみ再開されます。CTP のエンベロープには、トラフィックを含まない最後の Base-Time-Interval が含まれます。

  エンベロープのサイズは、パーキングメーターの場合のように一定ではありません。エンベロープの終わりは、過去に遡ることによってのみ判断できます。

- Quota-Holding-Time：サーバーは、Quota-Holding-Time AVP を使用して、付与されたクォータに関連付けられるアイドルタイムアウトを指定できます。この時間にわたって、クォータに関連付けられたトラフィックが観測されない場合、クライアントはトラフィックが停止したことを認識し、クォータがサーバーに返されます。クォータ消費が停止すると、クライアントがクォータホールドタイマーを開始します。これは常にトラフィックの終了時に発生します。つまり、タイマーは各パケットの終了時に再開されます。これは、付与された時間クォータと付与されたボリュームクォータに等しく適用されます。タイマーは、CCR の送信時に停止され、CCA を受信すると、以前に使用された値または Quota-Holding-Time の新しい値（受信した場合）で再初期化されます。

  または、この AVP が存在しない場合、クライアントのローカルに設定可能なデフォルト値が使用されます。Quota-Holding-Time の値がゼロの場合、このメカニズムは使用されません。

- Quota-Validity-Time：サーバーは、クライアントへの問い合わせ中にオプションでクォータの有効時間を送信できます。Validity-Time AVP は、MSCC レベルに存在し、そのカテゴリに存在するクォータ全体に等しく適用されます。クォータは有効時間の終了時に無効になり、CCR-Update が、Used-Service-Units AVP およびレポートの理由（VALIDITY_TIME）とともにサーバーに送信されます。そのカテゴリに存在するクォータ全体が Quota-Validity-Time の有効期限時に無効になり、そのカテゴリのクォータを含む CCA-Update を受信するまで、そのカテゴリのトラフィックが、設定に応じて渡されるかドロップされます。

  ゼロの Validity-Time は無効です。Validity-Time は相対的であり、絶対的ではありません。

  Final-Reporting では、「SN-Remaining-Service-Unit」AVP がエンコードされます。

  「SN-Remaining-Service-Unit」AVP の動作は「Used-Service-Unit」AVP から継承されます。この Final-Reporting は、現在組み込まれている Remaining-Service-Unit AVP にはありません。

ボリュームクォータ

サーバーは、サブスクライバにボリュームクォータを提供するために CC-Total-Octets AVP を送信します。DCCA は現在、アップリンクパケットとダウンリンクパケットに等しく適用され

る CC-Total-Octets AVP のみをサポートしています。アップリンクパケットとダウンリンクパケットの合計が許容されている CC-Total-Octets を超えると、クォータが使い果たされたと見なされます。

CC-Input-Octets と CC-Output-Octets のいずれかまたは両方が指定されている場合、指定に応じて、クォータは CC-Input-Octets と CC-Output-Octets のいずれかまたは両方に対してカウントされます。



重要 CC-Input-Octets と CC-Output-Octets に基づく使用量の制限は、このリリースではサポートされていません。

ユニットクォータ

サーバーは、パケットをユニットとしてカウントするために使用される CC-Service-Specific-Units クォータを送信できます。パケットあたりのユニット数は、設定可能なオプションです。

クォータの付与

Gy の実装では、CC-Total-Octets AVP が存在するときは常に、アップリンクとダウンリンクの両方にボリュームクォータが付与されていることが前提となっています。

Granted-Service-Unit にデータが含まれていない場合、Gy はこれを無効な CCA として扱います。

値がゼロの場合、クォータは付与されなかったと見なされます。

この AVP にデータのないサブ AVP が含まれている場合は、無限クォータと見なされます。

QHT、QCT などのカテゴリに関連する追加パラメータは、有効なボリュームまたは時間の付与を受信した後にカテゴリに設定されます。

サブスクライバに対してデフォルトクォータが設定されている場合、サブスクライバトラフィックを受信すると、デフォルトクォータに対してカウントされます。デフォルトクォータは最初の要求にのみ適用され、セッションの途中に再付与されることはありません。サブスクライバが切断されて再接続されると、最初の要求に対してデフォルトのクォータが再度適用されます。

クォータの要求

特定のカテゴリタイプのクォータは、CCR で Requested-Service-Unit AVP を使用して要求できます。MSCC には、トラフィックのカテゴリに対応する Rating-Group AVP と、Requested-Service-Unit (RSU) AVP がデータなしで入力されます。

Requested-Service-Unit には、具体的な時間または量の付与を要求するために使用される CC AVP を含めることができます。Gy CLI を使用して、カテゴリタイプのクォータを要求できます。

または、CCR-I の特定のカテゴリに関してプリエンプティブにサーバーからクォータを要求することもできます。サーバーがクレジット制御応答を介してプリエンプティブクォータを許可すると、そのカテゴリのトラフィックがヒットした場合にのみクォータが使用されます。クォータは、CLI を使用して、クレジット制御サーバーからプリエンプティブに要求できます。

MSCC AVP は、サーバーの再試行時に CCR-I でスキップされます。対応するクォータの使用状況は、次の CCR-U（USU および RSU を含む MSCC AVP）で報告されます。

クォータの報告

クォータは、次のようなさまざまな理由でサーバーに報告されます。

- Threshold
- QHT の期限切れ
- クォータ枯渇
- 評価条件の変更
- 強制再承認
- 有効期間の期限切れ
- サーバーからのカテゴリインスタンスの終了中の最後

QHT および終了中の最後の場合を除き、上記では Requested-Service-Unit AVP が CCR に存在します。

サーバーにクォータ報告の理由を知らせるために、報告理由が CCR に存在します。理由がすべてのクォータに適用されるか、単一のクォータに適用されるかに応じて、Reporting-Reason AVP が MSCC レベルまたは Used Service Unit（USU）レベルのいずれかに配置されます。

これらの条件のいずれかが満たされると、Reporting-Reason で使用状況を報告する理由、およびトリガーの適切な値（場合に応じて）を示す Multiple-Services-Credit-Control AVP を含む CCR 更新がサーバーに送信されます。しきい値に達した場合でも、DCCA は引き続き、しきい値で定義されたクォータ量を使用できます。

その他すべての報告理由については、クライアントは残りのクォータを破棄し、このカテゴリに一致する以降のユーザートラフィックを破棄するか、ユーザートラフィックの通過を許可するか、設定に従ってトラフィックをバッファします。

Reporting-Reason がレーティング条件の変更である場合、Gy では、CCR の一部として Trigger Type AVP を配置し、報告および再承認要求の原因となったトリガーイベントを示す必要があります。

エンドユーザーサービス拒否の Reporting-Reason は、カテゴリがクレジット管理サーバーによってブラックリストに登録されている場合に発生します。この場合、値がゼロの場合でも、使用されているサービスユニットとともに CCR-U が送信されます。その特定のカテゴリについてサーバーからさらにクォータを受信すると、ブラックリストの登録は削除されます。

サブスクライバに対してデフォルトクォータが設定されている場合、料金設定グループ、または料金設定グループとサービス ID の組み合わせに対して、サブスクライバに対して受信した最初の GSU からデフォルトクォータの通信量が差し引かれます。

デフォルトクォータ処理

- デフォルトクォータが 0 に設定されている場合、データは渡されたり報告されたりしません。
- デフォルトクォータが設定されており、OCS がクォータで応答する前にデフォルトクォータが使い果たされない限り、トラフィックは通過します。初期デフォルトクォータが使用

されると、割り当てられている初期クォータに照らしてカウントされます。割りてられているクォータが実際の使用量よりも少ない場合、実際の使用量が報告され、追加のクォータが要求されます。追加のクォータを使用できない場合、トラフィックは拒否されます。

- OCS が応答でクォータを拒否する前にデフォルトクォータが使い果たされていない場合、OCS 応答後にゲートウェイでトラフィックがブロックされます。この場合でも、ゲートウェイはデフォルトクォータの使用状況を CCR-U（FINAL）または CCR-T で報告します。
- OCS が応答する前にデフォルトクォータが使い果たされ、OCS のデッド状態が宣言されていない場合（上記の使用例 1 の定義を参照）、OCS が応答するまでトラフィックはブロックされます。

しきい値（Thresholds）

Gy クライアントは、次のしきい値タイプをサポートしています。

- Volume-Quota-Threshold
- Time-Quota-Threshold
- Units-Quota-Threshold

しきい値は常に、特定のクォータおよび特定のクォータタイプに関連付けられます。Multiple-Services-Credit-Control AVP では、Time-Quota-Threshold、Volume-Quota-Threshold、および Unit-Quota-Threshold は、オプションの AVP です。

これらは符号なしの数値で表され、時間クォータの単位は秒、ボリュームクォータの単位はオクテット、サービス固有クォータの単位はユニットです。クォータがしきい値に達すると、サーバーに対する追加のクォータの要求がトリガーされます。ユーザートラフィックのフローは、引き続き許可されます。ユーザーに有効なクォータがまだあるため、トラフィックの中断は発生しません。

Gy は、CCR-U を、1 つ以上の User-Service-Unit AVP で報告された使用状況、THRESHOLD に設定された Reporting-Reason、およびデータのない Requested-Service-Unit AVP を含む Multiple-Services-Credit-Control AVP とともに送信します。

複数のタイプのクォータがカテゴリに割り当てられており、それぞれに独自のしきい値が設定されている場合、いずれかのユニットタイプがそのしきい値に達すると、他のユニットタイプが消費されていなくても、しきい値に達したと見なされます。

ボリュームクォータを報告する場合、DCCA は常に、CC-Input-Octets AVP と CC-Output-Octets AVP をそれぞれ使用して、アップリンクとダウンリンクを別々に報告します。

Gy は、CCA で追加のクォータを受け取ると、CCR の送信以降にまだ消費されていないクォータを破棄します。そのため、現在消費可能なクォータの量は、新たに受け取った量から、CCR を最後に送信してから消費された可能性があるクォータを差し引いたものになります。

クォータの再承認の条件

クォータは、次のシナリオでサーバーから再承認/再要求されます。

- しきい値に達した
- クォータが枯渇した

- 有効期間の期限切れ
- 評価条件が変更された：
  - セル ID の変更：GGSN と P-GW の導入にのみ適用されます。
  - LAC の変更：GGSN および P-GW の導入にのみ適用されます。
  - QoS の変更
  - RAT の変更
  - SGSN/サービングノードの変更：GGSN および P-GW の導入にのみ適用されます。

トラフィックフローの破棄、許可、バッファリング

Gy が サーバーからの CCA を待機している場合、その特定のタイプのトラフィックが Gy で発生する可能性があります。パケットに対して実行する必要がある動作は、設定によって決まります。設定に基づいて、トラフィックの通過が許可されるか、サーバーからの CCA を待機している間に破棄またはバッファリングされます。

この動作は、次の場合にクライアントからサーバーへのすべての問い合わせに適用されます。

- その特定のカテゴリのクォータがない
- そのカテゴリの有効性タイマーが期限切れ
- そのカテゴリのクォータを使い果たした
- サーバーからの強制再承認

ユーザートラフィックの許可や破棄に加えて、クォータが使い果たされた場合や、トラフィックをバッファするクォータがない場合に使用できるオプションがあります。これは通常、サーバーが追加のクォータを要求したが、有効なクォータ応答がサーバーから受信されなかった場合に発生します。この場合、ユーザートラフィックはバッファに格納され、サーバーから有効なクォータ応答を受信すると、バッファリングされたトラフィックのパススルーが許可されます。

時間クォータの消費手順

- QCT がゼロ：QCT が非アクティブ化された場合、消費は実時間ベースです。パケットフローがない場合でも、消費は継続します。
- QCT がアクティブ：QCT が CCA にある、またはセッションに対してローカルに設定されている場合、クォータの消費は最初のパケットの到着時にのみ開始されます。クォータは、最後のパケットの到着に QCT の時間を加えた時間まで通常どおり消費され、次のパケットの到着までは消費がパスされます。

  問い合わせの途中に QCT 値が変更された場合、新しい QCT は CCA の受信時から有効になります。たとえば、QCT が CCA で非アクティブ化された場合、パケットフローがなくてもクォータの消費は通常どおり再開します。または、QCT が非アクティブからアクティ

ブ化された場合、クォータの消費は、CCA 後の最初のパケット受信後のみに再開されます。

- QHT がゼロ：QHT が非アクティブ化された場合、それ以上の使用がない（ボリュームクォータについて、かつ時間クォータの QCT を使用）場合において、ユーザーはクォータを無期限に保持します。QHT は CCA と次の CCR の間でアクティブになります。
- QHT がゼロでない：QHT が CCA にある、またはセッションに対してローカルに設定されている場合、QHT のアイドル時間の後に、CCR-Update の送信とクォータ使用状況の報告により、クォータがサーバーに返されます。CCR-U を受信しても、サーバーはクォータを付与しません。QHT タイマーは、CCR の送信時に停止し、QHT が CCA にある場合にのみ再開されます。

  QHT タイマーは、パケットが到着するたびにリセットされます。

エンベロープレポート

サーバーは、標準のクォータ管理に加えて、特定のアクティビティの開始時刻と終了時刻を示す付加的な詳細レポートが必要であると判断する場合があります。サーバーは、適切な値の Envelope-Reporting AVP を使用して CCA を送信することでこのレポートを制御します。DCCA クライアントは、コマンドを受信すると、Quota-Consumption-Time AVP によって制御される一定の期間トラフィックをモニターし、トラフィックが存在していた各 Quota-Consumption-Time の期限について、各期間を単一のエンベロープとしてレポートします。サーバーは、時間のみまたは時間とボリュームについて、エンベロープレポートを要求する可能性があります。クォータについてのサーバーへのレポートは、Envelope-Start-Time と Envelope-End-Time、および使用情報を使用して、Envelope AVP により制御されます。

クレジット制御要求

クレジット制御要求（CCR）は、クォータと承認を要求するためにクライアントからサーバーに送信されるメッセージです。CCR は、MIP セッション確立前と MIP セッション終了時に送信されます。より多くのクォータを要求するためにサービス提供中に送信できます。

- クレジット制御要求 - 初期（CCR-I）
- クレジット制御要求 - 更新（CCR-U）
- クレジット制御要求 - 終了（CCR-T）
- クレジット制御応答（CCA）
- クレジット制御応答 - 初期（CCA-I）
- クレジット制御応答 - 更新（CCA-U）

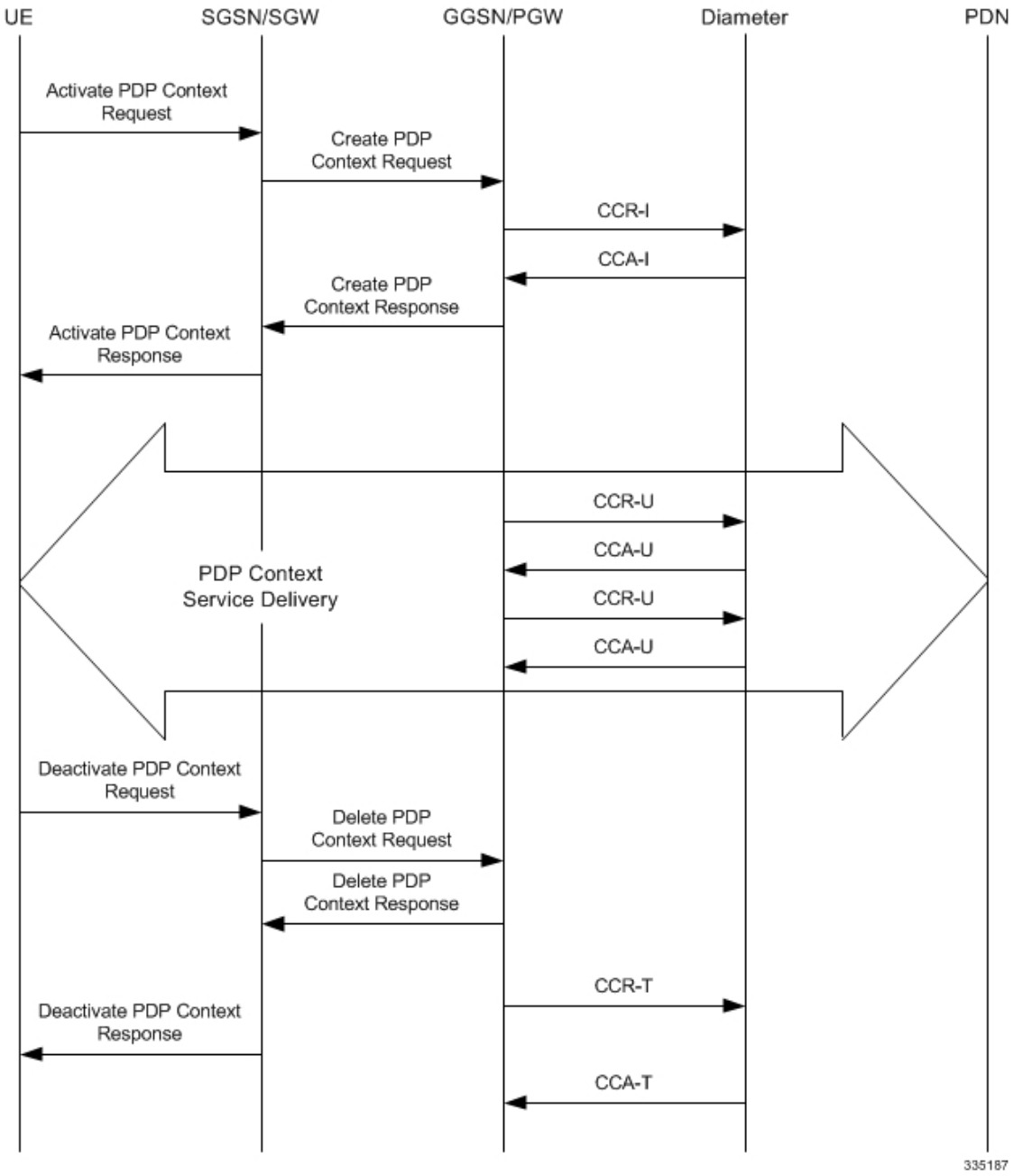
  MSCC AVP が CCA-U に含まれていない場合は、無効な CCA として扱われ、セッションは終了します。
- クレジット制御応答 - 終了（CCA-T）

保留中の更新があるときにコールがクリアされた場合、ゲートウェイは、CCA-U の着信またはタイムアウトの発生（どちらか早い方）を待ちます。

ICSR スイッチオーバー中の監査の失敗によりコールが終了した場合、DCCA は、Gy インターフェイスを介した CCR-T の生成を許可します。

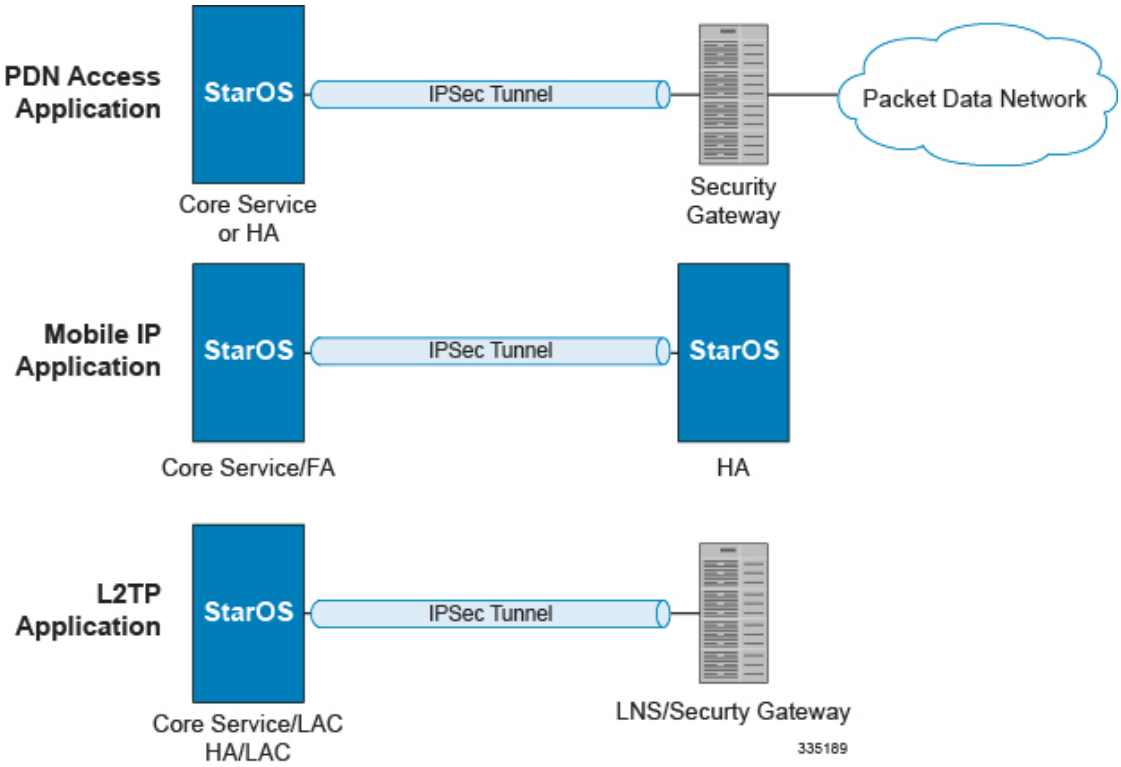
次の図は、GGSN/P-GW/IPSG Gy 実装における単純なコール要求のコールフローを示しています。

図 *68 : GGSN/P-GW/IPSG* の単純なコール要求の *Gy* コールフロー



次の図は、HA Gy 実装における単純なコール要求のコールフローを示しています。

図 *69 : HA* の単純なコール要求の *Gy* コールフロー



Tx タイマーの有効期限切れの動作

タイマーは、CCR がシステムから送信されるたびに開始され、応答は Tx 時間内に到着する必要があります。タイムアウト値は、Diameter クレジット制御コンフィギュレーションモードで設定できます。

Tx 期間内に特定の CCR について Diameter サーバーからの応答がなく、代替サーバーが設定されている場合は、「Tw タイマーの有効期限切れの動作」で説明されているように、Tw の有効期限が切れた後に CCR が代替サーバーに送信されます。

また、これは、以前の要求の Credit-Control-Session-Failover AVP 値にも依存します。この AVP が存在し、FAILOVER_SUPPORTED にコード化されている場合は、クレジット制御メッセージストリームがセカンダリサーバーに移動されます（セカンダリサーバーが設定されている場合）。AVP 値が FAILOVER_NOT SUPPORTED である場合は、セカンダリサーバーが設定されていても、コールは、失敗するとドロップされます。

CCR-U が Gy インターフェイスを介して送信されると、コンテナは、CCA-U を正常に受信した後にのみキャッシュされます。Rf トリガーは、CCA-U メッセージを受信した後にのみ送信されます。

リダイレクト

Final-Unit-Indication AVP では、Final-Unit-Action が REDIRECT の場合や Redirect-Server AVP がコマンドレベルで存在する場合、リダイレクトが実行されます。

リダイレクトは、指定されたカテゴリのクォータ消費の最後に行われます。Gy は RSU や Rating-Group AVP なしで CCR 更新を送信するため、サーバーはこれ以上のクォータを割り当てません。

Final-Unit-Action AVP が RESTRICT_ACCESS の場合は、Restriction-Filter-Rule AVP または Filter-Id AVP の設定に従います。Gy は、使用されたクォータを付けて CCR 更新をサーバーに送信します。

トリガー

Diameter サーバーは、クライアントが特定のカテゴリを再承認する必要があるトリガーを提供できます。トリガーはローカルでも設定できますが、サーバーからの CCA に存在するトリガーがすべて優先されます。



重要 このリリースでは、Gy トリガーは HA ではサポートされません。

サポートされているトリガータイプは次のとおりです。

- SGSN/サービングノードの変更
- QoS の変更 - 任意
- RAT の変更
- LAC の変更
- CellID の変更

トリガータイプで説明されている何らかのイベントが発生すると、クライアントはサーバーとの間でクォータの再承認を行います。レポートの理由は RATING_CONDITION_CHANGE に設定されます。

タリフ時間の変更

サーバーが料金変更メカニズムを適用する必要があることを示した場合は常に、料金変更の時点でアクティブ状態の各カテゴリインスタンスに料金変更メカニズムが適用されます。

デュアルクーポンの概念がサポートされています。このとき、サーバーはタリフ時間の変更を伴う 2 つのクォータを付与します。この場合、最初に付与されたサービスユニットが料金変更時間まで使用され、料金変更時間に達すると、その時点までの使用量が報告されます。追加の使用量は累積されず、2 番目に付与されたサービスユニットが使用されます。

サーバーが、自身が付与したクォータの有効時間内にタリフ変更が発生すると予想している場合、CCA に Tariff-Time-Change AVP を含めます。DCCA は使用量を報告しますが、2 つの Used-Service-Unit AVP を使用することで変更時間をまたぎます。1 つは Turiff-Change-Usage が

UNIT_BEFORE_TARIF_CHANGE に設定され、もう 1 つは Tariff-Change-Usage が UNIT_AFTER_TARFF_CHANGE に設定されます。これはアプリケーションで使用されるユニットのタイプとは無関係です。使用量と時間クォータの両方がこの方法で報告されます。

タリフ時間の変更機能も同様に、Validity-Time AVP を使用して実行されます。Validity-Time は Tariff Time Change に設定され、クライアントが Validity-Time の失効時にクォータを再承認して取得します。これでは特定の時間にサーバーに対して数多くの再承認要求がトリガーされてしまうため、推奨されません。

クライアントへの応答メッセージの Tariff-Time-Usage AVP と Tariff-Time-Change AVP は、Multiple-Services-Credit-Control で定義されたクォータがタリフ時間の変更前または後に使用されることを示します。2 つの個別のクォータの 1 つは Tariff-Time-Change の前、もう 1 つは Tariff-Time-Change の後に割り当てられます。これにより、通信事業者はユーザーに対して期間ごとに異なるクォータを割り当てることができます。この場合、DCCA は更新メッセージ内の使用前と使用後のカウントをサーバーに送信してはいけません。応答メッセージに Tariff-Time-Usage AVP がなく Tariff-Time-Change AVP が存在する場合、クォータは単一クォータメカニズムとして使用されます。クライアントは更新での使用前と使用後のクォータをサーバーに送信する必要があります。

重要 このリリースでは、Gy は UNIT_INDETERMINATE 値をサポートしていません。

StarOS 21.20.22 リリースでは、Tariff-Time-Change AVP のサポートが強化され、Tariff-Time-Change AVP が料金設定グループの Gy から受信された場合に、高速パスの継続的なトラフィックフローとユーザーのトラフィックレートが維持されるようになりました。

最終ユニット通知

Final-Unit-Indication AVP は、特定のクォータがサーバーからの最終クォータであり、AVP で指定された対応するアクションを実行する必要があることを示すために、サーバーからの CCA に存在する場合があります。

コマンドレベルでの最終ユニット通知

現在、Gy はコマンドレベルで FUI AVP をサポートしていません。この AVP がコマンドレベルで存在する場合は無視されます。FUI AVP がコマンドレベルで存在し、Final-Unit-Action AVP が TERMINATE に設定されている場合、Gy は USU AVP 内のすべてのクォータを使用して、クォータの期限切れ時に CCR-Terminate を送信します。

重要 コマンドレベルの FUI AVP は、終了アクションでのみサポートされています。

MSCC レベルでの最終ユニット通知

Final-Unit-Indication AVP が MSCC レベルで存在し、Final-Unit-Action AVP が TERMINATE に設定されている場合、割り当てられたクォータの期限切れ時に CCR 更新が送信され、終了したカテゴリの使用状況がレポートされます。

リダイレクションケースの詳細については、「リダイレクト（893 ページ）」を参照してください。

クレジット制御障害の処理（CCFH）

CCFH AVP は、クライアントとサーバー間に任意のタイプの障害が発生した場合に何を行う必要があるかを定義します。CCFH 機能は設定で定義できますが、CCFH AVP が CCA に存在する場合は、それが優先されます。CCFH AVP は、さまざまな障害処理を柔軟に実施できます。

Gy は、次の障害処理オプションをサポートしています。

- TERMINATE
- CONTINUE
- RETRY AND TERMINATE

フェールオーバーがサポートされている *CCFH*

セカンダリサーバーが設定されていて、CC-Session-Failover AVP が FAILOVER_SUPPORTED に設定されている場合は、次の動作が行われます。

- 終了：CCR-I でいずれかの Tx が期限切れになると、メッセージが破棄され、セッションが切断されます。CCR-Update および Terminate の場合、応答タイムアウト後にメッセージがセカンダリサーバーに送信され、セッションがセカンダリサーバーで続行されます。セカンダリサーバーにも障害が発生した場合、セッションは切断されます。
- 続行：いずれかの Tx が期限切れになると、応答タイムアウト後にメッセージがセカンダリサーバーに送信され、セッションがセカンダリサーバーで続行されます。セカンダリサーバーでも障害が発生した場合、セッションは確立されたままですが、クォータ管理は行われません。
- 再試行と終了：いずれかの Tx が期限切れになると、応答タイムアウト後にメッセージがセカンダリサーバーに送信されます。セカンダリサーバーにも障害が発生した場合、セッションは切断されます。

フェールオーバーがサポートされていない *CCFH*

セカンダリサーバーが設定されていて、CC-Session-Failover AVP が FAILOVER_NOT_SUPPORTED に設定されている場合は、次に示すように以下の動作が行われます。システムにセカンダリサーバーが設定されていない場合も同様です。

- 終了：いずれかの Tx の期限切れ時に、セッションは停止します。
- 続行：いずれかの Tx の有効期限が切れてもセッションは確立されたままですが、クォータ管理は行われません。
- 再試行と終了：いずれかの Tx の期限が切れると、セッションは停止します。

フェールオーバーのサポート

CC-Session-Failover AVP および Credit-Control-Failure-Handling（CCFH）AVP は、CCA-I の CC サーバーによって返される場合があり、フェールオーバー手順を管理するために DCCA によっ

て使用されます。これらがCCAに存在する場合、システムにローカルで設定されているデフォルト値を上書きします。

CC-Session-Failover が FAILOVER_NOT_SUPPORTED に設定されている場合、CC セッションは Diameter 代替サーバーに移動されません。

CC-Session-Failover の値が FAILOVER_SUPPORTED に設定されている場合、Gy は要求が失敗したと見なすと、CC セッションを代替サーバーに移動しようとします。次に例を示します。

- 結果コード「DIAMETER_UNABLE_TO_DELIVER」、「DIAMETER_TOO_BUSY」、または「DIAMETER_LOOP_DETECTED」を受信した場合。
- 要求タイムアウトの有効期限が切れたとき。
- サーバーがクライアントに直接接続されている場合に、DWA を受信せずに Tw が期限切れになったとき。

CCFH は障害時のクライアントの動作を決定します。Tx タイマーが期限切れになると、CCFH 値に基づいて次のアクションが実行されます。

- CONTINUE：中断（遅延応答）に関係なく、関連するカテゴリの MIP セッションとユーザートラフィックの続行を許可します。他のカテゴリのクォータ管理は影響を受けないことに注意してください。
- TERMINATE：MIP セッションを終了します。これは、すべてのカテゴリに影響を及ぼします。
- RETRY_AND_TERMINATE：中断（遅延応答）に関係なく、関連するカテゴリの MIP セッションとユーザートラフィックの続行を許可します。クライアントは送信失敗の状態を確認すると、CCR の送信を再試行します。これも失敗すると、MIP セッションは終了します。

フェールオーバーアクションが試行された後も、引き続き送信失敗や一時的なエラーが発生する場合は、CCFH アクションに応じて、次のアクションが実行されます。

- CONTINUE：MIP セッションの続行を許可します。
- TERMINATE：MIP セッションを終了します。
- RETRY_AND_TERMINATE：MIP セッションを終了します。

リカバリメカニズム

DCCA は、セッションマネージャに障害が発生した場合にデータを大量に失うことなくセッションを回復するために使用されるリカバリメカニズムをサポートしています。定期的な間隔で、また更新などの重要なイベントの発生時に、Gy データが継続的にチェックされます。



重要 DCCA は、ICSR チェックポイントおよびリカバリに関して最大 3 つのベアラー（デフォルトを含む）をサポートします。DCCA で 4 つ以上のベアラーが設定されている場合は、すべてのベアラーについて、チェックポイントがアクティブからスタンバイへと発生します。ただし、リカバリ時には、最初の 3 つのベアラーだけが回復され、残りは、リソースを消費するメモリに残ります。

リカバリメカニズムの詳細については、『*System Administration Guide*』を参照してください。

エラーメカニズム

サポートされているエラーメカニズムは以下のとおりです。

サポートされていない *AVP*

「M」ビットが設定されたサーバーからのサポートされていないすべての AVP は無視されます。

サーバーからの応答が無効

サーバーからの応答が無効な場合、CCFH の設定によって Gy アクションが決まります。

- continue の場合、MIP セッションコンテキストは Gy によってさらに制御されることなく続行されます。
- terminate および retry-and-terminate の場合、MIP セッションは終了し、CCR-T が Diameter サーバーに送信されます。

結果コードの動作

- DIAMETER_RATING_FAILED：このコードを受信すると、Gy は、そのカテゴリのすべてのトラフィックを破棄し、サーバーからのクォータを要求しなくなります。このコードは MSCC レベルでサポートされており、コマンドレベルではサポートされていません。
- DIAMETER_END_USER_SERVICE_DENIED：このコードを受信すると、Gy は該当するカテゴリを一時的にブラックリストに登録し、以降のトラフィックではサーバーからの新しいクォータが要求されます。このコードは MSCC レベルでサポートされており、コマンドレベルではサポートされていません。
- DIAMETER_CREDIT_LIMIT_REACHED：このコードを受信すると、Gy は、該当するカテゴリのすべてのトラフィックを破棄し、設定された時間待機します。その後、同じカテゴリのトラフィックが発生した場合は、サーバーからのクォータを要求します。このコードは MSCC レベルでサポートされており、コマンドレベルではサポートされていません。
- DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE：このコードを受信すると、Gy はセッションの確立を許可しますが、クォータ管理は行われません。このコードは、コマンドレベルでのみサポートされており、MSCC レベルではサポートされていません。

- DIAMETER_USER_UNKNOWN：このコードを受信すると、DCCA はクレジット制御セッションの確立を許可せず、セッションは終了します。この結果コードは、コマンドレベルでのみサポートされており、MSCC レベルではサポートされません。

他のすべての持続的/一時的な障害の場合、Gy アクションは CCFH の設定によって異なります。

サポートされる AVP

Gy 機能では、次の AVP がサポートされています。

- RFC 4006 で規定されている、サポートされている Diameter クレジット制御 AVP
  - CC-Input-Octets（AVP コード：412）：

    Gy は、この AVP を USU でのみサポートしています。
  - CC-Output-Octets（AVP コード：414）：

    Gy は、この AVP を USU でのみサポートしています。
  - CC-Request-Number（AVP コード：415）
  - CC-Request-Type（AVP コード：416）：

    Gy は現在、EVENT_REQUEST 値をサポートしていません。
  - CC-Service-Specific-Units（AVP コード：417）
  - CC-Session-Failover（AVP コード：418）
  - CC-Time（AVP コード：420）：

    Gy は、RSU ではこの AVP をサポートしていません。
  - CC-Total-Octets（AVP コード：421）：

    Gy は、RSU ではこの AVP をサポートしていません。
  - Credit-Control-Failure-Handling（AVP コード：427）
  - Final-Unit-Action（AVP コード：449）：

    Multiple Services-Credit-Control に分類された AVP レベルでサポートされます。コマンドレベルではサポートされません。
  - Last-Unit-Indication（AVP コード：430）：

    Multiple-Services-Credit-Control に分類された AVP レベルでは完全にサポートされ、コマンドレベルでは部分的に（TERMINATE）サポートされます。
  - Granted-Service-Unit（AVP コード：431）
  - Multiple-Services-Credit-Control（AVP コード：456）
  - Multiple-Services-Indicator（AVP コード：455）

- Rating-Group（AVP コード：432）
- Redirect-Address-Type（AVP コード：433）：

  Gy は現在、URL（2）の値のみをサポートしています。
- Redirect-Server（AVP コード：434）
- Redirect-Server-Address（AVP コード：435）
- Requested-Service-Unit（AVP コード：437）
- Result-Code（AVP コード：268）
- Service-Context-Id（AVP コード：461）
- Service-Identifier（AVP コード：439）
- Subscription-Id（AVP コード：443）
- Subscription-Id-Data（AVP コード：444）
- Subscription-Id-Type（AVP Code：450）
- Talf-Change-Usage（AVP コード：452）：

  Gy は UNIT_INDETERMINATE（2）値をサポートしていません。
- Talf-Time-Change（AVP コード：451）
- Used-Service-Unit（AVP コード：446）：

  Gy は、すべての AVP について、最後の CCA-U からの増分カウントのみを送信します。
- User-Equipment-Info（AVP コード：458）
- User-Equipment-Info-Type（AVP コード：459）：

  Gy は現在、IMEISV 値のみをサポートしています。

  Cisco GGSN と P-GW は、デフォルトで IMEISV をサポートしています。
- User-Equipment-Info-Value（AVP コード：460）
- Validity-Time（AVP コード：448）

• 3GPP TS 32.299 で規定されている、サポートされている 3GPP 固有の AVP

- 3GPP-Charging-Characteristics（AVP コード：13）
- 3GPP-Charging-Id（AVP コード：2）
- 3GPP-GGSN-MCC-MNC（AVP コード：9）
- 3GPP-GPRS-QoS-Negotiated-Profile（AVP コード：5）
- 3GPP-IMSI-MCC-MNC（AVP コード：8）

- 3GPP-NSAPI（AVP コード：10）
- 3GPP-PDP-Type（AVP コード：3）
- 3GPP-RAT-Type（AVP コード：21）
- 3GPP-Selection-Mode（AVP コード：12）
- 3GPP-Session-Stop-Indicator（AVP コード：11）
- 3GPP-SGSN-MCC-MNC（AVP コード：18）
- 3GPP-User-Location-Info（AVP コード：22）
- Base-Time-Interval（AVP コード：1265）
- Charging-Rule-Base-Name（AVP コード：1004）
- Envelope（AVP コード：1266）
- Envelope-End-Time（AVP コード：1267）
- Envelope-Reporting（AVP コード：1268）
- Envelope-Start-Time（AVP コード：1269）
- GGSN-Address（AVP コード：847）
- Offline-Charging（AVP コード：1278）
- PDP-Address（AVP コード：1227）
- PDP-Context-Type（AVP コード：1247）

  この AVP は CCR-I にのみ存在します。
- PS-Information（AVP コード：874）
- Quota-Consumption-Time（AVP コード：881）：

  このオプション AVP は、CCA にのみ存在します。
- Quota-Holding-Time（AVP コード：871）：

  このオプション AVP は、CCA コマンドにのみ存在します。これは、Multiple-Services-Credit-Control AVP に含まれています。これは、付与された時間クォータと付与されたボリュームクォータに等しく適用されます。
- Reporting-Reason（AVP コード：872）：

  Gyは現在、POOL_EXHAUSTED（8）値をサポートしていません。現在サポートされていないクレジットプーリングの場合に使用されます。
- Service-Information（AVP コード：873）：

  PS 情報のみサポートされています。
- SGSN-Address（AVP コード：1228）

- Time-Quota-Mechanism（AVP コード：1270）：

  Gy サーバーは、時間クォータを付与するときに、この AVP を Multiple-Services-Credit-Control AVP に含めることができます。

- Time-Quota-Threshold（AVP コード：868）
- Time-Quota-Type（AVP コード：1271）
- Triger（AVP コード：1264）
- Trigger-Type（AVP コード：870）
- Unit-Quota-Threshold（AVP コード：1226）
- Volume-Quota-Threshold（AVP コード：869）

- 3GPP TS 32.299 V8.1.0 で規定されている、サポートされている Diameter AVP
  - Auth-Application-Id（AVP コード：258）
  - Destination-Host（AVP コード：293）
  - Destination-Realm（AVP コード：283）
  - Disconnect-Cause（AVP コード：273）
  - Error-Message（AVP コード：281）
  - Event-Timestamp（AVP コード：55）
  - Failed-AVP（AVP コード：279）
  - Multiple-Services-Credit-Control（AVP コード：456）
  - Origin-Host（AVP コード：264）
  - Origin-Realm（AVP コード：296）
  - Origin-State-Id（AVP コード：278）
  - Redirect-Host（AVP コード：292）
  - Redirect-Host-Usage（AVP コード：261）
  - Redirect-Max-Cache-Time（AVP コード：262）
  - Rating-Group（AVP コード：432）
  - Result-Code（AVP コード：268）
  - Route-Record（AVP コード：282）
  - Session-Id（AVP コード：263）
  - Service-Context-Id（AVP コード：461）

- Service-Identifier（AVP コード：439）
- Supported-Vendor-Id（AVP コード：265）
- Termination-Cause（AVP コード：295）
- Used-Service-Unit（AVP コード：446）
- User-Name（AVP コード：1）

サポートされていない AVP

この項では、サポートされていない AVP を示します。

- RFC 4006 で指定されている、サポート対象外のクレジット制御 AVP：
  - CC-Correlation-Id
  - CC-Money
  - CC-Sub-Session-Id
  - CC-Unit-Type（AVP コード：454）
  - Check-Balance-Result
  - Cost-Information（AVP コード：423）
  - Cost-Unit（AVP コード：445）
  - Credit-Control
  - Currency-Code（AVP コード：425）
  - Direct-Debiting-Failure-Handling（AVP コード：428）
  - Exponent（AVP コード：429）
  - G-S-U-Pool-Identifier（AVP コード：453）
  - G-S-U-Pool-Reference（AVP コード：457）
  - Requested-Action（AVP コード：436）
  - Service-Parameter-Info（AVP コード：440）
  - Service-Parameter-Type（AVP コード：441）
  - Service-Parameter-Value（AVP コード：442）
  - Unit-Value（AVP コード：424）
  - Value-Digits（AVP コード：447）
- 3GPP TS 32.299 V8.1.0 で指定されている、サポート対象外の Diameter AVP：
  - Acct-Application-Id（AVP コード：259）

- Error-Reporting-Host（AVP コード：294）
- Experimental-Result（AVP コード：297）
- Experimental-Result-Code（AVP コード：298）
- Proxy-Host
- Proxy-Info
- Proxy-State

- 3GPP TS 32.299 V8.1.0 で指定されている、サポート対象外の 3GPP 固有 AVP：
  - 3GPP-CAMEL-Charging-Info（AVP コード：24）
  - 3GPP-MS-TimeZone（AVP コード：23）
  - 3GPP-PDSN-MCC-MNC
  - Authorised-QoS
  - Access-Network-Information
  - Adaptations
  - Additional-Content-Information
  - Additional-Type-Information
  - Address-Data
  - Address-Domain
  - Addressee-Type
  - Address-Type
  - AF-Correlation-Information
  - Alternate-Charged-Party-Address
  - Application-provided-Called-Party-Address
  - Application-Server
  - Application-Server-Information
  - Applic-ID
  - Associated-URI
  - Aux-Applic-Info
  - Bearer-Service
  - Called-Asserted-Identity
  - Called-Party-Address
  - Calling-Party-Address
  - Cause-Code
  - Charged-Party
  - Class-Identifier
  - Content-Class
  - Content-Disposition
  - Content-Length
  - Content-Size
  - Content-Type
  - Data-Coding-Scheme
  - Deferred-Location-Event-Type
  - Delivery-Report-Requested

- Destination-Interface
- Domain-Name
- DRM-Content
- Early-Media-Description
- イベント
- Event-Type
- Expires
- File-Repair-Supported
- IM-Information
- IMS-Charging-Identifier（ICID）
- IMS-Communication-Service-Identifier
- IMS-Information
- Incoming-Trunk-Group-ID
- Interface-Id
- Interface-Port
- Interface-Text
- Interface-Type
- Inter-Operator-Identifier
- LCS-APN
- LCS-Client-Dialed-By-MS
- LCS-Client-External-ID
- LCS-Client-ID
- LCS-Client-Name
- LCS-Client-Type
- LCS-Data-Coding-Scheme
- LCS-Format-Indicator
- LCS-Information
- LCS-Name-String
- LCS-Requestor-ID
- LCS-Requestor-ID-String
- Location-Estimate
- Location-Estimate-Type
- Location-Type
- Low-Balance-Indication
- MBMS-Information
- MBMS-User-Service-Type
- Media-Initiator-Flag
- Media-Initiator-Party
- Message-Body
- Message-Class
- メッセージ ID
- メッセージサイズ（Message-Size）
- Message-Type
- MMBox-Storage-Requested
- MM-Content-Type

- MMS-Information
- Node-Functionality
- Number-Of-Participants
- Number-Of-Received-Talk-Bursts
- Number-Of-Talk-Bursts
- Originating-IOI
- Originator
- Originator-Address
- Originator-Interface
- Originator-SCCP-Address
- Outgoing-Trunk-Group-ID
- Participant-Access-Priority
- Participants-Group
- Participants-Involved
- PDG-Address
- PDG-Charging-Id
- PoC-Change-Condition
- PoC-Change-Time
- PoC-Controlling-Address
- PoC-Group-Name
- PoC-Information
- PoC-Server-Role
- PoC-Session-Id
- PoC-Session-Initialtion-Type
- PoC-Session-Type
- PoC-User-Role
- PoC-User-Role-IDs
- PoC-User-Role-info-Units
- Positioning-Data
- 優先順位
- PS-Append-Free-Format-Data（AVP コード：867）：

  PCEF/GWは、オンライン課金セッションに対してPSフリー形式のデータが保存されていない場合、この AVP を無視します。

- PS-Free-Format-Data（AVP コード：866）
- PS-Furnish-Charging-Information（AVP コード：865）
- RAI（AVP コード：909）
- Read-Reply-Report-Requested
- Received-Talk-Burst-Time
- Received-Talk-Burst-Volume
- Recipient-Address
- Recipient-SCCP-Address
- Refund-Information
- Remaining-Balance

- Reply-Applic-ID
- Reply-Path-Requested
- Requested-Party-Address
- Role-of-node
- SDP-Answer-Timestamp
- SDP-Media-Component
- SDP-Media-Description
- SDP-Media-Name
- SDP-Offer-Timestamp
- SDP-Session-Description
- SDP-TimeStamp
- Served-Party-IP-Address
- Service-Generic-Information
- Service-ID
- Service-Specific-Data
- Service-Specific-Info
- Service-Specific-Type
- SIP-Method
- SIP-Request-Timestamp
- SIP-Response-Timestamp
- SM-Discharge-Time
- SM-Message-Type
- SM-Protocol-Id
- SMSC-Address
- SMS-Information
- SMS-Node
- SM-Status
- SM-User-Data-Header
- Submission-Time
- Talk-Burst-Exchange
- Talk-Burst-Time
- Talk-Burst-Volume
- Terminating-IOI
- Time-Stamps
- Token-Text
- Trunk-Group-ID
- Type-Number
- User-Participating-Type
- User-Session-ID
- WAG-Address
- WAG-PLMN-Id
- WLAN-Information
- WLAN-Radio-Container
- WLAN-Session-Id
- WLAN-Technology
- WLAN-UE-Local-IPAddress

PLMN およびタイムゾーンレポート

オンライン課金を実装すると、OCS が PCEF に対してロケーション固有のサブスクライバ情報レポートを要求する場合があります。特定のサブスクライバタイプの場合は、サブスクライバがロケーション、タイムゾーン、サービスネットワークを変更すると、PLMN、タイムゾーン、URI などのサブスクライバ情報が Gy インターフェイスを介して送信されるため、正確なオンライン課金サービスを提供できます。このような情報は、時間および使用量ベースのレポートとは別に報告できます。

PLMN およびタイムゾーンレポート機能が有効になっており、次の条件が満たされている場合、Gx からのトリガーに基づくロケーション イベント レポートがサポートされます。

- クレジット制御が有効になっているルールベースに課金アクションがないため、または Gy セッションの開始が遅延したため、セッションベースの Gy が開始されません。
- PLMN およびタイムゾーンレポート機能は、クレジット制御グループ内で有効になるか、Gx から受信したトリガーの使用によって有効になります。

セッションベースの Gy の開始に失敗した場合、または設定やネットワークの問題が原因でセッションがオフラインになった場合、イベントベースの Gy セッションは開始されません。

重要 障害処理はイベントベースの Gy ではサポートされないことに注意してください。

イベントベースの Gy では、複数のイベントを個別かつ同時に報告できますが、これは現在サポートされていません。以前に報告されたイベントの CCA-Event（CCA-E）の待機中にイベントが発生した場合、新しいイベントはキューに送られ、CCA-E を受信した場合かメッセージがタイムアウトになった場合にのみ報告されます。

PLMN およびタイムゾーンレポート機能を有効にするために、PCRF は CCA のコマンドレベルで Trigger AVP（Trigger Type 1、Trigger Type 2）を送信します。

イベントベースの Gy セッションは、次のシナリオで終了します。

- ベアラー/サブスクライバの終了（サブスクライバレベル Gy）。
- セッションベースの Gy セッションの開始（遅延セッション開始）。
- CCR-E トランザクションが完了すると、それ以降のイベントは報告されません。

この機能の設定方法については、Gy インターフェイス機能を使用する製品のアドミニストレーション ガイドの「*Gy Interface Support*」の章を参照してください。

セッションベース Gy とイベントベース Gy 間のインターワーキング

セッションベース Gy モードとイベントベース Gy モードの両方がアクティブである場合、セッションベース Gy モードが優先されます。つまり、対応するトリガーが有効であれば、すべてのイベントが CCR-U 経由でレポートされます。イベントベース Gy モードは、セッションベース Gy が無効になっており、その存続期間中に該当するセッションに対して以前にアクティブにされたことがない場合にのみアクティブになります。

OCS 到達不能障害処理機能

OCS がダウンした場合、または使用できなくなった場合に対処するには、OCS 到達不能障害処理機能が必要です。この機能は、Gy でのポジティブ想定としても示されます。

OCS は、次のシナリオでは使用不可または到達不能と見なされます。

- PCEF が CCR-U または CCR-I メッセージを送信したものの、指定されたタイムアウト時間までに応答が受信されない
- Diameter ウォッチドッグ要求が現在の RDR に対してタイムアウトし、TCP 接続状態がダウンとマークされる
- Diameter コマンドレベルのエラーコードが CCA で受信される
- PCEF が CCR-T の送信を正常に検証できないときに、ユーザーが切断しているため、PCEF によって暫定クォータが割り当てられない

CLI コマンド **servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code [to end-result-code] } }** を使用してエラー結果コードを設定し、サーバー到達不能モードをトリガーできます。同じ設定を更新要求にも適用できます。この CLI コマンドの詳細については、『*Command Line Interface Reference*』の「*Credit Control Configuration Mode Commands*」の章 [英語] を参照してください。ただし、CLI コマンド **no servers-unreachable behavior-triggers { initial-request | update-request } result-code { any-error | result-code [to end-result-code] }** が設定されている場合は、ハードコードエラーコードのデフォルトセットが適用されます。

デフォルトセットは次のとおりです。

- UNABLE_TO_DELIVER 3002
- UNABLE_TOO_BUSY 3004
- LOOP_DETECTED 3005
- ELECTION_LOST 4003
- 恒久的なエラー 5001 ～ 5999（5002、5003、5031 を除く）。

既存の障害処理メカニズムが強化され、トランスポート接続の障害が原因で OCS に到達不能になった場合や、Diameter 要求メッセージへの応答が遅いため OCS に到達不能であると思われる場合に、暫定ボリュームや暫定時間の事前設定された量をサブスクライバが参照できるようになりました。

この機能の目的は、OCS の障害が発生した場合に Gy ベースのデータセッションをサポートすることです。Diameter クライアントは、ユーザーのデータセッションを一定のクォータの間継続できるようにし、その後、OCS サーバーを再試行して通常の機能の復旧を試みます。この機能により、既存の障害処理メカニズムの精度が向上します。

この機能の導入により、サービス障害中の Gy レポートがサポートされます。OCS の障害が発生した場合、一時的な時間クォータやボリュームクォータがユーザーに割り当てられ、障害期間中に使用されます。

OCS のサービスが再開されると、GW は使用されたすべてのクォータを OCS に報告し、通常の Gy レポートを続行します。

各 DCCA サービスでは、次のオプションに CLI 制御を使用できます。

- 暫定クォータボリューム（バイト単位）およびクォータ時間（秒）。両方の値が同時に適用され（一緒に設定されている場合）、クォータ時間またはクォータボリュームのいずれかが使い果たされると、Diameter クライアントは OCS を再試行します。
- セッションに一時的なクォータを割り当てることができる回数を制限するオプション。ユーザーがこの量を超過すると、セッションは終了するか後払いに切り替えられます。

クォータ値は DCCA サービス設定の一部であり、その DCCA サービスを使用するすべてのサブスクライバに適用されます。一時クォータはボリューム（バイト）や時間（秒）で指定され、両方のクォータ追跡メカニズムを個別にまたは同時に適用できます。

障害処理シナリオで使用するために設定された暫定合計クォータまたは時間をユーザーが消費すると、GW は OCS サーバーを再試行して、機能が復旧されたかどうかを判断します。サービスが復旧された場合、クォータの割り当てと追跡は、標準の使用状況レポート手順に従って続行されます。障害中に使用されたデータが OCS に報告されます。

OCS サービスが復旧されていない場合、GW は設定された量のクォータや時間をユーザーに再割り当てします。OCS がオンラインに戻ると、GW は集積されたすべての使用済みデータを OCS に報告します。複数の再試行と暫定的な割り当てが発生した場合、GW はすべての割り当て期間中に使用されたクォータを報告します。このサイクルは、OCS サービスが正常に復旧されるか、またはクォータ割り当てが最大数に達するまで続行されます。

OCS の到達不能な CLI コマンドのサポートは、Diameter クレジット制御コンフィギュレーション モードで追加されます。

P-GW/XGW/GGSN の場合、この動作は、PCRF によってオンライン課金が有効になっているすべての APN およびサブスクライバに適用されます。HA の場合、この動作は AAA によってオンライン課金が有効になっているすべてのユーザーに適用されます。設定が DCCA サービスに適用されます。

次の拡張機能は、ポジティブ想定 Gy 機能の一部として導入されます。

- エラーコード処理ごとに、ポジティブ想定モードに入るように設定可能
- 5002 エラーを受信したグレースフルセッションの再起動



重要 グレースフルセッション再起動機能はお客様固有のものであることに注意してください。詳細については、シスコのアカウント担当者にお問い合わせください。

エラーコード処理ごとに設定可能

この機能により、お客様は、CLI コマンド「**servers-unreachable behavior-triggers**」を使用してエラー結果コードを設定できます。設定すると、CCR 初期メッセージと CCR 更新メッセージに対して、実行中にポジティブ想定モードの開始がトリガーされます。CCR 終了メッセージは現在サポートされていません。

CLI コマンドを使用して、3xxx ～ 5xxx の範囲にあるエラー結果コードを指定できます。この機能は、エラー結果コードに対してポジティブ想定モードがトリガーされる際のより柔軟で精度の高い方法を実現するために導入されています。

グレースフルセッション再起動

5002エラーコード受信後のグレースフルセッション再起動は、ポジティブ想定状態の間にサーバーが再試行した CCR-U メッセージでサポートされます。また、その時点から CCA-I を受信するまでにサーバーが CCR-U を再試行した後、未報告の使用状況は、同じ使用状況で CCR-U をトリガーすることですぐに報告されます。

重要 グレースフルセッション再起動機能はお客様固有のものであることに注意してください。詳細については、シスコのアカウント担当者にお問い合わせください。

5002 の CCA-U がサーバーから受信されると、保留中の更新はすべて中止されます。また、未報告の使用状況が保留中である場合にのみ、セッションの再起動直後に CCR-U がトリガーされます。

重要 サーバーが 5002 エラー結果コードで応答した場合、要求された料金設定グループに対して付与されたサービスユニットはこの応答に含まれません。

この機能のサポートで導入されたコマンドの詳細については、『*Command Line Interface Reference*』の「*Credit Control Configuration Mode Commands*」の章 [英語] を参照してください。

Gy の OCS 障害レポートの強化

機能説明

Cisco-Event-Trigger-Type AVP が CCA-I、CCA-U、または値が CREDIT_CONTROL_FAILURE（5）の RAR メッセージの PCRF によってインストールされる場合、シスコイベントグループ化 AVP が P-GW によって、OCS 障害コードの正確な値を含む CCR-U メッセージで PCRF に送信されます。このトリガーは、Gy で障害が発生した場合にのみ送信され、設定（クレジット制御障害の処理）に基づいて「続行」アクションが実行され、Gy セッションがオフライン状態に移行します。

この機能強化により、範囲ではなく正確な障害コードが PCRF に報告されます。たとえば、シスコ イベント トリガー タイプが CREDIT_CONTROL_FAILURE（5）で、CCA-U の OCS 障害コードが 3002 の場合、PCRF に送信される CCR-U では、シスコ CC 障害タイプ（グループ化された AVP シスコイベントの一部）が値 3002 で送信されます。

CDR のサーバー到達不能フィールドの追加

機能説明

オンライン課金システム（OCS）がネガティブメッセージを送信すると、ポリシー/課金適用機能（PCEF）と OCS 間のトランスポート接続が失敗します。接続エラーにより、セッションの

確立が失敗し、サブスクライバはサービスを使用できなくなります。接続エラーに対処するために、次の手順が使用されます。

- **障害処理（FH）**：既存のFHメカニズムは、Diameterセッションのフェールオーバーが発生した場合に動作し、システムは接続またはメッセージレベルのエラーが発生したときに、セッションを続行してオフラインに切り替えるか、セッションを終了するかを選択できます。
- **サーバー到達不能（SU）**：この障害処理メカニズムにより、障害時の手順をより詳細に制御できます。このメカニズムは、メッセージレベルおよび接続レベル（トランスポート）の障害後のセッションに加えて、OCSからの応答が遅い場合に使用されます。また、一定の期間セッションを続行するか、クォータを使い切ってから終了するオプションも提供されます。

  設定されたサーバーと暫定クォータ（通信量と時間）を使用するために、セッションがオフラインに変換される前、または終了する前に SU が再試行します。

gtpp attribute servers-unreachable が gtpp グループの下で設定され、SU 機能が有効になっている場合、serversUnreachableContinue または serversUnreachableTerminate を使用して、暫定または最終 CDR で次のプロセスフローが可能になります。

1. SU 障害がトリガーされる。
2. CDR が生成される。
3. コール制御プロファイルの SU 設定に基づいて、生成された CDR に serversUnreachableContinue フィールドまたは serversUnreachableTerminate フィールドが含まれる。

次の表で、CDR 内の serversUnreachable フィールドについて説明します。

表 *82 : CDR* の *ServersUnreachable* フィールド

フィールド名	Description	タグ	Format	**Size**	**ASN1 コード**
serversUnreachableContinue	サーバー到達不能手順が実行されると、 要素が発生します。	256	ブール値	1	0x9f8200
serversUnreachableTerminate	サーバー到達不能手順が実行されると、 要素が発生します。	257	ブール値	1	0x9f8201

表 *83 : ACS* 設定内のサーバー到達不能 *CDR* フィールド

SU の設定	**暫定状態時に SU が検出するフィールド**	**暫定状態の終了後に SU が検出するフィールド**	**SU が検出しないフィールド（Gy との通常のコール）**

server-unreachable initial-request terminate	CDRフィールドが別にトリガーされた場合、SU terminate フィールドは含まれない（暫定 CDR であるため）。 • **SU continue** が **FALSE** • 最終 CDR で **SU Terminate** が **FALSE**	• **SU continue** が **FALSE** • 最終 CDR で **SU Terminate** が **TRUE**	• **SU continue** が **FALSE** • 最終 CDR で **SU Terminate** が **FALSE**
server-unreachable update-request terminate	CDRフィールドが別にトリガーされた場合、SU terminate フィールドは含まれない（暫定 CDR であるため）。 • **SU continue** が **False** • 最終 CDR で **SU Terminate** が **False**	• 暫定 CDR と最終 CDRの両方で **SU continue** が **True** • 最終 CDR で **SU Terminate** が **False**	• **SU continue** が **False** • 最終 CDR で **SU Terminate** が **False**
server-unreachable initial-request continue	• **SU continue** が **False** • 最終 CDR で **SU Terminate** が **False**	• 暫定 CDR と最終 CDRの両方で **SU continue** が **True** • 最終 CDR で **SU Terminate** が **False**	• **SU continue** が **False** • 最終 CDR で **SU Terminate** が **False**
server-unreachable update-request continue	• **SU continue** が **False** • 最終 CDR で **SU Terminate** が **False**	• 暫定 CDR と最終 CDRの両方で **SU continue** が **True** • 最終 CDR で **SU Terminate** が **False**	• **SU continue** が **False** • 最終 CDR で **SU Terminate** が **False**

詳細については、『*SAEGW Administration Guide*』の Gy に関する章を参照してください。

CDR へのサーバー到達不能フィールドの追加

次の設定コマンドを使用して、CDR にサーバー到達不能フィールドを追加します。

```
configure
  context context_name
    gtpp group group_name
```

```
gtpp attribute servers-unreachable
end
```

注：

- **gtpp attribute servers-unreachable**：このオプションを指定すると、CDR にオプションのフィールド **ServersUnreachablesContinue** または **ServersUnreachablesTerminate** が追加されます。

モニタリングおよびトラブルシューティング

ここでは、show コマンドを使用してこの機能を監視およびトラブルシューティングする方法について説明します。

コマンドと出力の表示

このセクションでは、この機能のサポートにおける show コマンドとその出力について説明します。

show gtpp group name <group name>

フィールド	説明
到達不能なサーバーが存在します	サーバーが到達不能な要素の存在を示す「Yes」または「No」を表示します。

バックプレッシャ処理

Diameterベース（Diabase）はアウトバウンドストリームを維持します。アプリケーションがソケットにメッセージを書き込むとき、それらのメッセージのメッセージハンドルがアウトバウンドストリームに保存されます。対応する要求の応答を受信した場合にのみ、保存されているメッセージハンドルがアウトバウンドストリームから削除されます。ASR 5500 はサーバーから受信した応答に基づいてメッセージトランザクションにレート制限を適用するために、アウトバウンドストリームに保存されるメッセージ数の制限を維持します。これは、「max-outstanding <>」CLI を使用して行います（デフォルト値は 256 です）。アプリケーションによって作成されたメッセージの数が未処理の最大数を超えると、Diabase はアプリケーションに「バックプレッシャ」通知を送信し、Diabase から輻輳解消の通知を受信するまで待機してから、再試行するように伝えます。

サーバーからの応答を受信すると、対応する要求メッセージハンドルがアウトバウンドストリームから削除され、アプリケーションが別のメッセージを書き込むためのスロットが作成されます。このスロットの可用性を伝えるために、輻輳解消通知が登録済みのアプリケーションに送信されます。アプリケーションはすべてのセッションをループし、保留中の送信トリガーを処理します。

アプリケーションはシステム内のセッションをループするときに、ソートされた順序でセッションをトラバースし、保留中の CCR-Initial、CCR-Terminate、CCR-Update を送信する必要があるかどうかを各セッションでチェックします。最初のセッションでアウトバンドストリーム

に入るスロットが取得されると、メッセージがストリームに書き込まれます。これで、スロットは満杯状態に戻り、再び未処理数の上限に達します。したがって、残りのセッションは引き続きバックプレッシャ状態のままになります。

Credit-Control-Initial や Credit-Control-Terminate などのバックプレッシャ状態の要求は、セッションの作成や終了と関係があるため、Credit-Control-Update よりも高い優先順位が与えられます。そのため、DCCA には輻輳解消通知に加えて、定期的にメッセージの送信を試みる内部タイマーがあります。したがって、重度のバックプレッシャ状態の場合、CCR-I や CCR-T が送信される確率は CCR-U よりも高くなります。

Gy バックプレッシャの強化

この機能により、メッセージ（バックプレッシャリスト）の作成中にバックプレッシャとなった DCCA セッションのリストを維持でき、現在のポーリング手順が不要になります。また、バックプレッシャされるすべてのタイプのメッセージ（CCR-I、CCR-U、CCR-T、CCR-E）に対して単一のキューが維持されます。メッセージはキューから FIFO の順番に送信されます。

バックプレッシャキューからのセッションを処理した後、DCCA はピアの輻輳ステータスをチェックし、ピアの未処理メッセージのキューに空のスロットがある場合にのみ続行します。

最大未処理数が少なく、ネットワークが輻輳している場合、CPU 使用率は非常に高くなります。

（最大未処理数に達したときに）バックプレッシャにトリガーされた CCR メッセージに関連付けられているすべての DCCA セッションは、ACS マネージャインスタンス（クレジット制御）レベルごとに維持されるバックプレッシャリストに入れられます。

このリストには、入れられるセッション数に関する設定可能な特定の制限はありません。これは、サブスクライバまたは DCCA セッションの数に依存する固有の制限がすでに存在するためです。

この新しい個別のバックプレッシャリストを使用すると、バックプレッシャが高い場合に CPU 使用率が低下します。

GTP ベースの S2a/S2b の Gy サポート

P-GW での Wi-Fi 統合では、GTP ベースの S2a/S2b に Gy サポートが提供されます。この実装は、標準の Rel-11 非 3GPP アクセス仕様 32.399: S5-120748 S5-131017 S5-143090 に準拠しています。

この機能拡張の一部として、次の AVP の変更が導入されました。

- Serving-Node-Type AVP の新しい列挙値として TWAN が追加されました。
- 新しい Diameter AVP「TWAN-User-Location-Info」が追加されました。これはグループ化された AVP で、Trusted WLAN Access Network（TWAN）内の UE ロケーション（アクセスポイントの BSSID および SSID）が含まれます。

TWAN AVP は、3GPP リリース 11 でのみ有効で、標準の Gy ディクショナリにのみ追加されます。つまり、CLI コマンド「**diameter update-dictionary-avps 3gpp-rel11**」が設定されている場合にのみ、TWAN AVP が CCR-I/CCR-U/CCR-T メッセージに含まれます。

ルールと RG 間の関連付けの変更による OOC/ROC の生成

既存の Gy の実装により、同じルールの PCRF に対するクレジット不足/クレジット再割り当て（ROC）レポートの重複が防止されます。異なる料金設定グループを使用した同じルールでのサブスクライバ スロットリングは OOC イベントで機能しません。この問題を解決するため、次の設定の導入を考慮しました。

ある料金設定グループのクレジットが不足すると、その料金設定グループに現在関連付けられているすべてのルールに OOC が送信されます。この動作は、そのルールがすでに OOC になっているかどうかに関係なく実行されます。同様に、OOC 状態になった後に料金設定グループがクォータを取得すると、現在その料金設定グループに現在関連付けられているすべてのルールに ROC が送信されます。この動作は、そのルールがすでに ROC になっているかどうかに関係なく実行されます。

ルールレベルのステータスビットは、同様のバックツーバック OOC/ROC イベントを回避するために使用されなくなりました。今後、OOC/ROC イベントのトリガーは、MSCC の状態とトリガーにのみ依存するようになります。

お客様がルールと RG の関連付けを変更したり、オーバーライド機能を使用したりすると、Gx での OOC/ROC イベントが増加する可能性があります。

CCR のスタティックルールベース

APN とサブスクライバには 1 つのルールベースを適用できますが、CCR メッセージを介して異なるまたは同じルールベースを常に OCS に渡すようスタティックルールベースを設定できます。

CCR AVP「Charging-Rule-Base-Name」で、APN テンプレートまたはサブスクライバテンプレートに存在するルールベース名を上書きおよび変更するために、新しい CLI コマンド「**charging-rulebase-name** *rulebase_name*」がクレジット制御（CC）グループに導入されました。CC グループに設定されたルールベース値は、CCR 経由で OCS に送信されます。この CLI コマンドが設定されていない場合は、APN テンプレートまたはサブスクライバテンプレートから取得されたルールベースが OCS に送信されます。

CC グループに設定されたルールベースの値は、すべての CCR（I/U/T）メッセージで送信されます。これは、セッション中に CC グループのルールベース値が変更されると、これが反映されるのは次の CCR メッセージになることを意味します。

この機能を CLI コマンドでアクティブ化すれば、OCS システムでの企業ごとのサービスの追加や削除といった、サービスの設定に伴う複雑さが軽減されます。

CC ベース選択的 Gy セッション制御

このセクションでは、サブスクライバの課金特性（CC）プロファイルに基づいた選択的 Gy セッション制御機能の概要と導入について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

• 機能説明 （916 ページ）

• CC ベース選択的 Gy セッション制御の設定 （917 ページ）
• 選択的 Gy セッション制御機能のモニタリングと障害対応 （918 ページ）

機能説明

GGSN サービスでは、特定の課金特性（CC）値をプリペイドまたは後払いとして設定できる機能が利用できます。今回、この機能が P-GW サービスに拡張されました。

受信した CC 値に基づいて Gy セッションを有効化または無効化するために、APN 設定が拡張され、CC 値ごとに追加のクレジット制御グループおよびプリペイド禁止値を設定できるようになりました。

cc profile *cc-profile-index* **prepaid prohibited** CLI コマンドは、クレジット制御ベースの課金を無効にする CC 値を設定するために使用されます。この APN を使用する P-GW、GGSN、SAEGW サービス サブスクライバ セッションは、この設定を使用して、OCS への Gy メッセージのトリガーを停止できます。

UE は課金特性値を提供し、アクティブなサブスクライバは APN を介して接続されます。CC インデックスマッピングは、APN で設定されている対応する CC グループおよびプリペイド禁止値に対して行われます。一致すると、Gy セッションは OCS に対して有効または無効になります。

セッションコントローラは、AAA マネージャの APN 設定を保存および更新します。セッションのセットアップ中に、セッションマネージャはセッション認証要求で受信した CC 値を入力し、それを AAA マネージャに送信します。AAA マネージャは、これをローカルに保存された APN 設定と照合し、セッションに必要なクレジット制御グループまたはプリペイド禁止設定を選択します。次に、セッションマネージャは AAA マネージャから受信したこのクレジット制御グループまたはプリペイド禁止情報を ACS マネージャに渡します。

ローカル認証（セッションセットアップ要求）が完了すると、一致する課金特性を持つクレジット制御グループが選択され、使用されます。クレジット制御グループの選択で一致する課金特性設定が見つからない場合は、APN のデフォルトのクレジット制御グループが選択されます。

特定の CC がプリペイドとして設定されている場合、この CC とのセッションは Gy 接続をトリガーしません。セッションの存続期間中の CC の変更は無視されます。

CC ベース Gy セッション制御機能は、セッション確立中に GTP 認証要求を介して受信した CC 値にのみ適用されます。セッションのセットアップ後に AAA または PCRF を介して更新された CC 値により、すでに選択されているクレジット制御グループが変更されることはありません。セッションのセットアップ後にクレジット制御グループが選択されると、この機能は適用されなくなります。

Diameter エラーコードとカウンタ

SaMOG は、さまざまな StarOS プラットフォーム（ASR5500/ASR5700）上の P-GW LBO モジュールを介して、SaMOG（Web 認証）サービスのすべてのトランザクションと Diameter インターフェイスの Diameter エラーコードカウンタをサポートしています。

以下の結果コード固有カウンタは、Gy インターフェイスで OCS（オンライン課金システム）から受信した応答に使用できます。DCCA（Diameter クレジット制御アプリケーション）は、Gy インターフェイスで使用されるプロトコルです。

表 *84 :* 結果コード固有カウンタ

エラーカテゴリ	結果コード	結果コード値
一時的な障害（4XXX）	DIAMETER_END_USER_SERVICE_DENIED	4010
	DIAMETER_CREDIT_LIMIT_REACHED	4012
恒久的なエラー（5XXX）	DIAMETER_RATING_FAILED	5031

他の機能との関係

この機能は、GGSN サービスによって CC プロファイル設定が有効になっている場合にも使用できます。CC プロファイルが APN サービスと GGSN サービスで設定されている場合、サービスに関係なく、一致する CC プロファイルのプリペイド禁止設定が適用されます。

制限事項

この機能には次の制限があります。

- 1 つの課金特性値を 1 つの APN 内の 1 つの credit-control-group/prepaid-prohibited 設定にのみマッピングできます。
- 課金特性に基づく OCS の選択は、セッションのセットアップ中にのみ可能です。credit-control-group が選択されると（セッションセットアップ後）、この機能は適用されません。

CC ベース選択的 Gy セッション制御の設定

ここでは、サブスクライバの CC プロファイルに基づいて Gy セッション制御機能を設定するためのコマンドについて説明します。

CC（Charging Characteristic）値の設定

課金特性（Charging Characteristic）の値を後払い/前払いとして設定して、OCS への Gy セッションを無効/有効にするために、次のコマンドが使用されます。

```
configure
   context context_name
      apn apn_name
        cc-profile { cc_profile_index | any } { prepaid-prohibited |
credit-control-group cc_group_name }
        end
```

注：

- *cc_profile_index*：CC プロファイルインデックスを指定します。*cc_profile_index* は、0 ～ 15 までの整数にする必要があります。
- **any**：このキーワードは、オーバーライドされない任意の cc-profile インデックスに適用されます。このキーワードは、CC プロファイル値の特定の設定に対して最も低い優先度を持ちます。したがって、**any** キーワードを設定しても、APN の他の特定の設定がオーバーライドされることはありません。
- **prepaid-prohibited**：設定されたプロファイルインデックスのプリペイド Gy セッションを無効にします。
- *cc_group_name*：クレジット制御グループの名前を 1 ～ 63 文字の英数字文字列で指定します。
- **no cc-profile** *cc_profile_index*：このコマンドは、設定されている CC プロファイルインデックス値に関係なく、「any」の cc-profile 動作にフォールバックします。

選択的 Gy セッション制御設定の確認

選択的 Gy セッション制御機能の設定を表示または確認するには、Exec モードで次のコマンドを使用します。

```
show configuration
```

選択的 Gy セッション制御機能のモニタリングと障害対応

ここでは、選択的 Gy セッション制御機能のサポートにおける show コマンドおよびその出力について説明します。

show active-charging sessions

show active-charging sessions [callid | imsi | msisdn] コマンド出力の一部として表示される「クレジット制御」フィールドにより、ユーザーは、クレジット制御状態のオンライン課金対応セッションが「オン」かどうか、プリペイド禁止セッションが「オフ」かどうかを判別し、サブスクライバセッションをモニターできます。

ルールベースのクレジット制御グループの設定

このセクションでは、サブスクライバのルールベースに基づくクレジット制御（CC）グループ選択の概要と実装について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

- 機能説明 （919 ページ）
- ルールベースのクレジット制御グループの設定 （920 ページ）
- ルールベースでの CC グループ選択のモニタリングとトラブルシューティング （921 ページ）

機能説明

この機能は、ポジティブ想定シナリオでのさまざまなタイプのサブスクライバの動作をカスタマイズするために導入されました。このカスタマイズは、PCRFによって動的に選択されたルールベースに基づいて、ユーザーが目的のクレジット制御（CC）グループを指定できるようにすることによって実現されます。

通常、ポジティブ想定の動作は、CC グループ内で設定されます。今回、この CC グループ選択機能が、ルールベース設定に拡張されました。

この機能は、IMSA が使用されず、AAA サーバーが認証中に CC グループを送信できず、すべてのサブスクライバに 1 つの APN/サブスクライバプロファイルのみが使用されたシナリオで明示的に必要になります。このような状況において、この機能は、ルールベース内にプレミアム CC グループを提供して、タイプに基づいたサブスクライバに対するプレミアム処理を可能にすることを目的としています。

この機能により、ルールベース設定内に新しい設定可能なオプションが導入され、サブスクライバセッションのセットアップ中にルールベースが選択されるたびに、ユーザーが目的の CC グループを指定できるようになります。この設定された CC グループは、サブスクライバプロファイル/APN 内で設定済みの CC グループを上書きします（それらより高い優先順位を持つ）。AAA または PCRF サーバーが CC-Group AVP を送信すると、AVP を通じて定義された CC グループ値によって、ルールベースで設定された CC グループが上書きされます。

この機能を有効にすると、この設定により、ルールベース名と CC グループ間の関連付けを指定できるようになり、プレミアムサブスクライバの接続時にプレミアムルールベースとプレミアム CC グループが選択されるようになります。

重要 セッション中の設定変更は、システム内の既存のサブスクライバには影響しません。この設定変更は、新しいセッションにのみ影響します。

この新しい設定オプションの実装により、使用可能なクォータに基づいて、サブスクライバのさまざまなタイプのポジティブ想定の動作が有効になります。これにより、プレミアム顧客の優先処理が実現されます。

CC グループの選択の優先順位は、次のように定義されます。

- PCRF で提供される CC グループ
- AAA で提供される CC グループ
- ルールベースで設定された CC グループ
- サブスクライバプロファイル/APN で選択された CC グループ
- デフォルトのクレジット制御グループ



重要 この機能は、認証プロセス中に AAA サーバーが CC グループを送信するオプションがある場合は使用しないでください。認証中に、AAA サーバーが CC グループを送信し、選択されたルールベースに CC グループが定義されている場合は、ルールベースで定義された CC グループが、そのセッション用に選択されます。

制限事項

この機能には制限や制約事項はありません。ただし、CC グループ選択の優先順位に留意することが重要です。

ルールベースのクレジット制御グループの設定

ここでは、サブスクライバのルールベースに基づいてクレジット制御グループを設定するためのコマンドについて説明します。

クレジット制御グループの定義

PCRF によって選択されたルールベースの使用時に、該当するクレジット制御グループ名を設定するには、次のコマンドを使用します。

```
configure
require active-charging
active-charging service service_name
   rulebase rulebase_name
      credit-control-group cc_group_name
      end
```

- *cc_group_name*：クレジット制御グループの名前を 1 ～ 63 文字の英数字文字列で指定します。
- **no credit-control-group**：以前に設定した CC グループをルールベースの設定から削除します。これがデフォルトの設定です。
- この CLI 設定は、セッションのセットアップ中にのみ適用されます。CC グループのセッション中の変更は許可されません。
- これはオプションの CLI 設定であり、カスタマイズされたポジティブ想定の動作がサブスクライバに対して必要な場合にのみ使用されます。
- この CLI コマンドが設定されている場合、CC グループは優先順位に基づいて選択されます。つまり、ルールベースで定義された CC グループは、サブスクライバ/APN プロファイルで指定された CC グループの値よりも優先されます。
- CC グループの設定がルールベースに存在しない場合は、デフォルトのサブスクライバ/APN プロファイルの設定が適用されます。

クレジット制御グループ設定の確認

ルールベースの CC グループの設定を表示または確認するには、Exec モードで次のコマンドを使用します。

```
show configuration verbose
```

ルールベースでの CC グループ選択のモニタリングとトラブルシューティング

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show active-charging sessions full

この show CLI コマンドの出力には、セッションで選択されているクレジット制御グループが表示されます。出力の詳細は、この機能の問題の検証とトラブルシューティングに役立ちます。

show configuration errors コマンドを入力します。

この show CLI では、ルールベース内で設定されているクレジット制御グループが定義されていない場合、エラーが表示されます。

ユーザーが [support record] セクションを指定していない場合は、show configuration verbose

このコマンドでは、ルールベースに指定されている「credit-control-group」オプションが表示されます。トラブルシューティングのために、**show configuration verbose** と **show subscribers full** の出力を、「Radius Access-Accept」を含む **monitor-protocol** の出力とともにキャプチャしてください。

QoS 変更シナリオのための複合 CCR-U トリガー

EPS ベアラー QoS および APN AMBR のデフォルト値が変更されると、P-GW は、アクセス側に、デフォルトベアラーおよび APN AMBR を 1 つのメッセージで変更するための更新要求を送信します。P-GW は、それに応じて APN AMBR とデフォルトのベアラー QoS を適用し、この変更条件に対して Gy に CCR-U を 1 つだけ送信します。



重要 この動作変更は、P-GW コールにのみ適用されます。この変更は、Rf/CDR レコードおよび GGSN/P-GW eHRPD コールには影響しません。

また、この動作は、複数のベアラー更新要求がアクセス側に送信される分割 TFT の場合（QoS + APN AMBR + TFT）には適用されないことに注意してください。

障害後のオフライン Gy セッションの再アクティブ化

この項では、Diameter クレジット制御アプリケーションでの障害の検出時にオフライン Gy セッションを再度有効にする機能について説明します。

この項では、次のトピックについて取り上げます。

機能説明

この機能により、PCRF からの指示に基づいて、オフライン Gy セッションをオンライン課金に戻すためのメカニズムが導入されました。PCRF から Online AVP を受信すると、ゲートウェイは Gy セッションを確立します。

セッションがオフラインとしてマークされると Gy がアクティブ化される設定は存在しませんでした。Diameter クレジット制御アプリケーションで障害が検出されると、設定済みのクレジット制御障害処理（CCFH）アクションが実行されました。Gyセッションが CCFH 続行アクションを実行すると、サブスクライバセッションを再試行/再有効化することはできませんでした。

Charging-Rule-Definition の Online AVP は、CCFH 続行アクションが実行された後、オフライン Gy セッションを有効にするための PCRF からのトリガー/指示と見なされます。PCRF からのコマンドレベルでの Online AVP は、オフライン Gy セッションを有効にするトリガーとは見なされません。3GPP 29.212（リリース 12.12.0）に基づき、Online AVP（1009）は、Charging-Rule-Definition グループ AVP（1003）内のオプションの AVP です。

制限事項と制約事項

ここでは、この機能の制限事項と設定上の制約事項について説明します。

- この機能は、ボリューム クォータ メカニズムのみに限定されます。Quota-Validity-Time（QVT）タイマーおよび Quota-Hold-Time（QHT）タイマーに対して特別な処理は行われません。Gy セッションがオフラインになった後に復帰した場合、これらのタイマーは開始されません。次の CCA-U が OCS からの情報を提供する場合にのみタイマーが開始されます。
- Gy セッションがオンラインとマークされている場合、CDR のクローズは不要です。これは請求システムによって処理されます。
- この機能は、イベントベースのクレジット制御セッションには拡張されません。
- MSCC レベルの障害が原因で CCFH アクションが実行されると、既存の動作が保持され、次の動作が起こります。
  - CCFH 続行：Gy で課金せずにカテゴリ（MSCC）を続行します。これは MSCC に適用されます（セッション全体ではありません）。**show active-charging sessions full** コマンドの出力の MSCC ステータスには「Nocharge」と表示されます。
  - CCFH 終了/リトライと終了：ベアラーが終了されます。
- MSCC レベルで結果コード 4011（DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE）を受信すると、カテゴリは無料とマークされ、このカテゴリに対するそれ以上のアカウンティングは実行されません。この結果コードがコマンドレベルで受信されると、Gy セッションがオフラインになります。オフライン Gy セッションは PCRF の Online AVP を使用して再度オンラインにでき、アカウンティングは正常に再開されます（このセッションの OCS で CCR-U が認識されます）。

- CCFH 継続が設定されている場合に CCR-I 障害が発生すると、次の動作が起こります。
  - Diabase エラー：Diabase エラー（TCP 接続の切断）が発生すると、Gy セッションがオフラインとマークされ、セッション状態が維持されます（セッション ID が作成されます）。Gyセッションを再度有効にすると、新しいCCR-Iが（データを待たずに）すぐに送信されます。
  - 応答タイムアウト：応答タイムアウトが発生したときに、CCR-Iがセッションセットアップで送信され、セッション セットアップ タイムアウトが応答タイムアウトの前に発生した場合、ベアラー自体は終了します。**diameter send-crri traffic-start** 設定は、CCR-Iタイムアウトがベアラーの作成に影響を与えないようにするために、オプションで使用できます。
  - Gyセッションが CCR-I応答のタイムアウトによりオフラインになり、Gyセッションがオンラインとしてマークされている場合、同じセッション ID が使用されます。
  - CCR-I エラー応答が原因で Gy セッションがオフラインになった場合、セッション情報は削除されます（次に使用されるセッション ID は異なります）。
- オンラインルールが既存のベアラーに移動または関連付けられたりするような、ベアラー間（LTE から Wi-Fi またはその逆）でのルール移動が発生した場合、Gy セッションのステータスは変更されません。
- オフラインGyセッションをオンラインにマークするトリガーは、課金ルール定義のPCRFから受信した Online AVP にのみ基づきます。

障害後のオフライン Gy セッションの設定

次の項では、オフライン Gy セッションを再度有効にするための設定コマンドについて説明します。

オフライン Gy セッションの再有効化

障害の後にオフライン Gy セッションを再度有効にするには、次の設定を使用します。

```
configure
  active-charging service service_name
    credit-control
      [ no ] offline-session re-enable
      end
```

注：

- **offline-session re-enable** が設定され、PCRF が、「Online」 AVP 値が 1 に設定されたルールをインストールまたは変更すると、オフラインDCCAはオンラインとマークされます。
- デフォルトの設定は、**no offline-session re-enable** です。この機能はデフォルトで無効になっており、無効になっている場合、**show configuration verbose** コマンドでのみこの設定が表示されます。

設定の確認

オフライン/オンライン状態遷移のタイムスタンプを確認するには、次のコマンドを使用します。

show active-charging sessions full

障害後のオフライン Gy セッションの監視と障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

この機能に関連する障害をトラブルシュートするには、次の操作を実行する必要があります。

- **show active-charging sessions full** コマンドの CLI 出力を確認できます。「Last State Change Time」フィールドは、セッションがオフラインになったタイムスタンプおよびオンラインに戻ったタイムスタンプを示します。
- **monitor subscriber next-call** コマンドからのメッセージを「verbosity 3」で有効にすると、サブスクライバで発生するメッセージ交換を分析できます。
- 「acsmgr」および「debug」レベルのログを有効にして、さらに詳しくデバッグできます。

show active-charging sessions full

次の新しいフィールドがこのコマンドの出力に追加され、状態遷移のタイムスタンプが表示されるようになりました。

- Last State Change Time：
  - オフライン/オンライン：オフラインのタイムスタンプは、Gy セッションがオフラインになると更新されます。オンラインのタイムスタンプは、セッションがオンラインに戻ると更新されます。

AVP の抑制

この機能により、「Gx、Gy、および CDR の MVNO 情報のサポート」機能が強化されます。

機能説明

この機能により、「Gx、Gy、および CDR の MVNO 情報のサポート」機能が強化されます。SAEGW はこれらの AVP を PCRF から受信するたびに、OCS と CDR に Gy メッセージで MVNO-Reseller-ID および MVNO-Subclass-ID AVP を送信します。

この機能強化により、この動作が CLI で制御されるようになり、Gy インターフェイスで送信される AVP を抑制する新しい CLI コマンドが導入されました。

以前の動作：Reseller-id および subclass-id AVP は、ATT ディクショナリの PCRF から同じものを受信すると、Gy で送信されていました。

新しい動作：新しい CLI コマンド **suppress_avp** が追加されました。これにより、Reseller-id と subclass-id AVP を抑制できます。

コマンドの変更

suppress_avp

AVP を抑制するために、クレジット制御グループ コンフィギュレーション モードに新しい CLI コマンドが追加されました。この CLI コマンドを設定すると、MVNO-subclass-id AVP および MVNO-Reseller-Id AVP が抑制されます。

```
configure
  active-charging service <acs_service_name>
    credit-control group <group_name>
      diameter suppress-avp reseller-id subclass-id
     [ no | default ] diameter suppress-avp reseller-id subclass-id

  end
```

注：

- **no:** AVP の抑制を無効にします。PCRF が MVNO-subclassid AVP および MVNO-Reseller-id AVP を Gx インターフェイスで送信するたびに、同じものが Gy メッセージで送信されます。
- **default:** デフォルト設定を設定します。デフォルトでは AVP は抑制されません。PCRF が MVNO-subclassid AVP および MVNO-Reseller-id AVP を Gx インターフェイスで送信するたびに、同じものが Gy メッセージで送信されます。
- **suppress-avp:** MVNO-subclassid AVP および MVNO-Reseller-id AVP の両方を抑制します。
- **reseller-id:** MVNO-Reseller-Id AVP を抑制します。
- **subclass-id:** MVNO-Sub-Class-Id AVP を抑制します。

パフォーマンス指標の変更

show configuration

このコマンドは、以下の出力を表示するように変更されました。

```
credit-control group default
      diameter origin endpoint sundar
      diameter peer-select peer minid1 secondary-peer minid2
      diameter session failover
      diameter dictionary dcca-custom32
      failure-handling initial-request continue
      failure-handling update-request continue
      diameter dynamic-rules request-quota on-traffic-match
      diameter suppress-avp reseller-id subclass-id
```

Gy インターフェイスのサポートの設定

Gy インターフェイスのサポートを設定するには、次の手順を実行します。

手順

ステップ 1 このアドミニストレーション ガイドの説明に従って、コアネットワークサービスを設定します。

ステップ 2 セクション「GGSN/P-GW/IPSG Gy インターフェイスサポートの設定 （926 ページ）」および「HA/PDSN Gyインターフェイスのサポートの設定 （927ページ）」の説明に従って、Gyインターフェイスのサポートを設定します。

ステップ 3 「PLMNおよびタイムゾーンレポートの設定 （928ページ）」の説明に従って、イベントベースのGyのサポートを設定します。

ステップ 4 オプションです。「サーバー到達不能機能の設定 （929 ページ）」の説明に従って、OCS 到達不能障害処理機能または Gy でのポジティブ想定機能を設定します。

ステップ 5 オプションです。「CCR のスタティックルールベースの設定 （930 ページ）」の説明に従って、CCR のスタティックルールベースを設定します。

ステップ 6 オプションです。「GTP ベースの S2a/S2b の Gy の設定 （931 ページ）」の説明に従って、GTP ベースの S2a/S2b の Gy を設定します。

ステップ 7 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイスや、ネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

重要
この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンド、および/またはキーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

GGSN/P-GW/IPSG Gy インターフェイスサポートの設定

GGSN/P-GW/IPSG の標準 Gy インターフェイスサポートを設定するには、次の設定を使用します。

```
configure
     context <context_name>
          diameter endpoint <endpoint_name>
               origin realm <realm>
               origin host <diameter_host> address <ip_address>
               peer <peer> realm <realm> address <ip_address>
               exit
          exit
     active-charging service <ecs_service_name>
          credit-control [ group <cc_group_name> ]
               diameter origin endpoint <endpoint_name>
               diameter peer-select peer <peer> realm <realm>
               diameter pending-timeout <timeout_period>
```

```
                diameter session failover
                diameter dictionary <dictionary>
                failure-handling initial-request continue
                failure-handling update-request continue
                failure-handling terminate-request continue
                exit
          exit
     context <context_name>
           apn <apn_name>
                selection-mode sent-by-ms
                ims-auth-service <service>
                ip access-group <access_list_name> in
                ip access-group <access_list_name> out
                ip context-name <context_name>
                active-charging rulebase <rulebase_name>
                credit-control-group <cc_group_name>
                end
```

注：

- IP アクセスリストの設定の詳細については、『*System Administration Guide*』の「*Access Control Lists*」の章 [英語] を参照してください。
- ECS ruledef 設定の詳細については、『*Command Line Interface Reference*』の「*ACS Ruledef Configuration Mode Commands*」の章 [英語] を参照してください。
- ECS 課金アクション設定の詳細については、『*Command Line Interface Reference*』の「*ACS Charging Action Configuration Mode Commands*」の章 [英語] を参照してください。
- ECS ルールベース設定の詳細については、『*Command Line Interface Reference*』の「*ACS Rulebase Configuration Mode Commands*」の章 [英語] を参照してください。

HA/PDSN Gy インターフェイスのサポートの設定

HA/PDSN Gy インターフェイスのサポートを設定するには、次の設定を使用します。

```
configure
     context <context_name>
          diameter endpoint <endpoint_name>
               origin realm <realm>
               origin host <diameter_host> address <ip_address>
               peer <peer> realm <realm> address <ip_address>
               exit
          exit
     active-charging service <ecs_service_name>
          ruledef <ruledef_name>
               ip any-match = TRUE
               exit
          charging-action <charging_action_name>
               content-id <content_id>
               cca charging credit rating-group <rating_group>
```

```
                exit
          rulebase <rulebase_name>
                action priority <action_priority> ruledef <ruledef_name>
charging-action <charging_action_name>
                exit
          credit-control [ group <cc_group_name> ]
                diameter origin endpoint <endpoint_name>
                diameter peer-select peer <peer> realm <realm>
                diameter pending-timeout <timeout>
                diameter session failover
                diameter dictionary <dictionary>
                failure-handling initial-request continue
                failure-handling update-request continue
                failure-handling terminate-request continue
                pending-traffic-treatment noquota buffer
                pending-traffic-treatment quota-exhausted buffer
                exit
          exit
     context <context_name>
          subscriber default
                ip access-group <acl_name> in
                ip access-group <acl_name> out
                ip context-name <context_name>
                active-charging rulebase <rulebase_name>
                credit-control-group <cc_group_name>
                end
```

注：

- IP アクセスリストの設定の詳細については、『*System Administration Guide*』の「*Access Control Lists*」の章 [英語] を参照してください。
- ECS ruledef 設定の詳細については、『*Command Line Interface Reference*』の「*ACS Ruledef Configuration Mode Commands*」の章 [英語] を参照してください。
- ECS 課金アクション設定の詳細については、『*Command Line Interface Reference*』の「*ACS Charging Action Configuration Mode Commands*」の章 [英語] を参照してください。
- ECS ルールベース設定の詳細については、『*Command Line Interface Reference*』の「*ACS Rulebase Configuration Mode Commands*」の章 [英語] を参照してください。

PLMN およびタイムゾーンレポートの設定

PLMN およびタイムゾーンレポート機能を使用するには、APN またはサブスクライバの設定でクレジット制御グループを定義するか、デフォルトのクレジット制御グループが設定されている必要があります。次の CLI コマンドを使用して、PLMN およびタイムゾーンレポート機能を有効または無効にすることができます。

サブスクライバテンプレートを介して PLMN およびタイムゾーンレポートを有効にするには、次の設定を使用します。

```
configure
     context <context_name>
          subscriber name <subscriber_name>
               dns primary <primary_ipaddress>
               dns secondary <secondary_ipaddress>
               ip access-group test in
               ip access-group test out
               ip context-name <context_name>
               credit-control-client event-based-charging
               active-charging rulebase <rulebase_name>
               exit
               end
```

注：

- **credit-control-client event-based-charging** コマンドを使用して、PLMN およびタイムゾーンレポートを有効にする必要があります。

  PLMN およびタイムゾーンレポート機能の設定に関する詳細については、『*Command Line Interface Reference*』を参照してください。

APN テンプレートを介して PLMN およびタイムゾーンレポートを有効にするには、次の設定を使用します。

```
configure
     context <context_name>
          apn <apn_name>
               selection-mode sent-by-ms
               accounting-mode none
               ip access-group test in
               ip access-group test out
               ip context-name <context_name>
               ip address pool name<pool_name>
               credit-control-client event-based-charging
               active-charging rulebase <rulebase_name>
               exit
               end
```

ディクショナリ、エンドポイントなどのイベントベースの Gy に必要な残りのパラメータは、クレジット制御グループから選択されます。

CLI コマンドを介してトリガーが設定され、さらに別のトリガーセットを Gx から受信するシナリオでは、Gx からのトリガーが優先されます。

サーバー到達不能機能の設定

サーバー到達不能機能では、障害処理動作を Diameter クレジット制御の設定で定義する必要があります。次の CLI コマンドを使用して、OCS 到達不能障害処理機能を有効または無効にすることができます。

OCS 到達不能障害処理機能を有効にするには、次の設定を使用します。

```
configure
require active-charging
         active-charging service <service_name>
              credit-control
                servers-unreachable { initial-request | update-request
 } { continue | terminate }  [ { after-interim-volume <bytes> |
after-interim-time <seconds> } +   server-retries <retry_count> ]
                  servers-unreachable behavior-triggers {
initial-request | update-request } transport-failure [ response-timeout
 | tx-expiry ]
                 servers-unreachable behavior-triggers initial-request
 { result-code { any-error | result-code [ to end-result-code ] } }
                  servers-unreachable behavior-triggers update-request
 { result-code { any-error | result-code [ to end-result-code ] } }
                 end
```



重要 **configure**、**require active-charging** 、**active-charging service** <*service_name*>、および **credit-control** CLI コマンドを設定した後、設定を保存し、シャーシをリロードしてコマンドを有効にする必要があります。設定ファイルを保存してシャーシをリロードする方法については、使用している展開の『*System Administration Guide*』を参照してください。

注：

- この CLI コマンド「**servers-unreachable { initial-request | update-request } { continue | terminate } [{ after-interim-volume ...**」を使用すると、次の方法で interim-volume と interim-time を設定できます。
  - after-interim-volume <bytes> 単独で server-retries が続く。
  - after-interim-time <secs> 単独で server-retries が続く。
  - after-interim-volume <bytes> after-interim-time <secs> に server-retries が続く。
- この CLI コマンド「**servers-unreachable behavior-triggers**」を使用して、Tx の有効期限切れまたは応答タイムアウトのいずれかでサーバー到達不能障害処理をトリガーします（この CLI は「**failure-handling update-request continue retry-after-tx-expiry**」コマンドの retry-after-tx-expiry に似ています）。
- この CLI コマンド「**servers-unreachable behavior-triggers initial-request { result-code { any-error | result-code [to end-result-code] } }**」は、設定された Diameter エラー結果コードに基づいて、サーバー到達不能障害処理をトリガーするために使用されます。

この機能の設定に関する詳細については、『*Command Line Interface Reference*』[英語] を参照してください。

CCR のスタティックルールベースの設定

ルールベース名の静的設定を CCR メッセージを介して OCS に渡すことができるようにするには、次の設定を使用します。

```
configure
    require active-charging
    active-charging service service_name
         credit-control group  ccgroup_name
              charging-rulebase-name rulebase_name
              no charging-rulebase-name
              end
```



重要 **configure**、**require active-charging**、**active-charging service** *service_name*、および **credit-control group** *ccgroup_name* CLI コマンドを設定した後、設定を保存してから、コマンドのシャーシをリロードして有効にします。設定ファイルを保存してシャーシをリロードする方法については、使用している展開の『*System Administration Guide*』を参照してください。

注：

- デフォルトでは、APN/サブスクライバテンプレートから取得されたルールベースは、CCR メッセージを介して OCS に送信されます。

この機能の設定に関する詳細については、『*Command Line Interface Reference*』[英語] を参照してください。

GTP ベースの S2a/S2b の Gy の設定

P-GW で GTP ベースの S2a/S2b の Wi-Fi 統合に Gy サポートを提供するには、次の設定を使用します。

```
configure
    require active-charging
    active-charging service service_name
         credit-control group  ccgroup_name
              diameter update-dictionary-avps 3gpp-rel11
              [  default | no ] diameter update-dictionary-avps
              end
```

注：

- **3gpp-rel11**：標準 Gy ディクショナリ内で 3GPP Rel. 11 固有の AVP のサポートを提供します。

統計情報の収集

ここでは、Gy 関連の統計および設定情報を収集する方法について説明します。

次の表では、最初の列に、収集する統計が示されており、2 つ目の列に、実行するアクションが示されています。

統計/情報	実行するアクション
ECS セッションの完全な統計。	**show active-charging sessions full**

統計/情報	実行するアクション
アクティブ課金サービス（ACS）の詳細情報。	**show active-charging service all**
サービスに設定されているすべてのルール定義に関する情報。	**show active-charging ruledef all**
サービスに設定されているすべての課金アクションに関する情報。	**show active-charging charging-action all**
サービスに設定されているすべてのルールベースに関する情報。	**show active-charging rulebase all**
クレジット制御アプリケーション（DCCA）の統計。	**show active-charging credit-control statistics**
クレジット制御アプリケーション（DCCA）のセッションのステータス。	**show active-charging credit-control session-states [rulebase** <*rulebase_name*> **] [content-id** <*content_id*> **]**



第 45 章

Gy 障害処理の機能強化

- 機能の概要と変更履歴 （933 ページ）
- 機能説明 （934 ページ）
- 機能の仕組み （934 ページ）
- Gy 障害処理の設定 （935 ページ）
- Gy 障害処理のモニタリングと障害対応 （936 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	ASR 5500
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

重要 リリース 21.2 および N5.5 よりも前に導入された機能の改訂履歴の詳細は示していません。

改訂の詳細	リリース
セッションを続行しながらトラフィックをドロップする新しいオプションが、クレジット制御グループに関連付けられている FH テンプレートに導入されました。この機能を実現するために、既存の CLI コマンドが強化されています。	21.3
最初の導入。	21.2 よりも前

機能説明

21.3 よりも前のリリースでは、Gy failure-handling-template（FH-template）に、PDN セッションを保持しながら課金対象トラフィックをブロックするオプションがありませんでした。

21.3 以降のリリースでは、PDN セッションを保持しながら課金対象トラフィックをブロックするために、「continue discard-traffic」オプションが Gy failure-handling-template に追加されました。

機能の仕組み

このセクションでは、この機能の仕組みを簡潔に紹介します。

- セッションを続行しながらトラフィックをドロップする新しいオプションが、クレジット制御グループに関連付けられている FH テンプレートに導入されました。この機能を実現するために、既存の CLI コマンドが強化されています。
- 「Continue discard-traffic」FH アクションが適用されると、指定された DCCA セッションのすべてのトラフィックがブロックされます。DCCA セッションでは、PDN（およびその中に含まれるすべてのベアラー）または特定のベアラーが参照されます。DCCA セッションが対応するベアラーの照合は、FH アクション「続行」のためにそのまま続行されます。オンライン課金が必要なトラフィックだけがドロップされます。
- ルールの変更またはインストールが、純粋なダイナミックルールの PCRF から受信されない限り、「Continue discard-traffic」ステータスが適用されたままになります。オンライン AVP（オンライン = 1）は最終的に PCRF から送信され、指定されたベアラー（サブセッション）の Gy セッションが再開されます。この動作は、credit-control-group コンフィギュレーション モードで使用可能な「offline-session re-enable」CLIに基づいています。
- オンライン課金が必要なすべてのトラフィックがドロップされます。
- 課金アクションが識別され、その課金アクションに「オンライン」課金が必要な場合にのみ、対応するドロップアクションが実行されます。

- サブスクライバの「continue discard-traffic」ステータスは、リカバリ後もそのまま維持されます。Gx が Gy セッションを再度有効にしない限り、リカバリ後にトラフィックはブロックされます。

（注）

- **Gy 障害処理の強化**機能は、*PCRF* への *OCS* 障害レポート（リリース 21.0 で導入）および *Gy* による *OCS* 障害レポートの強化（リリース 21.2 で導入）機能と連携して動作します。詳細については、対応する『*Release Change Reference*』[英語] を参照してください。
- CCFH/FH テンプレートが Continue アクション（またはこの新しい FH テンプレートの「continue-discard」）を使用して設定され、対応するアクションが実行されている場合、PCRF へのレポートは *PCRF* への *OCS* 障害レポート機能に従って発生します。

Gy 障害処理の設定

サブスクライバセッションを保持しながらデータトラフィックを破棄するには、Diameter障害処理テンプレートの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。

```
configure
  failure-handling-template template_name
    msg-type { credit-control-initial | credit-control-terminate |
credit-control-update } failure-type any action continue discard-traffic

    end
```

注：

- **msg-type { credit-control-initial | credit-control-terminate | credit-control-update } failure-type any action continue discard-traffic** CLI コマンドを使用すると、プリペイドサーバーとの通信障害がある場合の動作を指定できます。同じメッセージタイプのテンプレート内に複数の障害処理が存在する場合、直近に発生したエラーに基づいてアクションが適用されます。
- アクション「continue」に「discard-traffic」の拡張機能が追加されました。これにより、サブスクライバセッションを保持している間、データトラフィックがブロックされます。
- 障害処理テンプレートに関連付けられている以前の設定は、**no msg-type { credit-control-initial | credit-control-terminate | credit-control-update } failure-type any** CLI コマンドを使用して削除できます。
- 「discard-traffic」キーワードは「continue」アクションと一緒にのみ設定でき、それぞれの障害発生で影響を受けます。
- このCLIオプションは、デフォルトで無効になっています。それぞれの廃棄アクションが必要な場合は、「discard-traffic」キーワードを明示的に設定する必要があります。

Gy 障害処理のモニタリングと障害対応

ここでは、この機能のモニタリングと障害対応について説明します。

Gy 障害処理の show コマンドと出力

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show active-charging credit-control statistics

この show コマンドの出力が拡張され、この機能をサポートする次の新しいフィールドが表示されるようになりました。

- Action-Drop：

出力例の一部を以下に示します。

```
Failure Handling Stats:
      Action-Terminated:       0            Action-Continue:         0
      Offline Active Sessions: 0            Action-Drop:             0
```



第 46 章

2019 コンプライアンスを遵守するための Gy インターフェイス仕様

- 機能の概要と変更履歴 （937 ページ）
- 機能説明 （938 ページ）
- 機能の仕組み （938 ページ）
- Presence Reporting Area の設定 （940 ページ）
- マルチサブスクリプション ID （941 ページ）
- 拡張帯域幅 QoS の設定 （941 ページ）
- show コマンドと出力 （942 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	すべて（All）
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.23

機能説明

この機能により、Gy インターフェイスの 3GPP 標準規格に準拠するためのプレゼンスレポートエリア（PRA）機能のサポートが追加されます。

プレゼンスレポートエリアは、エリア内の UE のプレゼンスをレポートするために、3GPP パケットドメイン内で定義されたエリアです。これはポリシー制御と課金シナリオに必要です。

現在、PRA 情報が受信されると、P-GW はプレゼンスレポートエリア情報を PCRF に転送します。この情報は OCS（Gy）には送信されません。

P-GW で特定の Gy インターフェイスをサポートするための具体的な要件は次のとおりです。

1. プレゼンスレポートステータス：CCA-I でトリガータイプ 73 が受信されると、P-GW は、S-GW を介して PRA ステータスの変更が報告されるたびに、CCRU/T でのプレゼンスレポートステータスを OCS に送信します。
2. QoS-Information AVP の一部として OCS への CCR メッセージで送信される拡張 QoS パラメータ
3. CCR-T の Enhanced-Diagnostics AVP：CCR-T での RAN-NAS リリース目的のみのレポート
4. 複数のサブスクリプション ID-E.164、IMSI、NAI のサポート

機能の仕組み

1. 次の手順では、Gyインターフェイスの PRA サポートとその関連動作について説明します。

   IP-CAN セッション中、PCRF は、PRA での UE プレゼンスの変更に関するレポートが IP-CAN セッションに必要かどうかを判断します。その後、PCRF は、サブスクライバのプロファイル設定とサポートされている AVP 機能に基づいて決定します。パラメータ CNO-ULI も同様に設定されます。IP-CAN セッションレポートの場合、PCRF は Presence-Reporting-Area-Information AVP を PCEF に提供します。この AVP には、Presence-Reporting-Area-Identifier AVP 内の PRA 識別子が含まれています。UE 専用 PRA の場合、PCRF は、Presence-Reporting-Area-Elements-List AVP 内の PRA で構成される要素のリストを PCEF に提供します。Presence-Reporting-Area-Elements-List は現在サポートされていません。PCRF は、IP-CAN セッション全体の任意の時点で、PCEF での CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT（48）イベントトリガーをサブスクライブし、PRA 内の UE プレゼンスのレポート変更をアクティブにします。

同じ IP-CAN セッションで、OCS は、Presence-Area-Information AVP で UE プレゼンスに OCS への更新が必要かどうかも判断できます。これをサポートするには、「trigger pra」設定を有効にする必要があります。OCS は、PGW への CCA-I の一部として、トリガー AVP でトリガータイプ CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA（73）を送信する必要があります。OCS はまた、CCA-I で Presence-Reporting-Area-Identifier も送信します（PCRF から送信された PRAID と同じであることが前提）。その後、PRA レポートが OCS に送信されます。

PGW は、CCA-I でトリガータイプ 73 を受信すると、S-GW を介して PRA ステータスの変更が報告されるたびに、CCRU/T で Presence-Reporting-Status を OCS に送信します。プレゼンスレポートのサポートは、Gx インターフェイスの CSReq で S-GW に対するプレゼンスアクションの開始と停止を更新するためにすでに利用可能です。Gy インターフェイスでは、同じコントロール プレーン インフラストラクチャが使用されます。Gy インターフェイスのクレジット制御に新しいトリガータイプが導入され、OCS から送信される CCA メッセージでトリガータイプ CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA（73）が処理されるようになりました。

トリガータイプ CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA（73）が Gy インターフェイスで有効になっている場合、PRA-ID は CCA-I または CCA-U で PGW に送信されます。PRA ステータスの変更（PRA の変更を含む MBReq）が発生するたびに、PRA 情報 AVP を含む CCR-U が OCS にも送信されます。

セッションが終了すると、CCR-T には最新の PRA-ID とステータスの詳細とともに PRA 情報 AVP が保持されます。現時点では、同じセッション用であるため、Gx 側と Gy 側が同じ PRA-ID に登録することが前提となっています。また、Gy 側の PRA-ID セッションの登録と登録解除では、すでに Gx 側から処理されているため、PRA の開始と停止を CSReq で SGW に送信しないことが想定されています。Gy 側は、プレゼンスレポートを OCS サーバーに送信する必要があるかどうかを示す PRA-ID のレコードのみを保持します。

2. QoS-Information AVP の一部として OCS への CCR メッセージで送信される拡張 QoS パラメータ

   OCS に送信される QoS-Information AVP に、次の拡張パラメータを含める必要があります。

   1. Extended-Max-Requested-BW-UL
   2. Extended-Max-Requested-BW-DL
   3. Extended-GBR-UL
   4. Extended-GBR-DL
   5. Extended-APN-AMBR-UL
   6. Extended-APN-AMBR-DL

   PCRF が特定のサブスクライバに拡張 QOS パラメータを設定している場合、拡張 QOS パラメータを CCR メッセージで OCS に送信する必要があります。CCR 初期、更新、および終了の一部として送信される新しい AVP は、特定のサブスクライバの PCRF から更新されたポリシーに従って適用されます。

ACSMGR にはベアラーの QoS パラメータに関する情報があり、これは DCCA および最終的には OCS サーバーに情報を送信するために使用されます。

3. CCR-T の Enhanced-Diagnostics AVP：CCR-T での RAN-NAS リリース目的のみのレポート

   Enhanced-Diagnostics AVP（AVP コード 3901）が OCS への CCR-T メッセージで送信され、PCN ノードからのオフライン課金の条件変更 AVP を補完します。RAN-NAS-Release-Cause AVP は、グループ化された AVP の下にあるため、将来的には、他のタイプのリリース原因へと拡張することが可能です。

4. 複数のサブスクリプション ID のサポート：E.164、IMSI、および NAI

   クレジット制御設定では、さまざまなサービスタイプに複数のサブスクリプション ID を有効化する必要があります。

   現在、複数サブスクリプション ID AVP は、ディクショナリおよびサービスタイプのチェックに基づいて Gy CCR にエンコードされます。サブスクリプション ID AVP を使用すると、お客様はさまざまなサービスに必要となるサブスクリプション ID タイプを有効にすることができます。

   各サービスは最大 3 つのサブスクリプション ID タイプ（E164、IMSI、NAI など）を持つことができます。この複数サブスクリプション ID の利点は、DCCA でのそれ以降のディクショナリ追加を最小限に抑えられることです。

Presence Reporting Area の設定

ここでは、この機能をサポートするために使用可能な設定コマンドについて説明します。

- Gx の PRA（cno-uri）の設定
- Gy の PRA の設定

Gx の PRA（cno-uri）の設定

PRA を有効にするには、次の設定コマンドを使用します。

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        { default | no }diameter encode-supported-features cno-uli
  end
```

Gy の PRA の設定

trigger-type PRA を有効にするには、次の設定コマンドを使用します。

```
configure
  active-charging service service_name
    credit-control group group_name
      trigger-type pra
  end
```

注：

- **pra**：プレゼンスレポートエリアの UE プレゼンスの変更を設定します。

マルチサブスクリプション ID

次のコンフィギュレーションコマンドを使用して、さまざまなサービスタイプのサブスクリプション ID を有効にします。

```
configure
  active-charging service service_name
    credit-control-group group_name
      subscription-id service-type closedrp ( e164 | imsi | nai }
  end
```

たとえば、お客様が E.164、IMSI および NAI 値を P-GW サービスの Gy CCR でエンコードすることを希望している場合、以下の CLI をクレジット制御設定モードで設定する必要があります。

```
subscription-id service-type pgw e164 imsi nai
```

注：

- **subscription-id**：サービスタイプのクレジット制御サブスクリプション ID を設定します。
- **service-type**：サービスタイプに基づいてクレジット制御サブスクリプション ID を設定します。
- **closedrp**：closedrp サービスのサブスクリプション ID を設定します。

拡張帯域幅 QoS の設定

拡張帯域幅 QoS を有効にするには、ポリシー制御設定で次の設定コマンドを使用します。

```
configure
          context context_name
            ims-auth-service ims_auth_service_name
              policy-control
                 [ no ]diameter encode-supported-features
extended-bw-newradio
     end
```

show コマンドと出力

show active-charging sessions full all

このコマンドの出力に、以下の新しいフィールドが表示されます。

- Pending Triggers: pra

show active-charging service all | grep pra

このコマンドの出力に、以下の新しいフィールドが表示されます。

- サービス名
- Credit Control
  - Trigger type:pra



第 47 章

異なる RG を使用した異なる DRA からの同時 Gy RAR の処理

- 機能の概要と変更履歴 （943 ページ）
- 機能説明 （944 ページ）
- 機能の仕組み （944 ページ）
- Gy インターフェイスを介した複数の DRA の設定 （945 ページ）
- モニタリングおよびトラブルシューティング （946 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide* • *Command Line Interface Reference*

マニュアルの変更履歴

改訂の詳細	リリース
複数の DRA を処理するための P-GW の Gy インターフェイスの機能拡張。	21.28

機能説明

P-GW に複数の Diameter ルーティングエージェント（DRA）があり、P-GW が同時に複数の再承認要求（RAR）を受信し、それぞれの要求が最後の Diameter 要求とは異なる DRA からの異なる料金設定グループ（RG）を持つ場合、P-GW は、以前のトランザクション（以前の RAR から保留中のクレジット制御要求更新メッセージがあるもの）を中止し、次のクレジット制御要求更新メッセージ（CCR-U）のために同じ cc-request-number を再使用します（新しいピアへのバインド）。

これにより、以前の RAR で受信した RG にクォータが適用されなくなりました。したがって、トラフィックはその料金設定グループまたは service-id wRA には転送されません。

StarOS 21.28 以降のリリースでは、P-GW は、ACS コンフィギュレーション モードで設定可能な CLI コマンド **diameter pending-ccau allow-on-rar-peer-switch** を使用して、異なるピアからの両方の RG を受け入れます。つまり、この CLI を使用すると、Gy インターフェイス上の別のホストまたはピアから受信した RAR の場合に、受信した保留中の CCRU 要求の中止を防ぐように DCCA クライアントを設定できます。

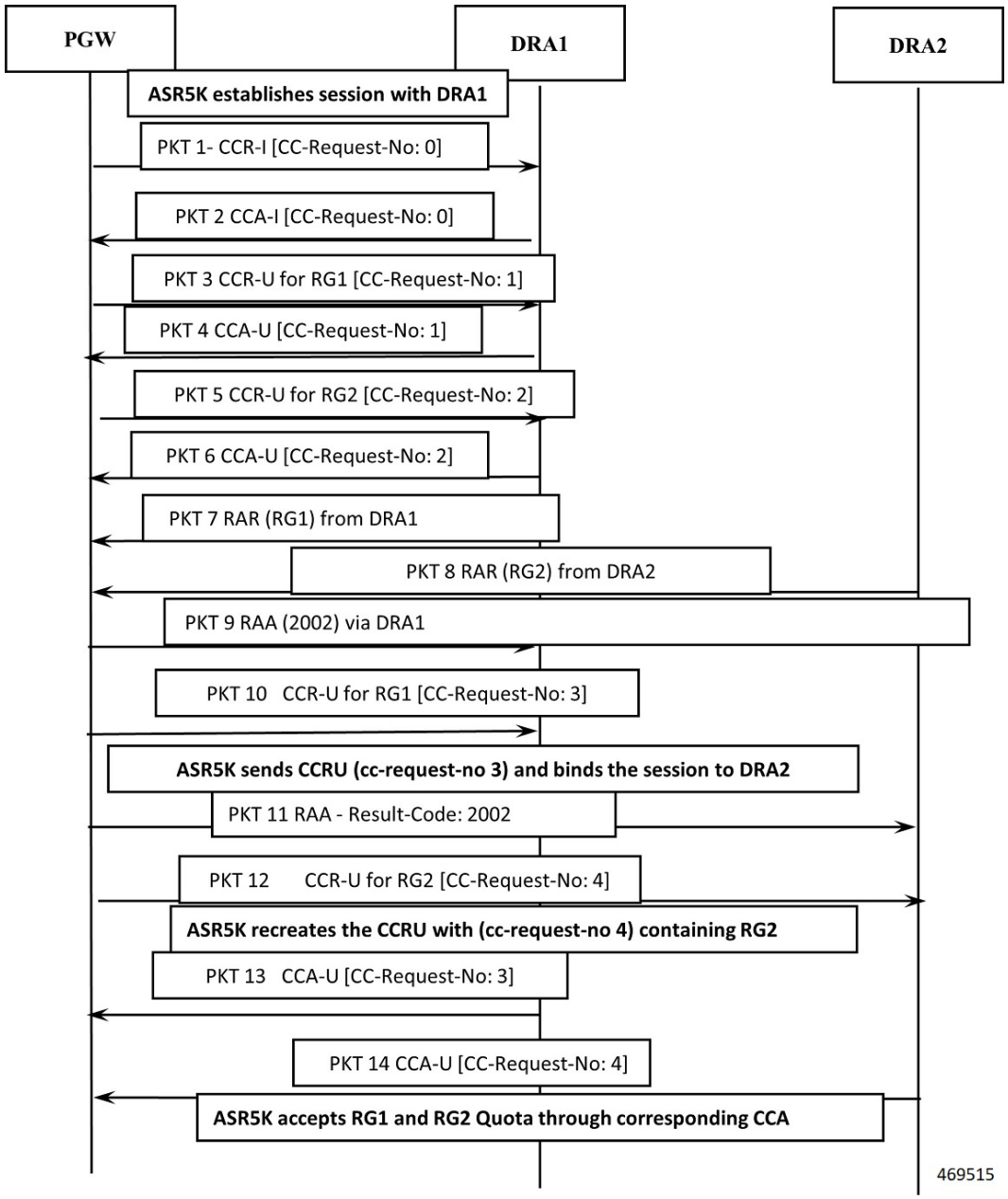
機能の仕組み

以前に保留にしたリクエストを中止する処理が変更されました。現在、DCCA クライアントが保留状態の場合、別のピアを介して RAR を受信すると、DCCA クライアントは（ACS マネージャレベルで）Diameter メッセージを中止します。複数の DRA 機能を処理するための P-GW 上の Gy インターフェイスの機能強化により、P-GW はこの以前に保留されていた要求の中止を回避し、異なるピアからの両方の RG を受け入れるようになりました。

新しいピアまたはホストから新しい RAR を受信した後、P-GW は新しいピアまたはホストへのセッションを更新します。次に、保留状態の Multiple Service Credit Control（MSCC）があるかどうかをチェックし、保留中の CCRU 要求の中止という後続のアクションを回避します。

次のコールフローとプロシージャは、P-GW が異なるピアから両方の RG を受け入れる方法を示しています。

図 *70* : 通話フロー



Gy インターフェイスを介した複数の DRA の設定

異なる DRA を設定するには、次の設定コマンドを使用します。

```
configure
     context context_name
     active-charging service acs_service_name>
```

```
credit-control [ group cc_group_name ]
     diameter dictionary dictionary
    [ no ] diameter pending-ccau allow-on-rar-peer-switch
exit
```

注：

- **diameter dictionary** *dictionary*：さまざまな DRA を処理するように Diameter ディクショナリを設定します。例：**diameter dictionary** *dcca-custom-26*
- **diameter pending-ccau allow-on-rar-peer-switch** ：Gy インターフェイスで異なるホストまたはピアから RAR を受信している場合に、DCCA クライアントが保留中の CCAU 要求を中止するのを防止できます。
- **[no] diameter pending-ccau allow-on-rar-peer-switch** ：保留中の CCAU 要求を DCCA クライアントが中止するのを防止する機能を無効にします。

モニタリングおよびトラブルシューティング

この項では、Gyインターフェイス上の複数のDRAメッセージのモニタリングと障害対応情報について説明します。

コマンドと出力の表示

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show active-charging service all

表 85 : show active-charging service all

フィールド	説明
保留中の CCA-U:	
allow-on-rar-peer-switch	Gyインターフェイス上の別のホストまたはピアからRARを受信した場合での、保留中のCCAU要求の中止が有効か無効かを表示します。この機能が有効になると、この機能は新しい Diameter セッションにのみ適用されます。



第 48 章

HSS および PCRF ベースの P-CSCF 復元のサポート

この機能により、HSS ベースおよび PCRF ベースの P-CSCF 復元のサポートが有効になり、UE が到達不能である時間を最小限に抑えることで、P-CSCF 障害後にコールを終了することができます。

- 機能説明 （947 ページ）
- 機能の仕組み （949 ページ）
- HSS/PCRF ベースの P-CSCF 復元の設定 （958 ページ）
- HSS および PCRF ベースの P-CSCF 復元のモニタリングと障害対応 （961 ページ）

機能説明

P-CSCF の復元手順が標準化され、P-CSCF 障害後のコール終了により UE と通信できなくなる時間が最小限に抑えられました。3GPP 標準規格リリース 13 に準拠して、この機能には次の P-CSCF 復元メカニズムが含まれています。

- 信頼できるまたは信頼できない WLAN アクセス（S2a/S2b）のための HSS ベース P-CSCF 復元
- LTE（S5/S8）および信頼できるまたは信頼できない WLAN アクセス（S2a/S2b）のための PCRF ベース P-CSCF 復元

重要 HSS ベースの P-CSCF 復元は、StarOS リリース 21.0 より前の LTE（S5 または S8）向けの P-GW でサポートされていました。

この機能は、基本と拡張の両方の P-CSCF 復元手順をサポートします。

WLAN での HSS ベースの P-CSCF 復元

P-CSCF 復元メカニズムがサポートされている場合、ゲートウェイは、S6b を介して送信される承認認証要求（AAR）メッセージ内の Feature-List AVP を介して AAA サーバーに復元サポー

トを示します。Feature-List AVP は、Supported-Features grouped AVP の一部です。Feature-List AVP のビット 0 は、WLAN での P-CSCF 復元サポートを示すために使用されます。

P-CSCF 復元中に、3GPP AAA サーバーは、P-GW が WLAN で HSS ベースの P-CSCF 復元をサポートしていることを確認した後、Re-authorization Request（RAR）コマンドで S6b を介して P-GW に P-CSCF 復元指示を送信します。 新しい Diameter AVP 「**RAR-Flags**」は、ビット 1 が設定された RAR メッセージ内にエンコードされ、AAA サーバーが WLAN で HSS ベースの P-CSCF 復元手順の実行を要求していることをゲートウェイに示します。

AAA グループ設定の既存の CLI コマンド **diameter authentication** が拡張され、AAR メッセージ内の Supported-Features AVP の一部として P-CSCF 復元機能をエンコードするようになりました。



重要 Supported-Features は、RAT タイプ WLAN のすべての AAR メッセージで送信されます。すべての AAR で機能のネゴシエーションが必要です。再認証 AAR は、機能の再ネゴシエーションも行います。

S5/S8 の緊急 PDN HSS ベースの P-CSCF 復元は、CLI が P-GW サービスで緊急 PDN の復元をサポートするように設定されている場合に実行されます。

PCRF ベースの P-CSCF 復元

P-CSCF 復元メカニズムをサポートする PCEF は、Supported-Features AVP を介して CCR-I メッセージで復元サポートを示します。Supported-Feature-List AVP の 24 番目のビットは、このメカニズムがサポートされているかどうかを示します。

ポリシー制御設定の既存の CLI コマンド **diameter encode-supported-features** が拡張され、PCRF による P-CSCF 復元機能サポートのネゴシエーションを許可するようになりました。P-CSCF 復元が要求されたことを PCEF に示すために、新しい Diameter AVP 「**PCSCF-Restoration-Indication**」が導入されました。これを行うには、AVP 値を 0 に設定します。

Supported-Features AVP は、すべてのアクセスタイプ（eHRPD、P-GW、GGSN）の CCR-I でネゴシエートされます。ただし、復元トリガーを受信した場合、このトリガーは eHRPD および GGSN では無視されます。

制限事項

- 3GPP 標準仕様に従って、S6b 再承認要求が WLAN の P-CSCF 復元に使用される場合、拡張 P-CSCF 復元のために、ゲートウェイは、必須の AVP のみを含む承認要求を送信できます。ただし、現在の実装では、拡張 P-CSCF 復元に使用される再承認は、通常の再承認の一般的な承認要求です。これには、再承認 AAR のすべての AVP が含まれます。
- P-CSCF FQDN を使用した P-CSCF 再検出中の P-CSCF 復元拡張メカニズムでは、ローカル DNS キャッシュが最初に照会されます。FQDN がローカル DNS キャッシュにすでに存在する場合、DNS クエリは DNS サーバーに送信されず、P-GW はすぐに DNS 応答を取得します。

ローカル DNS キャッシュのフラッシュは行われないため、オペレータはキャッシュを適切に設定する必要があります。

ライセンス

P-CSCF 復元を使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコの営業またはサポート担当者にお問い合わせください。

機能の仕組み

- 復元は、IPv4/IPv6/IPv4v6 コールでサポートされています。
- 拡張機能により、復元サポート UBR は常にデフォルトのベアラーを使用します。
- P-GW は、保存されているどの値も、新しく更新された P-CSCF IP アドレスと比較しません。 DNS で提供または検出された値に依存し、P-CSCF IP アドレスをそのまま転送します。
- P-CSCF の復元は、IMS/非 IMS の APN 設定に関係なく、すべての PDN 接続に対して実行されます。
- 拡張メカニズムの P-CSCF 復元トリガーが受信されると、P-CSCF FQDN で P-CSCF アドレス検出の優先順位が最初になります。FQDN がすでに DNS キャッシュに存在する場合、HSS ベース（S5/S8）P-CSCF 復元の現在の実装に従い、DNS クエリは DNS サーバーに送信されず、P-GW はすぐに DNS 応答を取得します。

  ローカル DNS キャッシュのフラッシュは行われないため、オペレータはキャッシュを適切に設定する必要があります。
- S6b RAR の場合、P-GW は、拡張復元サポートを使用して再認証要求および応答（AAR/AAA）を実行するかどうかの設定をサポートします。

  復元のための RAR 後の認証は、AAA サーバーでの認証シグナリングフローを増大させるため、必須ではありません。RAR 後の認証が必要な既存の Diameter リレーエージェント（DRA）/AAA サーバーとの後方互換性を維持するために、P-CSCF 復元を使用する RAR に対して認証を設定できます。
- FQDN の DNS 解決に失敗した場合、または P-GW に他の方法で P-CSCF アドレスが設定されていない場合、P-GW は、復元時に P-CSCF アドレス PCO/APCO なしで UBR を送信します。
- P-CSCF 復元がすでに進行中の場合、2 番目の復元指示が受信されても、復元が再度実行されることはありません。
- 基本的な P-CSCF 復元の場合、コールは切断理由「ue-pccf-reselect-not-supported (613)」でクリアされます。

- P-GW は、再認証中に S6b P-CSCF FQDN が変更されることを想定していません。S6b 再認証で P-CSCF FQDN が変更されるまれなシナリオでは、新しい FQDN が次の P-CSCF 検出で使用されます。P-CSCF FQDN は、再認証中に変更されると回復されません。
- S6b では、すべての AAR サポート対象機能がネゴシエートされます。再認証 AAR は、機能の再ネゴシエーションも行います。S6b AAA サーバーはすべての AAA で再ネゴシエーションを行うことが想定されています。この設定は、LTE-Wi-Fi およびその逆のハンドオフに特に適用されます。LTE 接続中は、サポート対象機能は送信されません。ただし、Wi-Fi ハンドオフ中は、P-CSCF 復元のサポートを AAR で示す必要があります。
- P-CSCF 復元に関して Gx でサポートされている機能は、ハンドオフシナリオをサポートするために、GGSN/eHRPD コールにも適用されます。
- S6b RAT タイプ WLAN の場合、AAA グループは、サポート対象機能とともに AAR が S6b サーバーに送信されるタイミングを制御する設定をサポートしています。AAA グループがこの機能を無効にしている場合、サポート対象機能が含まれる AAA 応答が受信されると、ネゴシエートされていないと見なされます。そのため、ネゴシエーションは、AAA 処理時のサポート対象機能の CLI 設定に左右されます。
- S6b での P-CSCF 復元に関するサポート対象機能は、RAT タイプ WLAN でのみ使用されます。
- IPv6 レポート S6b 情報の更新中に、情報更新 AAA が保留中で、復元用の RAR が受信された場合、復元のみが処理されます。この場合、拡張された復元に対する再認証は、設定されている場合でも実行されません。
- ePDG での拡張 P-CSCF 復元に関するベアラー更新要求（UBRequest）の APCO が、ベアラーコンテキストレベルで送信されます。APCO は UBRequest のメッセージレベルではありません。
- S6b RAR の再認証が保留中で、復元に関する RAR の受信時に再認証の AAA がまだ受信されていない場合、復元のみが処理されます。この場合、拡張された復元に対する再認証は、設定されている場合でも実行されません。
- PCRF ベースの P-CSCF 復元/HSS ベースの（S2a/S2b）P-CSCF 復元の場合、UE PDN タイプと PCO に要求された P-CSCF アドレスが一致しない場合（たとえば、PDN タイプは IPv4 で、PCO P-CSCF が IPv6 で要求されている場合およびその逆）、基本的な復元が実行されます。
- S5/S8 の UE 機能 PCO および P-CSCF の復元：

P-CSCF 再選択のサポート	要求された P-CSCF アドレス	MME によってトリガーされる復元	PCRF によってトリガーされる復元
✓	✓	拡張された復元	拡張された復元
✓	✗	無視された復元	基本的な復元
✗	✓	基本的な復元	基本的な復元
✗	✗	基本的な復元	基本的な復元

S2a の場合のみ、MCM モード/WPMSI フラグと UE P-CSCF 再選択サポートおよび P-CSCF アドレス要求が受信された場合、拡張 P-CSCF 復元のみが実行されます。他のすべてのシナリオでは、P-CSCF 復元指示が受信されると、基本的な P-CSCF 復元が実行されます。

MCM フラグと SCM フラグの両方が設定されている場合、SCM と見なされます。

S2b の場合のみ、確立中に UE P-CSCF 再選択サポートおよび P-CSCF アドレス要求が受信された場合、またはハンドオフが受信された場合、拡張 P-CSCF 復元のみが実行されます。他のすべてのシナリオでは、P-CSCF 復元指示が受信されると、基本的な P-CSCF 復元が実行されます。

コール フロー

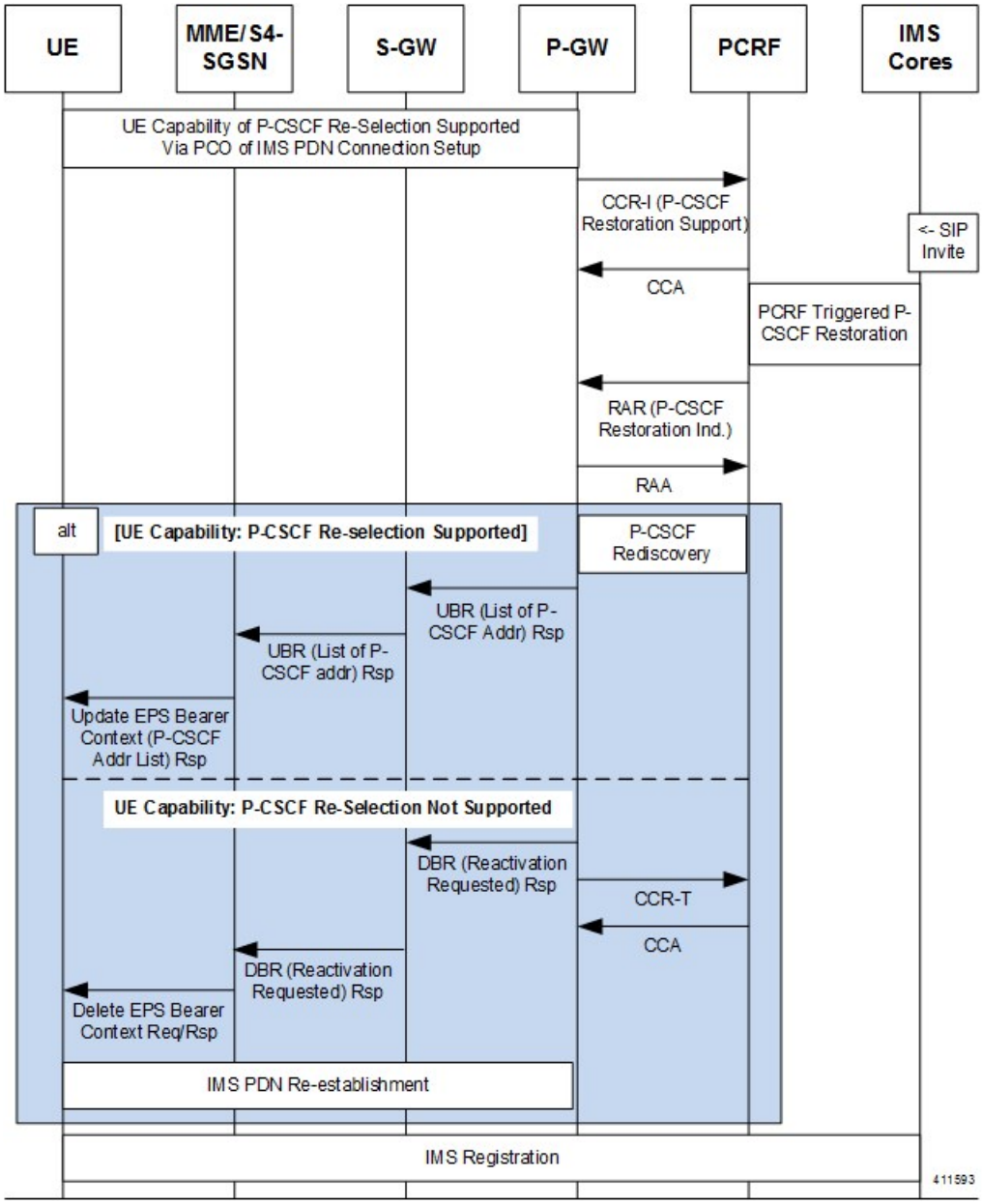
LTE（S5/S8）での PCRF ベースの P-CSCF 復元

PCRF ベースの P-CSCF 復元では、代替 P-CSCF および PCRF を介したパスを利用して、P-CSCF 復元に関する通知が P-GW に送られます。

P-CSCF 復元サポートを処理するメカニズムは 2 つあります。

1. **基本復元サポート**：UE は P-CSCF の再選択をサポートしていません。P-GW は UE に PDN 接続を解放するように通知します。P-GW は、「再アクティブ化が要求された」という理由で、デフォルトベアラーの非アクティブ化手順を開始します。
2. **拡張復元サポート**：P-GW は P-CSCF の再検出後に、代替 P-CSCF アドレスリストが存在する PCO を使用して UBR を送信します。オプションの拡張機能は PDN の非アクティブ化と再アクティブ化を回避し、P-GW に基づいて「P-CSCF 障害での PDP コンテキスト/ベアラーの更新」が UE でサポートされているかどうかを識別します。UE は PDN 接続をアクティブ化するときに、 PCO パラメータで P-GW にこの機能を示します。

図 *71 : PCRF* ベースの *P-CSCF* の復元：*EPC*



WLAN の P-CSCF の復元（S2a/S2b）

ここでは、WLAN アクセスが可能な UE の P-CSCF 復元をサポートするソリューションについて説明します。

P-CSCF 復元サポートを処理するメカニズムは 2 つあります。

1. **基本復元サポート**：HSS ベースのソリューションと PCRF ベースのソリューションの基本的なメカニズムは、PDN 接続の解放と、それに続く UE による新しい IMS 登録をトリガーするための PDN 接続の再確立に依存します。

2. **拡張復元サポート**：信頼できる WLAN および信頼できない WLAN アクセスの拡張メカニズムでは、PDN 接続を解放せず、既存の PDN 接続を介して UE による新しい IMS 登録をトリガーします。

   信頼できる WLAN の拡張メカニズムは、マルチ接続モード（MCM）でのみサポートされます。

TWAN アクセスまたは信頼できない WLAN アクセスの基本的な P-CSCF 復元では、P-GW は PDN 接続を切断するときに、原因「Reactivation requested」を設定します。

WLAN の P-CSCF 復元の目的で再許可要求を使用する場合は、P-CSCF 復元要求ビットのみを RAR フラグに設定する必要があります。

RAR フラグの P-CSCF 復元要求ビットが再許可要求（S6b）で設定されている場合：

- P-GW が拡張 P-CSCF 復元メカニズムをトリガーすると、P-GW は許可要求を送信できます。
- P-GW が P-CSCF 基本復元メカニズムをトリガーすると、P-GW は 3GPP AAA サーバーにセッション終了要求を送信します。

信頼できる WLAN アクセスの場合

- TWAN は、PDN 接続の確立（またはハンドオーバー）時に、S2a を介して WLCP PDN 接続変更の要求手順のサポートをアドバタイズします。これにより、P-GW はこの TWAN で P-CSCF 復元拡張機能を使用できるようになります。
- WLAN を介した PDN 接続の確立（またはハンドオーバー）時に P-GW に割り当てる UE 機能（TWAN アクセス用の P-CSCF 復元拡張の UE サポート）は、PCO IE を介して転送されます。
- P-GW はP-CSCF 復元通知を受信すると、次の場合にこの P-CSCF 復元拡張手順を呼び出すことができます。
  - UE がマルチ接続モードで TWAN を介して EPC にアクセスしている。
  - UE が PCO 経由の TWAN アクセスでこの拡張機能をサポートしていることを示した。
  - TWAN が WLCP PDN 接続変更手順をサポートしていることを示した。
  - UE が接続の確立時やハンドオーバー時に P-CSCF アドレスを要求した。

  上記場合は、基本復元手順が実行されます。
- シングル接続モードまたはトランスペアレントシングル接続モードの信頼できる WLAN では、基本的な P-CSCF 復元メカニズムのみを適用できます。
- TWAN アクセスの P-CSCF 復元拡張手順では、P-GW が PCO IE を使用して、使用可能な P-CSCF のアドレスの最新リストを TWAN 経由で UE に送信します。

図 *72 :* 信頼できる *WLAN* アクセスでの *PCRF* ベースの *P-CSCF* 復元

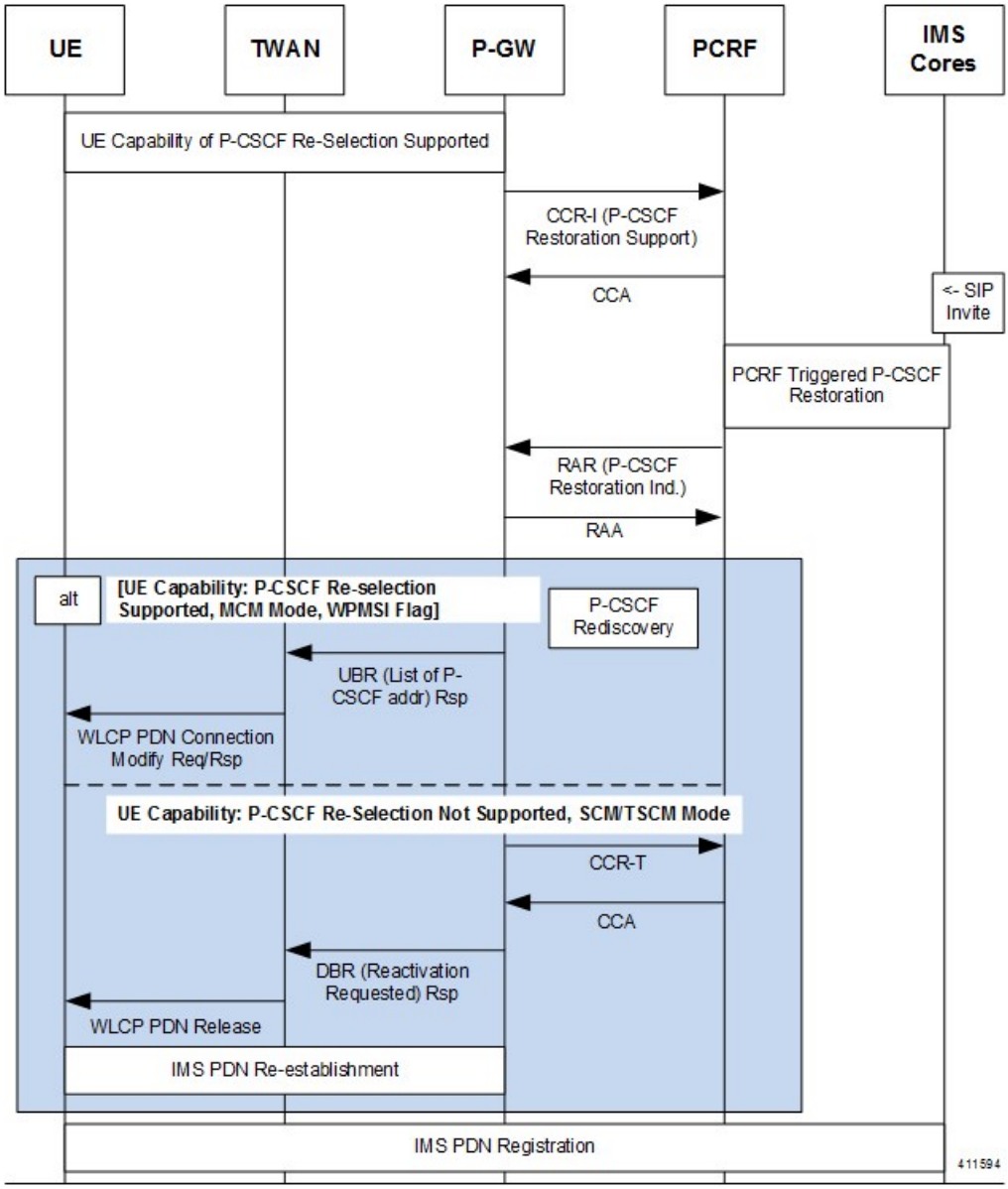
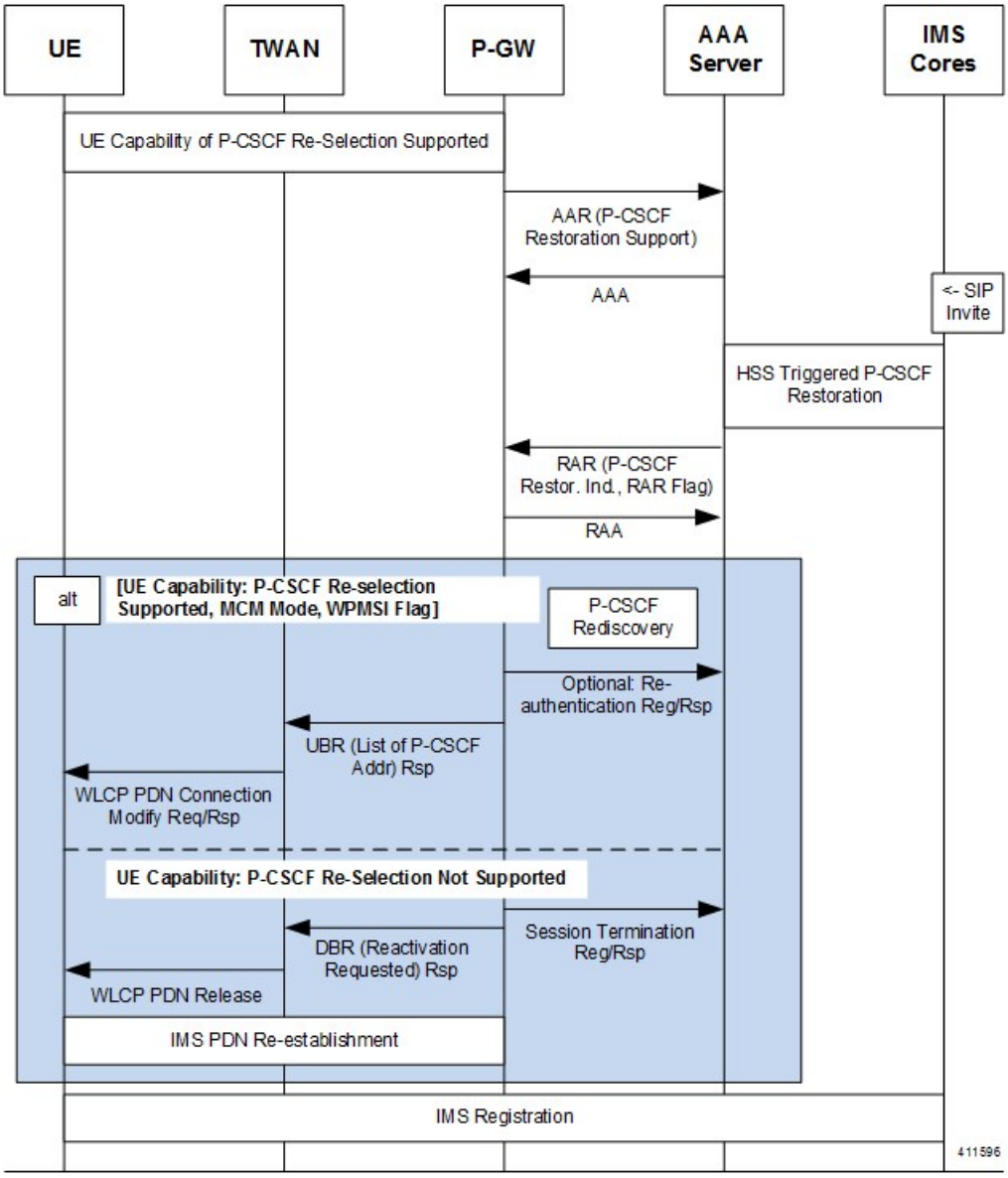


図 *73* : 信頼できる *WLAN* アクセスでの *HSS* ベースの *P-CSCF* 復元



重要 S6b でサポートされている機能は、RAT タイプの WLAN のすべての再認証で送信されます。

信頼できない WLAN アクセスの場合

信頼できない WLAN の P-CSCF 復元拡張機能をサポートする ePDG は、S2b 経由で PDN 接続を確立（またはハンドオーバー）するときに、APCO 情報要素の UE 機能（P-CSCF 復元拡張機能の UE サポート）をS2b インターフェイス経由で P-GW に転送します。

信頼できない WLAN アクセスの P-CSCF 復元拡張手順では、P-GW が APCO IE を使用して、使用可能な P-CSCF のアドレスの最新リストを ePDG 経由で UE に送信します。

図 *74 :* 信頼できない *WLAN* アクセスでの *PCRF* ベースの *P-CSCF* 復元

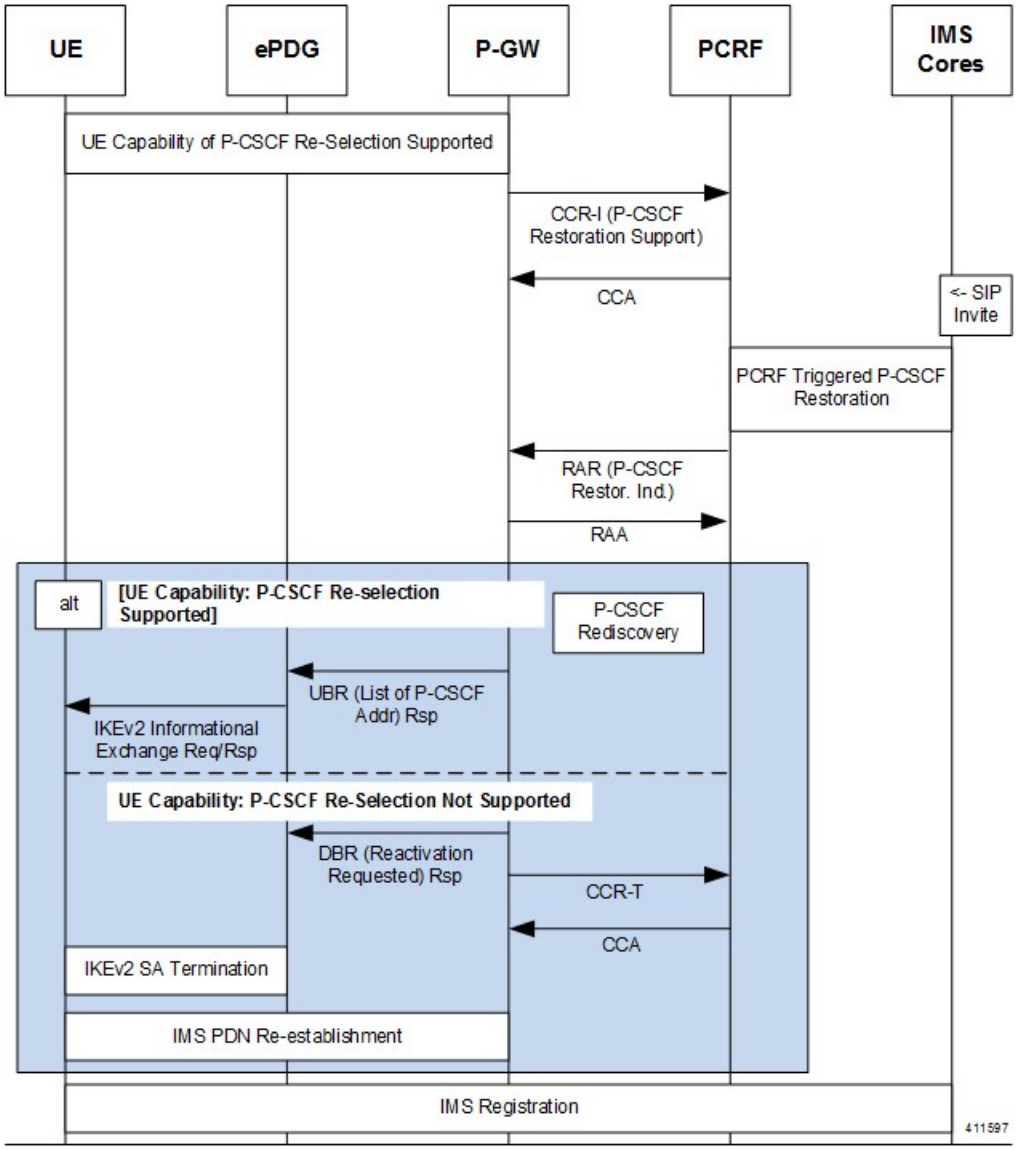
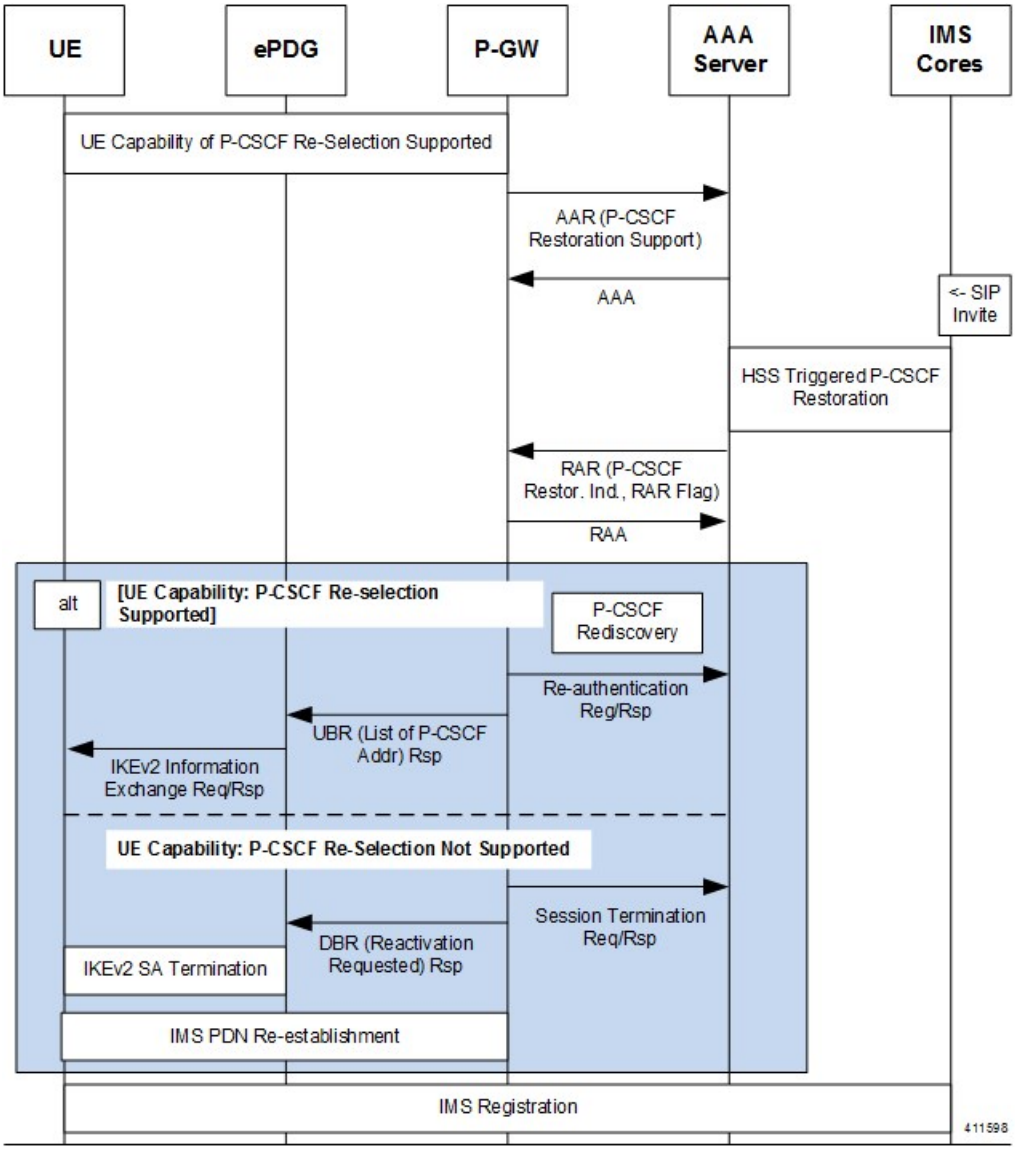


図 *75* : 信頼できない *WLAN* アクセスでの *HSS* ベースの *P-CSCF* 復元



標準準拠

- Release 13 3GPP TS 23.380: IMS Restoration Procedures
- Release 13 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols
- Release 13 3GPP TS 29.212: Policy and Charging Control (PCC); Reference points
- Release 13 3GPP TS 29.273: 3GPP EPS AAA Interfaces
- Release 13 3GPP TS 29.274: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3

HSS/PCRF ベースの P-CSCF 復元の設定

次の項では、HSS ベースおよび PCRF ベースの P-CSCF 復元機能のサポートを有効にするための設定コマンドについて説明します。

S6b AAA インターフェイスでの P-CSCF 復元通知の有効化

AAR メッセージ内の Supported-Features AVP を S6b インターフェイス経由で AAA サーバーに対してエンコードするには、次の設定コマンドを使用します。

```
configure
   context context_name
      aaa group group_name
         diameter authentication encode-supported-features
pcscf-restoration-indication
         end
```

注：

- **encode-supported-features**：Supported-Features AVP をエンコードします。
- **pcscf-restoration-indication**：P-CSCF 復元の通知機能を有効にします。
- **default encode-supported-features**：AAR メッセージで Supported-Features AVP を送信しないデフォルト設定を指定します。
- **no encode-supported-features**：Supported-Features AVP を送信しないように、CLI コマンドを無効にします。
- **pcscf-restoration-indication** ：キーワードはライセンスによって異なります。詳細については、シスコのアカウント担当者にお問い合わせください。

Gx インターフェイスでの P-CSCF 復元通知の有効化

P-CSCF 復元でサポートされている機能には、次の設定を使用します。

```
configure
   context context_name
      ims-auth-service service_name
         policy-control
            diameter encode-supported-features pcscf-restoration-ind
            end
```

注：

- **pcscf-restoration-ind**：P-CSCF 復元の通知機能を有効にします。このキーワードはライセンスによって異なります。詳細については、シスコのアカウント担当者にお問い合わせください。デフォルトでは、この機能は無効になっています。

- **default encode-supported-features**：サポートされている機能を削除/リセットするデフォルト設定。
- **no encode-supported-features**：以前に設定されたサポート対象機能を削除します。

緊急 PDN に対する P-CSCF 復元の有効化

緊急 PDN に対する P-CSCF 復元を有効にするには、次の設定を使用します。

```
configure
   context context_name
      pgw-service service_name
         pcscf-restoration { hss-solution | custom-hss-solution }
         pcscf-restoration emergency-pdn
         end
```

注：

- **{ hss-solution | custom-hss-solution }**：P-CSCF 復元用の標準ベースまたはプライベート拡張ベースの HSS ソリューションを有効にします。このキーワードは、**emergency-pdn** とは別のコマンドラインで設定する必要があります。
- **emergency-pdn**：緊急 PDN に対する P-CSCF 復元を有効にします。

  このキーワードはライセンスによって異なります。詳細については、シスコのアカウント担当者にお問い合わせください。デフォルトでは、この機能は無効になっています。
- **default pcscf-restoration**：P-CSCF 復元は緊急 PDN に対して無効になり、P-CSCF 復元にはプライベート拡張メカニズムが使用されるようになります。
- **no pcscf-restoration emergency-pdn**：緊急 PDN に対する P-CSCF 復元を無効にします。

S6b が WLAN の P-CSCF 復元をトリガーした後の再認証の有効化

S6b が WLAN の P-CSCF 復元をトリガーした後に再認証を有効にするには、次の設定を使用します。

```
configure
   context context_name
      pgw-service service_name
         pcscf-restoration s6b-reauth
         end
```

注：

- **s6b-reauth**：S6b が WLAN の P-CSCF 復元をトリガーした後に再認証を有効にします。S2a と S2b にのみ適用されます。デフォルトでは、S6b での P-CSCF 復元拡張について再認証が実行されます。

  このキーワードはライセンスによって異なります。詳細については、シスコのアカウント担当者にお問い合わせください。デフォルトでは、この機能は無効になっています。

- **default pcscf-restoration**：S6b での P-CSCF 復元拡張について再認証が実行されます。
- **no pcscf-restoration s6b-reauth**：S6b での P-CSCF 復元拡張後に再認証を無効にします。

HSS/PCRF ベースの P-CSCF 復元の確認

show aaa group all

この機能が AAA グループで設定されている場合、この show コマンドは、サポート対象機能の一部として **pccf-restoration-ind** を表示します。

```
show aaa group all
 Group name:    default
 Context:   local

 Diameter config:
  Authentication:
....
Supported-Features:   pcscf-restoration-ind
....
```

show ims-authorization sessions full all

このコマンドにより、この機能のネゴシエーションステータスを示す表示が生成されます。

次の表示例は、ネゴシエートされたサポート対象機能の中で **pcscf-restoration-ind** を示す出力の一部のみを示しています。

```
show ims-authorization sessions full all

 CallId: 00004e22            Service Name:  imsa-Gx
   IMSI: 123456789012341
   ....
 Negotiated Supported Features:
   3gpp-r8
   pcscf-restoration-ind
 ....
```

show pgw-service name <pgw_service>

このコマンドにより、この機能の設定ステータスを示す表示が生成されます。

次の表示例は、出力の一部にすぎません。

P-GW サービスの出力が拡張され、**MME トリガー**の HSS ベースのソリューションが明確に指定されるようになりました。その結果、HSS ベース S6b トリガーソリューションとの混同が回避されます。さらに、**緊急 PDN で P-CSCF 復元がサポートされている**かどうか、または **S6b トリガー P-CSCF 復元後の再承認**が有効になっているかどうかも表示します。

```
show pgw-service name <pgw_service>

    Service name : pgw_service
    Restoration solution : HSS-based MME-Triggered (Rel12)
    P-CSCF Restoration supported for Emergency PDNs : Yes/No
    Re-Auth After s6b Triggered P-CSCF Restoration : Enabled / Disabled
```

. . . .

HSS および PCRF ベースの P-CSCF 復元のモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

次の操作を実行して、この機能に関連する障害をトラブルシュートできます。

- **show ims-authorization sessions full all** および **show aaa group all** CLI コマンドを使用して、機能が有効になっているかどうかを確認します。有効になっていない場合は、ポリシー制御と AAA グループ設定の両方で必要な CLI コマンドを設定し、動作するかどうかを確認します。
- **monitor protocol** コマンドを実行し、P-CSCF 復元機能のサポートが CCR-I および AAR メッセージでネゴシエートされているかどうかを確認します。ネゴシエートされていない場合は、この機能のそれぞれの CLI コマンドを有効にします。
- それでも問題が解決しない場合は、次の情報を入手して、シスコのアカウント担当者に詳細な分析を依頼してください。
  - オプション 74（EGTPC）および 75（App Specific Diameter -Gx/S6b）をオンにした状態でのプロトコルのモニターのログ
  - sessmgr、imsa、および diameter-auth が有効な状態でのログ
  - **show session disconnect reason** CLI コマンドの出力とサービスレベルの関連統計

show コマンドの出力

show aaa group all

この show コマンド出力の **Supported Features** フィールドには、P-CSCF 復元機能が Supported-Features AVP の一部として設定されているかどうかが表示されます。

このサポートされている機能は、機能ライセンスが設定されている場合にのみ表示されます。

show ims-authorization sessions full all

この show コマンド出力の **Negotiated Supported Features** フィールドには、P-CSCF 復元機能が PCRF とネゴシエートされているかどうかが表示されます。

このサポートされている機能は、機能ライセンスが設定されている場合にのみ表示されます。

show license information コマンドを実行します。

P-CSCF 復元機能を有効にするライセンスが設定されている場合、**show license information** コマンドにより、関連するライセンス情報が表示されます。

show pgw-service name <pgw_service>

P-GW サービスの出力が拡張され、**MME トリガー**の HSS ベースのソリューションが明確に指定されるようになりました。その結果、HSS ベース S6b トリガーソリューションとの混同が回避されます。さらに、**緊急 PDN で P-CSCF 復元がサポートされている**かどうか、または **S6b トリガー P-CSCF 復元後の再承認**が有効になっているかどうかも表示します。

```
show pgw-service name <pgw_service>

    Service name : pgw_service
    Restoration solution : HSS-based MME-Triggered (Rel12)
    P-CSCF Restoration supported for Emergency PDNs : Yes/No
    Re-Auth After s6b Triggered P-CSCF Restoration : Enabled / Disabled

 ....
```

show pgw-service statistics all

このコマンドは、P-CSCF 復元の回数に関する統計を提供します。

MME が受信した P-CSCF 復元回数は、「**P-CSCF Restoration Indications received:**」から「**MME triggered Restoration**」に移動されました。現在、「**P-CSCF Restoration Indications received:**」には、受信した P-CSCF 復元通知（HSS トリガーおよび PCRF トリガー）の合計数が表示されます。バルク統計カウンタ「**sessstat-pcscf-recovery-count**」には、MME が受信した P-CSCF 復元のみが引き続き表示されます。

任意のインターフェイス（MME/PCRF/S6b）で受信されるトリガーの合計数は、基本 + 拡張 + 無視（すでに復元が進行中、ライセンスが存在しない、検証チェックが失敗した、コールが接続されていないなどの理由で無視されたもの）です。

```
PDNs Released By Reason:
  Network initiated release:           0    MME initiated release:             0
    Admin disconnect:                  0    S4 SGSN initiated release:         0
    GTP-U error ind:                   0
    SGW path failure:                  0
    Local fallback timeout:            0
    UE P-CSCF Reselect not supported:  0
…

 S2bGTP-to-eHRPD handover:               eHRPD-to-S2bGTP handover:
        Attempted:                       0      Attempted:                       0
        Succeeded:                       0      Succeeded:                       0
        Failed:                          0      Failed                           0
 …

     P-CSCF Restoration Indications received:              <total_count
 at service level>
       HSS Triggered Restoration:
         MME Triggered Restoration:                      <>
             Basic Restoration Performed:                <>
             Extension Restoration Performed:            <>
```

```
        S6b Triggered Restoration:                      <>
            Basic Restoration Performed:                <>
            Extension Restoration Performed:            <>
      PCRF Triggered Restoration:                       <>
          Basic Restoration Performed:                  <>
          Extension Restoration Performed:              <>

     Data Statistics Per Interface:
…
```

show srp checkpoint statistics active verbose

このコマンドは、次の P-CSCF 復元マイクロチェックポイント情報を提供します。

```
.
.
    Total pgw ubr_mbr micro-chkpnt sent:              0
    Total pcscf update micro-chkpnt sent:                 0
```

show srp checkpoint statistics standby verbose

このコマンドは、次の P-CSCF 復元マイクロチェックポイント情報を提供します。

```
.
.
 PGW ubr_mbr session microchkpt rcvd:          0

PCSCF info update microchkpt rcvd:             0
```

ログのモニタリング

ここでは、HSS および PCRF ベースの P-CSCF 復元機能に関連して生成されるログのモニター方法について説明します。

Gx Diameter プロトコルログ

Supported-Features で、CCR-I/CCA-I セクションの P-CSCF 復元の **Feature-List** が使用できます。生成される出力は次のように表示されます。

```
<<<<OUTBOUND  13:52:06:117 Eventid:92820(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
   [V] Feature-List: 16777217
....
INBOUND>>>>>  13:52:06:118 Eventid:92821(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
    [V] Feature-List: 16777216
....
```

PCSCF-Restoration-Indication AVP は RAR で使用できます。生成される出力は次のように表示されます。

```
INBOUND>>>>>  13:52:26:119 Eventid:92821(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
[V] PCSCF-Restoration-Indication: 0
....
```

S6b Diameter プロトコルログ

Supported-Features フィールドは、AAR および AAA セクションで使用できます。生成されるログの出力は次のように表示されます。

```
<<<<OUTBOUND  15:37:23:561 Eventid:92870(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
   [V] Feature-List: 1
....
INBOUND>>>>>  15:37:23:562 Eventid:92871(5)
....
 [V] [M] Supported-Features:
   [M] Vendor-Id: 10415
   [V] Feature-List-ID: 1
   [V] Feature-List: 1
....
```

RAR-Flags フィールドは、RAR セクションで使用できます。生成されるログの出力は次のように表示されます。

```
INBOUND>>>>>  15:37:43:562 Eventid:92871(5)
....
[M] Re-Auth-Request-Type: AUTHORIZE_ONLY (0)
[V] RAR-Flags: 2
....
```

バルク統計

P-GW スキーマ

次のカウンタは **pcscf-recovery** に固有です。

- sessstat-pcscf-recovery-count
- sessstat-pcscf-recovery-basic-count
- sessstat-pcscf-recovery-extension-count
- sessstat-s6b-pcscf-recovery-count
- sessstat-s6b-pcscf-recovery-basic-count
- sessstat-s6b-pcscf-recovery-extension-count
- sessstat-pcrf-pcscf-recovery-count
- sessstat-pcrf-pcscf-recovery-basic-count
- sessstat-pcrf-pcscf-recovery-extension-count

SAEGW スキーマ

次のカウンタは **pcscf-recovery** に固有です。

- pgw-sessstat-pcscf-recovery-count
- pgw-sessstat-pcscf-recovery-basic-count
- pgw-sessstat-pcscf-recovery-extension-count
- pgw-sessstat-s6b-pcscf-recovery-count
- pgw-sessstat-s6b-pcscf-recovery-basic-count
- pgw-sessstat-s6b-pcscf-recovery-extension-count
- pgw-sessstat-pcrf-pcscf-recovery-count
- pgw-sessstat-pcrf-pcscf-recovery-basic-count
- pgw-sessstat-pcrf-pcscf-recovery-extension-count



第 49 章

ICAP インターフェイスのサポート

この章では、コア ネットワーク サービス サブスクライバ用の外部アクティブ コンテンツ フィルタリング サーバーの設定について説明します。この章では、この機能の導入に使用する設定とコマンドについても説明します。

この章に記載の手順を実行する前に、各製品のアドミニストレーション ガイドの説明に従って、ご使用のサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

現在、次の製品が ICAP インターフェイス機能をサポートしています。

- GGSN
- P-GW

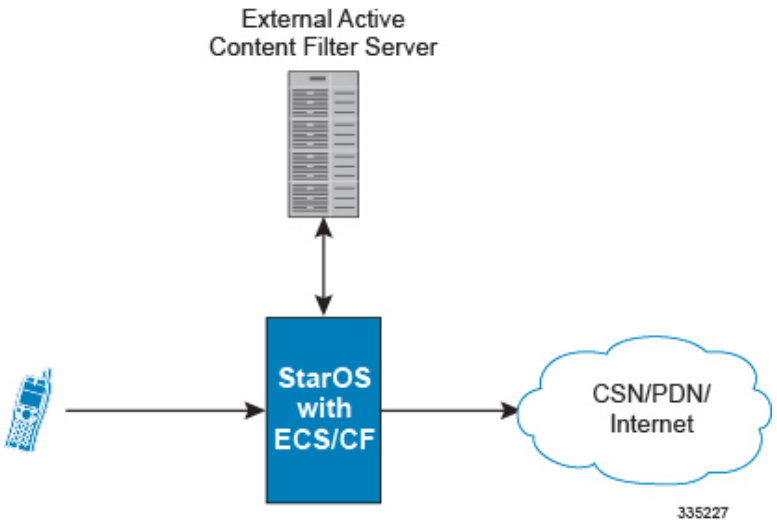
- ICAP インターフェイスサポートの概要 （967 ページ）
- ICAP インターフェイスサポートの設定 （973 ページ）

ICAP インターフェイスサポートの概要

この機能は、合理化された ICAP インターフェイスをサポートし、ディープ パケット インスペクション（DPI）を活用して、外部アプリケーションサーバーが DPI 機能を実行せずに、またデータフローに挿入されることなく、そのサービスを提供できるようにします。たとえば、外部のアクティブコンテンツフィルタリング（ACF）プラットフォームの使用時などが該当します。

次の図に、外部 ACF に対する合理化された ICAP インターフェイスサポートの概要を示します。

図 *76 :* 外部 *ACF* を使用して合理化された *ICAP* インターフェイスの概要図



ECS を使用するシステムは、DPI をサポートするように構成されており、システムはこの機能をコンテンツ課金にも使用します。WAP および HTTP トラフィックは、ICAP インターフェイスを介してコンテンツがフィルタリングされます。アダルトコンテンツを含むRTSP トラフィックも ICAP インターフェイスでコンテンツをフィルタリングできます。RTSP 要求パケットだけが、ICAP インターフェイスを介したコンテンツフィルタリングの対象となります。

サブスクライバが WAP（WAP1.x または WAP2.0）または Web セッションを開始すると、後続の GET/POST 要求が DPI 機能によって検出されます。GET/POST 要求の URL が抽出され、サブスクライバ識別情報とサブスクライバ要求とともに ICAP メッセージでアプリケーションサーバーに渡されます。アプリケーションサーバーは、カテゴリや、タイプ、アクセスレベル、コンテンツカテゴリなどの他の分類に基づいて URL をチェックし、要求を許可、ブロック、またはリダイレクトする必要があるかどうかを、次のメッセージでGET/POST メッセージに応答して決定します。

- 要求が受け入れられる場合、200 OK メッセージ。
- リダイレクトの場合、302 リダイレクトメッセージ。このリダイレクトメッセージには、サブスクライバのリダイレクト先となる URL が含まれます。
- RTSP 要求の拒否応答コード 200 はサポートされていません。403 "Forbidden" 拒否応答コードのみがサポートされます。

受信した応答に応じて、ECS を備えたシステムは要求を変更なしで渡すか、またはメッセージを破棄して、適切なリダイレクトメッセージまたはブロックメッセージでサブスクライバに応答します。

コンテンツの課金は、要求がアプリケーションサーバーによって制御された後にのみ、アクティブ課金サービス（ACS）によって実行されます。これにより、外部アプリケーションとコンテンツベースの課金との間の適切なインターワーキングが保証されます。特に、これにより、リダイレクトの場合に課金が適切な要求に適用されることが保証され、発生する可能性が

ある課金ベースのリダイレクト（課金通知、追加課金ページなど）が、アプリケーションサーバーによって行われる決定と干渉しないことが保証されます。

ACF には次の機能が含まれます。

- ICAP メッセージで渡されたサブスクライバのアイデンティティに基づくサブスクライバポリシーの取得
- サブスクライバのプロファイルに基づいた、コンテンツのタイプに応じて実行する適切なアクション（許可、拒否、リダイレクト）の決定
- URL に対するアクション（許可、拒否、またはリダイレクト）決定を ACS モジュールに戻す

サポート対象のネットワークとプラットフォーム

この機能は、システムで設定されているコアネットワークサービス用の Cisco ASR 5500 プラットフォームをサポートします。

プラットフォームの詳細については、該当する『*System Administration Guide*』[英語] を参照するか、シスコのアカウント担当者にお問い合わせください。

ライセンス要件

Internet Content Adaptation Protocol（ICAP）インターフェイスによる外部コンテンツ フィルタリング サーバーのサポートは、シスコのライセンス機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

再送信されたパケットでの障害アクション

再送信パケットのフローの ICAP 要求に対してデフォルトの ICAP 障害アクションが実行された場合、再送信パケットに対して ICAP 評価が有効になります。接続をリセットする必要があり、他に使用可能な冗長接続がない場合、ICAP デフォルト障害アクションは、接続で保留中の ICAP 要求に対して実行されます。たとえば、ICAP 要求タイムアウトのシナリオや、ICAP 接続タイムアウトのシナリオの場合があります。これらの場合、アップリンク方向に再送信されたパケットは、ICAP 評価のために再送信されます。

WAP CO の場合、ICAP 障害アクションが実行された WAP トランザクションのアップリンク再送信パケットが、ICAP 評価のために送信されます。再送信パケットの WSP ヘッダーは、WSP アナライザによって解析されません。そのトランザクションの前のパケットで受信した URL が、ICAP 評価に使用されます。同じフローの複数の WTP トランザクションで障害アクションが実行された場合（WTP 連結 GET 要求の場合など）、各トランザクションのアップリンク再送信パケットが評価のために再送信されます。

HTTP の場合、ICAP 障害アクションが実行された HTTP フローのアップリンク再送信パケットが、ICAP 評価のために送信されます。現在のセカンダリセッション（最後のアップリンク要求）に存在する URL が、ICAP 評価に使用されます。ただし、同じフロー（パイプライン処理された要求）に対して複数の未処理の ICAP 要求がある場合、再送信パケットについては、評価のために送信される URL は、最後の GET 要求の URL になります。

元の要求に対する ICAP 応答を受信せず、再送信された要求が着信した場合に、再送信パケットに対して実行されるさまざまな障害アクションにおける再送信は、次のとおりです。

- WSP CO：
  - Permit：アップリンクパケットが ICAP 評価のために送信され、ICAP 応答に応じて、WTP トランザクションが許可またはブロックされます。WAP ゲートウェイが、許可された GET 要求に対する応答を送信する可能性があります。そのため、競合状態が発生し、サブスクライバは、評価が redirect または content insert であった場合でも、Web ページを表示できる可能性があります。
  - Content Insert：再送信パケットは、ICAP 評価のために送信されません。
  - Redirect：再送信パケットは、ICAP 評価のために送信されません。
  - Discard：アップリンクパケットが ICAP 評価のために送信され、ICAP 応答に応じて、WTP トランザクションが許可またはブロックされます。
  - Terminate flow：アップリンクパケットが ICAP 評価のために送信され、ICAP 応答に応じて、WTP トランザクションが許可またはブロックされます。フローの終了中に送信された WSP 切断パケットが WAP ゲートウェイによって受信された場合、WAP ゲートウェイは、この GET 要求の中止トランザクションを送信する場合があります。
- [HTTP]：
  - Permit：アップリンクパケットが ICAP 評価のために送信され、ICAP 応答に応じて、最後の HTTP GET 要求が送信されます。HTTP サーバーが、許可された GET 要求に対する応答を送信する可能性があります。そのため、競合状態が発生し、サブスクライバは、評価が redirect または content insert であった場合でも、Web ページを表示できる可能性があります。
  - Content Insert：再送信パケットはドロップされ、課金されません。
  - Redirect：再送信パケットはドロップされ、課金されません。
  - Discard：アップリンクパケットが ICAP 評価のために送信され、ICAP 応答に応じて、WTP トランザクションが許可またはブロックされます。
  - Terminate flow：再送信パケットはドロップされ、課金されません。
- RTSP：

  次のシナリオでは、クライアントから RTSP 要求を受信した場合の障害アクションについて説明します。ICAP が有効になっている場合、要求は、コンテンツフィルタリングのために ICAP サーバーに送信されます。

- Allow：設定されている障害アクションが「allow」である場合、RTSP 要求パケットは、適切な判定結果アクションの適用後に送信されます。この場合、フローは、受信した ICAP 応答が 200 OK のときと同じであるままになります。
- Content Insert：設定された障害アクションが「content-insertion <string of size 1 to 128>」である場合、RTSP 要求に対するこの障害アクションはサポートされません。代わりに、このような RTSP 要求に対して障害アクション「Discard」がサポートされます。
- Redirect-URL：設定された障害アクションが「redirect-url <string of size 1 to 128>」である場合、RTSP「302 Moved Temporarily」応答ヘッダーを含む TCP FIN_ACK パケットが、リダイレクト用に指定された URL を含むクライアントに向けて挿入されます。TCP RST パケットがサーバーに向けて挿入されます。そのため、基礎となる TCP 接続が閉じられます。RTSP クライアントが、リダイレクトされた URL を再試行する場合は、新しい TCP 接続を開くことが開始される必要があります。
- Discard：設定された障害アクションが「discard」である場合、クライアントから受信した RTSP 要求パケットはサイレントに廃棄され、クライアントに通知は送信されません。
- Terminate flow：設定された障害アクションが「terminate-flow」である場合、クライアントに向けて TCP FIN-ACK を挿入し、サーバーに向けて RST パケットを挿入することによって、TCP 接続が切断されます。ただし、このフローの終了に関しては、RTSP クライアントおよびサーバーに通知が送信されません。

RFC 3507 準拠の ICAP クライアント通信

ICAP コンテンツ フィルタリング ソリューションは、RFC 3507（Internet Content Adaptation Protocol（ICAP））に準拠して、Cisco ASR 5500 P-GW および HA 上の ICAP サーバーとの ICAP クライアント通信をサポートするように拡張されています。このリリースでは、RFC 3507 に基づく HTTP 要求の変更とエラーコードの部分的な拡張にのみ対応しています。P-GW/HA で実行されている ICAP クライアントは、ICAP プロトコルを介して外部 ICAP サーバーと通信します。サブスクライバのコンテンツフィルタリングが有効になっている場合、そのサブスクライバからのすべての HTTP GET 要求がコンテンツフィルタリングサーバー（ICAP サーバー）によって検証され、コンテンツ分類要求に応じて、許可、拒否、またはリダイレクトされます。

コンテンツフィルタリングは、事前定義された静的ルールのオーバーライド制御（OC）機能、または L7 ダイナミックルールのアクティブ化機能のいずれかによって、サブスクライバに対して有効になります。設定可能なオプションがコンテンツ フィルタリングのサーバー グループ コンフィギュレーション モードに追加されました。これにより、サブスクライバの番号情報と CIPA（児童インターネット保護法）カテゴリの 2 つのパラメータを含む ICAP ヘッダーが設定されます。



重要　オーバーライド制御と L7 ダイナミックルールの有効化は、ライセンスにより制御される機能です。これらの機能を設定する前に、有効な機能ライセンスをインストールする必要があります。詳細については、シスコのアカウント担当者にお問い合わせください。

- サブスクライバ番号：「Subscription ID」AVP は、CCR メッセージでゲートウェイから PCRF に送信されます。AVP 値は、HSS からゲートウェイに送られます。ゲートウェイでは、CCI-A メッセージでこの AVP を受信しません。
- CIPA カテゴリ：カテゴリ文字列は PCRF によって提供され、ICAP 要求変更メッセージの拡張ヘッダーとして組み込まれます。AVP は、CCA-I または RAR で PCRF から受信されます。

ディクショナリおよび AVP のサポート

新しいコンテンツフィルタリング（CF）ディクショナリの「custom4」が導入され、次の新しい AVP が r8-gx-standard ディクショナリと custom4 ディクショナリに追加されます。

- Override-Content-Filtering-State：この属性は、ルールまたは課金アクションのコンテンツ フィルタリング ステータス（CF 状態）に関する情報を伝送します。この AVP は、静的ルールや事前定義されたルールのコンテンツ フィルタリング ステータスを上書きするために使用されます。この属性は Override-Control grouped AVP に含まれます。
- CIPA：この属性には、ICAP プランの識別子として扱われる児童インターネット保護法（CIPA）カテゴリの文字列値が含まれます。この識別子は、ICAP サーバーが正しいコンテンツ フィルタリング プラン（パケットの処理に基づく CIPA カテゴリ）を特定するのに役立ちます。

  この属性値は Gx インターフェイスを介して PCRF から受信され、ICAP 要求の送信時に ICAP ヘッダーに追加されます。
- L7-Content-Filtering-State：この属性は、L7 ルールのコンテンツ フィルタリング ステータス（CF 状態）に関する情報を伝送します。この属性は、PCRF からのインストールで受信した L7 課金ルール定義に対して ICAP 機能が有効か無効かを示します。この属性値に基づいて、ダイナミックルールに一致するトラフィックが ICAP サーバーに送信されます。

  L7 ルール処理のために、この属性が L7-Application-Description grouped AVP に追加されます。これは、HTTP プロトコルにのみ適用されます。



重要　OC および L7 ダイナミックルール機能を介してコンテンツフィルタリングを制御するための CIPA およびフラグは、r8-gx-standard ディクショナリにのみ適用されます。

新しい AVP のサポートに加えて、L7-Application-Description grouped AVP の L7-Field AVP は、ANY-MATCH を入力データとして受け入れるようにエンコードされます。現在のフレームワークは、課金アクション内にあるオーバーライド制御の既存の「vlan-id」フィールドをサポート

していません。したがって、Override-Content-Filtering-State AVP で Override-VLAN-ID を置き換えて OC をサポートします。

サブスクライバがセッション作成要求を開始すると、P-GW/HA は CCR-I メッセージを PCRF に送信してサブスクライバプロファイルを取得します。このサブスクライバの ICAP 機能が有効になっている場合、PCRF は CIPA と OC の情報を含む CCA-I メッセージで応答します。

L7 ダイナミックルールの場合、L7-Application-Description grouped AVP で L7-Content-Filtering-State AVP を送信すると、コンテンツフィルタリング機能が有効になります。ダイナミックルールの L7-Content-Filtering-State を受信した場合は、少なくとも 1 つの L7 フィルタが存在するはずです。L7-Content-Filtering-state AVP が L7 フィルタ情報 AVP とともに送信された場合、Content-Filtering の状態は考慮されません。したがって、L7-Content-Filtering-State で受信したフィルタは処理されず、L7 ルールが破棄されます。

オーバーライド制御の場合、サブスクライバに対してコンテンツフィルタリングが有効になっていると、PCRF は Override-Control AVP を介して ICAP フラグを送信します。この AVP は、そのサブスクライバの ICAP 機能を有効にするために課金アクションを上書きします。

サポートされる AVP の詳細については、『*AAA Interface Administration and Reference*』[英語] を参照してください。

制限事項

この機能の制限事項は次のとおりです。

- IPv4 アドレス方式のみがサポートされています。
- ICAP コンテンツフィルタリングは HTTP トラフィックにのみ適用されます。HTTPS トラフィックは、ICAP クライアントではサポートされていません。
- 高速パスは、この機能ではサポートされていません。

ICAP インターフェイスサポートの設定

ここでは、ICAP クライアントと ACF サーバー（ICAP サーバー）間の Internet Content Adaptation Protocol（ICAP）インターフェイスを介してコンテンツ フィルタリング サーバー グループ（CFSG）を設定する方法について説明します。

重要 システムの ICAP インターフェイスで外部コンテンツ フィルタリング サーバーを設定するための最小の命令セットについて説明します。追加のパラメータとオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*CFSG Configuration Mode Commands*」の章を参照してください。

外部コンテンツ フィルタリング サーバーで ICAP インターフェイスをサポートするようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 ICAP サーバーグループの作成およびアドレスのバインド（974 ページ）の設定例を適用して、コンテンツ フィルタリング サーバー グループを作成し、シャーシの発信元（ローカル）IP アドレスを使用して ICAP インターフェイスを作成します。

ステップ 2 ICAP サーバーおよびその他のパラメータの設定（974 ページ）の設定例を適用して、アクティブなコンテンツ フィルタリング サーバー（ICAP サーバー）の IP アドレスを指定し、CAP サーバーグループのその他のパラメータを設定します。

ステップ 3 ICAP サーバーグループの ECS ルールベースの設定（975 ページ）の設定例を適用して、ECS ルールベースのコンテンツ フィルタリング モードを外部コンテンツ フィルタリング サーバー グループ モードに設定します。

ステップ 4 ICAP サーバーグループの課金アクションの設定（976 ページ）の設定例を適用して、アクティブ課金設定モードで ICAP インターフェイス上の外部コンテンツ フィルタリング サーバーに HTTP/RTSP/WAP GET 要求を転送するよう課金アクションを設定します。

ステップ 5 ICAP サーバーグループ設定の確認（976 ページ）の手順に従って、ICAP インターフェイスと外部コンテンツ フィルタリング サーバー グループの設定を確認します。

ステップ 6 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

ICAP サーバーグループの作成およびアドレスのバインド

ICAP サーバーグループを作成し、IP アドレスをバインドするには、次の例に示すコマンドを使用します。

```
configure
   context <icap_ctxt_name> [ -noconfirm ]
      content-filtering server-group <icap_svr_grp_name> [ -noconfirm ]
         origin address <ip_address>
         end
```

注：

- <*ip_address*> is local IP address of the CFSG endpoint.

ICAP サーバーおよびその他のパラメータの設定

次の例を使用して、アクティブ コンテンツ フィルタリング（ICAP サーバー）および関連する他のパラメータを設定します。

```
configure
   context <icap_context_name>
      content-filtering server-group <icap_server_grp_name>
```

```
          icap server <ip_address> [ port <port_number> ] [ max <max_msgs>] [
priority <priority> ] [ standby ]
          connection retry-timeout <retry_timeout>
          deny-message <msg_string>
          dictionary { custom1 | custom2 | custom3 | custom4 | standard
 }
          failure-action { allow | content-insertion <content_string> |
discard | redirect-url <url> | terminate-flow }
          header extension options { cipa-category cipa_category_name |
subscriber-number subscriber_num_name } +
          response-timeout <timeout>
          end
```

注：

- コンテンツ フィルタリング サーバー グループごとに 1 つの ICAP サーバーのみを設定できます。
- **standby** キーワードを使用して、ICAP サーバーをスタンバイに設定できます。コンテンツ フィルタリング サーバー グループあたり最大 10 のアクティブおよびスタンバイ ICAP サーバーを設定できます。同じサーバーグループのアクティブサーバーとスタンバイサーバーは、アクティブ/スタンバイモードで動作するように設定できます。
- オプションの **max** <*max_msgs*> キーワードを使用して設定された、ICAP 接続あたりの未処理要求の最大数は 1 つに制限されています。したがって、**max** キーワードを使用して設定された他の値は無視されます。
- オプションです。ICAP URL 抽出動作を設定するには、コンテンツ フィルタリング サーバー グループ コンフィギュレーション モードで次のコマンドを入力します。

  url-extraction { after-parsing | raw }

  デフォルトでは、ACF クライアントから ICAP サーバーに送信される URL のパーセントエンコードされた 16 進文字は、対応する ASCII 文字に変換されて送信されます。
- **custom4** ディクショナリは、ICAP 要求メッセージのユーザー定義情報を指定するカスタム定義のディクショナリです。ICAP 要求メッセージには、サブスクライバ番号と CIPA カテゴリ値が含まれます。

  custom4 ディクショナリが設定されている場合、ICAP 要求は ICAP RFC 3507 要求モード要求の一部として作成されます。その他のディクショナリが設定されている場合、ICAP クライアントの以前の実装は一部 RFC に準拠しません。
- **header extension options** コマンドは、ICAP ヘッダーパラメータ（サブスクライバ番号と CIPA カテゴリ）を設定します。

ICAP サーバーグループの ECS ルールベースの設定

コンテンツフィルタリングの ECS ルールベースでコンテンツ フィルタリング モードを ICAP サーバーモードに設定するには、次の例を使用します。

```
configure
   require active-charging
   active-charging service <acs_svc_name> [ -noconfirm ]
      rulebase <rulebase_name> [ -noconfirm ]
         content-filtering mode server-group <cf_server_group>
         end
```

注：

- **optimized-mode** キーワードは使用できません。



重要　**configure**、**require active-charging**,、**active-charging service** <*acs_svc_name*> **[-noconfirm]**、**rulebase** CLI コマンドを設定した後、設定を保存し、シャーシをリロードしてコマンドを有効にする必要があります。設定ファイルを保存してシャーシをリロードする方法については、使用している展開の『*System Administration Guide*』を参照してください。

ICAP サーバーグループの課金アクションの設定

次の例を使用して、コンテンツ処理のために HTTP/WAP GET 要求を ICAP サーバーに転送するように課金アクションを設定します。

```
configure
   active-charging service <acs_svc_name>
      charging-action <charging_action_name> [ -noconfirm ]
         [ no ] content-filtering processing server-group
         end
```

注：

- 課金アクションによって提供されるコンテンツ フィルタリング フラグがオーバーライド制御機能の設定に必要な場合は、**no content-filtering processing** コマンドを設定する必要があります。これにより、コンテンツフィルタリング処理のオーバーライドを、オーバーライド制御機能を通じて有効または無効にすることができます。

ICAP サーバーグループ設定の確認

ここでは、cfgファイルに設定を保存した後に、それらの設定を表示して確認する方法と、サービスのアクティブな設定内のエラーや警告情報を取得する方法について説明します。



重要　ここに記載されているコマンドはすべて Exec モードで実行します。すべてのプラットフォームですべてのコマンドを使用できるわけではありません。

次の手順は、この機能の設定を確認するために使用します。

手順

ステップ 1 Exec モードで次のコマンドを入力して、ICAP コンテンツ フィルタリング サーバー グループの設定を確認します。

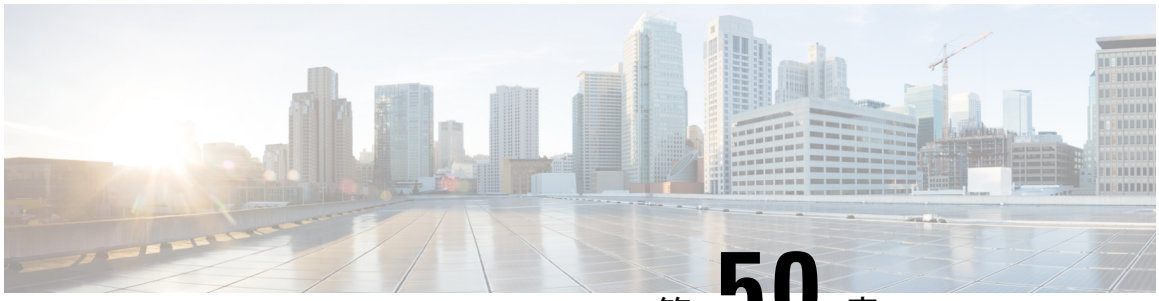
show content-filtering server-group

次に、出力例を示します。この例では、*icap_cfsg1* という名前の ICAP コンテンツ フィルタリング サーバー グループが設定されています。

```
Content Filtering Group:         icap_cfsg1
    Context:                             icap1
    Origin Address:                      1.2.3.4
    ICAP Address(Port):                  1.2.3.4(1344)
    Max Outstanding:                     256
    Priority:                            1
    Response Timeout: 30(secs)  Connection Retry Timeout: 30(secs)
    Dictionary:                          standard
    Timeout Action:                      terminate-flow
    Deny Message:                        "Service Not Subscribed"
    URL-extraction:                      after-parsing
    Header Extension Options:            subscriber-number i-sub
    Content Filtering Group Connections: NONE
Total content filtering groups matching specified criteria:  1
```

ステップ 2 Exec モードで次のコマンドを入力して、設定内のエラーを確認します。

show configuration errors



第 50 章

Gx がダウンしている場合の IMS PCO 設定

- 機能の概要と変更履歴 （979 ページ）
- 機能説明 （980 ページ）
- 機能の仕組み （980 ページ）
- Gx がダウンしている場合の IMS PCO 設定の構成 （983 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• S-GW • P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	N/A

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。 **重要** この機能は、すべてのお客様の展開シナリオでは検証されていません。詳細については、シスコのアカウント担当者にお問い合わせください。	21.23

機能説明

Gx がダウンしている場合、IMS パケットデータネットワーク（PDN）セッションはローカルポリシーを使用します。ただし、「ims-auth」プロファイルに属する既存のプロキシコールセッション制御機能（P-CSCF）PCO リスト設定は、ローカルポリシー内の PDN セッションには適用されません。代替設定は、APN 設定で P-CSCF IP を設定することです。この APN 設定では、IP アドレスが 3 つに制限されており、実稼働環境設定のニーズを満たすことができません。

IMS PDN セッションは、VoLTE レジリエンスを実現するために、ローカルポリシーにフォールバックした後、IMSA で P-CSCF リスト設定を使用します。この機能を使用すると、P-CSCF PCO リストがローカルポリシーの PDN セッションに適用されます。

機能の仕組み

UE は Session Initiation Protocol（SIP）要求を送信する前に、P-CSCF ディスカバリを実行します。UE が P-CSCF アドレスを追加するためにプロトコル設定オプション要素内のネットワークからパラメータを要求すると、P-GW は UE に P-CSCF アドレスを提供します。UE に複数の P-CSCF アドレスがある場合、設定ポリシーを使用して P-CSCF が選択されます。

P-GW での P-CSCF アドレス選択の優先順位は次のとおりです。

- DNS からのアドレス（S6b はアクセスポイント名（APN）の設定から受け取った FQDN を提供します）。
- IMSA が設定されたテーブル内のアドレス。
- APN 設定の一部である設定アドレス。

ローカルポリシーのフォールバックが発生し、Gx がダウンすると、IMSA プロファイルの P-CSCF リストが使用されます。ローカルポリシーが使用される場合のシナリオは次のとおりです。

- Gx がダウンしている場合の P-CSCF リスト
- CCR-I 応答の失敗

コール フロー

次のコールフローと手順では、P-CSCF アドレス選択と応答失敗のシナリオについて説明します。

P-CSCF アドレス選択コールフロー

PCO 要求とともにセッション作成要求（CSR）を受信すると、P-GW はピアをチェックします。すべてのピアがダウン状態であるか、使用可能なピアが存在しない場合、Gx インターフェ

イスはダウンしていると見なされます。PDNセッションは、ローカルポリシーにフォールバックし、IMSA からの P-CSCF リストを使用します。

仮想APN（VAPN）設定が使用可能で、Gx がダウンしている場合、P-CSCF は選択された VAPN の IMSA のアドレスを使用します。VAPN 設定が使用できない場合、APN の IMSA から P-CSCF アドレスリストが受信されます。

図 *77 : P-CSCF* アドレスの選択 - *Gx* ダウン

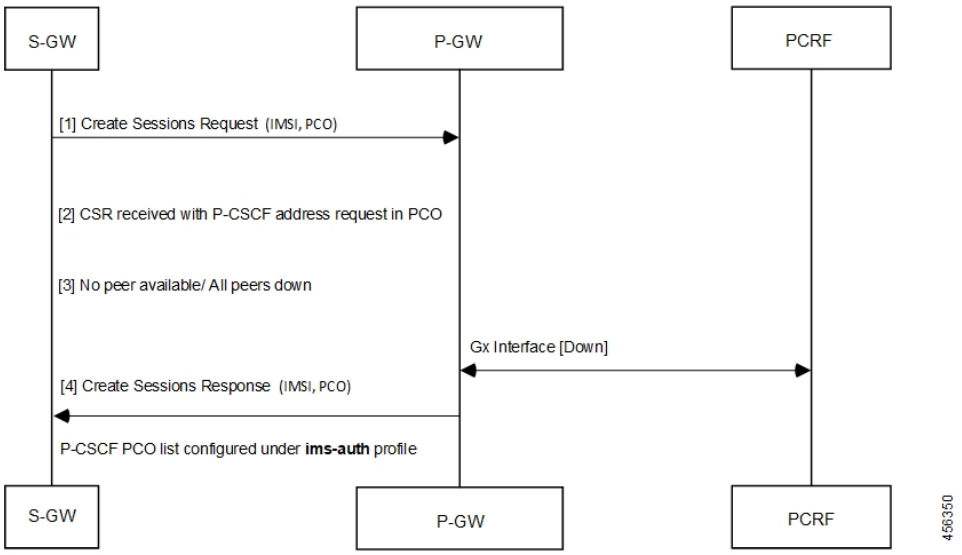


表 *86 :* 手順

ステップ	説明（Description）
1	S-GW は、セッション作成要求（IMSI、PCO）を P-GW に送信します。
2	P-GW は、S-GW から PCO の P-CSCF アドレス要求を含むセッション作成要求を受信し、Gx インターフェイスで使用可能なピアをチェックします。
3	ピアを使用できない場合、またはすべてのピアがダウンしている場合、Gx インターフェイスは PCRF と P-GW の間でダウンしていると見なされます。PDN セッションは、ローカルポリシーにフォールバックし、IMSA からの P-CSCF リストを使用します。
4	次に P-GW は、「ims-auth」プロファイルの P-CSCF PCO リスト設定を使用して、セッション作成応答を S-GW に送信します。

応答失敗コールフロー

PCO での P-CSCF アドレス要求とともに CSR が受信されると、P-GW はピアをチェックします。

ピアがアップ状態で到達可能である場合、Gx はアップ状態であると見なされ、プライマリホストに CCR-I が送信されます。P-GW がエラー応答を受信した場合、セカンダリホストが使用されます。セカンダリホストでも障害が発生した場合、PDNセッションは、ローカルポリシーにフォールバックし、IMSA からの P-CSCF リストを使用します。

図 *78 :* 応答失敗（*CCR* 初期要求）

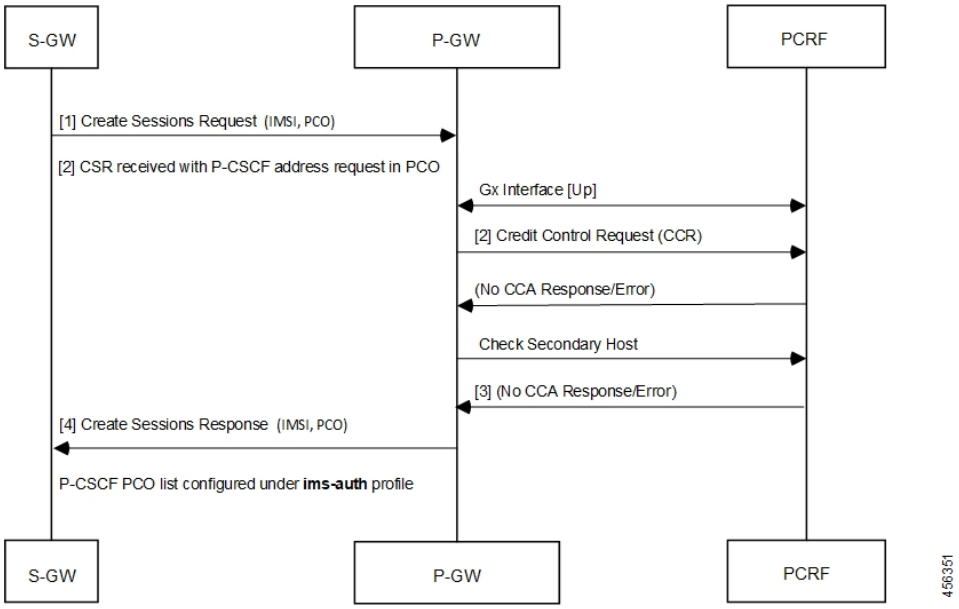


表 *87 : CCR-I* 応答の失敗

ステップ	説明（Description）
1	S-GW は、セッション作成要求（IMSI、PCO）を P-GW に送信します。
2	P-GW は、S-GW から PCO の P-CSCF アドレス要求を含むセッション作成要求を受信し、Gx インターフェイスで使用可能なピアをチェックします。 ピアがアップ状態で到達可能である場合、Gx はアップ状態です。 P-GW は、プライマリホストの PCRF にクレジット制御要求（CCR）を送信します。
3	PCRF は、クレジット制御応答（CCA）応答を送信しません。またはエラーコードを P-GW に送信します。 P-GW がエラー応答を受信した場合、セカンダリホストが使用されます。 セカンダリホストで障害が発生した場合、PDNセッションは、ローカルポリシーにフォールバックし、IMSA からの P-CSCF リストを使用します。
4	次に P-GW は、「ims-auth」プロファイルの P-CSCF PCO リスト設定を使用して、セッション作成応答を S-GW に送信します。

Gx がダウンしている場合の IMS PCO 設定の構成

この項では、Gx がダウンしている場合に IMS PCO 設定を構成する方法について説明します。

ローカルポリシーサービスでの IMSA からの P-CSCF アドレスの有効化

Gx がダウンしている場合に、P-CSCF がローカルポリシーサービスで IMSA からのアドレスを使用できるようにするには、次の設定を使用します。

```
configure
  local-policy-service service_name
    [ no ] use-pcscf-config-from-imsa
    end
```

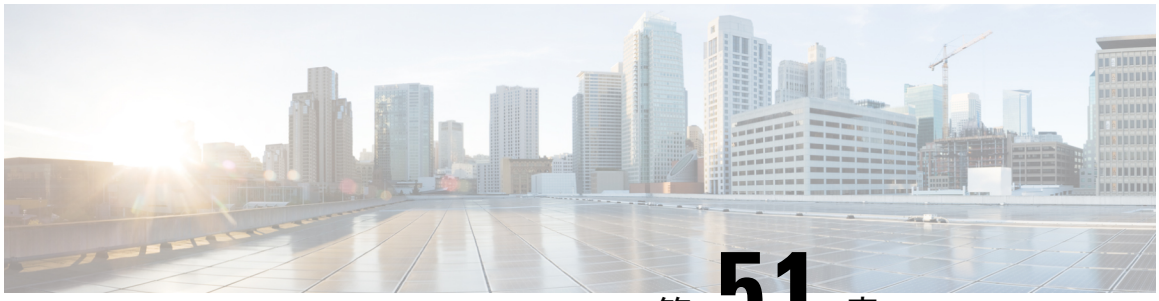
注：

- **no** ：この機能を無効化します。
- **use-pcscf-config-from-imsa**：ローカルポリシーで IMSA からの P-CSCF 設定を使用するように指定します。
- 使用する P-CSCF 検出方法を定義するには、IMS 承認サービス コンフィギュレーション モードで既存の **p-cscf discovery** CLI コマンドを使用します。
- P-CSCF 検出に優先順位を付けて、プライマリやセカンダリの IPv4/IPv6 アドレスを含む行を P-CSCF 検出テーブルに追加または付加するには、IMS 承認サービス コンフィギュレーション モードで既存の **p-cscf table** CLI コマンドを使用します。

ローカルポリシーでの P-CSCF 設定の確認

show configuration CLI コマンドを使用して、ローカルポリシーの P-CSCF 設定が有効か無効かを確認します。**use-pcscf-config-from-imsa** が無効な場合、このコマンドの出力にモードは表示されません。

show configuration verbose | grep “use-pcscf” use-pcscf-config-from-imsa CLI コマンドでは、**use-pcscf-config-from-imsa** のモードが表示されます（有効になっている場合）。



第 51 章

セッション作成要求に APN AMBR を含める

- 機能情報 （985 ページ）
- 変更された機能 （986 ページ）
- コマンドの変更 （986 ページ）
- パフォーマンス指標の変更 （987 ページ）

機能情報

要約データ

[ステータス（Status）]	新しい機能
導入されたリリース	21.2
変更されたリリース	該当なし
対象製品	P-GW
該当プラットフォーム	ASR 5500
デフォルト設定	有効
関連する **CDETS ID**	CSCvd00467
このリリースでの関連する変更点	N/A
関連資料	Command Line Interface Reference P-GW System Administration Guide Statistics and Counters Reference

マニュアルの変更履歴

重要　リリース 21.2 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

変更された機能

現在、APN AMBR は、PCRF によって変更されていない場合でも、セッション作成応答に含まれています。この機能は、3GPP 仕様に準拠するように実装されています。この機能により、受信された APN-AMBR が PCRF によって変更された場合、APN AMBR が S5/S8、S4/S11、および S2a/S2b インターフェイスに含められるようになりました。

以前の動作：APN AMBR は、PCRF によって変更されていない場合でも、セッション作成応答に含まれていました。

新しい動作：受信された APN-AMBR が PCRF によって変更された場合、APN AMBR が S5/S8、S4/S11、および S2a/S2b インターフェイスに含められるようになりました。新しい CLI コマンドが追加され、CRF が受信した変更済みの値について、APN-AMBR 値をセッション作成応答に含めることを有効または無効にできるようになりました。

重要　P-GW では、4294967 kbps までの APN-AMBR 値がサポートされます。

コマンドの変更

egtp

2 つの新しいキーワードが **egtp** コマンドに追加され、PCRF が受信した変更された値について、APN-AMBR 値をセッション作成応答に含めることを有効または無効にできるようになりました。

```
configure
  context context_name
    pgw service service_name
      [ default | no ] egtp create-session-rsp apn-ambr-always-include

       end
```

注：

- **default**：APN AMBR が PCRF から受信されていない場合、APN AMBR はセッション作成応答に含まれません。P-GW では、4294967 kbps までの APN-AMBR 値がサポートされます。
- **no**：セッション作成応答に APN AMBR が含まれません。これはデフォルトの動作です。
- **create-session-rsp**：セッション作成応答に APN-AMBR を含めるオプションを提供します。
- **apn-ambr-always-include**：セッション作成応答に常に APN-AMBR IE を含めます。

パフォーマンス指標の変更

show config

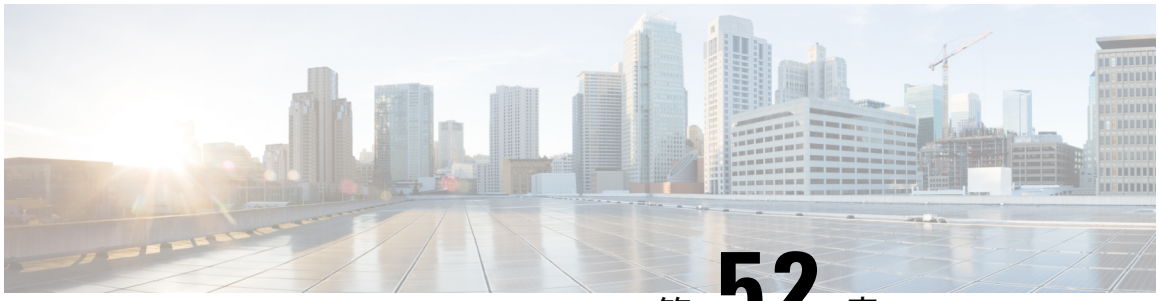
このコマンドは、以下の出力を表示するように変更されました。

```
plmn id mcc 404 mnc 00
plmn id mcc 404 mnc 005 primary
plmn id mcc 404 mnc 090
fqdn host abc.net realm 3gpp.org
dns-client context ISP1
associate ggsn-service GGSN
associate egtp-service PGW21EGTP
egtp create-session-rsp apn-ambr-always-include
```

show pgw-service name

このコマンドは、以下の出力を表示するように変更されました。

```
EGTP SGW Restoration Handling: Disabled
Session Hold Timer: n/a
Timeout: n/a
EGTP Modify bearer cmd negotiate qos: Disabled
EGTP GnGp Modify bearer res with APN-AMBR: Disabled
EGTP Modify bearer res with CHARGING-ID: Disabled
EGTP Modify bearer res with CHARGING-FQDN or CHARGING-GW-ADDRESS: Disabled
EGTP Modify bearer res with MSISDN: Disabled
EGTP Modify Bearer Response with Context Not Found cause if IMEI/IMEISV mismatch: Disabled
EGTP Bit Rate in Rounded Down Kbps: Disabled
EGTP Suppress Update Bearer Request (no bitrate change): Disabled
EGTP Create Session Response with APN-AMBR IE: Enabled
```



第 52 章

PMIP セッションのハートビートメカニズムでサポートされるピアのモニタリングの増加

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （989 ページ）
- 機能説明 （990 ページ）
- ハートビートメカニズム機能でサポートされる PMIP セッション数を増やすための設定 （991 ページ）
- モニタリングおよびトラブルシューティング （992 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC - SI • VPC - DI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.4

機能説明

既存のセットアップでは、HA マネージャはハートビートメカニズムを介して最大 256 のピアのプロキシモバイル IPv6（PMIP）セッションのモニタリングをサポートします。最近は、ピアのモニタリング対象を 256 から 128000 に増やすことが要求されるようになっています。

PMIP セッションの数を増やし、ハートビートメカニズムを利用してより多くのピアをモニタリングし、パス障害を検出できるようにするため、新しい CLI **monitor-max-peers** が LMA サービス コンフィギュレーション モードで追加されました。この機能は次の動作をサポートします。

- この CLI を設定すると、ハートビートモニタリングでサポートできるピアの最大数を 256 から 128000 ピアに増やすことができます。
- 最初の 128000 ピアは、ハートビートメカニズムが有効かどうかに関係なく、コール中に識別されます。
- 再送信ハートビートとバッチ処理の定期的なハートビートのリストは個別に保持されます。
- ピアをモニタリングするかどうかの決定は、コールのセットアップ、リカバリ、および ICSR の時点で行われます。たとえば、ハートビートのモニタリングが実行されているピアの数が 256 を超えているとします（CLI で最大 128000 ピアに設定されている）。この設定は後にデフォルト（最大 256 ピアのみをモニタリング）に変更されました。その後、HA マネージャのリカバリや ICSR（monitor-max-peers の設定が最大 256 ピア）が発生するまでは、すべてのピアでモニタリングが続行されます。
- ハートビートメッセージのバッチ処理のパラメータが次のように変更されました。

	バッチサイズ（以前）	バッチサイズ	バッチ間隔（以前）	バッチ間隔
定期的なハートビートバッチ	100	550	200 ms	200 ms
再送信ハートビートバッチ	100	550	200 ms	100 ミリ秒

- 10% を超えるピア（12800 ピア）から応答がない場合、ノードのパス障害の検出が遅延します。この遅延は、このような状態が発生したときにパフォーマンスに大きな影響を与えることを回避するためのものです。

計算に基づいて予想されるバッチサイズを超える再送信が開始されると、ハートビートメッセージはハートビートメッセージ送信用の定期的なタイマーに従います。たとえば、ハートビート間隔の設定が 60 秒の場合、再送信タイムアウトは 3 秒、最大再試行回数は 3 回です。

再送信のハートビートメッセージの数が予想されるバッチサイズを超える場合、3 秒ごとに再送信が発生する代わりに、ハートビートメッセージの再送信が 60 秒の間隔で開始されます。したがって、通常の状態でピアパス障害が最大 9 秒（3*3）で検出された場合、180 秒（60*3）で検出されるようになりました。

- 最小ハートビート間隔は 60 秒である必要があります。

  128000 ピアがハートビートのモニタリング対象に設定されている場合、ハートビート間隔を 60 秒未満に設定することはできません。ハートビート間隔を 60 秒未満に設定すると、設定エラーが表示されます。

- 最小のハートビート再送信タイムアウトは 3 秒にする必要があります。

  128000 ピアがハートビートのモニタリング対象に設定されている場合、ハートビート再送信のタイムアウトを 3 秒未満に設定することはできません。ハートビート間隔を 60 秒未満に設定すると、設定エラーが表示されます。

- CLI はサービスレベルで設定されますが、リストはインスタンスレベルで維持されます。したがって、すべてのサービスを同じ設定にすることを推奨します。

  サービスによって設定が異なる場合、それぞれのサービスレベルの設定に基づいて制限が適用されます。ただし、ピアの最大数は、そのインスタンスにすでに存在するピアの数に基づいて決定されます。

  たとえば、lma1 と lma2 の 2 つのサービスについて考えてみます。lma1 では、monitor-max-peers が 128000 ピアに設定されています。lma2 では、monitor-max-peers が 256 ピアで設定されています。これで、コールが lma1 から着信した場合は、128000 のピア上限がチェックされます。コールが lma2 から発信された場合は、256 のピア上限がチェックされます。ただし、lma2 には、lma1 でモニタリングされている 256 のピアすべてが含まれる可能性があります。

（注） これはお客様固有の機能です。詳細については、シスコのアカウント担当者にお問い合わせください。

ハートビートメカニズム機能でサポートされるPMIPセッション数を増やすための設定

次の項では、この機能を有効または無効にするための設定コマンドについて説明します。

heartbeat monitor-max-peers

この新しい CLI コマンドを使用すると、ハートビートメカニズムを利用して最大 128000 の PMIP セッションをモニタリングできます。この CLI は、LMA サービス コンフィギュレーション モードで追加されています。

PMIP セッションの最大数をモニタリングするよう設定するには、次のコマンドを入力します。

```
context context_name
 configure lma-service service_name
  [ default ] heartbeat monitor-max-peers
  end
```

注記

- **default**：ハートビートメカニズムを介して 256 個のピアをモニターします。デフォルトでは、この CLI は無効になっています。
- **heartbeat monitor-max-peers**：ハートビートメカニズムを介して最大 128000 個のピアをモニターします。

モニタリングおよびトラブルシューティング

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show コマンドと出力

この機能をサポートするために、次の CLI コマンドの出力範囲が拡張されています。

show lma-service all

次の **show lma-service all** CLI コマンドに、設定済みのハートビートモニター最大ピアの値が含まれるようになりました。

新しい CLI である heartbeat monitor-max-peers を設定する場合：

```
show lma-service all
  Heartbeat Support:        Enabled
  Heartbeat Interval:       60
  Heartbeat Retransmission timeout: 1
  Heartbeat Max Retransmissions: 1
  Heartbeat Monitor Max Peers: 128000
```

デフォルト CLI である default heartbeat monitor-max-peers を設定する場合：

```
show lma-service all
  Heartbeat Support:        Enabled
  Heartbeat Interval:       60
  Heartbeat Retransmission timeout: 1
  Heartbeat Max Retransmissions: 1
  Heartbeat Monitor Max Peers: 256
```

制約事項

- 新しい CLI では、最大 128000 の PMIP セッションをモニターできます。
- **heartbeat monitor-max-peers** CLI コマンドを設定するために、次の CLI 制限が追加されました。

  サービス起動時（Boxer 設定起動）：

  ハートビート間隔が 60 秒未満（LMA サービスについて）であるか、再送信タイムアウトが 3 秒未満（LMA サービス全体）である場合、monitor-max-peers コマンドでは設定エラーが表示され、monitor-max-peers 設定は適用されません。その逆も同様です。

  サービス設定の更新時：

  - 60 秒未満のハートビート間隔を設定しているときに、monitor-max-peers がその LMA サービスで、または LMA サービス全体ですでに設定されている場合は、設定エラーが表示されます。
  - 3 秒未満のハートビート再送信タイムアウトを設定しているときに、monitor-max-peers がその LMA サービスで、または LMA サービス全体ですでに設定されている場合は、設定エラーが表示されます。
  - monitor-max-peers を設定しているときに、その LMA サービスまたは LMA サービス全体のハートビート間隔が 60 秒未満であるか、ハートビート再送信タイムアウトが 3 秒未満である場合、設定エラーが表示されます。

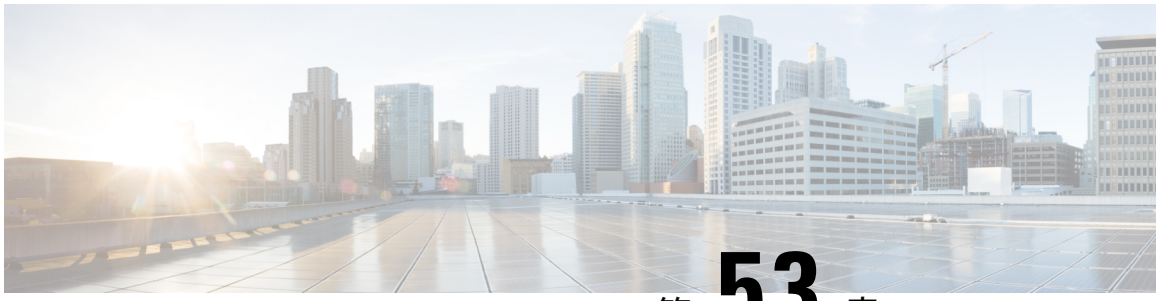
    次の CLI エラーが表示されます。

```
configure
contex pgw
lma-service lmav6
heartbeat interval 40
heartbeat monitor-max-peers
Failure: Recommended heartbeat interval: 60+, retransmission timeout: 3+, to
configure monitor-max-peers. Please retry.
heartbeat retransmission timeout 2
heartbeat monitor-max-peers
Failure: Recommended heartbeat interval: 60+, retransmission timeout: 3+, to
configure monitor-max-peers. Please retry.
end
```

```
configure
contex pgw
lma-service lmav6
heartbeat interval 60
heartbeat retransmission timeout 3
heartbeat monitor-max-peers
heartbeat interval 40
Failure: Recommended heartbeat interval: 60+, in presence of monitor-max-peers.
 Please retry.
heartbeat retransmission timeout 2
Failure: Recommended heartbeat retransmission timeout: 3+, in presence of
monitor-max-peers. Please retry.
end
```

  - 10% を超えるパス障害があり、パス障害の検出に遅延がある場合、次のような異常なログが表示されます。

```
"Retransmissons list size exceeds than expected, hb message will be sent with
periodicty of configured HB interval for callid 20016"
```



第 53 章

インライン TCP の最適化

この章では、次の事項について説明します。

- 機能の概要と変更履歴 （995 ページ）
- 機能説明 （996 ページ）
- 機能の仕組み （997 ページ）
- インライン TCP 最適化の設定 （998 ページ）
- モニタリングおよびトラブルシューティング （1002 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC - DI • VPC - SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、スループットゲインが引き上げられました。KPI：IP バージョン（IPv4/IPv6）およびアプリケーションプロトコル（HTTP/HTTPS）の個別のカウンタが追加されました。	21.10
このリリースでは、2 つの新しいコマンド（**accl-flags** と **cwnd-gain**）が TCP アクセラレーションプロファイルパラメータの設定に追加されています。これらのコマンドを設定すると、アクセラレーションされた TCP フローのスループットゲインが向上し、フロー途中のプロキシエンゲージメント手順が最適化されます。 また、**show tcp-acceleration-profile** コマンドの出力が更新されました。	21.9.1
インライン TCP 最適化エンジンが強化され、フローの途中で TCP アクセラレーション モジュールを動的に利用するようになりました。	21.9
最初の導入。	21.8

機能説明

インライン TCP 最適化は、TCP 接続の TCP フローのスループットを向上させるためのサービスプロバイダー向けの統合ソリューションです。このソリューションにより、データの転送が高速になり、ユーザーエクスペリエンスが向上します。

インライン TCP 最適化ソリューションは、所定の時間に効率的で最適なスループットを提供する独自のアルゴリズムを使用して TCP フローの高速化を保証します。TCP プロキシはこのソリューションと統合され、TCP 輻輳ウィンドウを監視および制御することで最適なスループットを実現します。

インライン TCP 最適化ソリューションでは、ワイヤレス要件に対応するためのスプリット TCP セッションもサポートされ、既存の他のインラインサービスと同等の機能を提供します。

（注） 最適化は、Gn インターフェイスのダウンリンクデータにのみ適用されます。

インライン TCP 最適化機能はライセンス制御されています。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

機能の仕組み

TCP 最適化機能には、次の機能が含まれます。

- TCP 接続の分割：TCP 接続が 2 つの接続に分割されます。P-GW 内の Gn への接続と Gi への接続に分割されます。接続は P-GW で透過的な方法で分割されるため、UE サーバーと Gi サーバーは分割される接続に対して透過的です。
- TCP プロキシにより、これら 2 つの TCP 分割接続でのデータのシームレスな移動が確実になります。
- TCP 最適化は、TCP スタックの（UE 側の）Gn インターフェイスに展開されます。P-GW のユーザー空間 TCP スタックが使用されます。
- TCP 最適化のためのシスコライブラリ：
  - TCP スループットを向上させるように設計されたアルゴリズムを提供します。
  - ユーザー空間 TCP スタック（Gn インターフェイス）とのインターフェイスとなり、TCP 接続で発生する適切なイベントについて通知し、それに応じたアクションを実行します。
  - シスコライブラリ（TCP 最適化用）と StarOS を統合するための API を提供します。

（注） TCP アクセラレーションは、TCP フローの開始中（SYN パケットの受信時）に有効になります。後でフローの実行中に無効にすることはできません。

選択された TCP フローのアクセラレーション

インライン TCP 最適化ソリューションは、最も適切な TCP フローを最適化するように設計されています。

次に、アクセラレーションの対象となる TCP フローを選択するいくつかの基準を示します。

- フローで確認されるデータの量を根拠とする：しきい値を超えるデータを含むフローがアクセラレーションの対象となります。
- TCP アクセラレーションは、スロットリングされた TCP フローに関する特定のシナリオでは回避されます。次に例を示します。
  - スロットリングされるように設定された ADC フロー。
  - OCS/PCRF によってトリガーされたデータ制限違反により、TCP フローがスロットリングされた。
  - スロットリングされているテザリング対象フロー。

- GBR/非 GBR を根拠とする：デフォルトベアラーの TCP フローのみが TCP アクセラレーションに適用されます。

（注） TCP アクセラレーションは、LTE RAT タイプでのみサポートされます。

インライン TCP 最適化の設定

アクティブ課金サービスでの TCP アクセラレーションの有効化

TCP アクセラレーションを有効にするには、次の設定を使用します。

```
configure
  require active-charging
  active-charging service service_name
    tcp-acceleration
    end
```

注：

- **tcp-acceleration**：ACS コンフィギュレーション モードで TCP アクセラレーションを有効にします。

トリガーアクションでの TCP アクセラレーションの有効化

TCP アクセラレーションを有効にするには、次の設定を使用します。

```
configure
  require active-charging
  active-charging service service_name
    trigger-action trigger_action_name
      tcp-acceleration profile profile_name
      end
```

注：

- **tcp-acceleration**：ACS トリガー アクション コンフィギュレーション モードで TCP アクセラレーションを有効にします。
- **profile**：TCP アクセラレーション プロファイルを特定します。*profile_name* は、1 ～ 63 文字の文字列です。

TCP アクセラレーション プロファイルの設定

TCP アクセラレーション プロファイルを設定するには、次の設定を使用します。

```
configure
  require active-charging
  active-charging service service_name
    [ no ] tcp-acceleration-profile profile_name
    end
```

注：

- **tcp-acceleration-profile**：インライン TCP 最適化のための TCP アクセラレーション機能プロファイルを設定します。
- **no**：TCP アクセラレーション プロファイルを無効にします。

TCP アクセラレーション プロファイル パラメータの設定

TCP アクセラレーション プロファイル パラメータを設定するには、以下のコマンドを使用します。

```
configure
  require active-charging
  active-charging service service_name
    [ no ] tcp-acceleration-profile profile_name
      accl-flags flag_value
      default accl-flags
      buffer-size { [ downlink [ 128KB | 256KB | 512KB | 1024KB |
1536KB | 2048KB | 2560KB | 3072KB | 3584KB | 4096KB ] [ uplink [ 128KB
 | 256KB | 512KB | 1024KB | 1536KB | 2048KB | 2560KB | 3072KB | 3584KB
 | 4096KB ] ] ] | [ uplink [ 128KB | 256KB | 512KB | 1024KB | 1536KB |
 2048KB | 2560KB | 3072KB | 3584KB | 4096KB ] [ downlink [ 128KB | 256KB
 | 512KB | 1024KB | 1536KB | 2048KB | 2560KB | 3072KB | 3584KB | 4096KB
 ] ] ] }
      cwnd-gain { dynamic { off | on } [ factor factor_value ] | factor
 factor_value [ dynamic { off | on } ] }
      default cwnd-gain
      default buffer-size [ downlink | uplink ]
      initial-cwnd-size window_size
      default initial-cwnd-size
      max-rtt max_rtt_value
      default max-rtt
      mss mss_value
      default mss
      end
```

注：

- **default**：後続のコマンドにデフォルト値を割り当てるか、復元します。
- **accl-flags**：TCP アクセラレーション関連の最適化フラグを設定します。flag_value は、0 ～ 65,535 の範囲の整数値です。
- **buffer-size**：ダウンリンクデータとアップリンクデータの TCP プロキシバッファサイズを KB 単位で設定します。

（注） このコマンドは、21.9.1以降のリリースでサポートされています。

- **cwnd-gain**：TCP 輻輳ウィンドウゲインを設定します。このコマンドは、実際の輻輳ウィンドウサイズを継続的に計算するためにTCP最適化エンジンによって使用されます。ウィンドウサイズのスケーリングにより、TCP最適化エンジンはエンジン内のデータの使用を管理できます。
  - このコマンドで **dynamic** オプションを使用すると、フロー中の RTT 変動を考慮して正しくサイズ設定されるように、輻輳ウィンドウゲインを自動的にスケールアップします。
  - **factor** オプションは、TCP 輻輳ウィンドウゲイン係数を設定します。*factor_value* は、1 ～ 16378 の範囲の整数値です。

（注） このコマンドは、21.9.1以降のリリースでサポートされています。

- **initial-cwnd-size**：初期の輻輳ウィンドウサイズの値をセグメント数で設定します。*window_size* は、1 ～ 65535 の範囲の整数値です。
- **max-rtt**：最大 RTT 値をミリ秒単位で設定します。*max_rtt_value* は、1 ～ 10000 の範囲の整数値です。
- **mss**：TCP の最大セグメントサイズをバイト単位で設定します。*mss_value* は、496 ～ 65535 の範囲の整数値です。

トリガー条件での後処理ルール名の設定

次のコマンドを使用して、後処理ルール名を設定します。

```
configure
  require active-charging
  active-charging service service_name
    trigger-condition trigger_condition_name
      post-processing-rule-name { = | contains | ends-with |
starts-with } rule_name
      [ no ] post-processing-rule-name rule_name
      end
```

注：

- **post-processing-rule-name**：特定の後処理ルールの条件を設定します。以下の演算子を使用して、ルールの一致方法を指定します。
  - **=**：等しい
  - **!=**：等しくない

- **contains**：次を含む
- **ends-with**：次の文字列で終わる
- **starts-with**：次の文字列で始まる

- *name*：後処理ルールの名前を指定します。

TCP アクセラレーション関連の EDR 属性の設定

EDR 属性を設定するには、次の設定を使用します。

```
configure
   require active-charging
   active-charging service service_name
      edr-format edr_format_name
         rule-variable tcp [ sn-tcp-accl | sn-tcp-accl-reject-reason |
sn-tcp-min-rtt | sn-tcp-rtt ] priority priority_value
         end
```

注：

- **rule variable**：EDR または UDR のルール変数属性を割り当てます。
- **tcp**：Transmission Control Protocol（TCP）関連フィールドを指定します。
  - **sn-tcp-accl**：TCP フローの TCP アクセラレーション ステータスを指定します。
    - **0**：フローの TCP アクセラレーションが有効ではありません。
    - **1**：フローの TCP アクセラレーションが有効です。
    - **2**：フローに適用可能であり、適用が試行されましたが、TCP アクセラレーションが有効になっていません。
    - **3**：フローに適用可能ですが、TCP アクセラレーションは試行されていません。
  - **sn-tcp-accl-reject-reason**：TCP フローがアクセラレーションされない理由を示します。
  - **sn-tcp-min-rtt**：アクセラレーションされた TCP フローに出現する最小 RTT を指定します。
  - **sn-tcp-rtt**：アクセラレーションされた TCP フローの平滑化 RTT を指定します。
- **priority**：EDR 内のフィールド（プロトコルルール）の CSV 位置を指定します。優先順位は 1 ～ 65535 の整数にする必要があります。

トリガーアクションでの TCP フローに関するフロー長しきい値の設定

TCP フローのフロー長しきい値は、サービススキーム フレームワークでトリガーアクションを使用して設定されます。フロー長のしきい値は、TCP アクセラレーション モジュールを動的に利用するために使用されます。

フローの途中でTCPアクセラレーションモジュールを利用するには、次の設定を使用します。

```
configure
  require active-charging
  active-charging service service_name
    trigger-action trigger_action_name
      tcp-acceleration flow-length threshold threshold_value
      no tcp-acceleration flow-length threshold
      end
```

注：

- **no**：トリガーアクションのフローリカバリを無効にします。
- **flow-length**：TCP フローのフロー長アクションを指定します。
- **threshold**：TCP フローのフロー長しきい値（バイト単位）を指定します。このしきい値は、1 ～ 10000 バイトの整数です。

トリガー条件での TCP フロー超過のフロー長しきい値の設定

TCP フローのフロー長条件 **exceed** は、サービススキーム フレームワークでトリガー条件を使用して設定されます。

TCP フロー長の条件を設定するには、次の設定を使用します。

```
configure
  require active-charging
  active-charging service service_name
    trigger-condition trigger_condition_name
      flow-length threshold exceed
      end
```

注：

- **flow-length**：TCP フローのフロー長条件を指定します。
- **threshold**：トリガーアクション設定で設定されるしきい値を指定します。
- **exceed**：フロー長超過時の超過条件を呼び出します。

モニタリングおよびトラブルシューティング

ここでは、この機能のモニタリングと障害対応について説明します。

コマンドや出力の表示

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show configuration

このコマンドの出力には、この機能の次のフィールドが表示されます。

- tcp-acceleration
- tcp-accelration profile tap
- buffer-size downlink *size* uplink *size*
- initial-cwnd-size
- max-rtt
- mss

show tcp-acceleration-profile { [all] | [name *profile-name*] }

このコマンドの出力には、この機能の次のフィールドが表示されます。

- TCP Acceleration Profile Name
  - Initial Congestion Window
  - Max RTT
  - MSS
  - Buffer Size (Downlink)
  - Buffer Size (Uplink)
  - Cwnd Gain Factor
  - Cwnd Gain Dynamic
  - Accl Flags
- Total tcp-acceleration-profile found

show active-charging tcp-acceleration info

このコマンドの出力には、この機能の次のフィールドが表示されます。

- TCP アクセラレーション ライブラリ情報
  - バージョン

show active-charging tcp-acceleration statistics sessmgr all

このコマンドの出力には、この機能の次のフィールドが表示されます。

- TCP アクセラレーション統計
  - 合計高速フロー
  - 現在の高速フロー
  - リリース済みの高速フロー
  - 拒否された高速フロー
    - サポートされていない機能
    - サポートされていない RAT タイプ
    - サポートされていないベアラー
    - 使用できないリソース（メモリ）
    - その他
  - サブスクライバレベル統計
    - 合計高速サブスクライバ
    - 現在の高速サブスクライバ
  - プロトコルレベル統計
    - 合計フロー（IPv4 および IPv6）
      - TCP
      - HTTP
      - HTTPS
    - アクティブフロー（IPv4 および IPv6）
      - TCP
      - HTTP
      - HTTPS
    - 現在のアイドルフロー（IPv4 および IPv6）
      - TCP
      - HTTP
      - HTTPS
    - アイドルタイマーごとのクリア度（IPv4 および IPv6）
      - TCP
      - HTTP

- HTTPS

- 制御統計
  - IPv4（ユーザー側とインターネット側）
    - TCP 終了 Rx
    - TCP 終了 Tx
  - IPv6（ユーザー側とインターネット側）
    - TCP 終了 Rx
    - TCP 終了 Tx

- データ統計
  - IPv4（ユーザー側とインターネット側）
    - Rx のパケット合計
    - Rx のバイト合計
    - Tx のパケット合計
    - Tx のバイト合計
    - HTTP（ユーザー側とインターネット側）
      - Rx のパケット合計
      - Rx のバイト合計
      - Tx のパケット合計
      - Tx のバイト合計
      - Rx の再送パケット数
      - Rx の再送バイト数
      - Tx の再送パケット数
      - Tx の再送バイト数
    - HTTPS（ユーザー側とインターネット側）
      - Rx のパケット合計
      - Rx のバイト合計
      - Tx のパケット合計

- Tx のバイト合計
- Rx の再送パケット数
- Rx の再送バイト数
- Tx の再送パケット数
- Tx の再送バイト数

- IPv6（ユーザー側とインターネット側）
  - Rx のパケット合計
  - Rx のバイト合計
  - Tx のパケット合計
  - Tx のバイト合計
  - HTTP（ユーザー側とインターネット側）
    - Rx のパケット合計
    - Rx のバイト合計
    - Tx のパケット合計
    - Tx のバイト合計
    - Rx の再送パケット数
    - Rx の再送バイト数
    - Tx の再送パケット数
    - Tx の再送バイト数
  - HTTPS（ユーザー側とインターネット側）
    - Rx のパケット合計
    - Rx のバイト合計
    - Tx のパケット合計
    - Tx のバイト合計
    - Rx の再送パケット数
    - Rx の再送バイト数
    - Tx の再送パケット数
    - Tx の再送バイト数

show active-charging flows full all

このコマンドの出力には、この機能の次のフィールドが表示されます。

- TCP Acceleration

show active-charging trigger-action name *trigger_action_name*

上記のコマンドを実行すると、この機能に関する次の新しいフィールドが表示されます。

- TCP Acceleration
- TCP Acceleration Treshold

show active-charging trigger-condition name *name*

このコマンドの出力には、この機能の次のフィールドが表示されます。

- Post-Processing Rule-name/GOR
- Flow-Length Threshold exceed

バルク統計

インライン TCP 最適化（フェーズ 2）機能をサポートするために、次のバルク統計が **CUSP** スキーマに追加されています。

バルク統計	説明
tcpaccl-totflows	TCP 高速フローの総数を示します。
tcpaccl-currflows	現在の TCP 高速フローの数を示します。
tcpaccl-usr-ipv4totpkts-rx	UE から受信した IPv4 TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv4totbytes-rx	UE から受信した IPv4 TCP 高速パケットの合計バイト数を示します。
tcpaccl-usr-ipv4totpkts-tx	UE に送信された IPv4 TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv4totbytes-tx	UE に送信された IPv4 TCP 高速パケットの合計バイト数を示します。
tcpaccl-inet-ipv4totpkts-rx	インターネットから受信した IPv4 TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv4totbytes-rx	インターネットから受信した IPv4 TCP 高速パケットの合計バイト数を示します。

バルク統計	説明
tcpaccl-inet-ipv4totpkts-tx	インターネットに送信された IPv4 TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv4totbytes-tx	インターネットに送信された IPv4 TCP 高速パケットの合計バイト数を示します。
tcpaccl-usr-ipv6totpkts-rx	UE から受信した IPv6 TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv6totbytes-rx	UE から受信した IPv6 TCP 高速パケットの合計バイト数を示します。
tcpaccl-usr-ipv6totpkts-tx	UE に送信された IPv6 TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv6totbytes-tx	UE に送信された IPv6 TCP 高速パケットの合計バイト数を示します。
tcpaccl-inet-ipv6totpkts-rx	インターネットから受信した IPv6 TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv6totbytes-rx	インターネットから受信した IPv6 TCP 高速パケットの合計バイト数を示します。
tcpaccl-inet-ipv6totpkts-tx	インターネットに送信された IPv6 TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv6totbytes-tx	インターネットに送信された IPv6 TCP 高速パケットの合計バイト数を示します。

インライン TCP 最適化（フェーズ 3）機能をサポートするために、次のバルク統計が **CUSP** スキーマに追加されています。

バルク統計	説明
tcpaccl-tot-subs	1 つ以上の TCP 高速フローを使用するサブスクライバの総数を示します。
tcpaccl-curr-subs	1 つ以上の TCP 高速フローを使用するアクティブサブスクライバの数を示します。
tcpaccl-ipv4-tot-tcp-flows	TCP 高速 IPv4 フローの総数を示します。
tcpaccl-ipv6-tot-tcp-flows	TCP 高速 IPv6 フローの総数を示します。
tcpaccl-ipv4-tot-http-flows	TCP 高速 IPv4 HTTP フローの総数を示します。
tcpaccl-ipv6-tot-http-flows	TCP 高速 IPv6 HTTP フローの総数を示します。

バルク統計	説明
tcpaccl-ipv4-tot-https-flows	TCP 高速 IPv4 HTTPS フローの総数を示します。
tcpaccl-ipv6-tot-https-flows	TCP 高速 IPv6 HTTPS フローの総数を示します。
tcpaccl-ipv4-curr-tcp-flows	アクティブな TCP 高速 IPv4 フローの現在の数を示します。
tcpaccl-ipv6-curr-tcp-flows	アクティブな TCP 高速 IPv6 フローの現在の数を示します。
tcpaccl-ipv4-curr-http-flows	アクティブな TCP 高速 IPv4 HTTP フローの現在の数を示します。
tcpaccl-ipv6-curr-http-flows	アクティブな TCP 高速 IPv6 HTTP フローの現在の数を示します。
tcpaccl-ipv4-curr-https-flows	アクティブな TCP 高速 IPv4 HTTPS フローの現在の数を示します。
tcpaccl-ipv6-curr-https-flows	アクティブな TCP 高速 IPv6 HTTPS フローの現在の数を示します。
tcpaccl-ipv4-curr-tcp-idleflows	アイドル状態の TCP 高速 IPv4 フローの現在の数を示します。
tcpaccl-ipv6-curr-tcp-idleflows	アイドル状態の TCP 高速 IPv6 フローの現在の数を示します。
tcpaccl-ipv4-curr-http-idleflows	アイドル状態の TCP 高速 IPv4 HTTP フローの現在の数を示します。
tcpaccl-ipv6-curr-http-idleflows	アイドル状態の TCP 高速 IPv6 HTTP フローの現在の数を示します。
tcpaccl-ipv4-curr-https-idleflows	アイドル状態の TCP 高速 IPv4 HTTPS フローの現在の数を示します。
tcpaccl-ipv6-curr-https-idleflows	アイドル状態の TCP 高速 IPv6 HTTPS フローの現在の数を示します。
tcpaccl-ipv4-tcp-flows-idle-timeout	アイドルタイムアウトによりクリアされた TCP 高速 IPv4 フローの総数を示します。
tcpaccl-ipv6-tcp-flows-idle-timeout	アイドルタイムアウトによりクリアされた TCP 高速 IPv6 フローの総数を示します。

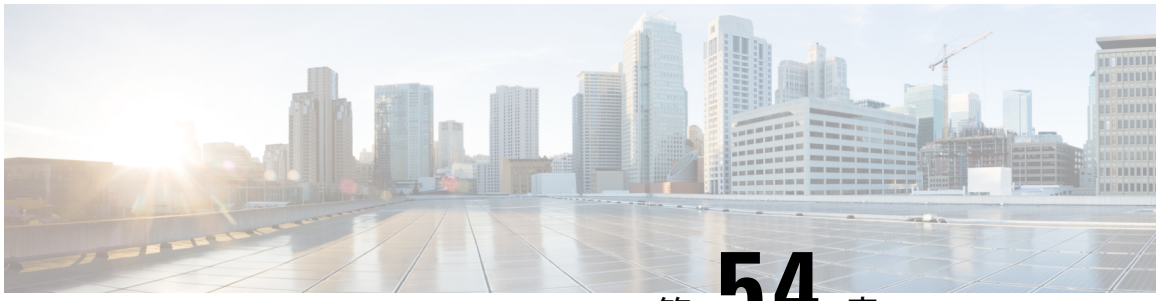
バルク統計	説明
tcpaccl-ipv4-http-flows-idle-timeout	アイドルタイムアウトによりクリアされたTCP高速 IPv4 HTTP フローの総数を示します。
tcpaccl-ipv6-http-flows-idle-timeout	アイドルタイムアウトによりクリアされたTCP高速 IPv6 HTTP フローの総数を示します。
tcpaccl-ipv4-https-flows-idle-timeout	アイドルタイムアウトによりクリアされたTCP高速 IPv4 HTTPS フローの総数を示します。
tcpaccl-ipv6-https-flows-idle-timeout	アイドルタイムアウトによりクリアされたTCP高速 IPv6 HTTPS フローの総数を示します。
tcpaccl-usr-ipv4-tcpterm-rx	TCP 高速 IPV4 フローで UE から受信した TCP リセット終了要求の総数を示します。
tcpaccl-usr-ipv6-tcpterm-rx	TCP 高速 IPV6 フローで UE から受信した TCP リセット終了要求の総数を示します。
tcpaccl-usr-ipv4-tcpterm-tx	TCP 高速 IPV4 フローで UE に送信した TCP リセット終了要求の総数を示します。
tcpaccl-usr-ipv6-tcpterm-tx	TCP 高速 IPV6 フローで UE に送信した TCP リセット終了要求の総数を示します。
tcpaccl-inet-ipv4-tcpterm-rx	TCP 高速 IPV4 フローでサーバーから受信した TCP リセット終了要求の総数を示します。
tcpaccl-inet-ipv6-tcpterm-rx	TCP 高速 IPV6 フローでサーバーから受信した TCP リセット終了要求の総数を示します。
tcpaccl-inet-ipv4-tcpterm-tx	TCP 高速 IPV4 フローでサーバーに送信した TCP リセット終了要求の総数を示します。
tcpaccl-inet-ipv6-tcpterm-tx	TCP 高速 IPV6 フローでサーバーに送信した TCP リセット終了要求の総数を示します。
tcpaccl-usr-ipv4-http-totpkts-rx	UE から受信した IPv4 HTTP TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv4-http-totbytes-rx	UE から受信した IPv4 HTTP TCP 高速パケットの合計バイト数を示します。
tcpaccl-usr-ipv4-http-totpkts-tx	UE に送信された IPv4 HTTP TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv4-http-totbytes-tx	UE に送信された IPv4 HTTP TCP 高速パケットの合計バイト数を示します。

バルク統計	説明
tcpaccl-inet-ipv4-http-totpkts-rx	インターネットから受信した IPv4 HTTP TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv4-http-totbytes-rx	インターネットから受信した IPv4 HTTP TCP 高速パケットの合計バイト数を示します。
tcpaccl-inet-ipv4-http-totpkts-tx	インターネットに送信された IPv4 HTTP TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv4-http-totbytes-tx	インターネットに送信された IPv4 HTTP TCP 高速パケットの合計バイト数を示します。
tcpaccl-usr-ipv6-http-totpkts-rx	UE から受信した IPv6 HTTP TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv6-http-totbytes-rx	UE から受信した IPv6 HTTP TCP 高速パケットの合計バイト数を示します。
tcpaccl-usr-ipv6-http-totpkts-tx	UE に送信された IPv6 HTTP TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv6-http-totbytes-tx	UE に送信された IPv6 HTTP TCP 高速パケットの合計バイト数を示します。
tcpaccl-inet-ipv6-http-totpkts-rx	インターネットから受信した IPv6 HTTP TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv6-http-totbytes-rx	インターネットから受信した IPv6 HTTP TCP 高速パケットの合計バイト数を示します。
tcpaccl-inet-ipv6-http-totpkts-tx	インターネットに送信された IPv6 HTTP TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv6-http-totbytes-tx	インターネットに送信された IPv6 HTTP TCP 高速パケットの合計バイト数を示します。
tcpaccl-usr-ipv4-https-totpkts-rx	UE から受信した IPv4 HTTPS TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv4-https-totbytes-rx	UE から受信した IPv4 HTTPS TCP 高速パケットの合計バイト数を示します。
tcpaccl-usr-ipv4-https-totpkts-tx	UE に送信された IPv4 HTTPS TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv4-https-totbytes-tx	UE に送信された IPv4 HTTPS TCP 高速パケットの合計バイト数を示します。

バルク統計	説明
tcpaccl-inet-ipv4-https-totpkts-rx	インターネットから受信した IPv4 HTTPS TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv4-https-totbytes-rx	インターネットから受信した IPv4 HTTPS TCP 高速パケットの合計バイト数を示します。
tcpaccl-inet-ipv4-https-totpkts-tx	インターネットに送信された IPv4 HTTPS TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv4-https-totbytes-tx	インターネットに送信された IPv4 HTTPS TCP 高速パケットの合計バイト数を示します。
tcpaccl-usr-ipv6-https-totpkts-rx	UE から受信した IPv6 HTTPS TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv6-https-totbytes-rx	UE から受信した IPv6 HTTPS TCP 高速パケットの合計バイト数を示します。
tcpaccl-usr-ipv6-https-totpkts-tx	UE に送信された IPv6 HTTPS TCP 高速パケットの総数を示します。
tcpaccl-usr-ipv6-https-totbytes-tx	UE に送信された IPv6 HTTPS TCP 高速パケットの合計バイト数を示します。
tcpaccl-inet-ipv6-https-totpkts-rx	インターネットから受信した IPv6 HTTPS TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv6-https-totbytes-rx	インターネットから受信した IPv6 HTTPS TCP 高速パケットの合計バイト数を示します。
tcpaccl-inet-ipv6-https-totpkts-tx	インターネットに送信された IPv6 HTTPS TCP 高速パケットの総数を示します。
tcpaccl-inet-ipv6-https-totbytes-tx	インターネットに送信された IPv6 HTTPS TCP 高速パケットの合計バイト数を示します。
tcpaccl-usr-ipv4-http-pktsretrans-tx	TCP 高速 IPv4 HTTP フローで UE に再送信されたパケットの総数を示します。
tcpaccl-usr-ipv4-http-pktsretrans-rx	TCP 高速 IPv4 HTTP フローで UE から受信した再送信パケットの総数を示します。
tcpaccl-usr-ipv4-http-bytesretrans-tx	TCP 高速 IPv4 HTTP フローで UE に再送信されたパケットの合計バイト数を示します。
tcpaccl-usr-ipv4-http-bytesretrans-rx	TCP 高速 IPv4 HTTP フローで UE から受信した再送信パケットの合計バイト数を示します。

バルク統計	説明
tcpaccl-inet-ipv4-http-pktsretrans-tx	TCP 高速 IPv4 HTTP フローでサーバーに再送信されたパケットの総数を示します。
tcpaccl-inet-ipv4-http-pktsretrans-rx	TCP 高速 IPv4 HTTP フローでサーバーから受信した再送信パケットの総数を示します。
tcpaccl-inet-ipv4-http-bytesretrans-tx	TCP 高速 IPv4 HTTP フローでサーバーに再送信されたパケットの合計バイト数を示します。
tcpaccl-inet-ipv4-http-bytesretrans-rx	TCP 高速 IPv4 HTTP フローでサーバーから受信した再送信パケットの合計バイト数を示します。
tcpaccl-usr-ipv6-http-pktsretrans-tx	TCP 高速 IPv6 HTTP フローで UE に再送信されたパケットの総数を示します。
tcpaccl-usr-ipv6-http-pktsretrans-rx	TCP 高速 IPv6 HTTP フローで UE から受信した再送信パケットの総数を示します。
tcpaccl-usr-ipv6-http-bytesretrans-tx	TCP 高速 IPv6 HTTP フローで UE に再送信されたパケットの合計バイト数を示します。
tcpaccl-usr-ipv6-http-bytesretrans-rx	TCP 高速 IPv6 HTTP フローで UE から受信した再送信パケットの合計バイト数を示します。
tcpaccl-inet-ipv6-http-pktsretrans-tx	TCP 高速 IPv6 HTTP フローでサーバーに再送信されたパケットの総数を示します。
tcpaccl-inet-ipv6-http-pktsretrans-rx	TCP 高速 IPv6 HTTP フローでサーバーから受信した再送信パケットの総数を示します。
tcpaccl-inet-ipv6-http-bytesretrans-rx	TCP 高速 IPv6 HTTP フローでサーバーから受信した再送信パケットの合計バイト数を示します。
tcpaccl-usr-ipv4-https-pktsretrans-tx	TCP 高速 IPv4 HTTPS フローで UE に再送信されたパケットの総数を示します。
tcpaccl-usr-ipv4-https-pktsretrans-rx	TCP 高速 IPv4 HTTPS フローで UE から受信した再送信パケットの総数を示します。
tcpaccl-usr-ipv4-https-bytesretrans-tx	TCP 高速 IPv4 HTTPS フローで UE に再送信されたパケットの合計バイト数を示します。
tcpaccl-usr-ipv4-https-bytesretrans-rx	TCP 高速 IPv4 HTTPS フローで UE から受信した再送信パケットの合計バイト数を示します。

バルク統計	説明
tcpaccl-inet-ipv4-https-pktsretrans-tx	TCP 高速 IPv4 HTTPS フローでサーバーに再送信されたパケットの総数を示します。
tcpaccl-inet-ipv4-https-pktsretrans-rx	TCP 高速 IPv4 HTTPSフローでサーバーから受信した再送信パケットの総数を示します。
tcpaccl-inet-ipv4-https-bytesretrans-tx	TCP 高速 IPv4 HTTPS フローでサーバーに再送信されたパケットの合計バイト数を示します。
tcpaccl-inet-ipv4-https-bytesretrans-rx	TCP 高速 IPv4 HTTPS フローでサーバーから受信した再送信パケットの合計バイト数を示します。
tcpaccl-usr-ipv6-https-pktsretrans-tx	TCP 高速 IPv4 HTTPS フローでサーバーから受信した再送信パケットの合計バイト数を示します。
tcpaccl-usr-ipv6-https-pktsretrans-tx	TCP 高速 IPv6 HTTPS フローで UE に再送信されたパケットの総数を示します。
tcpaccl-usr-ipv6-https-pktsretrans-rx	TCP 高速 IPv6 HTTPS フローで UE から受信した再送信パケットの総数を示します。
tcpaccl-usr-ipv6-https-bytesretrans-tx	TCP 高速 IPv6 HTTPS フローで UE に再送信されたパケットの合計バイト数を示します。
tcpaccl-usr-ipv6-https-bytesretrans-rx	TCP 高速 IPv6 HTTPS フローで UE から受信した再送信パケットの合計バイト数を示します。
tcpaccl-inet-ipv6-https-pktsretrans-tx	TCP 高速 IPv6 HTTPS フローでサーバーに再送信されたパケットの総数を示します。
tcpaccl-inet-ipv6-https-pktsretrans-rx	TCP 高速 IPv6 HTTPS フローでサーバーから受信した再送信パケットの総数を示します。
tcpaccl-inet-ipv6-https-bytesretrans-tx	TCP 高速 IPv6 HTTPS フローでサーバーに再送信されたパケットの合計バイト数を示します。
tcpaccl-inet-ipv6-https-bytesretrans-rx	TCP 高速 IPv6 HTTPS フローでサーバーから受信した再送信パケットの合計バイト数を示します。



第 54 章

S11-U TEID のないベアラー変更要求の MME 間ハンドオーバー

- 機能の概要と変更履歴 （1015 ページ）
- 機能説明 （1016 ページ）
- 機能の仕組み （1016 ページ）
- S11-U TEID のないベアラー変更要求の MME 間ハンドオーバーの設定 （1019 ページ）
- モニタリングおよびトラブルシューティング （1019 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• S-GW • P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	N/A

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。 **重要** この機能は、すべてのお客様の展開シナリオでは検証されていません。詳細については、シスコのアカウント担当者にお問い合わせください。	21.23

機能説明

NB-IoT/コントロールプレーン CIoT EPS 最適化時に、ユーザーデータが転送されるか、SMS メッセージが MME を介して渡されます。これは、非アクセス階層（NAS）でカプセル化することによって実行され、短いデータトランザクションを処理するときのコントロールプレーンメッセージの合計数が削減されます。コントロールプレーン CIoT EPS 最適化が適用される場合、MME は、次のようになります。

- NAS ユーザーデータの S11 インターフェイス ユーザー プレーン（S11-U）トンネリングを示し、S-GW へのダウンリンク（DL）データ転送のために、独自の S11-U IP アドレスと MME DL トンネルエンドポイント識別子（TEID）を送信します。
- S-GW は、コントロールプレーン CIoT EPS 最適化のためのセッション作成応答を、S11-U の S-GW アドレスおよび S-GW TEID とともに返します。これらは、MME によって、アップリンク（UL）データを S-GW に転送するために使用されます。

このようなインスタンスには、次の制約がある可能性があります。

- S-GW は、S11-U F-TEID のないベアラー変更要求（MBR）を検証します。
- S11TF フラグが設定されているときは F-TEID が必須と見なされるため、MBR に S11-U F-TEID がない場合、S-GW は、MME 間ハンドオーバー（HO）を拒否します。

上記の制約を克服し、IoT デバイスの要件に対応するために、S-GW は、NB-IoT サブスクライバ向けに、S11-U TEID 機能を使用せずに MME 間ハンドオーバーベアラー変更要求をサポートします。

機能の仕組み

この機能が S-GW サービス コンフィギュレーション モードで有効になっている場合、次の検証が行われます。

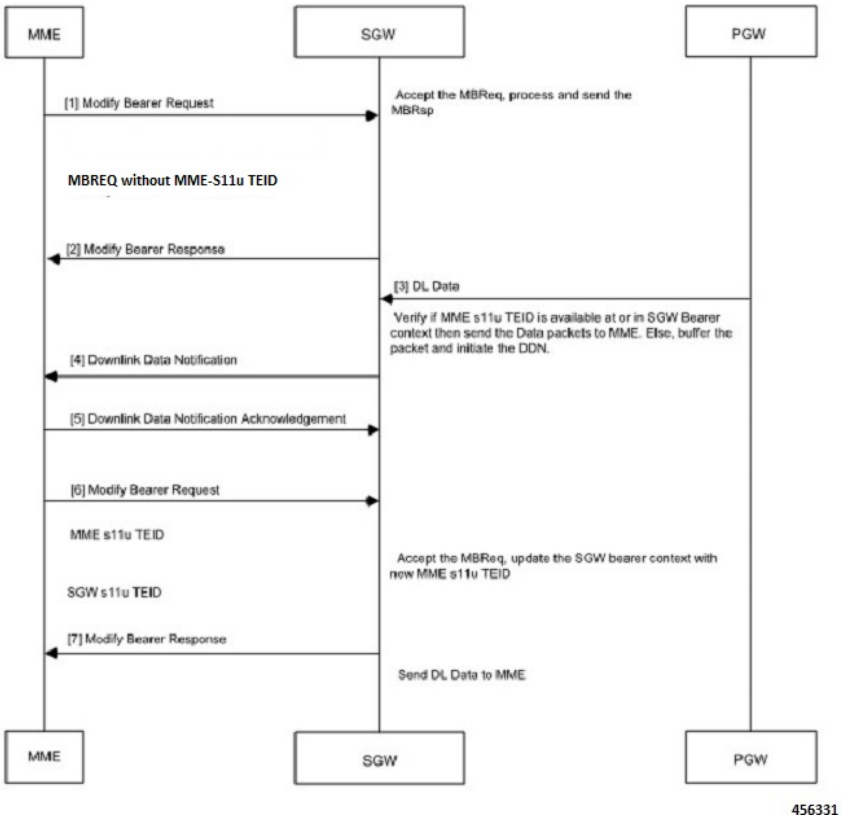
- EGTP プロトコルでの IE 検証の処理
- ダウンリンクデータの処理
- アップリンクデータの処理

通話フロー

EGTP プロトコルでの IE 検証の処理：S-GW サービス コンフィギュレーション モードで **mme-s11u-without-teid**CLI コマンドを使用して、EGTP プロトコルでの IE 検証の処理を有効にすると、フラグが TRUE に設定されます（デフォルトは FALSE）。

- S11-U TEID 検証はバイパスされます。
- S-GW は、ベアラー変更要求を受け入れ、ハンドオーバーが成功するまでプロセスを続行します。

図 *79 : EGTP* プロトコルで *IE* 検証の処理のコールフロー



次の表で、初期アタッチ手順における MME と S-GW の間の機能について説明します。

表 *88 :* 手順

ステップ	説明
1	ユーザー機器（UE）が、初期アタッチを MME に送信し、送信元 MME、S-GW、および P-GW を使用してコントロールプレーン CIoT 最適化 S11-U EPS ベアラーを確立します。
2	しばらくすると、UE がアイドル状態に移行します。

ステップ	説明
3	アクティビティがないため、送信元 MME が、S-GW との S11-U トンネルをリリースします。
4	UE が、新しい eNB でアクティブ状態に移行し、トラッキングエリア更新（TAU）要求をターゲット MME に送信します。
5	ターゲット MME が、TAU 要求を使用し、コンテキスト要求を送信元 MME に送信します。
6	送信元 MME が、コンテキスト応答の新しいターゲット MME にすべての GTP-C GTP-U F-TEID を提供します。
7	ターゲット MME が、ベアラー変更要求のベアラーコンテキスト内の MME GTP-U S11-U TEID、S5/S8 関連情報を送信しなかった場合、ターゲット MME からのベアラー変更要求が、MME S11-U TEID および S5/S8 に関する情報なしで S-GW に到達します。
8	S-GW が、ベアラー変更要求を検証し、要求メッセージに S11-U TEID が欠落していることを確認します。ベアラー変更要求メッセージで S11TF フラグが設定されている場合、S11-U TEID は必須 IE と見なされます。MME S11TF フラグが設定されているのに、機能 CLI が有効になっているときに MME S11-U-Teid が存在しない場合でも、S-GW はベアラー変更要求を拒否しません。

ダウンリンクデータの処理：S-GW が、P-GW からダウンリンクデータを受信します。MME S11-U TEID が S-GW ベアラーコンテキストで使用できない場合、または S11-U インターフェイスが非アクティブである場合、S-GW は、DL パケットをバッファし、次の手順で MME へのダウンリンクデータ通知を開始します。

表 *89 :* 手順

ステップ	説明
1	MME S11-U TEID のないベアラー変更要求を受信します。
2	MME に送信されるベアラー変更応答に S-GW S11-U TEID が含まれます。
3	S-GW が、S5/S8 インターフェイスで P-GW からダウンリンクデータを受信します。
4	ダウンリンクデータ通知が MME に送信されます。

アップリンクデータの処理：S-GW が、MME から受信したアップリンクデータを受け入れ、そのデータを S5/S8 インターフェイス上の P-GW に転送します。たとえば、MME S11-U TEID のないベアラー変更要求を受信した場合、アップリンクデータの処理時に次の手順が発生します。

表 *90 :* 手順

ステップ	説明
1	MME S11-U TEID のないベアラー変更要求を受信します。
2	MME に送信されるベアラー変更応答に S-GW S11-U TEID が含まれます。
3	S11 インターフェイス データ トンネル上の MME からアップリンクデータを受信します。
4	アップリンクデータが、S5/S8 インターフェイス データ トンネル上の P-GW に転送されます。

S11-U TEID のないベアラー変更要求の MME 間ハンドオーバーの設定

S11-U TEID 機能を使用しないベアラー変更要求の MME 間ハンドオーバーを有効または無効にするには、次の設定を使用します。

```
configure
    context context_name
      sgw-service service_name
        [ no | default ] egtp modify-bearer-req accept
mme-s11u-without-teid
          end
```

注：

- **default**：この機能を無効化します。この機能はデフォルトで無効に設定されています。
- **egtp modify-bearer-req accept mme-s11u-without-teid** ：S-GW が、要求メッセージに存在する、S11u TEID IE のない MBR を受け入れられるようにします。
- **no**：この機能を無効化します。

S11-U TEID 機能設定を使用しないベアラー変更要求の MME 間ハンドオーバーの確認

この機能が有効か無効かを確認するには、**show sgw-services name** *sgw_service* または **show configuration** CLI コマンドを使用します。

モニタリングおよびトラブルシューティング

ここでは、P-GW/S-GW で S11-U TEID のないベアラー変更要求の MME 間ハンドオーバーをモニターおよびトラブルシュートする際に使用できるコマンドについて説明します。

コマンドと出力の表示

S11-U TEID がないベアラー変更要求の MME 間ハンドオーバーをサポートするために、次の CLI コマンドを使用できます。

show sgw-service statistics all

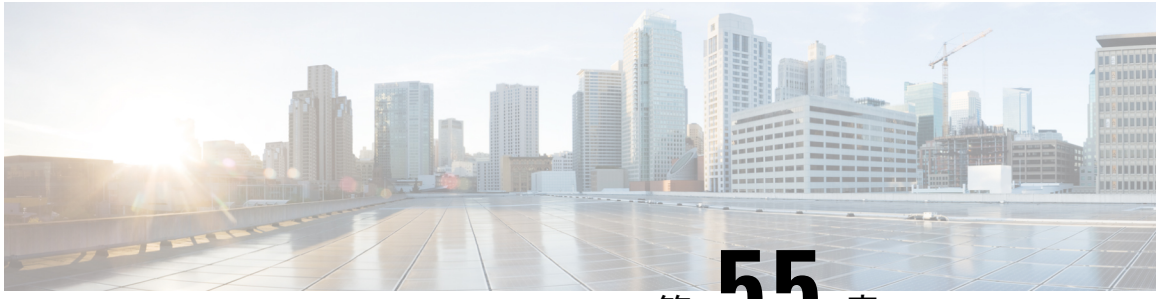
この CLI コマンド（および、**show saegw-service statistics all function sgw** CLI コマンド）の出力範囲が拡張され、次のフィールドが表示されるようになりました。

フィールド	説明
S11-U Buffered Data Statistics Without MME TEID：	
アップリンク	バッファされたアップリンクデータパケットの合計数を示します。 （注） このフィールドは、S11-U TEID 機能を使用しない MME 間ハンドオーバーベアラー変更要求には適用されません。
パケットの総数	MME から受信したパケットの合計数を示します。 （注） このフィールドは、S11-U TEID 機能を使用しない MME 間ハンドオーバーベアラー変更要求には適用されません。
ダウンリンク	MME S11-U TEID がない場合に S-GW でバッファされたダウンリンクデータパケットの合計数を示します。
パケットの総数	MME S11-U TEID がない場合にバッファされるダウンリンクパケットの合計数を示します。

show egtpc statistics

この CLI コマンドの出力範囲が拡張され、次のフィールドが表示されるようになりました。

フィールド	説明
Modify Bearer Request Without MME S11u TEID	
Total Rx	MME S11-U TEID 情報要素（IE）なしで受信したベアラー変更要求メッセージの合計数を示します。
Accepted	MME S11-U TEID 情報要素（IE）なしで受け入れたベアラー変更要求メッセージの合計数を示します。



第 55 章

IP Network Enabler

ここでは、StarOS IP Network Enabler（IPNE）機能について説明します。また、この機能の動作と、IPNE の設定およびモニター方法について説明します。

- 機能説明 （1021 ページ）
- 機能の仕組み （1023 ページ）
- IPNE 機能の設定 （1028 ページ）
- IPNE サービスのモニタリング （1030 ページ）

機能説明

この項では、IPNE 機能について説明します。

IPNE（IP Network Enabler）は、P-GW、GGSN、HA、HNBGW など、通信事業者のネットワーク内のさまざまなネットワークノードで実行される MINE クライアントコンポーネントです。セッションおよびネットワークの情報を収集して MINE サーバーに配布します。MINE クラウドサービスは、ワイヤレス通信事業者とパートナーがセッションおよびネットワークの情報を共有および交換してインテリジェントなサービスを実現するための、一元化されたポータルを提供します。

この情報は、MINE サーバーと IPNE サービスの間で XML データの形式で共有されます。IPNE サービスにおけるコアオブジェクトは、XMPP プロトコルエンジンです。設定された MINE サーバーピアごとに 1 つの XMPP プロトコル エンジン インスタンスがあります。エンジンは FSM を使用して XMPP プロトコルを実装します。

共有されるすべての情報は、その時点でのコンテキストから得られます。また、IPNE サービスレベルスケジューラも実装されており、すべてのハンドルのフィードおよび通知アクティビティをレート制御して、コール処理およびデータパスのパフォーマンスに影響を与える過負荷を回避します。

他の機能との関係

ここでは、IPNE サービスが他の機能とどのように関連するかについて説明します。

IPNE を設定する前に、次の GW サービスのいずれかを StarOS で設定する必要があります。

- GGSN
- HA
- HNBGW
- P-GW

設定手順については、『*GGSN Administration Guide*』、『*HA Administration Guide*』、『*HNBGW Administration Guide* 』、および『*P-GW Administration Guide*』を参照してください。

MINE クラウドサービスは、ワイヤレス通信事業者とパートナーがセッションおよびネットワークの情報を共有および交換してインテリジェントなサービスを実現するための一元化されたポータルを提供します。MINE クライアントコンポーネントは、PGW、HA など、通信事業者のネットワーク内のさまざまなネットワークノードで実行され、セッションおよびネットワークの情報を収集して MINE サーバーに配布します。クライアントは IPNE です。

IPNE クライアントは、設定可能なサービスとして StarOS 上で実行されます。Enhanced Charging Service（ECS）コンポーネントは、定義された要件を満たすために IPNE クライアントと連携します。

最高の IPNE パフォーマンスを実現するために、ECS コンポーネントは次の機能を提供する必要があります。

- ECS によって、フロー情報パラメータが IPNE に提供される必要があります。
  - タプル情報
  - URL
  - ユーザエージェント（User Agent）
  - アプリケーションプロトコル
  - フロー作成時間

ECS によって、NBR 情報パラメータが IPNE に提供される必要があります。

- NAT-IP アドレス
- 開始ポート
- 終了ポート

ECS は、サブスクライバのコール ID でインデックス化された MINE サーバーからのクエリに対応する応答内のすべてのアクティブフローに対して、上記のパラメータを提供する必要があります。

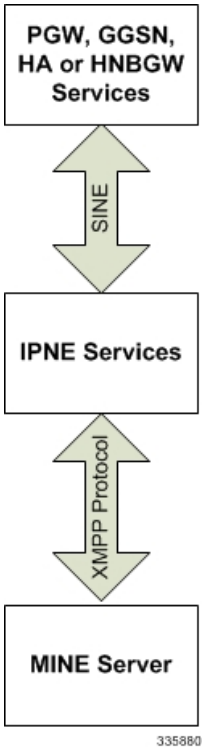
サブスクライバのコール ID に対して IPNE クライアントによってインストールされたサブスクリプションの場合、ECS は、サブスクリプショントリガーが検出されるたびに通知メッセージを IPNE クライアントに送信する必要があります。

機能の仕組み

IPNE

次の図は、IPNE インターフェイスのアーキテクチャについて説明しています。セッションマネージャと IPNE は、SINE インターフェイスを介して対話します。情報は、clp ハンドルの形式でモジュール間で交換されます。セッションごとに 1 つの IPNE ハンドルが作成されます。情報は、IPNE クライアント側のローカルデータベースに保存されます。

図 *80 : IPNE* アーキテクチャの概要



対話は、次のタイミングで行われます。

- IPNE 側でセッション情報を追加するためのセッションセットアップ
- フィードメッセージを MINE サーバーに渡す
- MINE サーバーから送信されたクエリ要求に応答しているとき
- IPNE クライアントから MINE サーバーへのサブスクリプション通知

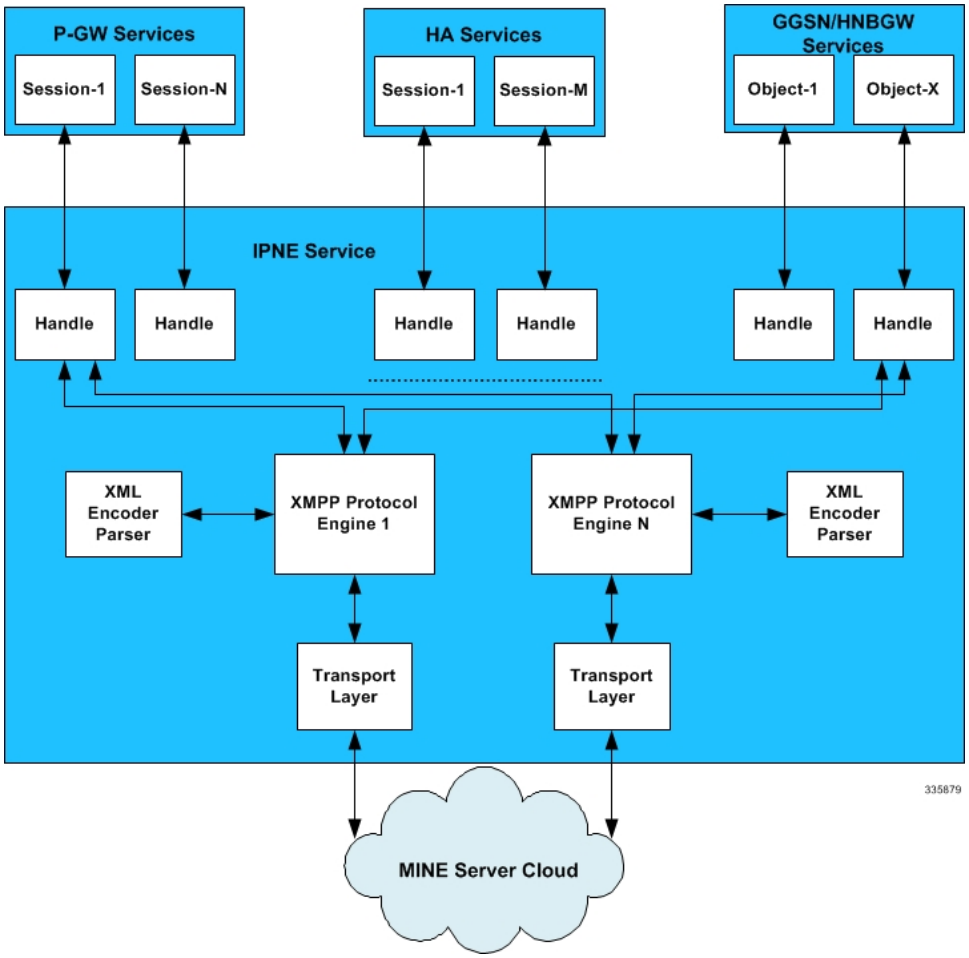
MINE サーバーと IPNE クライアントは、すべての手順において XMPP プロトコルを使用して SINE インターフェイスを介して相互に対話します。IPNE クライアント側に保存されている情報は XML 形式に変換されて MINE サーバーに渡されます。MINE サーバーからメッセージ（クエリ要求）を受信すると、IPNE はそれをデコードし、対応する clp ハンドルをセッションマ

ネージャに送信します。共有される情報は、その時点のセッション/フロー/nbr コンテキストのスナップショットです。

アーキテクチャ

MINE IPNE クライアントは、次に示すように、P-GW、HA、GGSN、HNBGW サービス上の設定可能なサービスとして実装されます。

図 *81 :* 詳細な *IPNE* アーキテクチャ



制限事項

IPNE 機能には、次の制限があることに注意してください。

- IPNE サービスは、XMPP インターフェイスを介してフロー制御メカニズムを実装します。その結果、設定されたキューのしきい値を超えるこのインターフェイスを介したメッセージングはすべて廃棄されます。

フロー

この項では、IPNE クエリ、サブスクリプション、フィード、追加、および削除のシナリオのコールフロー図を示します。一部のフロー図では、例として P-GW を使用していますが、GGSN、HA、および HNBGW にも適用されます。

図 *82 : MINE* サーバーからのクエリの *IPNE* 処理

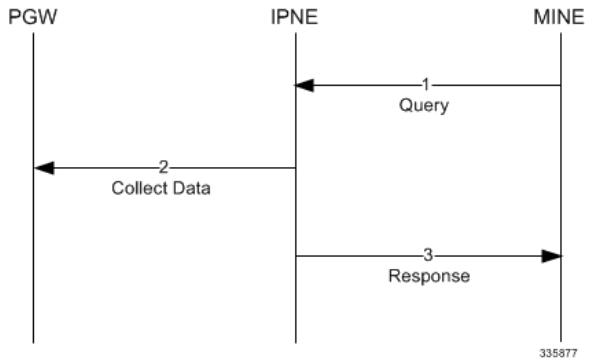


表 *91 : MINE* サーバーからのクエリの *IPNE* 処理

ステップ	説明
1	MINE サーバーは XMPP ストリームを介して IPNE サービスにクエリを送信します。クエリは XML でエンコードされ、query-id、セッションをルックアップするキー（例：sessmgr instance:callid）、および関連する情報を指定するセグメントのリストが含まれます。
2	クエリを受信すると、IPNE サービスは XML データを解析し、MINE サーバーから提供されたキーを使用して ハンドルを特定し、登録済みのコールバック関数を呼び出してセッション情報を収集します。要求された情報は、ビットマスクの形式でもコールバック関数に提供されます。
3	XML エンコーダを使用して、IPNE サービスはセッション情報を XML 形式に変換し、MINE サーバーに送信します。

図 *83 : MINE* サーバーからのサブスクリプションを処理する *IPNE* サービス

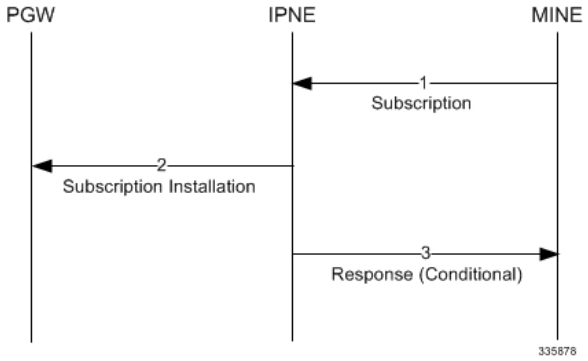


表 *92 : MINE* サーバーからのサブスクリプションを処理する *IPNE* サービス

ステップ	説明
1	MINE サーバーは XMPP ストリームを介して IPNE サービスにサブスクリプションを送信します。サブスクリプションは XML でエンコードされ、クエリメッセージと同様の形式（フィードトリガーを指定するフラグメントのリストなど）となります。
2	サブスクリプションのインストールは、IPNE によってハンドルごとに維持されます。
3	このステップは条件付きです。サブスクリプションにリストされているトリガーのいずれかに一致する既存のセッションがある場合、成功確認応答メッセージが MINE サーバーに送信されます。

図 *84 : IPNE* サービスが *MINE* サーバーに要求されていないフィードメッセージを送信する

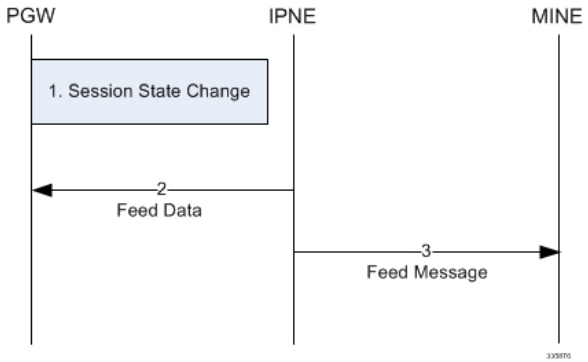


表 *93 : IPNE* サービスが *MINE* サーバーに要求されていないフィードメッセージを送信する

ステップ	説明
1	セッションで何らかの状態変更（ハンドオフによる RAT の変更など）が検出されます。
2	セッションは、ハンドル上のパブリック API を呼び出して、IPNE サービスに変更を通知します。
3	変更が IPNE ハンドルにインストールされているサブスクリプションのインストールのいずれかと一致する場合、フィードメッセージが作成されて MINE サーバーに送信されます。

図 *85 : IPNE* セッションの追加

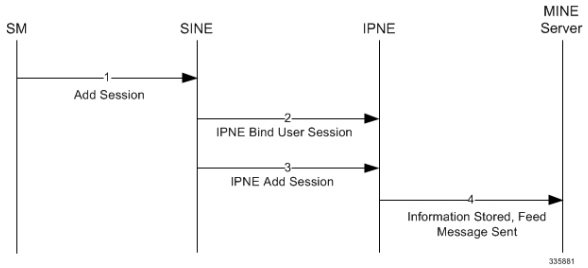


表 *94 : IPNE* セッションの追加

ステップ	説明
1	セッションのセットアップ中に、セッション マネージャ アプリケーションは IPNE が有効かどうかを確認します。
2	IPNE が有効になっている場合、SM はセッション追加情報を SINE インターフェイスに送信します。
3	SINE はセッション情報をバインドし、IPNE アプリケーションに向けて追加イベントを送信します。
4	情報が保存され、その情報がフィードメッセージとして XML データの形式で MINE サーバーに渡されます。

図 *86 : IPNE* セッションの削除

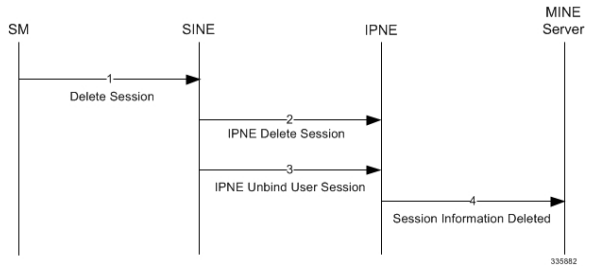


表 *95 : IPNE* セッションの削除

ステップ	説明
1	セッションを解放する前に、セッション マネージャ アプリケーションは delete_session を要求します。
2	SINE は、セッション削除イベントを呼び出します。
3	SINE はセッション情報のバインドを解除します。
4	対応するセッション情報が IPNE アプリケーションから削除され、タイプが delete であるフィードメッセージが MINE サーバーに送信されます。

標準準拠

StarOS IPNE 機能は、次の標準規格に準拠しています。

- RFC 6120 Extensible Messaging and Presence Protocol（XMPP）：コア、セクション 4.7（ストリーム属性）

IPNE 機能の設定

ここでは、IPNE 機能の設定方法と、設定の確認方法について説明します。

IPNE の設定

ここでは、IPNE 機能の設定方法について説明します。

IPNE の設定には、IPNE サービスの設定と、IPNE サービスと GGSN、HA、HNBGW、または P-GW サービスとの関連付けが含まれます。

次の設定例を使用して、IPNE サービスを作成します。

```
config
 context context_name
 ipne ipne_service_name
```

```
ipne-endpoint
bind [ ipv4 ipv4_address | ipv6 ipv6_address ]
peer [ ipv4 | ipv6 ] protocol tcp
end
```

注：

- **bind** と **peer** キーワードは両方とも、IPv4 および IPv6 アドレッシングをサポートします。
- **tcp** はデフォルトのトランスポートプロトコルです。現時点では、SCTP はサポートされていません。
- デフォルトの XMPP プロトコルポートは 5222 です。
- 現時点では、**fqdn**、**priority** および **weight** キーワードはサポートされていません。

HNBGW のみ。通常、通知メッセージはサブスクリプションでのみ送信されます。ただし、HNBGW UE の登録/登録解除については例外が生じています。HNBGW UE の登録/登録解除は、サブスクリプションなしで常に通知されます。このような要求していない通知の送信を制御するには、次のコマンドを入力します。

```
configure
      context ipne_service_name
            unsolicited-notify-trigger hnb-ue
            end
```

注

- **unsolicited-notify-trigger hnb-ue** が設定されている場合、IPNE サービスは HNBGW からの要求を受信した時点で、UE 登録/登録解除要求の通知を送信します。
- **no ununsolicited-notify-trigger hnb-ue** が設定されている場合、IPNE は UE 登録/登録解除通知を送信しません。これがデフォルトの設定です。

IPNE サービスが作成されたら、設定済みの GGSN、HA、P-GW、または HNBGW サービスに関連付ける必要があります。次の例を使用して、IPNE サービスを設定済みのゲートウェイサービスに関連付けます。

```
configure
      context gw_context_name
 associate ipne-service ipne_service_name
            end
```

注：

- **context** *gw_context_name* は、StarOS で設定されている GGSN、HA、P-GW、または HNBGW サービスの名前です。
- IPNE サービスとゲートウェイサービスとの関連付けを削除するには、 **no associate ipne-service** コマンドを使用します。

IPNE 設定の確認

この項では、IPNE 設定を確認する方法について説明します。

Exec モードで次のコマンドを発行して IPNE 設定を確認します。

show ipne peers all

このコマンドの出力は、各 IPNE サービスインスタンスに関する次の情報を提供します。

- IPNE サービス名
- コンテキスト ID
- ピア IP アドレス
- ピアへの TCP 接続の状態

IPNE サービスのモニタリング

ここでは、StarOS IPNE 機能をモニターする方法について説明します。

IPNE show コマンド

ここでは、StarOS IPNE 機能をサポートする show コマンドとその出力について説明します。

ここに示されている show コマンドは、StarOS IPNE 機能をサポートするために使用できます。

show ipne peers all

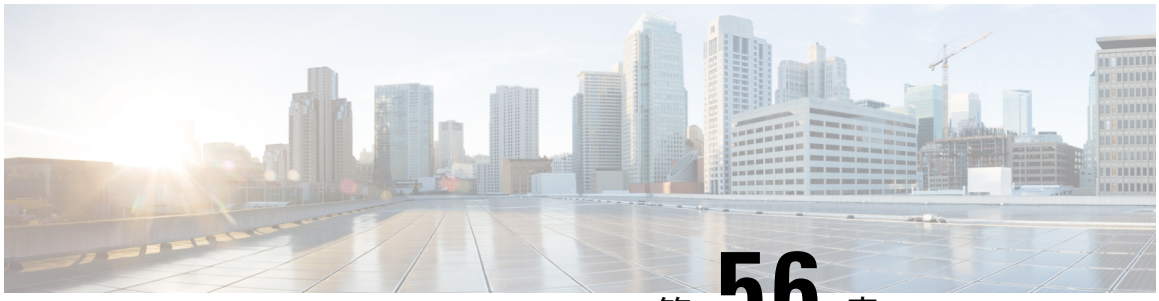
このコマンドは、各 IPNE サービスのピアのリストと、TCP 接続の状態を表示します。

show ipne statistics all

このコマンドは、各 IPNE サービスのハンドルの総数と、クエリ、応答、サブスクリプション、およびフィードのカウンタの合計を表示します。

show active-charging subscsribers full all

このコマンドは、MINE サーバーが現在この ACS セッションの通知を登録しているかどうか（**IPNE enabled** または **disabled**）を表示します。また、この ACS セッションについて MINE サーバーに送信された通知の数も示します。現在のフローと削除されたフローすべてに渡って通知数の履歴が保存されます。MINE サーバーが通知用に登録されていない場合、このフィールドには **n/a** が表示されます。



第 56 章

IP ソース違反

- 機能の概要と変更履歴 （1031 ページ）
- 機能説明 （1032 ページ）
- IP ソース違反の設定 （1032 ページ）
- モニタリングおよびトラブルシューティング （1033 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide* • *Command Line Interface Reference*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.28

機能説明

P-GW は、コントロールプレーンでのパケット送信元の検証をサポートします。コントロールプレーンからの設定がユーザープレーンにプッシュされ、その情報に基づいて、ユーザープレーンが送信元違反パケットに対処します。

送信元の検証は、パケットスプーフィングが疑われる場合や、ネットワーク内でのパケットの回送およびラベル付けの確認に有効です。送信元検証では、受信パケットの送信元アドレスが、セッション中にサブスクライバに静的または動的に割り当てられた IP アドレスと一致する必要があります。

StarOS 21.28.0 以降のリリースでは、APN コンフィギュレーション モードの一部である **ip source-violation** コマンドを使用して、IPv4 および IPv6 アドレスの IP 送信元違反の動作を追跡します。

IP ソース違反の設定

特定の APN に対するパケット送信元の検証を有効または無効にするには、次の設定を使用します。

```
configure
  context context_name
    apn apn_name
      ip source-violation { ignore | check [ drop-limit limit ] [
exclude-from-accounting ][ drop-count-timeout time-interval ] }[
traffic-type { ipv4 | ipv6 } ]
      default ip source-violation
      end
```

注：

- **default**：サブスクライバから受信した送信元アドレスの違反チェックを有効にします。セッションが削除される前にサブスクライバから受信できる無効パケットのドロップ制限数は 10 です。
- **ignore**：APN の送信元アドレスチェックを無効にします。
- **check [drop-limit** *limit* **]**：デフォルトは [Enabled] で、limit は 10 です。

  サブスクライバから受信した送信元アドレスの違反チェックを有効にします。drop-limit を設定して、セッションが削除される前にサブスクライバから受信できる無効なパケット数に対する制限を設定できます。

  limit：0 ～ 10000 の任意の整数値に設定できます。値 0 は、すべての無効なパケットが廃棄され、セッションはシステムによって削除されないことを示します。
- **exclude-from-accounting**：アカウンティングレコード用に生成された統計情報から、IP ソース違反で識別されたパケットを除外します。

- **check [drop-count-timeout time-interval]**：**drop-count-timeout** を使用すると、違反ドロップ数の更新タイマーの時間間隔を設定できます。これによりドロップカウンタ値を更新する時間間隔が指定されます。時間間隔は分単位で指定する必要があります。デフォルト値は 120 秒（2 分）です。
- **check [traffic-type { ipv4 | ipv6 }]**：パケットトラフィックのタイプを IPv4 または ipv6 で指定します。デフォルトでは、設定は IPv4 と IPv6 の両方に共通です。CLI が「traffic-type」で設定されている場合、その traffic-type の「ip source violation」CLI は、「traffic-type」なしで設定された CLI よりも優先されます。

（注） ドロップ制限とタイマーの値がゼロの場合でも、違反カウントは増分します。セッションは削除されませんが、違反したパケットはドロップされます。

モニタリングおよびトラブルシューティング

この項では、IP ソース違反機能のモニタリングと障害対応について説明します

コマンドと出力の表示

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show subscribers full all

IPv4 および IPv6 のカウンタ違反に関連するすべての統計を個別に表示します。

表 *96 : show subscribers full all* コマンド出力の説明

フィールド	説明
ipv6 source violations	IPv6 送信元検証違反の数。
ipv6 source violations no acct	検出されたが統計に含まれていない IPv6 送信元検証違反。
ipv6 source violations ignored	検出されたが、無視された IPv6 送信元検証違反。
ipv6 source violations active	アクティブな IPv6 送信元検証違反の合計数。

show apn name *apn_name*

IPv4 および IPv6 のカウンタ違反に関連するすべての統計を個別に表示します。

表 *97 : show apn name apn_name* コマンド出力の説明

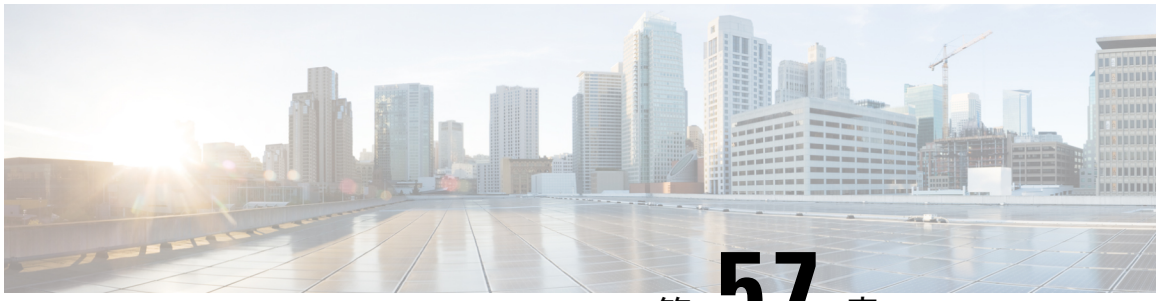
フィールド	説明
ipv4 source violations	IPv4 送信元検証違反の数。
drop limit	IPv4 送信元検証違反のドロップ制限の数。
ipv4 source violations no acct	検出されたが統計に含まれていない IPv4 送信元検証違反。
ipv6 source violations	IPv6 送信元検証違反の数。
drop limi	IPv6 送信元検証違反のドロップ制限の数。
ipv6 source violations no acct	検出されたが統計に含まれていない IPv6 送信元検証違反。

show apn statistics name *apn_name*

IPv4 および IPv6 のカウンタ違反に関連するすべての統計を個別に表示します。

表 *98 : show apn statistics name apn_name* コマンド出力の説明

フィールド	説明
IPv4 src violations	IPv4 送信元検証違反の数。
IPv4 src violations no acct	検出されたが統計に含まれていない IPv4 送信元検証違反。
IPv4 src violations ignored	検出されたが、無視された IPv4 送信元検証違反。
ipv6 src violations	IPv6 送信元検証違反の数。
ipv6 src violations no acct	検出されたが統計に含まれていない IPv6 送信元検証違反。
IPv6 src violations ignored	検出されたが、無視された IPv6 送信元検証違反。



第 57 章

L2TP アクセスコンセントレータ

この章では、Cisco ASR 5500 シャーシのレイヤ 2 トンネリングプロトコル（L2TP）アクセスコンセントレータ（LAC）機能サポートについて、またその設定方法について説明します。

製品アドミニストレーションガイドには、システム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、それぞれの製品のアドミニストレーションガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

重要 L2TP アクセスコンセントレータは、シスコのライセンス供与された機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

セッションライセンスと機能使用キーによって有効にすると、システムで L2TP がサポートされ、LAC と 1 つまたは複数の L2TP ネットワークサーバー（LNS）ノードの間のデータパケットがカプセル化されます。システムでは、このオプションのパケットカプセル化（トンネリング）は、コンテキスト内で L2TP アクセスコンセントレータ（LAC）サービスを設定することによって実行されます。

重要 LAC から LNS への L2TP セッションの確立中に、ユーザーの PPP 接続が確立されます。サーバーは、CHAP 認証プロトコルを使用して接続を認証します。サーバーが受信した CHAP チャレンジに対する CHAP 応答を計算しているとき、サーバーは CHAP パスワードを考慮しません。

重要 LAC サービスは、UDP ポート 13660 から 13668 を、LNS にパケットを送信するための送信元ポートとして使用します。

この章は、次の内容で構成されています。

• 対象製品と関連するセクション （1036 ページ）
• PDSN 簡易 IP でサポートされる LAC サービス設定 （1037 ページ）
• GGSN および P-GW でサポートされる LAC サービス設定 （1042 ページ）
• モバイル IP でサポートされる LAC サービス設定 （1049 ページ）
• L2TP サポート用のサブスクライバプロファイルの設定 （1052 ページ）
• 機能説明 （1056 ページ）
• LAC サービスの設定 （1057 ページ）
• L2TP サポートのための PDSN サービスの変更 （1059 ページ）
• L2TP をサポートするための APN テンプレートの変更 （1061 ページ）

対象製品と関連するセクション

LAC 機能は、さまざまな製品でサポートされています。この機能がサポートされている製品と、その製品に関連する章の参照先を次の表にを示します。

対象製品	参照先
PDSN/FA/HA	• *PDSN* 簡易 *IP* でサポートされる *LAC* サービス設定 • モバイル *IP* でサポートされる *LAC* サービス設定 • *L2TP* サポート用のサブスクライバプロファイルの設定 • 使用される *RADIUS* とサブスクライバのプロファイル属性 • *L2TP* サポート用のローカル サブスクライバ プロファイルの設定 • *RADIUS* 属性を使用しない特定コンテキスト内のすべてのサブスク のトンネリング • *LAC* サービスの設定 • *L2TP* サポートのための *PDSN* サービスの変更
GGSN/SGSN/FA/P-GW	• *GGSN* でサポートされる *LAC* サービス設定 • モバイル *IP* でサポートされる *LAC* サービス設定 • *L2TP* サポート用のサブスクライバプロファイルの設定 • 使用される *RADIUS* とサブスクライバのプロファイル属性 • *L2TP* サポート用のローカル サブスクライバ プロファイルの設定 • *L2TP* を介したマルチキャストサービスの有効化 • *LAC* サービスの設定 • *L2TP* をサポートするための *APN* テンプレートの変更

対象製品	参照先
ASN GW	• モバイル *IP* でサポートされる *LAC* サービス設定 • *L2TP* サポート用のサブスクライバプロファイルの設定 • 使用される *RADIUS* とサブスクライバのプロファイル属性 • *L2TP* サポート用のローカル サブスクライバ プロファイルの設定 • *RADIUS* 属性を使用しない特定コンテキスト内のすべてのサブス のトンネリング • *LAC* サービスの設定

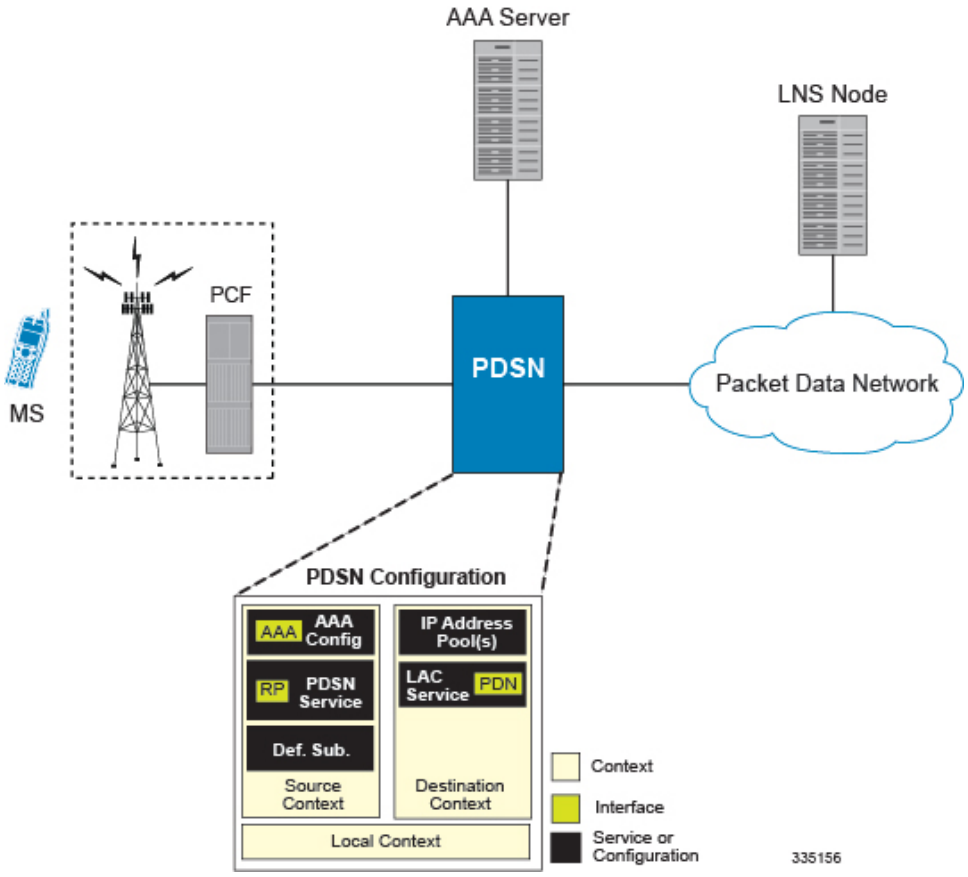
PDSN 簡易 IP でサポートされる LAC サービス設定

LACサービスを着信PPPセッションに適用するには、次のいずれかのメソッドを使用します。

- **属性ベースのトンネリング**：このメソッドは、認証中に識別された特定のユーザーのみのPPPパケットをカプセル化するために使用されます。このメソッドでは、通信可能なLACサービスパラメータと許可されるLNSノードが、特定のサブスクライバのユーザープロファイルによって制御されます。ユーザープロファイルは、システム上でローカルで設定できますし、RADIUSサーバー上でリモートで設定することもできます。
- **PDSN サービスベースの強制トンネリング**：このトンネリングメソッドは、RPインターフェイスからPDSNサービスに着信するすべての着信PPPトラフィックをカプセル化し、認証のためにそれをLNSピアにトンネリングするために使用されます。すべての認証がピアLNSによって実行されるため、このメソッドではサブスクライバの設定が考慮されないことに注意してください。

各LACサービスは、同じシステムコンテキスト内で設定された単一のシステムインターフェイスにバインドされます。次の図に示すように、このコンテキストを接続先コンテキストにすることを推奨します。

図 *87 : SIP* 用の *LAC* サービスの設定



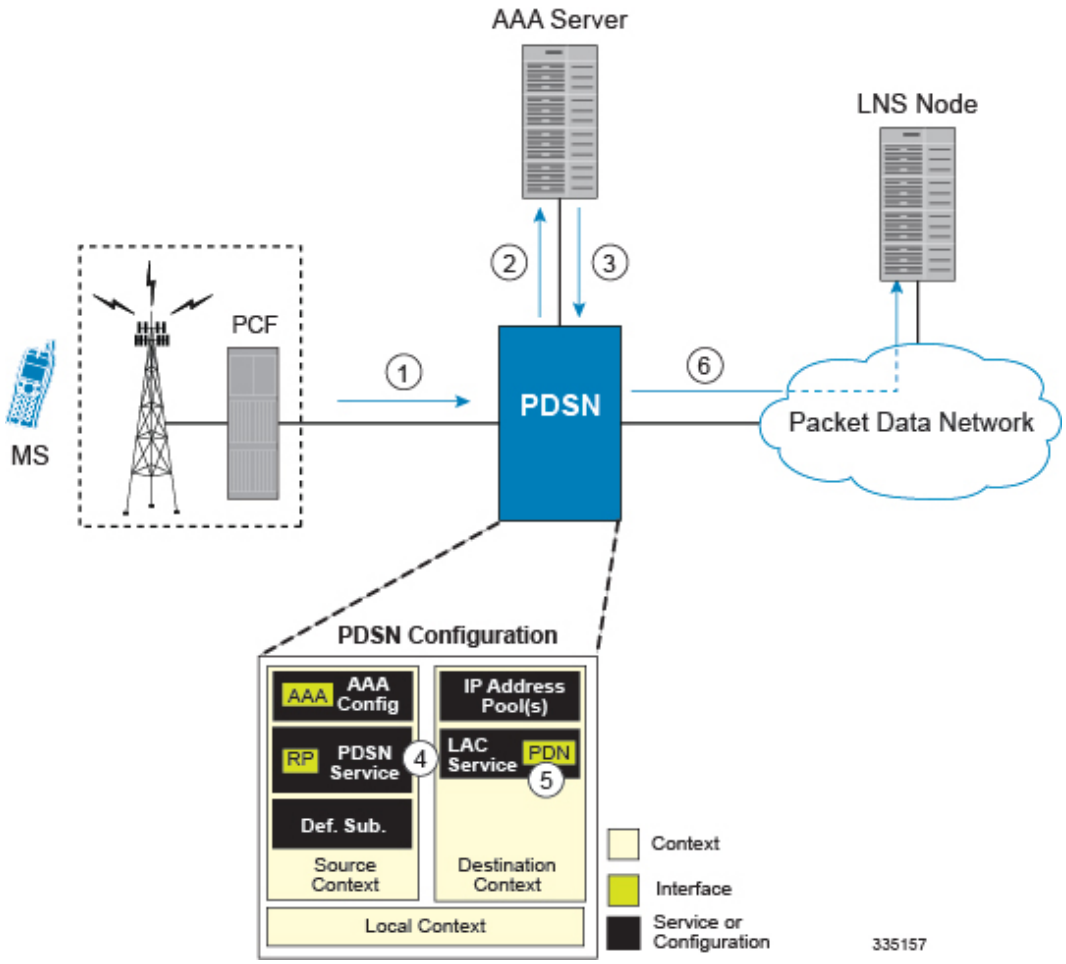
属性ベーストンネリング

このセクションでは、属性ベーストンネリングの動作とその設定について説明します。

属性ベース L2TP 設定の仕組み

次の図とその後のテキストは、システムを使用して属性ベーストンネリングがどのように実行されるかを示しています。

図 *88 : SIP* の属性ベース *L2TP* セッション処理



1. PCF からのサブスクライバセッションは、R-P インターフェイスを介して PDSN サービスによって受信されます。
2. PDSN サービスは、サブスクライバの認証を試みます。サブスクライバは、ローカルで設定することも、RADIUS サーバー上にリモートで設定することもできます。上図は、RADIUS AAA サーバーを使用したサブスクライバ認証を示しています。
3. RADIUS サーバーが Access-Accept メッセージを返します。このメッセージには、セッションデータが L2TP を使用してトンネリングされることを示す属性と、使用する LAC サービスの名前と場所が含まれています。接続先の LNS ピアを示す属性も提供されます。
4. PDSN サービスは、この情報を受信すると、宛先コンテキスト内に設定された LAC サービスにパケットを転送します。
5. LAC サービスは、パケットを受信すると、情報をカプセル化し、LNS に配信するために適切な PDN インターフェイスに転送します。
6. カプセル化されたパケットは、パケットデータネットワークを介してピア LNS に送信され、ここでカプセル化が解除されます。

PDSN 簡易 IP に対する属性ベースの L2TP サポートの設定

この項では、属性ベースの L2TP サポートを設定し、PDSN 簡易 IP アプリケーションで使用するために必要な手順のリストを示します。一覧表示されている各手順では、必要な手順を実行するための具体的な指示を含む別のセクションが参照されています。



重要 これらの手順は、システムがサブスクライバ データ セッションを PDSN としてサポートするように事前に設定されていることを前提としています。

手順

ステップ 1 この章の「*L2TP* サポート用のサブスクライバプロファイルの設定」の項に記載されている情報および手順に従って、サブスクライバプロファイルを設定します。

ステップ 2 この章の「*LAC* サービスの設定」セクションに記載されている情報と手順に従って、1 つ以上の LAC サービスを設定します。

ステップ 3 この章の「*L2TP* サポートのための *PDSN* サービスの変更」の項に記載されている手順に従って、トンネル コンテキスト ロケーションを使用して PDSN サービスを設定します。

ステップ 4 Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

PDSN サービスベース強制トンネリング

このセクションでは、サービスベース強制トンネリングの動作とその設定について説明します。

PDSN サービスベース強制トンネリングの動作の仕組み

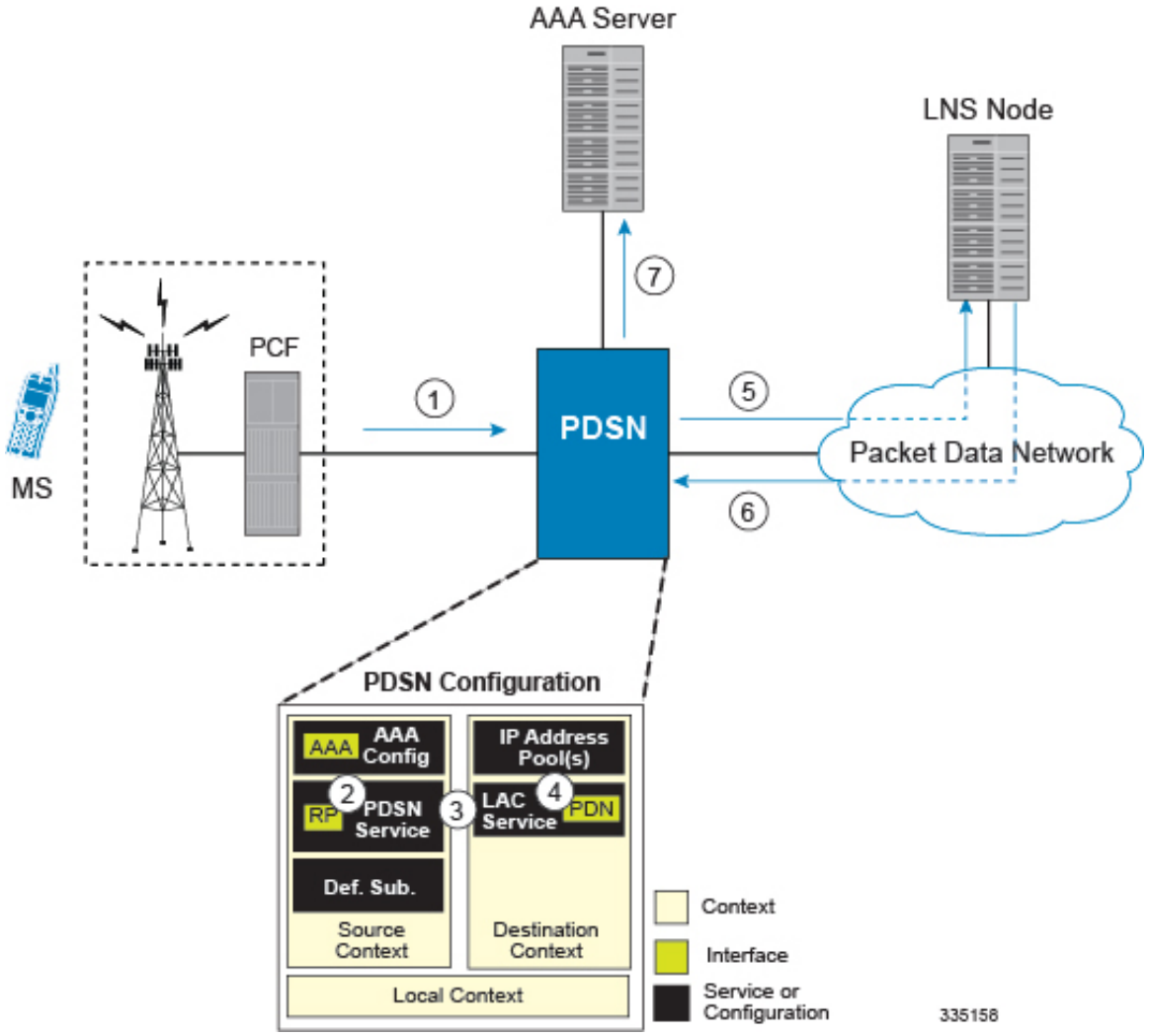
PDSN サービスベースの強制トンネリングにより、ワイヤレス通信事業者は、すべての PPP トラフィックを L2TP トンネルを介してリモート LNS ピアに送信し、認証を行うことができます。これは、システムで PPP 認証が実行されないことを意味します。

アカウンティング開始レコードと中間アカウンティングレコードは、引き続きシステムの AAA サービス設定で設定されたローカル RADIUS サーバーに送信されます。L2TP セッションのセットアップが完了すると、システムはコールカウンタを開始し、RADIUS サーバーに信号を送ってアカウンティングを開始します。アカウンティングレコードのサブスクライバ名は、セッションごとに作成される NAI 構造の名前に基づきます。

PDSN サービスベースの強制トンネリングでは、1 つ以上の PDSN サービスを変更し、1 つ以上の LAC サービスを設定する必要があります。

次の図およびそれに続くテキストは、システムを使用してPDSNサービスベースの強制トンネリングがどのように実行されるかを示しています。

図 *89 : PDSN* サービスベース強制トンネリングのセッション処理



1. PCF からのサブスクライバセッションは、R-P インターフェイスを介して PDSN サービスによって受信されます。
2. PDSN サービスは、その **tunnel-type** パラメータが L2TP に設定されていること、およびその **tunnel-context** パラメータが接続先コンテキストに設定されていることを検出します。
3. PDSNは、セッションのすべてのパケットを、接続先コンテキストで設定されたLACサービスに転送します。複数の LAC サービスが設定されている場合、セッショントラフィックはラウンドロビンアルゴリズムを使用して各サービスにルーティングされます。
4. LAC サービスは、設定の一部としてリストされている LNS ピアの 1 つへの L2TP トンネルを開始します。

5. セッションパケットは、認証のためにパケットデータネットワークを介して LNS に渡されます。
6. LNS はセッションを認証し、PDSN に Access-Accept を返します。
7. PDSN サービスでは、構造化された NAI を使用して、セッションのアカウンティングを開始します。

   セッション データ トラフィックは、ステップ 4 で確立した L2TP トンネルを介して渡されます。

PDSN 簡易 IP に対する L2TP 強制トンネリングのサポート

このセクションでは、L2TP 強制トンネリングのサポートを設定し、PDSN 簡易 IP アプリケーションで使用するために必要な手順のリストを示します。一覧表示されている各手順では、必要な手順を実行するための具体的な指示を含む別のセクションが参照されています。

重要 これらの手順は、システムがサブスクライバ データ セッションを PDSN としてサポートするように事前に設定されていることを前提としています。

手順

ステップ 1 この章の「*LAC* サービスの設定」セクションに記載されている情報と手順に従って、1 つ以上の LAC サービスを設定します。

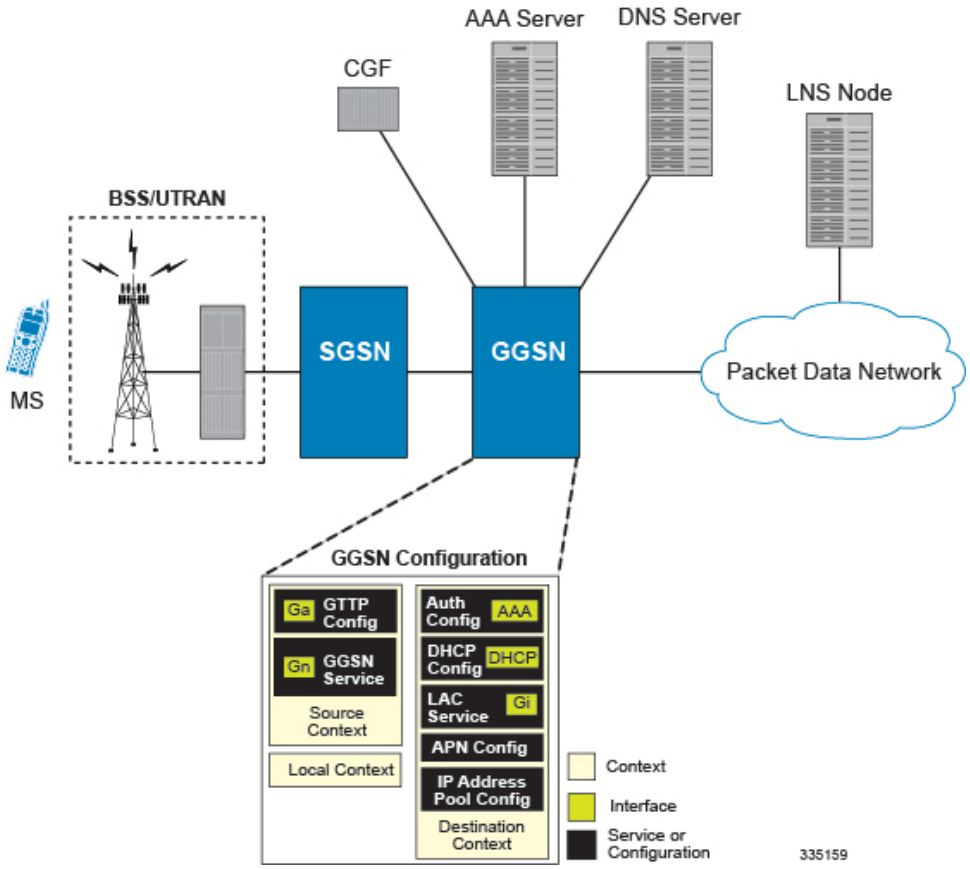
ステップ 2 この章の「*L2TP* サポートのための *PDSN* サービスの変更」セクションに記載されている手順に従って、PDSN サービスを設定します。

ステップ 3 Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイスやネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

GGSN および P-GW でサポートされる LAC サービス設定

前述したとおり、L2TP はシステムでの LAC サービス設定を通じてサポートされます。次の図に示すように、各 LAC サービスは、同じシステム接続先コンテキスト内で設定された単一のシステムインターフェイスにバインドされます。

図 *90 : GGSN LAC* サービスの設定



LAC サービスは、GGSN のアクセスポイント名（APN）のテンプレートまたはサブスクライバのプロファイルにある属性の設定に基づいて、着信サブスクライバの PDP コンテキストに適用されます。サブスクライバプロファイルは、システム上でローカルで設定することも、RADIUS サーバー上でリモートで設定することもできます。

LAC サービスは、LNS を使用したドメインベースの L2TP トンネリングもサポートします。この方法を利用して、LAC と LNS の間に複数のトンネルが作成されます。このとき、Access-Accept でトンネル選択と作成用のキーとして AAA サーバーから受信した「Tunnel-Client-Auth-ID」や「Tunnel-Server-Auth-ID」属性の値に基づいて作成されます。LAC が新しい L2TP セッションを確立する必要がある場合、まずキーの「Tunnel-Client-Auth-ID」や「Tunnel-Server-Auth-ID」の属性値に基づいて、ピア LNS との既存の L2TP トンネルがあるかどうかを確認します。キーにそのようなトンネルが存在しない場合は、LNS との新しいトンネルが作成されます。

LAC サービスが LNS との新しい L2TP セッション用に新しいトンネルを確立する必要があり、トンネル作成の上限に達したためにトンネル作成要求に失敗した場合、LAC は Access-Accept メッセージで AAA サーバーから受信した他の LNS アドレスを試します。使用可能なすべてのピア LNS が使い果たされている場合、LAC サービスはコールを拒否します。

L2TP トンネルパラメータは APN テンプレート内で設定され、APN にアクセスするすべてのサブスクライバに適用されます。ただし、以下で説明するように、L2TP の動作はサブスクライバの PDP コンテキストタイプによって異なります。

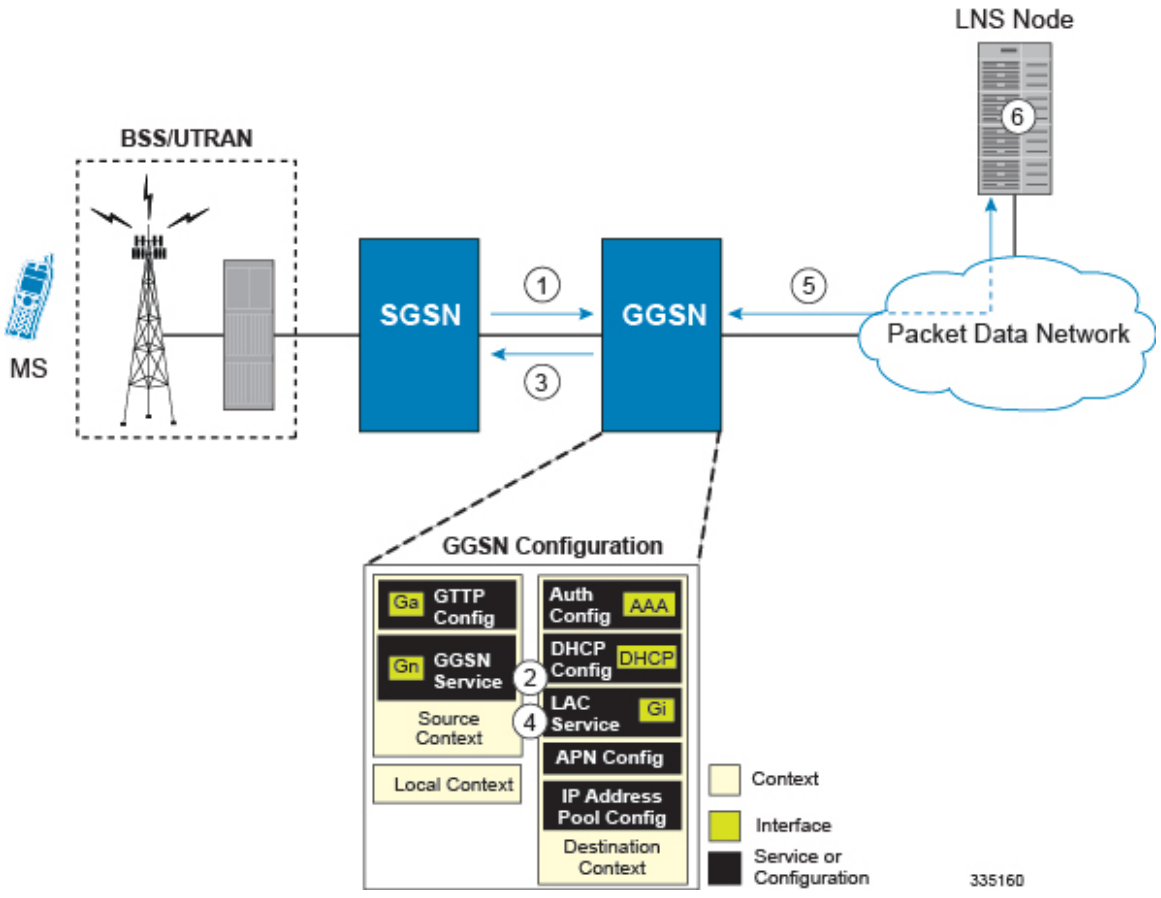
- **Transparent IP**：APNテンプレートのL2TPパラメータ設定がセッションに適用されます。
- **Non-transparent IP**：認証が必要であるため、サブスクライバプロファイルの L2TP パラメータ属性（設定されている場合）が APN テンプレートの設定よりも優先されます。
- **PPP**：APN テンプレートの L2TP パラメータ設定が適用され、サブスクライバのすべての PPP パケットが指定された LNS に転送されます。

詳細については、以降の項を参照してください。

L2TP サポートによる透過 IP PDP コンテキスト処理

次の図とその後のテキストで、L2TP トンネリングが有効な場合の透過 IP PDP コンテキストの処理方法について説明します。

図 *91 : L2TP* トンネリングによる透過 *IP PDP* コンテキストのコール処理



1. サブスクライバセッションの PDP コンテキスト作成要求メッセージが、Gn インターフェイスを介して SGSN から GGSN サービスに送信されます。このメッセージには、PDP タイプ、APN、課金特性などの情報が含まれます。

2. GGSN が、メッセージで指定されたものと同じ APN が設定で使用されているかどうかを判定します。同じであれば、APNの設定に基づいてセッションの処理方法を決定します。

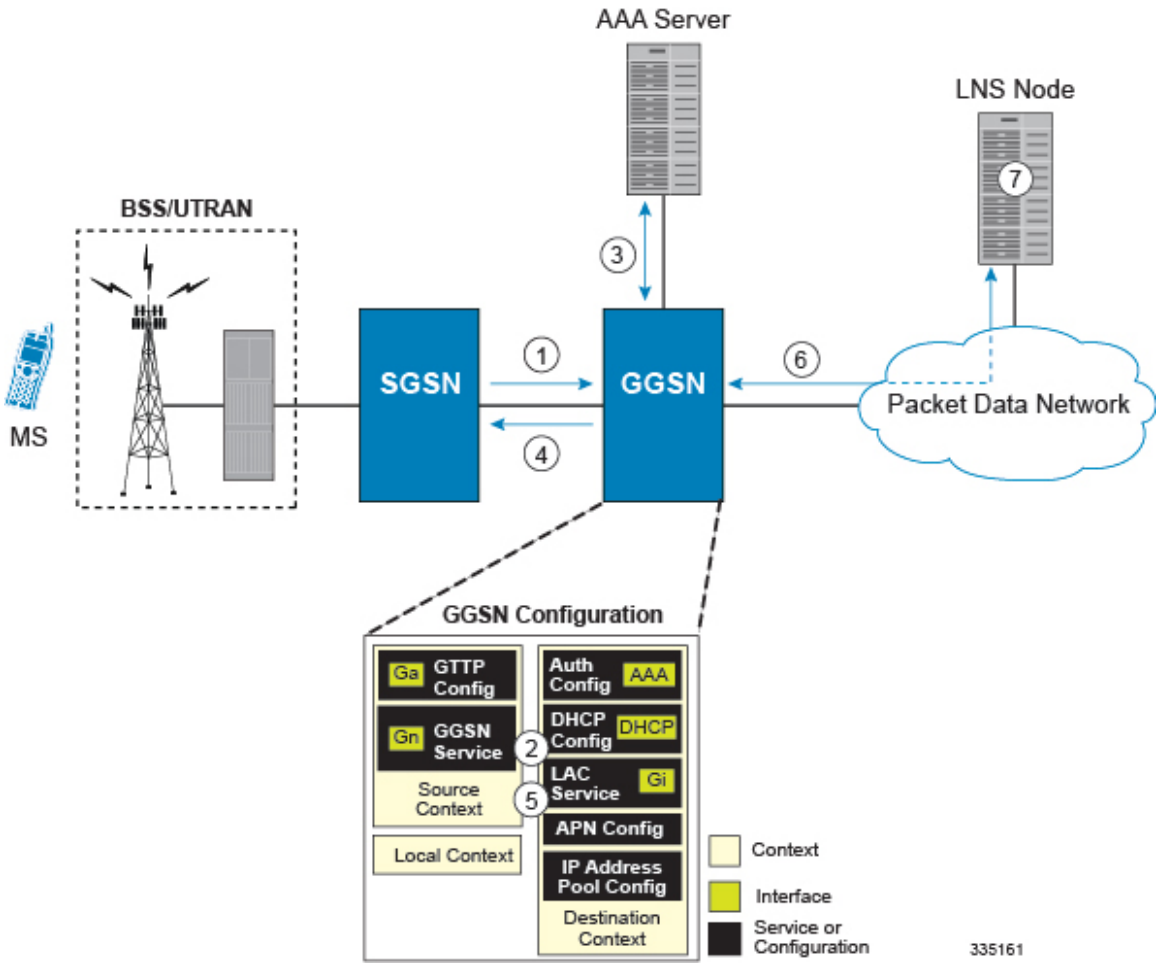
   APN 設定には、LNS の IP アドレス、LAC サービスが設定されているシステム接続先コンテキスト、着信セッションを認証するためにLNSが使用するアウトバウンドユーザー名とパスワードなどが示されています。アウトバウンド情報が設定されていない場合は、サブスクライバの International Mobile Subscriber Identity（IMSI）がピア LNS のユーザー名として使用されます。

1. GGSN が、Gn インターフェイスを介して SGSN に肯定的な PDP コンテキスト作成応答を返します。
2. GGSN が、MS から受信したデータを LAC サービスに渡します。
3. LAC サービスが、IP パケットをカプセル化し、適切な Gi インターフェイスに転送して LNS に配信します。
4. LNSはパケットのカプセル化を解除し、必要に応じて処理します。この処理には、IPアドレスの割り当てが含まれます。

L2TP サポートによる非透過 IP PDP コンテキスト処理

L2TP トンネリングが有効な場合の非透過 IP PDP コンテキストの処理方法について、次の図とともに解説します。

図 *92 : L2TP* トンネリングによる非透過 *IP PDP* コンテキストのコール処理



1. サブスクライバセッションの PDP コンテキスト作成要求メッセージが、Gn インターフェイスを介して SGSN から GGSN サービスに送信されます。このメッセージには、PDP タイプ、APN、課金特性などの情報が含まれます。
2. GGSN が、メッセージで指定されたものと同じ APN が設定で使用されているかどうかを判定します。同じであれば、APN の設定に基づいてセッションの処理方法を決定します。

   APN 設定には、LNS の IP アドレス、LAC サービスが設定されているシステム接続先コンテキスト、着信セッションを認証するために LNS が使用するアウトバウンドユーザー名とパスワードなどが示されています。アウトバウンド情報が設定されていない場合は、サブスクライバのユーザー名がピア LNS に送信されます。

3. GGSN サービスが、サブスクライバを認証します。サブスクライバは、ローカルで設定することも、RADIUS サーバー上にリモートで設定することもできます。上図は、RADIUS AAA サーバーを使用したサブスクライバ認証を示しています。

   認証の一部として、RADIUS サーバーが Access-Accept メッセージを返します。

このメッセージには、セッションデータが L2TP を使用してトンネリングされることを示す属性と、使用する LAC サービスの名前および場所が含まれる可能性があります。接続先の LNS ピアを示す属性も提供されます。

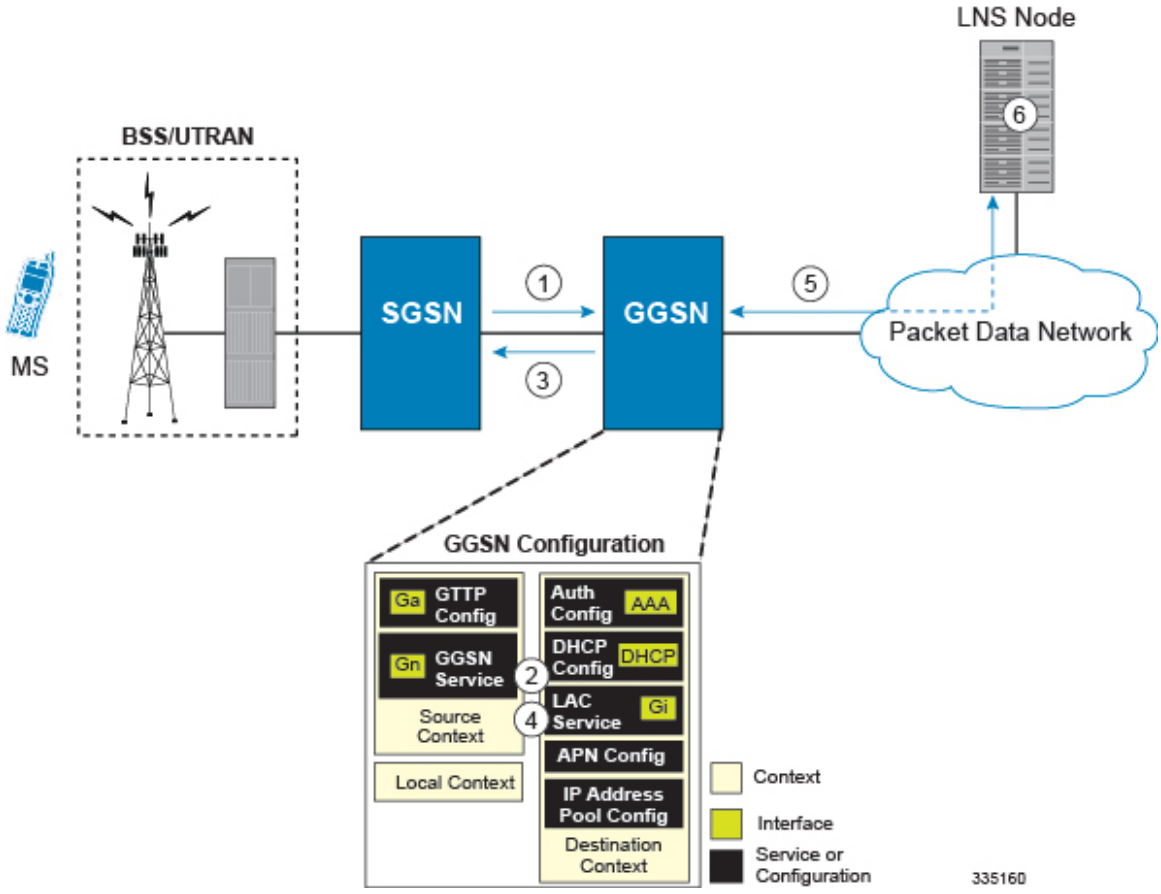
これらの属性が指定されている場合、それらは、APNテンプレートで指定されている属性よりも優先されます。

4. GGSN が、Gn インターフェイスを介して SGSN に肯定的な PDP コンテキスト作成応答を返します。
5. GGSN が、MS から受信したデータを LAC サービスに渡します。
6. LAC サービスが、IP パケットをカプセル化し、適切な Gi インターフェイスに転送して LNS に配信します。
7. LNS が、パケットのカプセル化を解除し、必要に応じて処理します。この処理には、認証と IP アドレスの割り当てが含まれます。

L2TP サポートによる PPP PDP コンテキスト処理

L2TP トンネリングが有効な場合の非透過 IP PDP コンテキストの処理方法について、次の図とともに解説します。

図 *93 : L2TP* トンネリングによる *PPP PDP* コンテキストのコール処理



1. サブスクライバセッションの PDP コンテキスト作成要求メッセージが、Gn インターフェイスを介して SGSN から GGSN サービスに送信されます。このメッセージには、PDP タイプ、APN、課金特性などの情報が含まれます。
2. GGSN が、メッセージで指定されたものと同じ APN が設定で使用されているかどうかを判定します。同じであれば、APN の設定に基づいてセッションの処理方法を決定します。

   APN 設定には、LNS の IP アドレス、LAC サービスが設定されているシステム接続先コンテキストが示されています。

   L2TP サポートは、サブスクライバのプロファイルでも設定できます。APN が L2TP トンネリング用に設定されていない場合、システムはサブスクライバの認証を試みます。その後、サブスクライバのプロファイルのトンネリングパラメータを使用して、ピアの LNS が決定されます。
3. GGSN が、Gn インターフェイスを介して SGSN に肯定的な PDP コンテキスト作成応答を返します。
4. GGSN は、MS から受信した PPP パケットを LAC サービスに渡します。
5. LAC サービスは、PPP パケットをカプセル化し、適切な Gi インターフェイスに転送して LNS に配信します。
6. LNS はパケットのカプセル化を解除し、必要に応じて処理します。この処理には、PPP の終了、認証（サブスクライバから提供されたユーザー名/パスワードを使用）、IP アドレスの割り当てが含まれます。

L2TP をサポートするための GGSN または P-GW の設定

ここでは、L2TP をサポートするように GGSN または P-GW を設定するために必要な手順を示します。一覧表示されている各手順では、必要な手順を実行するための具体的な指示を含む別のセクションが参照されています。

重要 該当する指示は、システムがサブスクライバ データ セッションを GGSN または P-GW としてサポートするように事前に設定されていることを前提としています。

手順

ステップ 1 この章の「*L2TP* をサポートするための *APN* テンプレートの 変更」に示されている情報と手順に従って、L2TP トンネリングをサポートするよう に APN テンプレートを設定します。

重要
L2TP トンネリングは、APN テンプレートを使用したサポートの設定とは対照的に、またはそれに加えて、個々のサブスクライバプロファイル内で設定できます。サブスクライバプロファイルの設定については、この章の「*L2TP* サポート用のサブスクライバプロファイルの設定」を参照してください。

ステップ 2 この章の「*LAC* サービスの設定」セクションに記載されている情報と手順に従って、1 つ以上の LAC サービスを設定します。

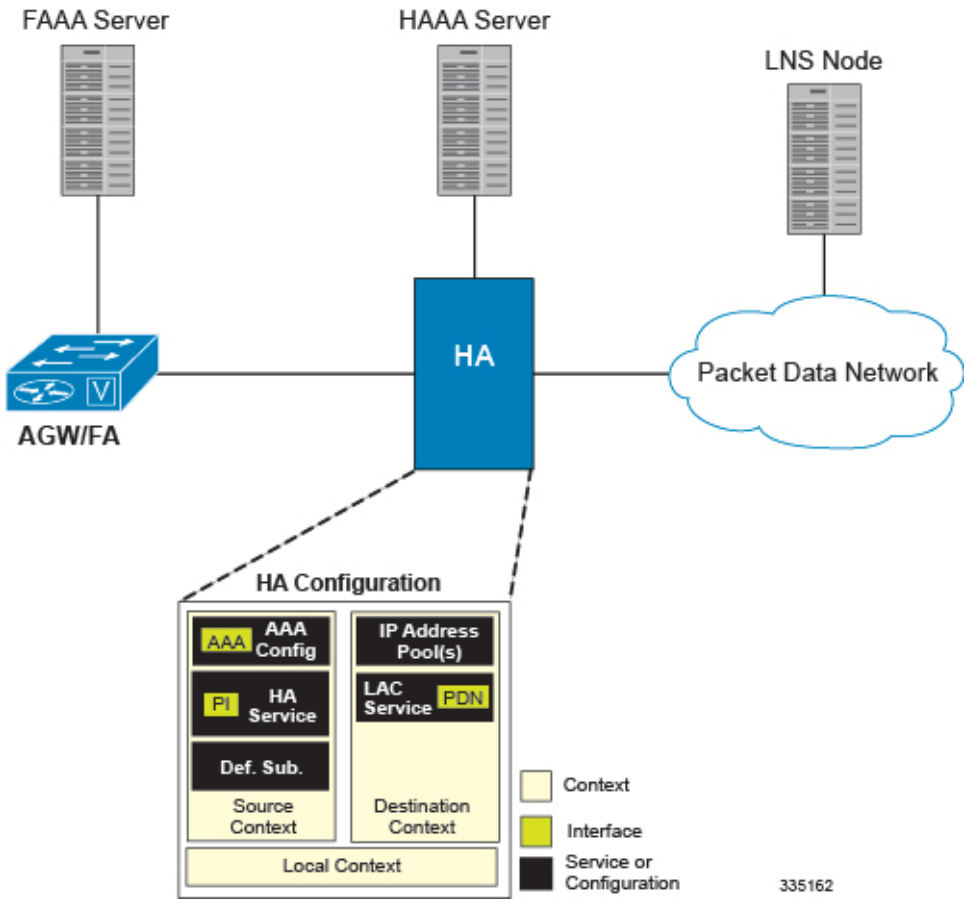
ステップ 3 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

モバイル IP でサポートされる LAC サービス設定

LAC サービスは、属性ベースのトンネリングを使用して、着信 MIP セッションに適用できます。属性ベースのトンネリングは、認証中に識別された特定のユーザーの PPP パケットをカプセル化するために使用されます。このメソッドでは、通信可能な LAC サービスパラメータと許可される LNS ノードが、特定のサブスクライバのユーザープロファイルによって制御されます。ユーザープロファイルは、システム上でローカルで設定できますし、RADIUS サーバー上でリモートで設定することもできます。

各 LAC サービスは、同じシステムコンテキスト内の単一のシステムインターフェイスにバインドされます。次の図に示すように、このコンテキストを接続先コンテキストにすることを推奨します。

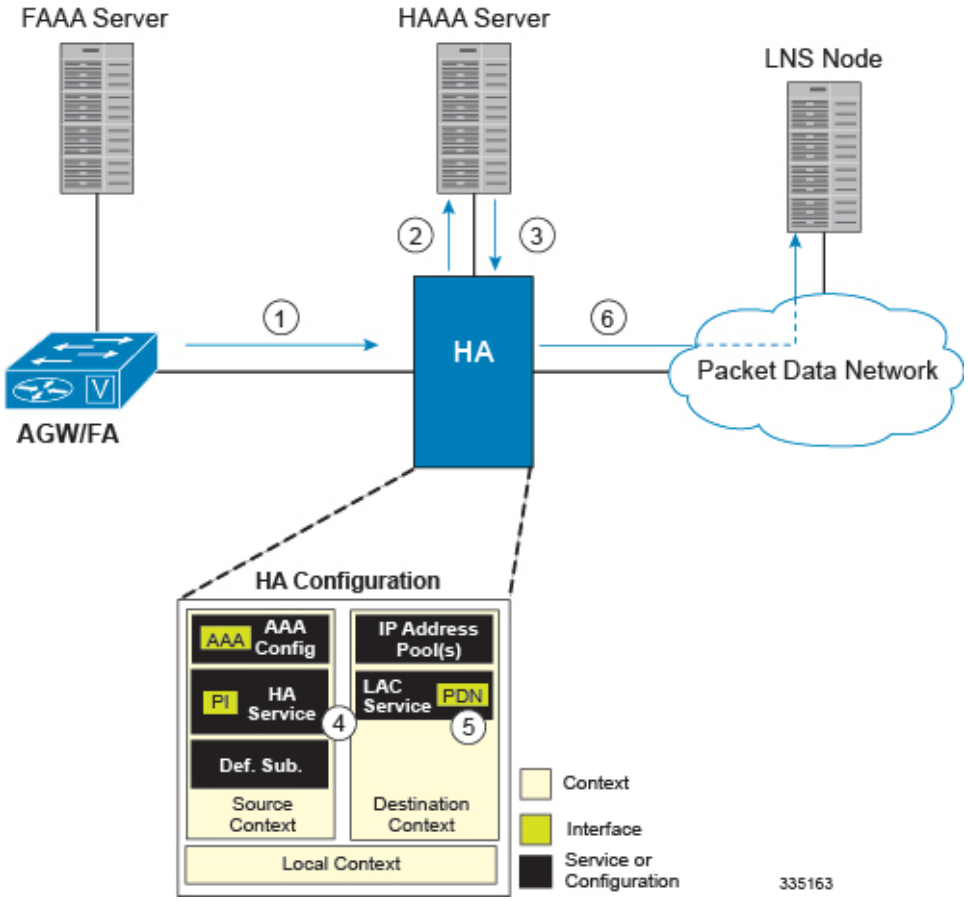
図 *94 : MIP* 用の *LAC* サービスの設定



MIP の属性ベース L2TP 設定の仕組み

次の図とその後のテキストは、システムを使用して MIP の属性ベーストンネリングがどのように実行されるかを示しています。

図 *95 : MIP* の属性ベース *L2TP* セッション処理



1. FA からのサブスクライバセッションは、Pi インターフェイスを介して HA サービスによって受信されます。
2. HA サービスは、サブスクライバの認証を試みます。サブスクライバは、ローカルで設定することも、RADIUS サーバー上にリモートで設定することもできます。上図は、RADIUS AAA サーバーを使用したサブスクライバ認証を示しています。
3. RADIUS サーバーが Access-Accept メッセージを返します。このメッセージには、セッションデータが L2TP を使用してトンネリングされることを示す属性と、使用する LAC サービスの名前と場所が含まれています。接続先の LNS ピアを示す属性も提供されます。
4. HA サービスは、この情報を受信すると、宛先コンテキスト内に設定された LAC サービスにパケットを転送します。
5. LAC サービスは、パケットを受信すると、情報をカプセル化し、LNS に配信するために適切な PDN インターフェイスに転送します。
6. カプセル化されたパケットは、パケットデータネットワークを介してピア LNS に送信され、ここでカプセル化が解除されます。

HA モバイル IP に対する属性ベースの L2TP サポートの設定

ここでは、属性ベースの L2TP サポートを設定し、HA モバイル IP アプリケーションで使用するために必要な手順のリストを示します。一覧表示されている各手順では、必要な手順を実行するための具体的な指示を含む別のセクションが参照されています。

重要 該当する指示は、システムがサブスクライバ データ セッションを HA としてサポートするように事前に設定されていることを前提としています。

手順

ステップ 1 この章の「*L2TP* サポート用のサブスクライバプロファイルの設定」の項に記載されている情報および手順に従って、サブスクライバプロファイルを設定します。

ステップ 2 この章の「*LAC* サービスの設定」セクションに記載されている情報と手順に従って、1 つ以上の LAC サービスを設定します。

ステップ 3 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

L2TP サポート用のサブスクライバプロファイルの設定

この項では次のプロシージャの機能と操作手順について説明します。

- 使用される RADIUS とサブスクライバのプロファイル属性 （1052 ページ）
- L2TP サポート用のローカル サブスクライバ プロファイルの設定 （1054 ページ）
- ローカルサブスクライバの設定 （1055 ページ）
- L2TP 設定の確認 （1056 ページ）

重要 サブスクライバの設定手順は RADIUS サーバーアプリケーション間で異なるため、この項では、サブスクライバプロファイルに追加できる個々の属性についてのみ説明します。サブスクライバの設定手順については、RADIUS サーバーに付属のマニュアルを参照してください。

使用される RADIUS とサブスクライバのプロファイル属性

属性ベースの L2TP トンネリングは、システムにローカルに保存されているか、またはリモートで RADIUS サーバーに保存されているサブスクライバプロファイルに設定された属性を使用

してサポートされます。次の表に、LACサービスのサポートで使用される属性を示します。これらの属性は、標準ディクショナリと VSA ディクショナリに含まれています。

表 *99 : L2TP* サポートのためのサブスクライバ属性

RADIUS 属性	ローカルサブスクライバ属性	説明	変数
Tunnel-Type	tunnel l2tp	サブスクライバセッションに使用されるトンネルのタイプを指定します。	L2TP
Tunnel-Server-Endpoint	tunnel l2tp peer-address	トンネルの接続先であるピア LNS の IP アドレスを指定します。	引用符で囲まれたドッ式の IPv4 アドレス
Tunnel-Password	tunnel l2tp secret	LAC と LNS との間での共有秘密を指定します。	引用符で囲まれた 1 ～英字および数字の文字
Tunnel-Private-Group-ID	tunnel l2tp tunnel-context	使用する LAC サービスが配置されているシステムに設定されている、接続先コンテキストの名前を指定します。 **重要** LAC サービスと出力インターフェイスがコアサービスまたはHAサービスと同じコンテキストで設定されている場合、この属性は必要ありません。	引用符で囲まれた 1 ～英字および数字の文字
Tunnel-Preference	tunnel l2tp preference	複数の LNS ノードが設定されている場合に、各ピア LNS の優先順位を設定します。 **重要** この属性は、**loadbalance-tunnel-peers** パラメータまたは **SN-Tunnel-Load-Balancing** 属性が優先されるように設定されている場合にのみ使用されます。	1 ～ 65535 の整数

RADIUS 属性	ローカルサブスクライバ属性	説明	変数
SN-Tunnel-Load-Balancing	loadbalance-tunnel-peer	複数の LNS ピアがサブスクライバプロファイルに設定されている場合に、RADIUS サーバーでの LNS ノードの選択方法を定義する選択アルゴリズムを指定するために使用されるベンダー固有の属性（VSA）。	• **Random**：LNS の順序ダムに選択します。L選択において **Tunnel-Preference** 属用されません。 • **Balanced**：設定された の LNS ノード間で負等配置するよう LNS に選択します。LNS において **Tunnel-Pref** 属性は使用されませ • **Prioritized**：**Tunnel-Preference** 属り当てられた優先順位いて LNS が選択され
Client-Endpoint	local-address	サブスクライバの L2TP セッションを利用しやすくするために使用する、システムに設定されている特定の LAC サービスの IP アドレスを指定します。 この属性は、複数の LAC サービスが設定されている場合に使用されます。	ドット 10 進表記の IPv4 ア ス。（xxx.xxx.xxx.xxx）

RADIUS タギングのサポート

システムは、トンネル属性の RADIUS 属性タギングをサポートしています。ユーザープロファイルで複数の LNS ノードが定義されている場合、これらの「タグ」により、複数の属性が異なるグループに編成されます。タギングは、特定のサーバーに使用されるすべての属性をシステムがグループ化するために役立ちます。特定の RADIUS サーバーで属性タギングがサポートされていない場合、システムは、暗黙的に、アクセス承認パケットに列挙された順で属性を編成します。

L2TP サポート用のローカル サブスクライバ プロファイルの設定

ここでは、L2TP をサポートするように、ローカル サブスクライバプロファイルをシステムで設定する手順について説明します。

重要 RADIUS ベースのサブスクライバプロファイルの設定については、このドキュメントでは説明していません。詳細については、ご使用の RADIUS サーバーに関するドキュメントを参照してください。

重要 ここでは、システムで L2TP サポート用のローカル サブスクライバ プロファイルを設定するための最小の命令セットについて説明します。追加のパラメータやオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*LAC Service Configuration Mode Commands*」の章 [英語] を参照してください。

L2TP サポートをサブスクライバに提供するようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 「ローカルサブスクライバの設定」の設定例を適用して、L2TP トンネルパラメータおよびロード バランシング パラメータとアクションを使用して「ローカル」サブスクライバを設定します。

ステップ 2 「*L2TP* の設定 の確認」の手順に従って、L2TP の設定を確認します。

ステップ 3 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

ローカルサブスクライバの設定

L2TP トンネルパラメータを使用してローカルサブスクライバを設定するには、次の例に示すコマンドを使用します。必要に応じて、複数の LNS サーバー間でロードバランシングを設定できます。

```
configure
   context <ctxt_name> [-noconfirm]
      subscriber name <subs_name>
         tunnel l2tp peer-address <lns_ip_address> [ preference <integer> | [
encrypted ] secret <secret_string> | tunnel-context <context_name> |
local-address <local_ip_address> }
         load-balancing { random | balanced | prioritized }
         end
```

注：

- *<ctxt_name>* は、サブスクライバプロファイルを設定するシステムコンテキストです。

- <*lns_ip_address*> は LNS サーバーノードの IP アドレスで、<*local_ip_address*> は LAC サービスにバインドされているシステムの IP アドレスです。

L2TP 設定の確認

これらの手順は、L2TP の設定を確認するために使用されます。

手順

特定のコンテキストの Exec モードで次のコマンドを入力して、L2TP が適切に設定されていることを確認します。

show subscriber configuration username *user_name*

このコマンドの出力には、サブスクライバパラメータの設定が簡潔に一覧表示されます。

RADIUS 属性を使用しない特定コンテキスト内のすべてのサブスクライバのトンネリング

システムでサポートされている他のサービスと同様に、RADIUS Access-Accept メッセージの一部として返されないサブスクライバプロファイル属性の値は、default というサブスクライバの、ローカルに設定されたプロファイルを使用して取得できます。default のサブスクライバプロファイルは、AAA コンテキスト（つまり、AAA 機能が設定されているコンテキスト）で設定する必要があります。

時間節約機能として、RADIUS ベースのサブスクライバ向けに追加の設定を行わずに、default というサブスクライバに対して L2TP サポートを設定できます。これは、特定のサブスクライバに個別の送信元/AAA コンテキストがある場合に特に役立ちます。

default というサブスクライバのプロファイルを設定するには、上記のローカルサブスクライバの設定手順に従い、default という名前を入力します。

機能説明

モバイル顧客宅内機器（CPE）にマルチキャストサービスが設定されている場合、APN は L2TP トンネルを使用して設定され、P-GW は L2TP アクセスコンセントレータ（LAC）として機能します。マルチキャストセッションを設定するには、ビデオクライアント/モバイル CPE が、SGi L2TP トンネルを介してビデオヘッドエンドサーバーとの間で PIM（プロトコル独立マルチキャスト）メッセージ（TTL=1）を送受信する必要があります。

P-GW は、デフォルトの L2TP LAC に従い、L2TP トンネル内のカプセル化された IP トラフィックを検査および処理します。このプロセスは、CPE と TTL=1 トラフィックを送信する LNS の間の特定のアプリケーションの機能を阻止します。21.21.1 より前のリリースでは、IP パケッ

トが送信されると、存続可能時間（TTL）値（255 など）がホップごとに 1 ずつ減少していました。P-GW は、TTL 値が 0 または 1 のパケットをドロップし、TTL 値を減少させ（TTL > 1 の場合）、データパケットの新しいチェックサムを計算しました。このリリースでは、CLI を使用して、L2TP 機能を介したマルチキャストセッションを有効にします。

- P-GW は TTL 値を無視してパケットを転送します。
- L2TP パケットと通常のパケットは sessmgr_ipv4.c の L2TP トンネルタイプで区別され、有効になっている CLI コンフィギュレーション モードが検証されます。

LAC サービスの設定

重要 すべてのコマンド、キーワード、および関数を使用できるわけではありません。機能はプラットフォームおよびライセンスによって異なります。

この項では、ピア LNS ノードと通信できるようにシステムで LAC サービスを設定するための情報と手順について説明します。

重要 システムで LAC サービス機能を設定するための最小の命令セットについて説明します。追加のパラメータとオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*LAC Service Configuration Mode Commands*」の章を参照してください。

システムで LAC サービスを設定するには、次の手順を実行します。

手順

ステップ 1 「*LAC* サービスの 設定」の項の設定例を適用して、システムに LAC サービスを設定し、IP アドレスにバインドします。

ステップ 2 オプションです。Tunnel-Service-Endpoint 属性がサブスクライバプロファイルで設定されていない場合、または PDSN 強制トンネリングがサポートされている場合は、「*LNS* ピアの設定」の項の設定例を適用して、LNS ピア情報を設定します。

ステップ 3 「LAC サービスの設定の確認」の項の手順に従って、LAC の設定を確認します。

ステップ 4 Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

LAC サービスの設定

LAC サービスを作成し、そのサービスを IP アドレスにバインドするには、次の例を使用します。

```
configure
   context <dst_ctxt_name> [-noconfirm]
      lac-service <service_name>
         bind address <ip_address>
         end
```

注：

- *<dst_ctxt_name>* は、LAC サービスを設定する接続先コンテキストです。

L2TP を介したマルチキャストサービスの設定

L2TP を介したマルチキャストセッション機能を有効または無効にするには、次の CLI コマンドを使用します。デフォルトでは、この機能は無効になっています。

```
configure
   context context_name
      lac-service service_name
         ttl-ignore
         end
```

注：

- **ttl-ignore**：TTL 値を無視してパケットを転送します。

LNS ピアの設定

LNS ピアや複数の LNS ピア間でのロードバランシングを設定するには、次の例を使用します。

```
configure
   context <dst_ctxt_name> [ -noconfirm ]
      lac-service <service_name>
         tunnel selection-key tunnel-server-auth-id
        peer-lns <ip_address> [encrypted] secret <secret> [crypto-map <map_name>
 {[encrypted] isakmp-secret <secret> }] [description <text>] [ preference
<integer>]
         load-balancing { random | balanced | prioritized }
         end
```

注：

- *<dst_ctxt_name>* は、LAC サービスを設定する接続先コンテキストです。

LAC サービス設定の確認

次の手順は、LAC サービスの設定を確認するために使用します。

手順

特定のコンテキストの Exec モードで次のコマンドを入力して、LAC サービスが適切に設定されていることを確認します。

show lac-service name *service_name*

以下の出力では、LAC サービスのパラメータの設定が簡潔に一覧で示されます。

```
Service name: vpn1
Context:                        isp1
Bind:                           Done
Local IP Address:               192.168.2.1
First Retransmission Timeout:   1 (secs)
Max Retransmission Timeout:     8 (secs)
Max Retransmissions:            5
Max Sessions:                   500000      Max Tunnels: 32000
Max Sessions Per Tunnel:        512
Data Sequence Numbers:          Enabled     Tunnel Authentication:  Enabled
Keep-alive interval:            60          Control receive window: 16
Max Tunnel Challenge Length:    16
Proxy LCP Authentication:       Enabled
Load Balancing:                 Random
Service Status:                 Started
Newcall Policy:                 None
```

L2TP サポートのための PDSN サービスの変更

PDSN サービスの変更は強制トンネリングでは必須であり、属性ベースのトンネリングでは任意です。

属性ベースのトンネリングでは、設定エラーが発生する可能性があります。例えば、認証が成功すると、システムは、サブスクライバセッションが L2TP を必要としていると判断するものの、提供された属性からでは、適切な LAC サービスが設定されているコンテキストの名前を特定できません。予防措置として、PDSN サービス設定オプションにパラメータが 1 つ追加されました。このパラメータは、使用するコンテキストの名前を示します。このパラメータを設定することを強く推奨します。

この項では、強制または属性ベースのいずれかのトンネリング用にPDSNサービス設定を変更する手順について説明します。



重要 この項では、システムで L2TP をサポートするように PDSN サービスを変更するための最小の命令セットについて説明します。追加のパラメータやオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*LAC Service Configuration Mode Commands*」の章 [英語] を参照してください。

システムで LAC サービスを設定するには、次の手順を実行します。

手順

ステップ 1 「*PDSN* サービスの変更」セクション の設定例を適用して、LAC コンテキストを関連付け、トンネルタイプを定義して、L2TP をサポートするように PDSN サービスを変更します。

ステップ 2 「*L2TP* サポートのための *PDSN* サービスの確認」の項の手順に従って、PDSN サービスを変更するための設定を確認します。

ステップ 3 Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

PDSN サービスの変更

次の例を使用して、LAC コンテキストを関連付けてトンネルタイプを定義することで、L2TP をサポートするように PDSN サービスを変更します。

```
configure
  context <source_ctxt_name> [ -noconfirm ]
    pdsn-service <pdsn_service_name>
      ppp tunnel-context <lac_context_name>
      ppp tunnel-type { l2tp | none }
      end
```

注：

- <*source_ctxt_name*> は、L2TP サポートのために変更する PDSN サービスを含むソースコンテキストの名前です。
- <*pdsn_service_name*> は、L2TP サポートのために変更する事前設定済みの PDSN サービスの名前です。
- <*lac_context_name*> は通常、LAC サービスが設定されている接続先コンテキストです。

L2TP サポートのための PDSN サービスの確認

PDSN サービスの設定を確認するには、これらの手順を使用します。

手順

特定のコンテキストの Exec モードで次のコマンドを入力して、PDSN が適切に設定されていることを確認します。

```
show pdsn-service name pdsn_service_name
```

このコマンドの出力には、PDSN サービスのパラメータの設定が簡潔に一覧表示されます。

L2TP をサポートするための APN テンプレートの変更

ここでは、システムで設定されている APN テンプレートで L2TP サポートを追加する手順について説明します。

重要 システムで LAC サービス機能を設定するための最小の命令セットについて説明します。追加のパラメータやオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*LAC Service Configuration Mode Commands*」の章 [英語] を参照してください。

システムで LAC サービスを設定するには、次の手順を実行します。

手順

ステップ 1 「*APN* テンプレートでの *LNS* ピアアドレスの割り当て」の項の設定例を参考にして、LNS サーバーアドレスやその他のパラメータを使用して L2TP をサポートするように APN テンプレートを変更します。

ステップ 2 オプションです。L2TP を使用してトランスペアレント IP PDP コンテキストをトンネリングする場合は、「アウトバウンド認証の設定」の項の設定例を適用して、APN のアウトバウンドユーザー名とパスワードを設定します。

ステップ 3 「*APN* の設定 の確認」の項の手順に従って、APN の設定を確認します。

ステップ 4 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

APN テンプレートでの LNS ピアアドレスの割り当て

APN テンプレートに LNS サーバーアドレスを割り当てるには、次の例を使用します。

```
configure
   context <dst_ctxt_name> [-noconfirm]
      apn <apn_name>
         tunnel l2tp [ peer-address <lns_address> [ [ encrypted ] secret
<l2tp_secret> ] [ preference <integer> ] [ tunnel-context <l2tp_context_name> ]
[ local-address <local_ip_address> ] [ crypto-map <map_name> { [ encrypted ]
isakmp-secret <crypto_secret> } ]
         end
```

注：

- <*dst_ctxt_name*> は、APN が設定されているシステム接続先コンテキストの名前です。
- <*apn_name*> は、L2TP サポートのために変更する、事前設定された APN テンプレートの名前です。
- <*lns_address*> は LNS サーバーノードの IP アドレスで、<*local_ip_address*> は LAC サービスにバインドされているシステムの IP アドレスです。

アウトバウンド認証の設定

LNS ピアや複数の LNS ピア間でのロードバランシングを設定するには、次の例を使用します。

```
configure
  context <dst_ctxt_name> [ -noconfirm ]
    apn <apn_name>
      outbound { [ encrypted ] password <pwd> | username <name> }
      end
```

注：

- <*dst_ctxt_name*> は、APN テンプレートが設定されている接続先コンテキストです。
- <*apn_name*> は、L2TP サポートのために変更する、事前設定された APN テンプレートの名前です。

APN 設定の確認

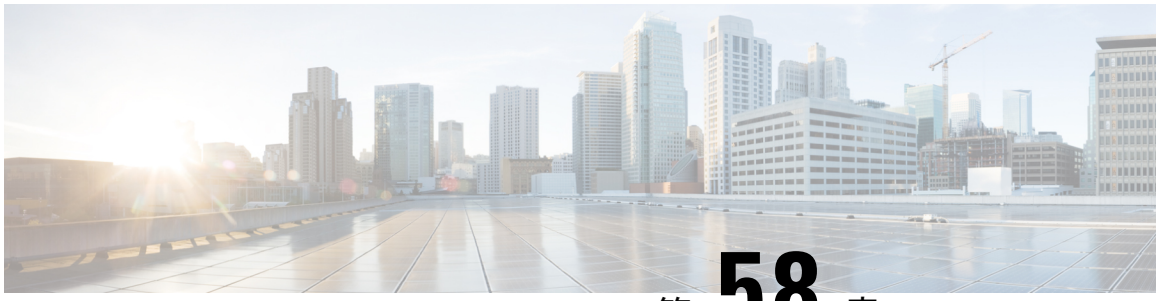
次の手順は、APN の設定を確認するために使用されます。

手順

特定のコンテキストの Exec モードで次のコマンドを入力して、APN が適切に設定されていることを確認します。

```
show apn name apn_name
```

出力では、APN のパラメータの設定が簡潔に一覧表示されます。



第 58 章

ダウンリンクおよびアップリンクのデータボリューム転送における LBO 制限

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （1063 ページ）
- 機能説明 （1064 ページ）
- 機能の仕組み （1064 ページ）
- ダウンリンクおよびアップリンクのデータボリューム転送における LBO 制限の設定 （1065 ページ）
- ダウンリンクおよびアップリンクのデータボリューム転送における LBO 制限のモニタリングと障害対応 （1065 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	ASR 5500
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.5

機能説明

サブスクライバクォータが使い果たされた場合、実行中のすべてのファイルのダウンロードを中止し、UE にユーザー定義のサーバー（セルフケアポータル）のみへのアクセスを許可する必要があります。

この機能はCLI制御メカニズムによって、ダウンリンクとアップリンクのデータボリューム転送におけるローカルブレークアウト（LBO）制限を実現します。

機能の仕組み

以下に、この機能の動作の概要を示します。

1. ユーザーがポータルにリダイレクトされ、OTP を入力します。サブスクライバセッションは、認証後も続行されます。
2. インターネットルールとデフォルトルールが PCRF によってインストールされ、クォータが OCS によって付与されます。
3. サブスクライバクォータを使い果たすと、PCRF はセルフケア再アドレス付けルールをインストールし、以前にインストールされたインターネットルールを削除します。
4. 再アドレス付けルールの適用後は、次のように動作します。
   - UDP の場合：進行中のダウンリンクパケットが破棄される一方、すべての新しいアップリンクパケットはセルフケアポータルに再アドレス付けされます。
   - TCP の場合：インターネットルールに一致するすべての既存のフローは、UE に FIN を送信し、サーバーに RST を送信することで終了します。

制限事項

再アドレス付けルールをインストールした後、最初のパケットは課金対象になりますが、UE には送信されません。後続のパケットは課金対象にならず、UE に送信もされません。

ダウンリンクおよびアップリンクのデータボリューム転送における LBO 制限の設定

ここでは、この機能をサポートするために使用可能な CLI コマンドについて説明します。

ダウンリンクおよびアップリンクのデータボリューム転送における LBO 制限の有効化

この機能を有効にするには、ACS ルールベース コンフィギュレーション モードで次の設定を使用します。

```
configure
  active-charging service service_name
    rulebase rulebase_name
      ip readdress failure-action terminate
      { default | no } ip readdress failure-action
      end
```

注：

- **ip readdress**：IP 再アドレス指定オプションを設定します。
- **failure-action**：IP 再アドレス指定の障害アクションを設定します。
- **terminate**：フローを終了します。
- 以前に設定されている場合は、**{ default | no } ip readdress failure-action** CLI コマンドを使用して機能を無効にします。

ダウンリンクおよびアップリンクのデータボリューム転送における LBO 制限のモニタリングと障害対応

ここでは、この機能のモニタリングや障害対応に使用できる CLI コマンドについて説明します。

show コマンドと出力

show active-charging rulebase statistics

この機能をサポートするために、この CLI コマンドの出力範囲が拡張されています。UDP の再アドレス付けに失敗すると、次の既存のカウンタが更新されます。

- 再アドレス付け失敗の合計回数

- ドロップされたパケット数

show active-charging sessions full all

この機能をサポートするために、この CLI コマンドの出力範囲が拡張されています。TCP フローの再アドレス付けに失敗すると、次の既存のカウンタが更新されます。

- フローアクション終了フロー

show active-charging charging-action statistics name *<charging_action_name>*

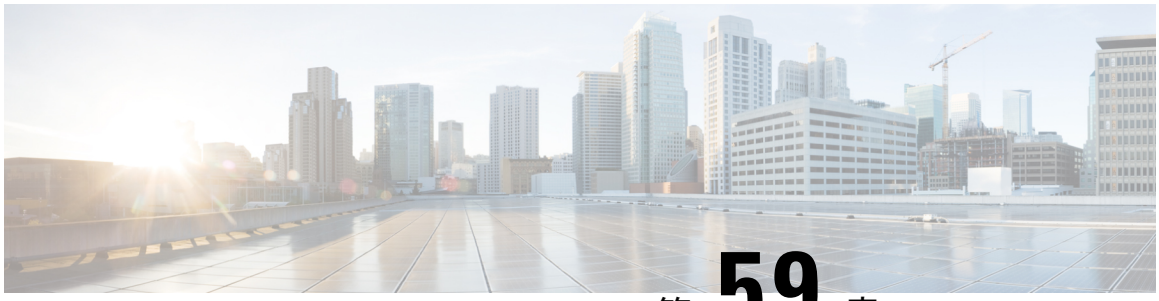
この機能をサポートするために、この CLI コマンドの出力範囲が拡張されています。TCP フローの再アドレス付けに失敗すると、次の既存のカウンタが更新されます。

- 終了フロー

show active-charging service statistics

この機能をサポートするために、この CLI コマンドの出力範囲が拡張されています。UDP の再アドレス付けに失敗すると、次の既存のカウンタが更新されます。

- ドロップされたパケット数



第 59 章

LTE から Wi-Fi（S2bGTP）へのシームレスハンドオーバー

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （1067 ページ）
- 機能説明 （1068 ページ）
- 機能の仕組み （1069 ページ）
- LTE から Wi-Fi へのシームレスハンドオーバーの設定 （1070 ページ）
- モニタリングおよびトラブルシューティング （1071 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC - DI • VPC - SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

重要　リリース 21.2 および N5.1 よりも前に導入された機能の変更履歴の詳細は示されません。

改訂の詳細	リリース
このリリースでは、サブスクライバの LTE から Wi-Fi（S2bGTP）へのシームレスなハンドオーバーのサポートが追加されています。	21.8
最初の導入。	21.2 よりも前

機能説明

LTE から Wi-Fi へのハンドオーバーが開始され、セッション作成応答（CSR）が Wi-Fi トンネルで送信されるとすぐに、ベアラー削除要求（DBR）が LTE トンネルを介して送信されます。このとき、ePDG での IPSec トンネル確立の遅延により、パケット損失が発生します。パケット損失の問題に対処するために、リリース 21.8 に拡張機能が導入されました。これにより 2 つのトンネル（LTE と Wi-Fi）が保持され、アップリンクデータが Wi-Fi トンネルで確認された場合、または設定されたハンドオーバータイマーの期限が切れたとき（アップリンクデータがない場合）のいずれか早い方でのみ、LTE トンネルでベアラー削除要求が送信されるようになります。LTE トンネルがアクティブである限り、アップリンクとダウンリンクのデータは LTE トンネルで交換されます。ハンドオーバーが完了すると、アップリンクとダウンリンクのデータが Wi-Fi トンネルで交換されます。これにより、パケット損失を防げます。

この機能拡張によるメリットは次のとおりです。

- LTE から Wi-Fi（S2bGTP）へのハンドオーバー中のパケット損失を最小限に抑え、ハンドオーバーをシームレスにします（つまり、メイクビフォアブレーク）。
- P-GW で両方のトンネルが確立されている場合、LTE 手順は LTE トンネルを介して正常に処理されます。
- P-GW で両方のトンネルが確立されている場合、Wi-Fi 手順は Wi-Fi トンネルを介して正常に処理されます。
- 同じサブスクライバに対して 2 つのトンネル（LTE と Wi-Fi）が確立されている場合、LTE または Wi-Fi トンネル（デフォルトまたは専用ベアラー）上での GTP-U エラー通知と GTP-U パス障害が移行期間中に適切に処理されます。

機能の仕組み

次の項では、LTE から Wi-Fi（S2bGTP）へのシームレスなハンドオーバーについて説明します。

LTE から Wi-Fi へのハンドオフ

LTE から Wi-Fi へのハンドオフは、次のように行われます。

1. P-GW は、次の時点まで S-GW への DBR の送信を遅延させます。
   - CSR の有効期限が ePDG に送信される（デフォルトの動作）。
   - Wi-Fi トンネルでアップリンクデータが送信される。
   - ハンドオーバータイマーが期限切れになる。タイマーが期限切れになった場合、ePDG はハンドオフの完了を通知するために、ベアラー変更要求（MBR）を送信しません。
2. LTE から Wi-Fi へのハンドオフの CSR を受信した後、LTE アクセスからのコントロールプレーン GTPv2（GTP-C）メッセージは P-GW で処理されません。これらのメッセージは EGTPC でブロックされます。
3. LTE トンネルは、移行期間中に GTP-U トラフィックを伝送します。移行期間は CSR（LTE から Wi-Fi へのハンドオフの受信）からハンドオーバーが完了するまでの時間として定義されます。このシナリオでは、ハンドオフ完了の MBR は予期されません。
4. 複数の未処理の CCR-U がサポートされている場合、ハンドオフ要求前のすべての要求はドロップされます。これは IMSA で行われます。
5. 移行期間中：
   - ベアラー変更コマンド（MBC）が Wi-Fi で受信された場合、サービス拒否メッセージを付けて拒否されます。
   - 専用ベアラーのベアラー削除コマンドが LTE で受信された場合は破棄されます。
   - ポリシー変更のために PCRF が RAR を送信する場合、ハンドオーバーの完了後に処理されます。
   - 新しいトンネル（つまり、Wi-Fi）は GTP-U トラフィックを伝送しません。移行期間中に Wi-Fi で受信された GTP-U トラフィックはドロップまたは無視されます。同様に、Wi-Fi で受信されたダウンリンクトラフィックは、DBR が Wi-Fi トンネルで送信されるまで、古いトンネル（つまり、LTE トンネル）で送信されます。これは、CSR が Wi-Fi トンネルで送信される場合にも当てはまります。アップリンクトラフィックが、タイマーの期限切れによってハンドオーバーの完了がトリガーされる前に Wi-Fi トンネルで受信された場合、それ以降のすべてのトラフィックは Wi-Fi トンネル経由でのみ転送されます。

- LTEアクセスで保留中のトランザクションはすべて破棄されます。たとえば、CBRまたはUBRがLTEアクセス用に送信され、CBRまたはUBRトランザクションが完了する前にハンドオフが開始された場合、CBRまたはUBRはP-GWで無視されます。PCRFには障害が通知されません。
- ASRが受信されると、コールドロップが発生して、両方のトンネルがダウンします。
- PCRFからセッション解放が発生した場合、コールはドロップされ、CSRが「リソースなし」という理由で送信されます。
- LTEを介したGTP-UまたはGTP-Cパスで障害が発生した場合、Wi-Fi通話が継続中にLTEアクセスでコールがドロップされます。
- Wi-Fiを介したGTP-UまたはGTP-Cパスで障害が発生した場合、コールのドロップにつながります。両方のトンネルがクリアされます。
- HO-Indが1に設定された状態で（ガードタイマー後）、ユーザーがLTEに戻る（つまり、LTEからWi-Fi、LTEへのハンドオフが繰り返される）場合、HOは正常に処理され、ユーザーセッションは再びLTEに移行されます。
- ユーザーがHO-Indを0に設定した状態でLTEに戻る（つまり、LTEからWi-Fi、LTEへのハンドオフを繰り返す）場合、コンテキストの置換が発生します。古いコールはコンテキスト置換という理由でWi-Fiアクセスでクリアされ、LTEを介した新しいコールのように処理されます。

セッションリカバリと ICSR

移行期間中、古いアクセスが安定した状態と見なされ、LTEからWi-Fi（S2bGTP）へのハンドオーバーが完了すると、フルチェックポイントがトリガーされます。これは、セッションリカバリとICSRの両方に対して行われます。

LTE から Wi-Fi へのシームレスハンドオーバーの設定

ここでは、機能を有効または無効にするために使用できるCLIコマンドについて説明します。

LTE から Wi-Fi へのハンドオーバータイマーの設定

次のCLIコマンドを使用して、LTEからWi-Fiへのハンドオーバータイマーを設定します。

```
configure
  context context_name
    apn apn_name
      lte-s2bgtp-first-uplink timeout
      { default | no } lte-s2bgtp-first-uplink
      end
```

注：

- **default**：Wi-Fi トンネルでセッション作成応答が送信された時点での、LTE から Wi-Fi へのハンドオーバーの完了を有効にします。
- **no**：機能を無効にし、セッション作成応答時点でハンドオーバーが完了します。
- **lte-s2bgtp-first-uplink** *timeout*：LTE から S2bGTP へのハンドオーバー完了タイムアウトを 100 ミリ秒の倍数で設定します。有効な範囲は 100 ～ 3000 です。推奨設定は 1000 ミリ秒です。
- デフォルトでは、Wi-Fi トンネルでセッション作成応答が送信された時点で、LTE から Wi-Fi へのハンドオーバーが完了します。ただし、ハンドオーバータイムアウトの設定後、ハンドオーバーは、タイムアウトするまで、または Wi-Fi トンネルでアップリンクデータが受信されるまで遅延されます。

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングとトラブルシューティングのサポートで使用できる CLI コマンドについて説明します。

コマンドや出力の表示

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show apn statistics name <name>

この CLI コマンドの出力が拡張され、APN に関する次のフィールドが表示されるようになりました。

- LTE-to-S2bGTP handover Succeeded on First Uplink Data on S2b tunnel：アップリンクパケットによるハンドオーバーの回数を指定します。
- LTE-to-S2bGTP handover Succeeded on Timer Expiry：タイマー時間の終了によるハンドオーバーの回数を指定します。

注：

この機能の一部として導入された新しいフィールドは、次の CLI コマンドでも表示されます。

- **show pgw-service statistics name** *service_name* **verbose**
- **show pgw-service statistics all verbose**
- **show saegw-service statistics all function pgw verbose**

バルク統計

この機能のサポートには、次の統計情報が含まれています。

APN スキーマ

LTE から Wi-Fi へのシームレスなハンドオーバー機能をサポートするために、APN スキーマの APN に次のバルク統計が追加されています。

バルク統計	説明
apn-handoverstat-ltetos2bgtpsucc-timerexpiry	タイマーの期限切れ時の、成功した LTE から S2bGTP へのハンドオーバーの数。
apn-handoverstat-ltetos2bgtpsucc-uplnkdata	S2b トンネル上のアップリンクデータで成功した LTE から S2bGTP へのハンドオーバーの数。

P-GW スキーマ

LTE から Wi-Fi へのシームレスなハンドオーバー機能をサポートするために、P-GW スキーマで P-GW に次のバルク統計が追加されています。

バルク統計	説明
handoverstat-ltetos2bgtpsucc-timerexpiry	ハンドオーバー統計：タイマーの期限切れ時の LTE から GTP S2b への成功したハンドオーバーの数。
handoverstat-ltetos2bgtpsucc-uplnkdata	ハンドオーバー統計：S2b トンネルのアップリンクデータにおける LTE から GTP S2b への成功したハンドオーバーの数。

SAEGW スキーマ

LTE から Wi-Fi へのシームレスなハンドオーバー機能をサポートするために、SAEGW スキーマで SAEGW に次のバルク統計が追加されています。

バルク統計	説明
pgw-handoverstat-ltetos2bgtpsucc-timerexpiry	P-GW ハンドオーバー統計：タイマーの期限切れ時の LTE から GTP S2b への成功したハンドオーバーの数。
pgw-handoverstat-ltetos2bgtpsucc-uplnkdata	P-GW ハンドオーバー統計：S2b トンネルのアップリンクデータにおける LTE から GTP S2b への成功したハンドオーバーの数。



第 60 章

SAEGW、P-GW、および S-GW サービスにおける LTE-M RAT タイプのサポート

- 機能の概要と変更履歴 （1073 ページ）
- 機能説明 （1074 ページ）
- 機能の仕組み （1075 ページ）
- 仮想 APN の設定 （1078 ページ）
- qci-qos-mapping の設定 （1078 ページ）
- モニタリングおよびトラブルシューティング （1079 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• S-GW • P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
デフォルト設定	有効を常にオン
このリリースでの関連する変更点	N/A

関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administartion Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.24

機能説明

LTE-M（LTE-MTC 低消費電力広域（LPWA））は、3GPP が規定する、低消費電力広域接続ソリューション対応の新しいセルラー無線アクセス技術です。具体的には、IoT LTE-M に適した LTE UE の特定のカテゴリを指します。IoT LTE-M は、デバイスの複雑さを軽減して IoT をサポートし、カバレッジを拡大すると同時に、LTE インストールベースの再利用を可能にします。

RAT タイプ IE は、多くのインターフェイス間のさまざまなコールフローに含まれます。不明な RAT タイプを含むセッション作成要求を受信した場合、RAT タイプはこのメッセージの必須 IE であるため、S-GW または P-GW がセッション作成要求を拒否する場合があります。

この StarOS 21.24 リリースでは、S-GW、P-GW、および SAEGW 製品の LTE-M RAT（無線アクセステクノロジー）タイプがサポートされています。

RAT タイプは、IE（GTPv2-C、GTPP など）、AVP（Diameter ベースのインターフェイスなど）として、または多くのインターフェイスにまたがる属性（EDR など）として存在します。

S-GW、P-GW、および SAEGW の LTE-M ソリューションは、以下のインターフェイスプロトコルおよびディクショナリで次の新しい LTE-M RAT タイプ属性値をサポートします。

- GX インターフェイス：Diameter プロトコル
- GY インターフェイス：Diameter プロトコル
- GZ/RF インターフェイス：GTPP/Diameter/RADIUS
- S6B インターフェイス：Diameter プロトコル
- S11/S5/S8 インターフェイス：GTPv2-C
- ディクショナリ RADIUS APV、およびディクショナリ
- CDR 生成用の Rf インターフェイス
- EDR の属性

既存機能の拡張

RAT タイプ LTE-M をサポートするために、次の既存機能が拡張されます。

- **RAT タイプに基づく仮想 APN の選択**：仮想 APN は、単一の APN 内におけるサービスの差別化を可能にします。仮想 APN 機能により、キャリアは単一の APN を使用してサービスの差別化を設定できます。MME によって提供される APN は、複数の設定可能パラメータを使用して P-GW により評価されます。次に、P-GW は、指定された APN とそれらの設定可能パラメータに基づいて APN 設定を選択します。APN 設定は、APN ごとにポリシーが異なる P-GW において、セッションのあらゆる側面を決定します。

  ベース APN 下に直接設定することで、仮想APNを選択できます。このAPNの選択は、RAT タイプに基づいて行われます。このリリースでは、CLI を使った LTE-M RAT タイプに応じた仮想 APN の選択がサポートされるようになりました。

- **QCI および QoS マッピング**：P-GW は、RAT タイプ LTE-M に基づく APN との QCI および QoS マッピングの関連付けをサポートします。QCI および QoS マッピングを使用すると、QoS クラスインデックス（QCI）の QoS へのマッピング設定モードでクイックアクションを実行できます。このモードは、QoS クラスインデックスを適用可能な QoS パラメータにマッピングするために使用されます。マッピングは、LTE ネットワークのサービングゲートウェイ（S-GW）あるいは PDN ゲートウェイ（P-GW）、またはその両方で発生する可能性があります。

- **PCRF ベースの処理**：P-GW はクレジット制御要求 - 初期および更新済みメッセージを介して RAT タイプの変更を PCRF に通知し、PCRF は新しい PCC ルールを提供します。ポリシーおよび課金ルール機能（PCRF）から新しいポリシーおよび課金制御（PCC）ルールを適用することで、ベアラーを作成できます。

機能の仕組み

アーキテクチャ

次の表に、LTE-M RAT タイプをサポートするさまざまなインターフェイスのフィールドとその値を示します。標準ディクショナリとカスタマイズされたディクショナリのみが変更されます。

表 *100 :*

フィールド	P	メッセージ	属性
インターフェイス (af retnl)			
P-GW 製品			
RAT タイプ（1032）直径	M	- E-TACS (7001)	• クレジット制御要求：初期 • クレジット制御要求：更新
3GPP RAT タイプ（21）直径	M	- E-TACS (9)	• クレジット制御要求：初期 • クレジット制御要求：更新
3GPP RAT タイプ（21）	M	- E-TACS (9)	• アカウンティング要求：開始 • アカウンティング要求：終了 • アカウンティング要求：中間
3GPP RAT タイプ（21）直径	M	- E-TACS (9)	• アカウンティング要求：開始 • アカウンティング要求：終了 • アカウンティング要求：中間
3GPP RAT タイプ（1032）直径	M	- E-TACS (9)	• 認証 • 承認 • 要求
RAT タイプ	M	– ETL (9)	
RAT タイプ（30）GTPP	M	- E-TACS (9)	• GTPP データレコード • 転送要求
S-GW 製品			
RAT タイプ（30）	M	- E-TACS (9)	• GTPP データレコード • 転送要求

制限事項

新しい LTE-M RAT タイプ機能の既知の制限を以下に示します。

- ECS でのルール照合
- ローカルポリシーでの ruledef 照合

サポートされる標準

シスコの LTE RAT タイプの実装は、次の標準に準拠しています。

- 3GPP 23.401：eGPTC Interface
- 3GPP 29.274 リリース 15.4.0：3GPP GTPv2 Protocol Specification Reference table for LTE-M Rat type support。RAT タイプ IE の詳細については、egtpc IE エンコーディングおよび復号化に関する次の表を参照してください。
  - 表 7.2.1-1：Information Elements in a Create Session Request
  - 表 7.2.7-1：Information Elements in a Modify Bearer Request
  - 表 7.2.7-1：Information Elements in a Modify Bearer Request
- 3GPP 23.401 リリース 15.4.0：3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP 32.299 リリース 15.4.0：3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC)。
- 3GPP 29.060：3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface。
- 3GPP 29.061：3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP 32.298：3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP 29.212 リリース 15.4.0：3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC)。

仮想 APN の設定

追加オプション（LTE-M）の「RAT タイプ」ベースの仮想 APN 選択を表示するには、次の設定を使用します。

```
configure
  context  context_name
    apn  apn_name
       virtual-apn  preference  value apn  apn_name rat-type lte-m
       end
```

注：

- **apn** *apn_name*：APN 名を条件として指定することを可能にします。*apn_name* は、1 ～ 63 文字の英数字の文字列である必要があります。
- **virtual-apn preference** *value* **apn** *apn_name* ：仮想 APN（virtual.ipv4）を設定します。
- **rat-type lte-m**：LTE-M を追加の RAT タイプとして有効にします。

qci-qos-mapping の設定

APN コンフィギュレーション モードで QCI-QOS マッピングを設定し、追加の RAT タイプ（LTE-M）を関連付けするには、次の設定を使用します。

```
configure
  context  context_name
    apn  apn_name
      qci table
       qci-qos-mapping
            qci  qci_val non-gbr { downlink  user-datagram dscp-marking
value }
           end
```

注：

- **apn** *apn_name*：APN 名を条件として指定することを可能にします。*apn_name* は、1 ～ 63 文字の英数字の文字列である必要があります。
- **qci-qos-mapping**：APN の QCI-QoS マッピングを設定します。
- **qci** *qci_val*：QoS クラス識別子を指定します。*qci_val* は、1 ～ 9、80、82、83 の整数である必要があります。
  - **downlink**：この QoS 設定を適用する必要があるトラフィックの方向を指定します。

QCI-QoS マッピングの関連付け

qci-qos-mapping RAT タイプを選択するには、この設定を使用します。

```
configure
  context  context_name
    apn  apn_name
      associate  qci-qos-mapping table rat-type lte-m
      end
```

注：

- **associate qci-qos-mapping table rat-type lte-m** ：RAT タイプに基づいて apn qci-qos-mapping を関連付けます。

モニタリングおよびトラブルシューティング

ここでは、SAEGW、P-GW、および S-GW サービスにおける LTE-M RAT タイプのサポートのモニタリングおよび障害対応に使用できるコマンドについて説明します。

show コマンドと出力

ここでは、LTE-M RAT タイプの機能の show コマンドとコマンド出力について説明します。

show apn name

セッションセットアップ時に RAT タイプに基づいて仮想 APN が選択された場合、次の出力が表示されます。

Output:

```
show apn name <>
Virtual APN Configuration:
  Preference  Selected-APN           Rule-Definition
  10          verizon.ipv4           CC Profile Index = 3
   RAT Type = lte-m [local]qvpc-si# show configuration
```

show apn all

show apn all コマンドと **show apn name** *apn_name* **all** コマンドの出力が拡張され、RAT タイプ **lte-m** での qci-qos-mapping の APN 設定がモニターされるようになりました。

例：

```
show apn name <>
qci-qos-mapping Name for RAT-Type:
GERAN :N/A            UTRAN :N/A
EUTRAN : N/A          LTE-M : table
Stats Profile Name : N/A
```

show qci-qos-mapping table all

追加の RAT タイプ（LTE-M）に基づいて qci-qos-mapping テーブルを関連付ける前の出力例を次に示します。

```
QCI-QOS Table Name: table
```

```
 Qci:  1
  uplink: n/a
  downlink: user-datagram            dscp-marking 0x3e
  maximum packet delay:  n/a         maximum error rate:  n/a
  delay class:  n/a             precedence class:     n/a
  reliability class:  n/a            qci type:   non-gbr
  volte:   n/a                       traffic policing interval:  n/a

 Qci:  2
  uplink: n/a
  downlink: internal-qos priority 1
  maximum packet delay:  n/a         maximum error rate:  n/a
  delay class:     n/a               precedence class:  n/a
  reliability class:     n/a         qci type:   gbr
  volte:     n/a                     traffic policing interval:  n/a
```

show configuration

仮想 APN が LTE-M RAT タイプで設定されている場合、出力に **virtual-apn preference** *value* **apn** *apn_name* **rat-type lte-m** が表示されます。出力の例を以下に示します。

```
[local]qvpc-si# show configuration
apn intershat
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode subscribed sent-by-ms chosen-by-sgsn
      accounting-mode radius
      ims-auth-service ims-ggsn-auth
      ip access-group acl4-1 in
      ip access-group acl4-1 out
      authentication pap 1 chap 2 allow-noauth
      ip context-name egress
      virtual-apn preference 10 apn verizon.ipv4 rat-type lte-m
      ipv6 access-group acl6-1 in
      ipv6 access-group acl6-1 out
      active-charging rulebase prepaid
    exit
```

同様に、**associate qci-qos-mapping table rat-type lte-m** の出力は、RAT タイプに基づく qci-qos 関連付けの変更に対して表示されます。出力の例を以下に示します。

```
 [local]laas-setup# show configuration
                apn intershat
                context ingress
               subscriber default
                nexthop-forwarding-address
                exit
                apn intershat
                associate qci-qos-mapping table rat-type lte-m
                exit
```

show subscribers full

この show コマンドの出力は、サブスクライバコールのモニタリングに使用されます。コールの RAT タイプは LTE-M として表示されます。新しいフィールド **LTE-M** が Access Technology に追加されています。出力の例を以下に示します。

```
[local]laas-setup# show subscribers all
Access  (X) - CDMA 1xRTT                (E) - GPRS GERAN    (I) - IP
||    Tech:       (D) - CDMA EV-DO      (U) - WCDMA UTRAN   (W) - Wireless LAN
||                (A) - CDMA EV-DO REVA (G) - GPRS Other    (M) - WiMax
```

```
||                (C) - CDMA Other      (J) - GAN           (O) - Femto IPSec
||                (P) - PDIF            (S) - HSPA          (L) - eHRPD
||                (T) - eUTRAN          (B) - PPPoE         (F) - FEMTO UTRAN
||                (N) - NB-IoT          (Q) - WSG           (R)- LTE-M
                  (.) - Other/Unknown
```

show subcscribers full all

次の show コマンドの出力は、サブスクライバコールのモニタリングに使用されます。コールのアクセステクノロジーは、LTE-M と表示されます。

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                     Access Network Peer ID: n/a
  callid: 02fb3ea1                       msid: 404005123456789
  Card/Cpu: 1/0                          Sessmgr Instance: 11
  state: Connected
  connect time: Tue Mar 23 04:33:55 2021 call duration: 00h00m46s
  idle time: 00h00m40s                idle time left:  n/a
```

show subs pgw-only full / show subs pgw-only full all

show subs pgw-only full / **show subs pgw-only full all** コマンドは、コールのアクセステクノロジーを LTE-M として表示します。出力例を次に示します。

```
Access Type: gtp-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                   pgw-service-name: PGW21
  Callid: 02fb3ea2                     IMSI: 404005123456789
  MSISDN: 9890098900                   External ID: n/a
  Interface Type: S5S8GTP              Low Access Priority: N/A
  TWAN Mode: N/A
  eMPS Bearer: No
  Emergency Bearer Type: N/A
  IMS-media Bearer: No
  S6b Auth Status: N/A
```

show subs sgw-only full / show subs sgw-only full all

show subs sgw-only full および **show subs sgw-only full all** コマンドでは、コールのアクセステクノロジーが LTE-M として表示されます。出力例を次に示します。

```
 Card/Cpu        : 1/0         Sessmgr Instance : 11
  Idle time       : 00h05m47s
  MS TimeZone     : n/a                  Daylight Saving Time: n/a

  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                           sgw-service-name: SGW21
  Callid: 02fb3ea1                       IMSI: 404005123456789
  MSISDN: 9890098900
  eMPS Bearer: No
```

show subs saegw-only full / show subs saegw-only full all

show subs saegw-only full / **show subs saegw-only full all** コマンドは、コールのアクセステクノロジーを LTE-M として表示します。出力例を次に示します。

```
 Callid   : 02fb3ea3                    IMSI               : 404005123456789
  Card/Cpu          : 1/0                        Sessmgr Instance    : 11
  Source context    : EPC2                       Destination context : ISP1
```

```
  Bearer Type       : Default                     Bearer-Id           : 5
  Access Type       : gtp-pdn-type-ipv4-ipv6      Network Type        : IPV4+IPv6
  Access Tech       : LTE-M                       saegw-service-name  : SAEGW21
  MSISDN            : 9890098900                  External ID         : n/a
  TWAN Mode         : N/A
  eMPS Bearer       : No
  WPS Bearer        : No
```

show subs pgw-only all

show subs pgw-only all コマンドを実行すると、次の出力が表示されます。

```
|+------Access    (U) - UTRAN     (G) - GERAN
||      Tech:     (W) - WLAN                (J) - GAN
||                (U) - HSPA Evolution      (E) - eUTRAN
||                (H) - eHRPD               (.) - Unknown
||                (N) - NB-IoT              (R) - LTE-M
```

show subs sgw-only all

show subs sgw-only all コマンドを実行すると、次の出力が表示されます。

```
|+----Access   (U) - UTRAN  (G) - GERAN           (W) - WLAN
||    Tech:    (J) - GAN              (S) - HSPA Evolution  (E) - eUTRAN
||             (.) - Unknown          (N) - NB-IoT         (R) - LTE-M

||
```

show subs saegw-only all

show subs saegw-only all コマンドを実行すると、次の出力が表示されます。

```
|+----Access   (U) - UTRAN  (G) - GERAN           (W) - WLAN
||    Tech:    (J) - GAN              (S) - HSPA Evolution  (E) - eUTRAN
||             (H) - eHRPD            (.) - Unknown        (N) - NB-IoT
||             (R) - LTE-M
```

show subscribers callid

show subscribers callid *callid*コマンドは、コールのアクセステクノロジーを LTE-M として表示します。出力例を次に示します。

```
|+----Access  (X) - CDMA 1xRTT(E) - GPRS GERAN      (I) - IP
||    Tech:   (D) - CDMA EV-DO          (U) - WCDMA UTRAN     (W) - Wireless LAN
||            (A) - CDMA EV-DO REVA     (G) - GPRS Other      (M) - WiMax
||            (C) - CDMA Other          (J) - GAN             (O) - Femto IPSec
||            (P) - PDIF                (S) - HSPA            (L) - eHRPD
||            (T) - eUTRAN              (B) - PPPoE           (F) - FEMTO UTRAN
||            (N) - NB-IoT              (Q) - WSG             (R) - LTE-M

||            (.) - Other/Unknown
```

show session subsystem

次の出力には、セッション関連の統計が表示されています。

```
LTE-M Data Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
NB-IoT Connection Statistics
```

```
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
LTE-M Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
```

同様に、**show session subsystem full** は、RAT タイプごとのデータパケット数とサブスクライバ数を表示するように拡張されています。

show session subsystem verbose

show session subsystem verbose コマンドを実行すると、次の出力が表示されます。

```
NB-IoT Data Statistics
             packets to User:             0    octets to User:   0
             packets from User:           0    octets from User: 0

LTE-M Data Statistics
             packets to User:             0    octets to User:   0
             packets from User:           0    octets from User: 0

 NB-IoT Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
 LTE-M Connection Statistics
       0 Total Sessions                  0 Total calls arrived
       0 Total calls connected           0 Total calls disconnected
```

show session summary

show session summary コマンドを実行すると、次の出力が表示されます。

```
4G LTE (EUTRAN): 0
2G (GERAN): 0
3G (UTRAN): 0
WiFi (WIRELSS LAN): 0
eHRPD: 0
3G HA: 0
NB-IoT: 2
LTE-M: 0
Others: 0
```

show subscribers subscription full

show subscribers subscription full コマンドを実行すると、次の出力が表示されます。

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                     Access Network Peer ID: n/a
  callid: 02fb3ea1                       msid: 404005123456789
  Card/Cpu: 1/0                          Sessmgr Instance: 11
  state: Connected
  connect time: Wed Mar 17 09:59:47 2021 call duration: 00h01m19s
  idle time: 00h01m13s                idle time left:  n/a
  session time left:  n/a
```

show subscribers activity all

show subscribers activity all コマンドは、コールのアクセステクノロジーを LTE-M として表示します。出力例を次に示します。

```
Username: 9890098900           Status: Online/Active
  Access Type: sgw-pdn-type-ipv4-ipv6    Network Type: IPV4+IPv6
  Access Tech: LTE-M                     Access Network Peer ID: n/a
  callid: 02fb3ea1                       msid: 404005123456789
```

show apn statistics all-name

show output コマンドは、APN ごとに統計を表示し、また LTE-M RAT タイプの開始されたセッションとアクティブなセッションの数も APN ごとに表示します。出力の例を以下に示します。

```
Initiated Sessions per RAT Type:
    EUTRAN:  0    UTRAN:   0
    GERAN:   0    EHRPD:   0
    S2A GTP: 0    S2B GTP: 0
    S2B PMIP:0    NB-IoT:  0
    LTE-M :  0

  Active Sessions per RAT Type:
   EUTRAN: 0   UTRAN: 0
   GERAN:  0   WLAN:  0
   HSPA:   0   NB-IoT:0
   LTE-M:  0   OTHER: 0
```

show saegw-service statistics all-name

このshow出力コマンドは、SAEGWサービスごとの統計情報を表示し、また、SAEGWサービスごとに現在のサブスクライバ、 現在の PDN を NB-IoT RAT タイプとともに表示します。出力の例を以下に示します。

```
Current Subscribers By RAT-Type:
  EUTRAN:                          0    UTRAN:                          0
  GERAN:                           0    NB-IoT:                         0
  LTE-M:                           0    OTHER:                          0

Current PDNs By RAT-Type:
    EUTRAN:                        0    UTRAN:                        0
    GERAN:                         0    NB-IoT:                       0
    LTE-M:                         0    OTHER:                        0
```

show pgw-service statistics all-name

show output コマンドでは、各 P-GW サービスの統計、開始された PDN の数、および各 P-GW サービスの NB-IoT RAT タイプを持つ現在の PDN が表示されます。出力の例を以下に示します。

```
Initiated PDNs By RAT-Type:
  EUTRAN:                          0    UTRAN:                          0
  GERAN:                           0    EHRPD:                          0
  S2A GTP:                         0    S2B GTP:                        0
  S2B PMIP:                        0    NB-IoT:                         0
  LTE-M                          0

Current PDNs By RAT-Type:
  EUTRAN:                          0    UTRAN:                          0
  GERAN:                           0    WLAN:                           0
  NB-IoT:                          0    LTE-M                           0
  OTHER:                           0
```

show sgw-service statistics

この show コマンドは、各 S-GW サービスの統計情報を表示します。この CLI が拡張され、各 S-GW サービスについて NB-IoT RAT タイプの現在のサブスクライバおよび現在の PDN が表示されるようになりました。出力の例を以下に示します。

```
Current Subscribers By RAT-Type:
  EUTRAN:                           0    UTRAN:                            0
  GERAN:                            0    NB-IoT:                           0
  LTE-M:                            0    OTHER:                            0
Current PDNs By RAT-Type:
    EUTRAN:                         0    UTRAN:                            0
    GERAN:                          0    NB-IoT:                           0
    LTE-M:                          0    OTHER:                            0
```

バルク統計

LTE-M RAT タイプ機能をサポートするために、次の統計情報が追加されました。

APN スキーマ

APN スキーマでは、次の LTE-M RAT タイプ機能関連のバルク統計を使用できます。

バルク統計	説明
active-lte-m-sessions	RAT タイプが LTE-M の、APN ごとのアクティブ LTE-M セッションの合計数。
initiated-lte-m-sessions	開始された LTE-M セッションの合計数。

P-GW スキーマ

P-GW スキーマでは、次の LTE-M RAT タイプ機能に関連するバルク統計を使用できます。

バルク統計	説明
sesstat-pdn-rat-lte-m	アクティブな PDN の合計数タイプ別統計 – LTE-M。
sessstat-rat-init-lte-m	開始された LTE-M PDN（RAT タイプが LTE-M）の合計数。

P-GW スキーマ

S-GW スキーマでは、次の LTE-M RAT タイプ機能に関連するバルク統計を使用できます。

バルク統計	説明
sessstat-totcur-ue-lte-m	RAT タイプが LTE-M のアクティブ UE の合計数。

バルク統計	説明
sessstat-totcur-pdn-lte-m	RAT タイプが LTE-M のアクティブ PDN の合計数。

SAEGW スキーマ

SAE-GW スキーマでは、次の LTE-M RAT タイプ機能に関連するバルク統計を使用できます。

バルク統計	説明
sgw-sessstat-totcur-ue-lte-m	RAT タイプが LTE-M のアクティブ UE の合計数。
sgw-sessstat-totcur-pdn-lte-m	RAT タイプが LTE-M の LTE-M PDN（P-GW アンカー/Collapsed PDN）の合計数。
pgw-sesstat-pdn-rat-lte-m	RAT タイプが LTE-M の LTE-M PDN（P-GW アンカー/Collapsed PDN）の合計数。
pgw-sessstat-pdn-rat-init-lte-m	開始された LTE-M PDN の合計数。
saegw-sgw-anchor-pdn-rat-lte-m	RAT タイプが LTE-M の LTE-M PDN（SGW アンカー）の合計数。
saegw-pgw-anchor-pdn-rat-lte-sm	RAT タイプが LTE-M の LTE-M PDN（PGW アンカー）の合計数。
saegw-collapsed-pdn-rat-lte-m	RAT タイプが LTE-M の LTE-M PDN（P-GW アンカー/Collapsed PDN）の合計数。



第 61 章

最大受信ユニット設定のサポート

- 機能の概要と変更履歴 （1087 ページ）
- 機能説明 （1088 ページ）
- 機能の仕組み （1088 ページ）
- MRU 機能の設定 （1088 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAE-GW • S-GW
該当プラットフォーム	ASR 5500
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *S-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.24

機能説明

MRU 設定がサポートされる前は、最大受信ユニット（MRU）の設定は最大伝送ユニット（MTU）の設定と同じでした。

S1-U インターフェイスの eNB の MTU が 2000 バイトに増やされましたが、SAE-GW の S1-U インターフェイスの MTU には変更が加えられず、1500 バイトを超えるサイズのパケットが SAE-GW で受信されました。その結果、これらのパケットは、SAE-GW の S1-U インターフェイスにおいて **Lport_MRU_exceeded** 例外でドロップされました。この動作は、IKE トンネルを設定しようとしている UE に影響を与えました。

この MRU 設定機能を使用して、MTU とは別に MRU を設定できます。

機能の仕組み

MTU とは独立して MRU を処理するために、ネットワーク処理ユニット（NPU）、NPUSIM、NPUMGR、および CLI に変更が加えられます。

MRU 機能の設定

このセクションでは、インターフェイス設定で **ip mtu** キーワードを使用して、MTU とともに IP インターフェイスの MRU を設定する方法について説明します。

MRU の設定

イーサネット インターフェイス構成モードで MTU と MRU を設定するには、次の設定例を使用します。

```
config
  context context_name
    interface interface_name broadcast
    ip mtu mtu_size [ mru mru_size ]
    end
```

注：

- **ip mtu** *mtu_size*：MTU サイズを指定します。*mtu_size* は、5762048 バイトの範囲の整数である必要があります。
- **mru***mru_size*：MRU サイズを指定します。*mru_size* は、5762048 バイトの範囲の整数である必要があります。
- MTU 設定を無効にするには、**no ip mtu** コマンドを使用します。
- MTU に設定できる最大値は 2048 バイトです。MTU が設定されていない場合、デフォルト値は 1500 バイトです。

- MRU 属性はオプションであり、設定されていない場合、MRU は MTU と同じ値に設定されます。
- オプションの MRU 属性は、VPC-DI および VPC-SI プラットフォームには適用されません。この属性は ASR 5500 にのみ表示されます。
- CUPS または ICUPS で、インターフェイスで MRU を設定しようとすると、次のエラーが表示されます。

  ```
  Failure: Configure MRU Feature is not supported when ICUPS/CUPS is
  enabled!
  ```

- 同一インターフェイス上で非対称の MTU 値および MRU 値を設定できますが、ネットワーク上で望ましくない動作を引き起こす可能性があるため、推奨できません。

MTU が指定されていない場合の MRU 機能の設定

MTU = デフォルト MTU、MRU = デフォルト MTU

次に例を示します。

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     bfd interval 300 min_rx 300 multiplier 3
     #exit
#exit
```

MRU が指定されていない場合の MTU 機能の設定

MRU = 後方互換性のために設定された MTU。MRU = MTU = 1,970 バイト。

次に例を示します。

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     ip mtu 1970
     bfd interval 300 min_rx 300 multiplier 3
#exit
```

MTU と MRU の両方が指定されている場合の MTU 機能の設定

MTU = デフォルト MTU、MRU = デフォルト MTU

次に例を示します。

```
configure
   interface SGi-VLAN400
     logical-port-statistics
     ip address 172.26.96.3 255.255.255.248
     ipv6 address 2600:300:2030:1104::3/64 secondary
     ip mtu 1600 mru 1700
     bfd interval 300 min_rx 300 multiplier 3
#exit
```

設定済み MRU の確認

設定された MRU 値を表示するように、出力が強化されました。

次に例を示します。

```
[EPC2]26kl-chassis# config
[EPC2]26kl-chassis(config)# context EPC2
[EPC2]26kl-chassis(config-ctx)# interface TO-EPC2-SGW-INGRESS
[EPC2]26kl-chassis(config-if-eth)# ip mtu 1500 mru 1970
[EPC2]26kl-chassis(config-if-eth)# end
[EPC2]26kl-chassis# show ipv6 interface
Intf Name: TO-EPC1-SGW-INGRESS
Intf Type: Broadcast
Description:
VRF: None
IP State: UP (Bound to 5/20 vlan id 190, 802.1P prior 0, ifIndex 85196802)
Router Advertisement: disabled MTU: 1500 MRU: 1970
IPv6 Link-Local Address: fe80::d272:dcff:fea3:8543/64
IPv6 Global Unicast Address: 2001::1:21/64
L3 monitor LC-port switchover: Disabled
Number of Secondary Addresses: 5
IPv6 Address: 2001::1:31/64
IPv6 Address: 2001::1:205/64
IP Address: 10.10.10.21 Subnet Mask: 255.255.255.0
IP Address: 10.10.10.31 Subnet Mask: 255.255.255.0
IP Address: 10.10.10.200 Subnet Mask: 255.255.255.0
```

注：

- 設定可能な MTU の設定が有効か無効かを確認するには、**show ipv6 interface** コマンドを使用します。
- **no ip mtu**：設定可能な MTU の設定を無効にします。



第 62 章

GTPC を介したメッセージ優先度通知

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （1091 ページ）
- 機能説明 （1092 ページ）
- 機能の仕組み （1094 ページ）
- GTP 機能でのメッセージ優先順位の設定 （1097 ページ）
- モニタリングおよびトラブルシューティング （1099 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC - SI • VPC - DI
機能のデフォルト	無効：ライセンスが必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide*

マニュアルの変更履歴

重要 リリース 21.2 および N5.5 よりも前に導入された機能の改訂履歴の詳細は示していません。

改訂の詳細	リリース
GTP を介したメッセージ優先順位表示機能では、eMPSセッションおよび非eMPSセッションでの、GTPCメッセージおよびGxメッセージの Gx DRMP AVP に対する GTPC MP フラグとメッセージ優先順位の値の設定をサポートします。	21.4
最初の導入。	21.3

機能説明

GTPC メッセージの優先順位や Gx Diameter Routing Message Priority（DRMP）AVP は、メッセージの優先順位を示します。これは、メッセージ全体を開くことなくメッセージの優先順位を決定するという目的に適合します。

GTP 機能を介したメッセージ優先順位表示機能は、GTPC の MP フラグとメッセージの優先順位値の設定をサポートします。MP フラグとメッセージの優先順位値は、eMPS および非 eMPS セッションで GTPC メッセージおよび Gx メッセージの Gx DRMP AVP に設定できます。

GTPC メッセージの優先順位と DRMP AVP は、セッションが Enhanced Multimedia Priority Service（eMPS）であることを示しているわけではありません。

この機能は GTPC メッセージの次の動作をサポートします。

1. eMPS セッションで着信 GTPC メッセージに MP フラグが設定され、メッセージの優先順位が 0 に設定されている場合、このメッセージは GTP Demux 着信スロットリングから除外されます。これは CLI で制御されます。

   eMPS セッションの着信 GTPC メッセージは、負荷の過負荷制御、つまり自己過負荷保護（すでにサポートされている）により、スロットリングから除外されます。

   したがって、eMPS セッションで MP フラグが設定され、メッセージの優先順位が 0 の着信 GTPC メッセージのすべてが、以下から除外されます。

   - Demux 着信スロットリング
   - 負荷/過負荷制御（自己過負荷保護）によるスロットリング

2. GTPC 要求メッセージでは、GTPC MP フラグは「1」に設定され、GTP ヘッダーでは GTPC メッセージの優先順位値は「0」に設定されます。これは、eMPS セッションのネットワーク開始手順（PCRF）またはセッションの eMPS ステータスの切り替えにつながる操作が原因で P-GW が送信するメッセージに適用されます（つまり、eMPS アップグレードまたはダウングレードシナリオ）。これは CLI で制御されます。

3. GTPC 要求メッセージの GTPC MP フラグと GTPC メッセージの優先順位値は、対応する着信「コマンド」メッセージで受信された GTP ヘッダー内のそれぞれの値と同じになるように設定されます。UE がすべてのセッション（eMPS および非 eMPS）で開始した手順

（つまり、着信「コマンド」メッセージ）が原因でトリガーされたときに、P-GW が送信するメッセージがこれに該当します。これは CLI で制御されません。

着信コマンドメッセージについては、次の 2 つのシナリオでの動作に注意してください。

- GTPC 要求メッセージに対してピアから受信した応答に「ハンドオーバー/TAU/RAU 手順が進行中のため一時的に拒否」の理由が付いていた場合、GTPC 要求メッセージの送信を再試行しても、着信コマンドメッセージの GTPC MP フラグと GTPC メッセージの優先順位値は伝送されません。UE が開始した手順（つまり、着信「コマンド」メッセージ）が原因でトリガーされたときに、P-GW が送信するメッセージがこれに該当します。したがって、ポイント番号 2 で説明されている動作は、このようなメッセージに適用されます。
- 着信コマンドメッセージが、ベアラーを作成または更新するベアラーリソースコマンドで、TFT のサイズがベアラー作成要求メッセージや更新要求メッセージで送信可能な最大サイズを超えている場合、2 つの要求メッセージを送信するように求めます。つまり、ベアラー作成要求の後にベアラー更新要求が続くか、ベアラー更新要求の後にベアラー更新要求メッセージが続きます（これは従来の P-GW の動作です）。この場合、最初の要求メッセージは、着信コマンドメッセージの GTPC MP フラグおよび GTPC メッセージの優先順位値とともに送信されます。ただし、2 番目の要求メッセージでは、着信コマンドメッセージの GTPC MP フラグと GTPC メッセージの優先順位値は伝送されません。したがって、ポイント番号 2 で説明されている動作は、このようなメッセージに適用されます。

4. GTPC 応答メッセージ内の GTPC MP フラグと GTPC メッセージの優先順位値は、対応する着信要求メッセージで受信された GTP ヘッダー内のそれぞれの値と同じになるように設定されます。すべてのセッション（eMPS および非 eMPS）で P-GW が送信するメッセージがこれに該当します。これは CLI で制御されません。
5. eMPS セッションまたはセッションの eMPS ステータスの切り替えによる発信 Gx メッセージ（CCR-I/U/T）（つまり、eMPS アップグレードまたはダウングレード シナリオ）の場合、DRMP AVP 値は 0 に設定されます。これは CLI で制御されます。
6. 発信 Gx RAA メッセージは、セッション優先順位付けの CLI 設定に関係なく、PCRF から RAR で送信された DRMP 値と一致します。

GTP を介したメッセージの優先順位表示機能は、次のコマンドを使用して設定できます。

- **emps-profile**：これは既存の CLI コマンドです。
- **message-priority**：これは、この機能をサポートするために導入された新しい CLI コマンドです。
- **gtpc overload-protection ingress**：これは既存の CLI コマンドですが、新しい priority-message キーワードが追加されました。
- **diameter session-prioritization**：これは既存の CLI コマンドですが、この機能をサポートするために動作が変更されています。

diameter session-prioritization CLI コマンドを実行すると、eMPS セッションと eMPS アップグレードおよびダウングレードの Gx クレジット制御要求（Initial、Update、Terminate）メッセージで、DRMP AVP の値が 0 に設定されます。これにより、中間ノードは優先順位の高いメッセージをルーティングできます。エンコーディングは、eMPS 対応セッションおよびセッションの eMPS アップグレードやダウングレード時に適用されます。

diameter session-prioritization CLI コマンドは、最初は eMPS アップグレードやダウングレード トランザクシンの eMPS セッションで Gx メッセージの優先順位付けを制御していました。

diameter session-prioritization CLI コマンドは、eMPS セッションや eMPS アップグレード/ダウングレード トランザクションで、Gx インターフェイスを介してクレジット制御要求（Initial、Update、Terminate）メッセージに 0 の値を設定し、DRMP AVP の送信も制御するようになりました。

（注）

- eMPS プロファイルの設定（eMPS ベアラーまたはセッションとしてベアラーまたはセッションを識別するために使用される eMPS ARP の設定）、および eMPS 統計に関連する補足情報については、『*P-GW Administration Guide*』または『*SAEGW Administration Guide*』の「*VoLTE*/緊急コールの拡張優先順位付け」の章を参照してください。
- eMPS の Gx サポートに関する補足情報については、『*P-GW Administration Guide*』または『*SAEGW Administration Guide*』を参照してください。

重要 この機能はライセンスで制御されています。ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

他の機能との関係

この機能は、eMPS プロファイル、負荷/過負荷制御、Gx RLF スロットリング、および最大未処理設定機能に関連しています。これらの機能のうち、1 つ以上を使用するには、追加のライセンスキーをインストールする必要があります。

機能の仕組み

次の項では、この機能の仕組みを簡潔に紹介します。

GTP 着信スロットリングのバイパス

GTP 着信スロットリングのバイパスは、P-GW 入力インターフェイスのデマルチプレクサマネージャ（egtpinmgr）に到達する着信 GTPC 要求メッセージに適用できます。

- **高優先度メッセージ**：P-GW 入力インターフェイスで「MP」フラグが設定され、「Message Priority」値が 0 に設定された着信 GTPC メッセージ。
- **高優先度 CSReq メッセージ**： P-GW 入力インターフェイスで「MP」フラグが設定され、「Message Priority」値が 0 に設定された着信 CSReq メッセージ。
- **優先度の低いメッセージ**： MP フラグのないその他のすべての着信 GTPC メッセージ。

新しい **exclude priority-message** CLI キーワードが設定されている場合、次の動作が適用され、優先順位の高いメッセージの着信スロットリングがバイパスされます。

- 優先順位の高いメッセージでは、デマルチプレクサの「msg-rate」と「queue-size」のデフォルト設定が適用されます（異なる値で設定されている場合でも）。「msg-rate」のデフォルト値は 0 であり、これは高優先度の設定が無効になっていることを意味します。「queue-size」のデフォルト値は 10000 です。
- 優先度の高いメッセージの「delay-tolerance」パラメータにより、スロットリングは適用されません。
- また、優先度の高いセッション作成要求（CSReq）メッセージは、他のメッセージよりも優先されます。ただし、優先度の高い CSReq メッセージは順番に処理されます。
- 高優先度メッセージが受信され、キューが過負荷になると、高優先度メッセージを収容するために低優先度メッセージがキューから破棄されます。
- キュー内のすべてのメッセージが高優先度であり、キューが過負荷になっているまれなシナリオでは、新しい高優先度のメッセージがドロップされることがあります。
- 「gtpc overload-protection ingress」と「exclude priority-message」オプションを使用して、入力スロットリングが設定されている場合、デマルチプレクサ メッセージ キューサイズに基づく P-GW、S-GW、GGSN、および SAEGW Demux マネージャの輻輳制御計算において、デフォルトのキューサイズ値 10,000 が使用されます。（これは、**exclude sgw-interface** が選択されている場合と同じ動作です）。
- 入力スロットリングが「exclude」オプションなしで「gtpc overload-protection ingress」を使用して設定されている場合、デマルチプレクサ メッセージ キューサイズに基づく P-GW、S-GW、GGSN、および SAEGW Demux マネージャの輻輳制御計算では、設定された queue-size 値が使用されます。

  次の表では、**exclude priority-message** が設定されている場合の動作について説明します。

GTPC 着信スロットリング デマルチプレクサ キューサイズの設定（100 ～ 10000）	「exclude priority-message」が設定されているかどうか	S-GW/GGSN/「低優先度」P-GW メッセージの GTPC 着信スロットリングに使用されるデマルチプレクサ キューサイズ	「高優先度メッセージ」P-GW メッセージに使用されるデマルチプレクサ キューサイズ	P-GW/GGSN/S-GW の輻輳制御しきい値で考慮されるキューサイズ
設定なし/デフォルト設定	非対応	10000（デフォルト）	10000（デフォルト）	Configured_congestion_threshold * 10000（デフォルト）
設定なし/デフォルト設定	はい	10000（デフォルト）	10000（デフォルト）	Configured_congestion_threshold * 10000（デフォルト）
5000（または 100 ～ 10000 の任意の設定値）	非対応	5000（または設定値）	5000（または設定値）	Configured_congestion_threshold * 5000（デフォルト）
5000（または 100 ～ 10000 の任意の設定値）	はい	5000（または設定値）	10000（「exclude priority-message」が設定されているため）	Configured_congestion_threshold * 10000（「exclude priority-message」が設定された場合の輻輳制御の動作変更）

Gx DRMP AVP エンコード

ポリシー制御アプリケーションの IMS 承認ポリシー制御設定モードで **diameter session-prioritization** CLI が有効になっている場合、Gx DRMP AVP がエンコードされます。次の表では、さまざまな設定およびシナリオに基づいて送信される DRMP AVP 値の概要を示します。

session prioritization CLI	セッションの eMPS ステータス	シナリオ	DRMP エンコーディング/値
消灯	いずれか	CCR メッセージ	エンコードされない
任意	任意	DRMP による RAR への RAA 応答 X	エンコードされる/X
消灯	eMPS	CCR メッセージ	エンコードされない
点灯	はい	CCR メッセージ	エンコードされない

session prioritization CLI	セッションの eMPS ステータス	シナリオ	DRMP エンコーディング/値
点灯	eMPS	CCR メッセージ	エンコードされる/0
点灯	非 eMPS	eMPS の状態が無効から有効に変更されたときに CCR-U が生成される。	エンコードされる/0
点灯	eMPS	eMPS の状態が有効から無効に変更されたときに CCR-U が生成される。	エンコードされる/0
点灯	非 eMPS	eMPS のアップグレードに失敗し、CCR-U が続く	エンコードされる/0

GTP 機能でのメッセージ優先順位の設定

次の項では、この機能を有効または無効にするための設定コマンドについて説明します。

emps-profile

eMPS プロファイル コンフィギュレーション モードの場合に、emps-profile コマンドで eMPS プロファイルがサポートされるようになりました。これにより、ベアラーまたはセッションを eMPS ベアラーまたはセッションとして識別またはマークできるようになりました。

eMPS プロファイルを設定するには、次のコマンドを入力します。

```
configure
 emps-profile  emps_profile_name
  earp earp_value earp_value
  end
```

（注） eMPS プロファイルの設定（eMPS ベアラーまたはセッションとしてベアラーまたはセッションを識別するために使用される eMPS ARP の設定）、および eMPS 統計に関連する補足情報については、『*P-GW Administration Guide*』または『*SAEGW Administration Guide*』の「*VoLTE*/緊急コールの拡張優先順位付け」の章を参照してください。

優先順位メッセージ

gtpc overload-protection ingress CLI コマンドは、新しいキーワード **priority-message** を追加して提供されるようになりました。このキーワードを使用すると、着信GTPC要求メッセージのGTP ヘッダーで「MP」フラグが 1 に設定され、メッセージの優先順位値が 0 に設定され、Demux 着信スロットリングをバイパスできるようになります。

メッセージの優先順位を有効にするには、次のコマンドを入力します。

```
configure
 context context_name
  gtpc overload-protection ingress { msg-rate msg_rate  }  delay-tolerance
 dur ] [ queue-size size ] [ exclude { sgw-interface [ priority-message
 ] } | { priority-message [ sgw-interface ] } ]
  end
```

注：

priority-message：GTPC 着信メッセージの GTP ヘッダーにメッセージの優先順位フラグが設定され、メッセーの優先順位値が 0 に設定されるため、P-GW 入力インターフェイスで着信スロットリングをバイパスします。このキーワードが設定されている場合、P-GW、S-GW、および GGSN の輻輳制御機能で考慮されるメッセージキューは、デフォルト値の 10,000 にリセットされます。

デフォルトでは、この CLI は無効になっています。

priority-message キーワードは、P-GW にのみ適用されます。

メッセージの優先度

この新しいコマンドでは、GTPC ヘッダーの GTPC MP フラグを「1」に設定し、 GTPC メッセージの優先度を「0」に設定できます。これは、eMPS セッションのネットワーク開始手順（PCRF）またはセッションの eMPS ステータスの切り替えにつながる操作（つまり、eMPS アップグレードまたはダウングレードシナリオ）が原因で P-GW が送信する GTPC 要求メッセージに適用されます。

メッセージ優先度を有効にするには、次のコマンドを入力します。

```
configure
 emps-profile profile_name
  [ no ]  message-priority
  end
```

注：

- **no**：コマンドをディセーブルにします。
- **message-priority**：次のいずれかのシナリオで、ネットワーク開始手順（PCRF）によりトリガーされて P-GW によって送信されたすべての要求メッセージの GTPC ヘッダーで MP フラグを 1 に、メッセージ優先順位の値を 0 に設定します。
  - eMPS セッション

- eMPS セッションへの 非 eMPS セッション
- 非 eMPS セッションへの eMPS セッション

• デフォルトでは、この CLI は無効になっています。

diameter session-prioritization

IMS 承認サービス コンフィギュレーション モードでは、**diameter session-prioritization** CLI コマンドが拡張され、これを実行すると、eMPS セッションと eMPS アップグレードおよびダウングレードの Gx クレジット制御要求（Initial、Update、Terminate）メッセージで、DRMP AVP の値が 0 に設定されます。これにより、中間ノードは優先順位の高いメッセージをルーティングできます。エンコーディングは、eMPS 対応セッションおよびセッションの eMPS アップグレードやダウングレード時に適用されます。また、eMPS セッションと eMPS アップグレードおよびダウングレードに関する Gx メッセージの優先順位付けの既存動作は続行されます。

CCR メッセージの DRMP AVP 値を設定するには、次のコマンドを入力します。

```
context context_name
 ims-auth-service service_name
  policy control
   [ no ] diameter session-prioritization
   end
```

注：

- **no**：eMPS セッションと eMPS アップグレードおよびダウングレードに関する Gx メッセージの優先順位付けを無効にします。また、eMPS セッションと eMPS アップグレードおよびダウングレードに関するクレジット制御要求（初期、更新、および終了）メッセージに含まれる DRMP AVP（値 0）のエンコーディングも無効になります。
- **session-prioritization**：eMPS セッションのクレジット制御要求メッセージに関して、DRMP AVP 値を優先順位付けし、0 に設定します。
- デフォルトでは、この CLI は無効になっています。

モニタリングおよびトラブルシューティング

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show コマンドと出力

この機能をサポートするために、以下の CLI コマンドの出力が拡張されています。

show emps-profile

show emps-profile name *name* および show emps-profile all CLI コマンドの出力に、この機能をサポートする message-priority フィールドが追加されました。

「message-priority」が設定されていない、または「no message-priority」が設定されている場合：show emps-profile name

```
show emps-profile name abcd
eMPS Profiles
---------------------------------
  eMPS Profile Name : abcd
  earp configured : None
  dscp-marking configured : None
  message-priority : Disabled
```

「message-priority」が設定されていない、または「no message-priority」が設定されている場合：show emps-profile name all

```
show emps-profile name all
eMPS Profiles
---------------------------------
  eMPS Profile Name : xyz
  earp configured :  2 3
  dscp-marking configured : None
  message-priority : Disabled
```

「message-priority」が設定されている場合：show emps-profile name

```
show emps-profile name abcd
eMPS Profiles
---------------------------------
  eMPS Profile Name : abcd
  earp configured : None
  dscp-marking configured : None
  message-priority : 0
```

「message-priority」が設定されている場合：show emps-profile name all

```
show emps-profile name all
eMPS Profiles
---------------------------------
  eMPS Profile Name : xyz
  earp configured :  2 3
  dscp-marking configured : None
  message-priority : 0
```

show pgw-service

show pgw-service name *name* および show pgw-service all CLI コマンドの出力に、この機能をサポートするプライオリティメッセージ拡張フィールドが追加されました。

デフォルト設定：show pgw-service name

```
show pgw-service name pgw_service
  Service name                  : pgw_service
  Service-Id                    : 4
  Context                       : ingress
  Status                        : STARTED
  EGTP Service                  : egtp_service
  LMA Service                   : Not defined
  GGSN Service                  : ggsn-service
```

```
  IPNE Service                  : Not defined
  Peer Map                      : Not defined
  Session-Delete-Delay Timer    : Disabled
  Session-Delete-Delay Timeout  : n/a
  PLMN ID List                  : Not defined
  Newcall Policy                : None
  dns-client Context Name       : ingress
  gx-li context                 : ingress
  gx-li transport               : udp
  Internal QOS Application      : Backward-compatible
  QCI-QOS Mapping Table Name    : n/a
  Authorize                     : Disabled
  Setup Timeout                 : 60(secs)
  Message Timestamp Drift       : 180(secs)
  .
  .
  .
  GTPC Incoming Throttling Params: Configured
  Message Rate (per sec):          100
  Delay Tolerance (secs):          2
  Queue Size:                      300
  SGW interface Excluded:          Yes
  Priority message Excluded:       No

  Queue size for Congestion Control : 10000
```

デフォルト設定：**show pgw-service all**

```
show pgw-service all
  Service name                  : pgw_service
  Service-Id                    : 4
  Context                       : ingress
  Status                        : STARTED
  EGTP Service                  : egtp_service
  LMA Service                   : Not defined
  GGSN Service                  : ggsn-service
  IPNE Service                  : Not defined
  Peer Map                      : Not defined
  Session-Delete-Delay Timer    : Disabled
  Session-Delete-Delay Timeout  : n/a
  PLMN ID List                  : Not defined
  Newcall Policy                : None
  dns-client Context Name       : ingress
  gx-li context                 : ingress
  gx-li transport               : udp
  Internal QOS Application      : Backward-compatible
  QCI-QOS Mapping Table Name    : n/a
  Authorize                     : Disabled
  Setup Timeout                 : 60(secs)
  Message Timestamp Drift       : 180(secs)
  .
  .
  .
  GTPC Outgoing Throttling:        Disabled
  RLF Template Name:               N/A
  Throttling override:             Disabled
  Throttling override Policy:      N/A

  GTPC Incoming Throttling Params: Configured
  Message Rate (per sec):          100
  Delay Tolerance (secs):          2
  Queue Size:                      300
  SGW interface Excluded:          Yes
 Priority message Excluded:       No
```

```
  Queue size for Congestion Control : 10000
```

「exclude priority-message」が設定されている場合：show pgw-service name

```
show pgw-service name pgw_service
  Service name                  : pgw_service
  Service-Id                    : 4
  Context                       : ingress
  Status                        : STARTED
  EGTP Service                  : egtp_service
  LMA Service                   : Not defined
  GGSN Service                  : ggsn-service
  IPNE Service                  : Not defined
  Peer Map                      : Not defined
  Session-Delete-Delay Timer    : Disabled
  Session-Delete-Delay Timeout  : n/a
  PLMN ID List                  : Not defined
  Newcall Policy                : None
  dns-client Context Name       : ingress
  gx-li context                 : ingress
  gx-li transport               : udp
  Internal QOS Application      : Backward-compatible
  QCI-QOS Mapping Table Name    : n/a
  Authorize                     : Disabled
  Setup Timeout                 : 60(secs)
  Message Timestamp Drift       : 180(secs)
  .
  .
  .
  GTPC Incoming Throttling Params: Configured
  Message Rate (per sec):          100
  Delay Tolerance (secs):          2
  Queue Size:                      300
  SGW interface Excluded:          Yes
  Priority message Excluded:       Yes

  Queue size for Congestion Control : 10000
```

「exclude priority-message」が設定されている場合：show pgw-service all

```
show pgw-service all
  Service name                  : pgw_service
  Service-Id                    : 4
  Context                       : ingress
  Status                        : STARTED
  EGTP Service                  : egtp_service
  LMA Service                   : Not defined
  GGSN Service                  : ggsn-service
  IPNE Service                  : Not defined
  Peer Map                      : Not defined
  Session-Delete-Delay Timer    : Disabled
  Session-Delete-Delay Timeout  : n/a
  PLMN ID List                  : Not defined
  Newcall Policy                : None
  dns-client Context Name       : ingress
  gx-li context                 : ingress
  gx-li transport               : udp
  Internal QOS Application      : Backward-compatible
  QCI-QOS Mapping Table Name    : n/a
  Authorize                     : Disabled
  Setup Timeout                 : 60(secs)
  Message Timestamp Drift       : 180(secs)
  .
  .
```

```
.
GTPC Outgoing Throttling:        Disabled
RLF Template Name:               N/A
Throttling override:             Disabled
Throttling override Policy:      N/A

GTPC Incoming Throttling Params: Configured
Message Rate (per sec):          100
Delay Tolerance (secs):          2
Queue Size:                      300
SGW interface Excluded:          Yes
Priority message Excluded:       Yes
Queue size for Congestion Control : 10000
```



第 63 章

モバイル IP の登録失効

この章では、モバイル IP およびプロキシモバイル IP の登録失効について説明し、その設定方法について説明します。製品アドミニストレーション ガイドには、システム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、本アドミニストレーション ガイドの説明に従って、ご使用のサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

重要 このライセンスは、デフォルトで有効になっています。ただし、すべての機能がすべてのプラットフォームでサポートされているわけではなく、この章で説明するように、すべての機能を使用するには他のライセンスが必要になる場合があります。

この章では、次の事項について説明します。

- 概要 （1105 ページ）
- 登録失効の設定 （1107 ページ）

概要

登録失効は、同じモバイルノードにモバイル IP 機能を提供している HA または FA のいずれかが、バインドの終了を他のモビリティエージェントに通知できる一般的なメカニズムです。この機能には次の利点があります。

- FA や HA でのモバイル IP リソースのタイムリーなリリース
- 正確なアカウンティング
- モバイルノードへのサービス変更のタイムリーな通知

モバイル IP の登録失効は、次のいずれかによって FA でトリガーできます。

- 何らかの理由でモバイルノードでセッションが終了した
- セッションの再ネゴシエーション
- コールの管理クリア

- セッション マネージャ ソフトウェアのタスク停止による FA セッションの喪失（回復できなかったセッション）



重要 登録失効機能は、プロキシモバイル IP でもサポートされています。ただし、プロキシ MIP コールの失効を開始できるのは HA のみです。

モバイル IP 登録失効は、次のいずれかによって HA でトリガーできます。

- コールの管理クリア
- アクセスゲートウェイ間のハンドオフ。これにより、以前のアクセスゲートウェイまたは FA のバインディングが解放されます。
- セッション マネージャ ソフトウェアのタスク停止による FA セッションの喪失（回復できなかったセッションの場合）
- セッションアイドルタイマーの期限切れ（失効を送信するように設定されている場合）
- ローカルポリシーが原因でバインディングが終了するその他の条件（重複 IMSI の検出、重複するホームアドレスの要求など）。

FA と HA は、モバイル IP コールの確立時に登録失効のサポートをネゴシエートします。失効のサポートは、エージェントアドバタイズメントの「X」ビットを MN に設定することで、FA からモバイルノード（MN）に通知されます。ただし、MN はコールの失効のネゴシエーションや失効プロセスには関与しません。通知を受け取るだけです。エージェントアドバタイズメントの X ビットは、FA で失効がサポートされていることを MN に知らせるだけで、HA とネゴシエートできることを保証するものではありません。

FA で失効が有効になっていて、FA-HA SPI が設定されている場合、MN から受信され FA-HA 認証拡張によって保護される RRQ に、失効サポート拡張が付加されます。HA で RRQ が受け入れられ、HA が失効をサポートしている場合、HA は失効サポート拡張を含む RRP で応答します。失効サポートは、正常な登録交換中に両側で失効サポート拡張が含まれている場合に、バインドに対してネゴシエートされたと見なされます。



重要 RRQ または RRP の失効サポート拡張は、FA-HA 認証拡張で保護する必要があります。したがって、これを成功させるには、FA と HA で FA-HA SPI を設定する必要があります。

FA で失効が有効になっているが、特定の HA に対して FA-HA SPI が FA で設定されていない場合、FA はコールの失効サポート拡張をその HA に送信しません。したがって、失効サポートがネゴシエートされずにコールが発生する可能性があります。

HA が失効サポート拡張を持つ RRQ を受信しても、FA-HA 認証拡張で保護されていない場合、「FA 認証の失敗」エラーで拒否されます。

FA が失効サポート拡張を持つ RRP を受信しても、FA-HA 認証拡張で保護されていない場合、「HA 認証の失敗」エラーで拒否されます。

また、初期、更新、またはハンドオフ RRQ および RRP メッセージにも失効サポート拡張が含まれていることに注意してください。失効拡張は FA からの登録解除 RRQ には含まれておらず、HA は受信した登録解除 RRQ でこれらを無視します。

登録失効の設定

MIP の登録失効をサポートするには、次の設定が必要です。

- **FA サービス**：登録失効を有効にし、必要に応じて動作パラメータを設定する必要があります。
- **HA サービス**：登録失効を有効にし、必要に応じて動作パラメータを設定する必要があります。



重要 これらの説明は、それぞれの製品のアドミニストレーション ガイドに記載されている手順に従って、FA や HA を備えたコアネットワークサービスのサブスクライバ データ セッションをサポートするようシステムがあらかじめ設定されていることを前提としています。



重要 この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンドや、キーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

FA サービスの設定

次の設定例を適用して、MIP 登録失効をサポートするように FA サービスを設定します。

```
configure
   context <context_name>
      fa-service <fa_service_name>
         revocation enable
         revocation max-retransmission <number>
         revocation retransmission-timeout <time>
         end
```

Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

HA サービスの設定

次の設定例を適用して、MIP 登録失効をサポートするように HA サービスを設定します。

```
configure
   context <context_name>
      ha-service <ha_service_name>
         revocation enable
         revocation max-retransmission <number>
         revocation retransmission-timeout <time>
         end
```

EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。



第 64 章

RADIUSアカウンティングでのモバイルホットスポットの使用

- 機能の概要と変更履歴 （1109 ページ）
- 機能説明 （1110 ページ）
- RADIUS アカウンティングにおける MHS の使用の設定 （1111 ページ）
- モニタリングおよびトラブルシューティング （1112 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ICUPS • VPC-DI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*P-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、P-GW は RADIUS アカウンティングでのモビリティホットスポット（MHS）の使用をサポートしています。	21.23

機能説明

RADIUS アカウンティングでは、サブスクライバのデータ使用量は、タイプ、長さ、値（TLV）、つまり Acct-Input-Octets と Acct-Output-Octets を使用して監視され、累積データ使用状況レポートを受け取ります。この StarOS 21.23 リリースでは、RADIUS アカウンティングにおける、4G モバイルホットスポット（MHS）データ使用量、5G MHS データ使用量、および 5G コンポジットデータ使用量の差異を効果的に把握するために、次の新しい TLV が導入されました。

- 4G_MHS_Acct_Input_Octets
- 4G_MHS_Acct_Output_Octets
- 5G_MHS_Acct_Input_Octets
- 5G_MHS_Acct_Output_Octets
- 5G_Comp_Acct_Input_Octets
- 5G_Comp_Acct_Output_Octets

RADIUS 中間メッセージおよび終了メッセージにより、MHS データ使用量が報告されます。MHS データ使用状況レポートは、ベアラーごとに使用できます。これらの TLV は、以前の中間メッセージと raw バイトからの累積値で構成されます。

MHS データ使用状況レポートを有効または無効にすると、この変更は新しいコールに対してのみ有効になります。

（注） MHS データ使用状況レポートでは、EUTRAN タイプおよび NB_IOT 無線アクセス技術（RAT）タイプのみがサポートされています。

APN レベルに関連付けられている PRA プロファイルに設定されている PRA ID は、5G データ使用量を識別するために使用されます。

他の機能との関係性

この機能は、スマートフォンのテザリング検出サポート機能に関連しています。スマートフォンのテザリング検出サポート機能の詳細については、『*P-GW Administration Guide*』の「*PDN Gateway Overview*」の章 [英語] を参照してください。

ライセンス要件

RADIUS アカウンティング機能でモバイルホットスポットを使用するには、テザリング検出ライセンスを有効にする必要があります。特定のライセンス要件の詳細については、アカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『*System*

Administration Guide』の「*Software Management Operations*」の「*Managing License Keys*」のセクション [英語] を参照してください。

制限事項

機能の既知の制限事項を次に示します。

- MHS は、custom76 ディクショナリのみをサポートします。

RADIUS アカウンティングにおける MHS の使用の設定

ここでは、RADIUS アカウンティングにおける MHS の使用の設定について説明します。

PRA プロファイルの設定

トラフィックを区別するように PRA プロファイルを設定するには、次のコマンドを使用します。

```
configure
          context context_name
            pra-profile pra_profile_name
             [ no ] pra-id pra_id_value traffic-map-type type_value
          end
```

注：

- **pra-profile**：トラフィックを区別するように PRA プロファイルを設定します。
- **pra-id**：PRA ID を設定します。
- **no**：PRA ID を削除します。
- **traffic-map-type**：トラフィックマップタイプを設定します。
- **type_value**：ENUM 値（5G）を入力します。

注：

5G トラフィックを区別するために、APN レベルの PRA リストおよび関連する PRA リストごとに最大 3 つの PRA ID が許可されます。

APN レベルでの PRA プロファイルの関連付け

APN レベルで PRA プロファイルを関連付けるには、次の CLI コマンドを使用します。

```
configure
  context context_name
    apn apn_name
```

```
    [ no ] pra-profile profile_value
exit
```

注：

- **apn**：APN を設定します。
- **pra-profile**：APN レベルで PRA プロファイルを関連付けます。
- **no**：APN レベルで PRA プロファイルを削除します。

AAA グループの設定

次のコマンドを使用して、新しく追加された TLV が RADIUS アカウンティングメッセージを送信するように AAA グループを設定します。

```
configure
        context context_name
          aaa group group_name
            [ no ] radius accounting mhs-traffic enable
            radius dictionary custom76
        end
```

注：

- **mhs-traffic**：MHS データ使用量レポートを指定します。
- **enable**：MHS データ使用量レポートを有効にします。
- **no**：MHS データ使用量レポートを無効にします。

モニタリングおよびトラブルシューティング

ここでは、この機能をサポートするために使用できる show コマンドによるモニタリングとトラブルシューティングの方法について説明します。

show コマンドと出力

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show subscribers pgw-only full all

show subscribers pgw-only full all コマンドの出力には、次の情報が表示されます。

フィールド	説明
4G MHS Input Bytes	4G テザリングで使用された入力バイトの総数。
4G MHS Output Bytes	4G テザリングで使用された出力バイトの総数。

フィールド	説明
5G MHS Input Bytes	5G テザリングで使用された入力バイトの総数。
5G MHS Output Bytes	5G テザリングで使用された出力バイトの総数。
5G Composite Input Bytes	5G コンポジット（テザリングおよび非テザリング）で使用された入力バイトの総数。
5G Composite Output Bytes	5G コンポジット（テザリングおよび非テザリング）で使用された出力バイトの総数。

show subscribers saegw-only full all

show subscribers saegw-only full all コマンドの出力には、次の情報が表示されます。

フィールド	説明
4G MHS Input Bytes	4G テザリングで使用された入力バイトの総数。
4G MHS Output Bytes	4G テザリングで使用された出力バイトの総数。
5G MHS Input Bytes	5G テザリングで使用された入力バイトの総数。
5G MHS Output Bytes	5G テザリングで使用された出力バイトの総数。
5G Composite Input Bytes	5G コンポジット（テザリングおよび非テザリング）で使用された入力バイトの総数。
5G Composite Output Bytes	5G コンポジット（テザリングおよび非テザリング）で使用された出力バイトの総数。

show apn name

show apn name コマンドの出力では、次の詳細情報が表示されます。

フィールド	説明
pra-profile Name	5G トラフィックを区別するために APN で関連付ける PRA 名を示します。

show aaa group name

show aaa group name コマンドの出力では、次の詳細情報が表示されます。

フィールド	説明
Allow accounting MHS Traffic	RADIUS アカウンティングメッセージでの MHS データ使用量のレポートを有効にします。

show pra-profile name

show pra-profile name コマンドの出力には、次の情報が表示されます。

フィールド	説明
pra profile name	5G トラフィックを区別するために APN で関連付ける PRA プロファイル名。
Context	コンテキストの名前。
PRA Id	APN に関連付けられる PRA ID。
Traffic mapping type	5G トラフィックマップのタイプ。

show pra-profile all

show pra-profile all コマンドの出力には、次の情報が表示されます。

フィールド	説明
pra profile name	5G トラフィックを区別するために APN で関連付ける PRA プロファイル名。
Context	コンテキストの名前。
PRA ID	APN に関連付けられる PRA ID。
Traffic mapping type	5G トラフィックマップのタイプ。



第 65 章

マルチプロトコル ラベル スイッチング（MPLS）のサポート

この章では、BGP/MPLS VPN のシステムサポートについて説明し、その設定方法を示します。製品アドミニストレーション ガイドには、特定のシステム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、それぞれの製品のアドミニストレーション ガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

機能ライセンスキーを介して有効にすると、システムはMPLS をサポートし、システムから企業のネットワークに VPN 接続を提供します。

重要 このリリースでは、直接接続された PE ルータに対してのみ BGP/MPLS VPN が提供されます。

MP-BGP はルートをネゴシエートし、VPN のトラフィックを分離するために使用されます。ネットワークノードは接続されたプロバイダーエッジ（PE）から VPN ルートを学習し、PE はネットワーク機能によって提供されるルートをルーティングテーブルに入力します。

- 概要 （1115 ページ）
- サポートされる標準 （1118 ページ）
- サポート対象のネットワークとプラットフォーム （1118 ページ）
- ライセンス （1118 ページ）
- 利点 （1119 ページ）
- スタティックラベルを使用した BGP/MPLS VPN の設定 （1119 ページ）
- ダイナミックラベルを使用した BGP/MPLS VPN の設定 （1122 ページ）

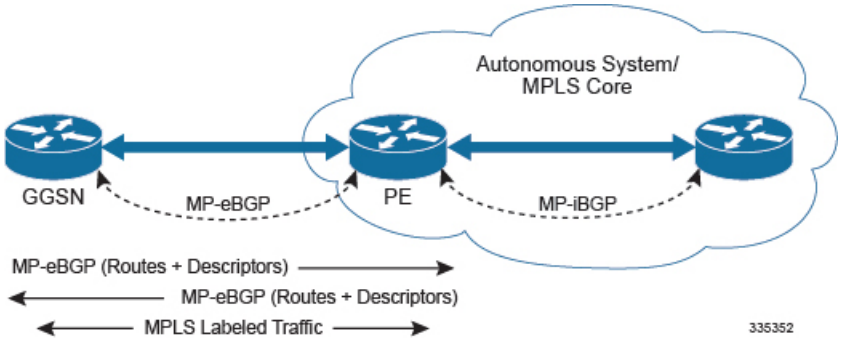
概要

次のシナリオに示すように、ネットワークで BGP/MPLS-VPN をサポートしながら、シャーシをルータとして展開できます。

- プロバイダーエッジ（PE）に接続する MPLS カスタマーエッジ（MPLS-CE）としてのシャーシ
- 自律システム境界ルータ（ASBR）に接続する MPLS カスタマーエッジ（MPLS-CE）としてのシャーシ

PE に接続する MPLS-CE としてのシャーシ

図 *96 : PE* に接続する *MPLS-CE* としてのシャーシ



このシナリオのシステムは、入力トラフィックと出力トラフィックに静的または動的な MPLS ラベルを使用します。静的ラベルの設定情報については「スタティックラベルを使用した BGP/MPLS VPN の設定（1119 ページ）」のセクションを、動的ラベルの設定については「スタティックラベルを使用した BGP/MPLS VPN の設定（1119 ページ）」を参照してください。

システムは、プロバイダーエッジ（PE）とは別の自律システム（AS）内にあります。システムは PE と通信し、すべての VPN ルートが MP-BGP を介して交換されます。異なる VPN に属するルートは、別々の Virtual Route Forwarding（VRF）テーブルを使用して論理的に分離されます。

各 VPN のルートは VPN-IPv4 ルートとしてアドバタイズされます。VPN-IPv4 ルートでは、ルーティングテーブル内で一意になるように、Route Distinguisher が通常の IPv4 ルートの前に付加されます。BGP 拡張コミュニティ属性に追加されるルートターゲットによって、異なる VPN アドレス空間が識別されます。ダウンストリームピアによって適切な VRF にルートがインポートされる、特定のアップストリーム BGP ピアルーティングドメイン（VPN）は、アドバタイズされた NLRI の拡張コミュニティで識別されます。

すべての VPN ルートに対して一意のラベルも受信またはアドバタイズされます。

カスタマーエッジ（CE）も、NLRI を使用して、PE にルートをアドバタイズします。NLRI には、VPN を区別するルート識別子、VRF を識別するための拡張コミュニティ、および後でデータトラフィックの転送に使用される MPLS ラベルが含まれます。

CE と PE の間には 1 つの MPLS 対応リンクがあります。MP-BGP は、IP を介した TCP セッションとしてこのリンクを使用して通信します。データパケットは、MPLS カプセル化パケットとして双方向に送信されます。

このソリューションでは、MPLS プロトコルは使用されません。即時のアップストリームネイバーに対応する MPLS ラベルは、ダウンストリームルータで静的に設定でき、同様に逆方向にも設定できます。

アップストリーム方向のサブスクライバパケットを PE に転送する場合、CE は、アップストリーム VRF（NLRI で送信されるラベル）と直近のネクストホップを識別する MPLS ヘッダーを使用して、パケットをカプセル化します。PE は、パケットを受信すると、ラベルをスワップして転送します。

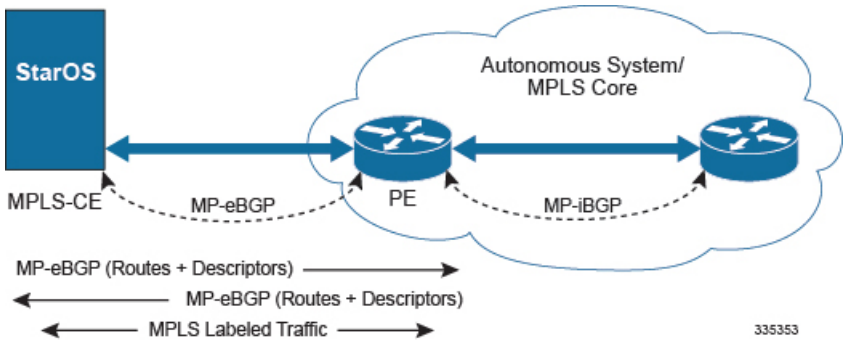
CE では、MPLS プロトコル（LDP または RSVP-TE）は実行されません。

PE からダウンストリーム方向でデータパケットを受信すると、宛先 VRF を識別するためにラベルがチェックされます。次に、パケットが IP パケットへとカプセル化解除され、処理のためにセッションサブシステムに送信されます。

重要 MPLS ping/トレース ルート デバッグ ファシリティはサポートされません。

ASBR に接続された MPLS-CE としてのシャーシ

図 *97 : ASBR* に接続された *MPLS-CE* としてのシャーシ



このシナリオのシステムは、入力トラフィックと出力トラフィックに静的または動的な MPLS ラベルを使用します。静的ラベルの設定情報については スタティックラベルを使用した BGP/MPLS VPN の設定 （1119 ページ） を、動的ラベルの設定については ダイナミックラベルを使用した BGP/MPLS VPN の設定 （1122 ページ） を参照してください。

このシナリオでは、MPLS-CE 機能は変わりませんが、ピア機能に関しては PE を使用する MPLS-CE のシナリオとは異なります。PE を使用する MPLS-CE のシナリオと同様、MPLS-CE システムはさまざまな VRF で VRF ルートを維持し、MP-eBGP セッションを介してルート情報をピアと交換します。

このシナリオのピアは PE ルータではなく、自律システム境界ルータ（ASBR）です。ASBR は、VRF の設定を維持する必要はありません。PE ルータは、IBGP を使用して、ラベル付き VPN-IPv4 ルートを ASBR、または ASBR がクライアントになっているルート リフレクタに再配布します。その後、ASBR は eBGP を使用して、それらのラベル付き VPN-IPv4 ルートを別の AS の MPLS-CE に再配布します。eBGP 接続であるため、ASBR はネクストホップを変更

し、iBGP ピアから学習したルートにラベルを付けてから、MPLS-CE にアドバタイズします。MPLS-CE は eBGP ピアリングに直接接続されており、MP-eBGP のみを使用してルートをアドバタイズおよび学習します。MPLS-CE は、ASBR との間で単一のラベルをプッシュまたはポップします。このラベルは MP-eBGP 接続を介して学習されます。このシナリオでは、MPLS-CE で設定済みの、PE での VRF の設定をしなくて済みます。

エンジニアリングルール

- BGP プロセスごとに複数の VRF にまたがる最大 5,000 の「ホスト ルート」。シャーシあたり 6,000 のプールルートに制限されています。
- シャーシあたり最大 2,048 の VRF。

サポートされる標準

このインターフェイスサポートに伴い、次の標準規格および Requests for Comments（RFC）のサポートが追加されました。

- RFC 4364, BGP/MPLS IP VPNs
- RFC 3032, MPLS Label Stack Encoding



重要 上記の IETF の 1 つ以上のセクションで、この機能が部分的にサポートされています。準拠表明に関する詳細については、シスコのアカウント担当者にお問い合わせください。

サポート対象のネットワークとプラットフォーム

この機能は、StarOS リリース 9.0 以降をネットワーク機能サービスと同時に実行しているすべての ASR 5500 プラットフォームをサポートしています。

ライセンス

マルチプロトコル ラベル スイッチング（MPLS）は、ライセンス供与されたシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

利点

MPLS は、アプリケーションを管理し、ロケーション間で情報を移動するためのより効率的な方法をネットワークに提供します。MPLS はネットワークトラフィックに優先順位を付けるため、管理者は、他のアプリケーションより優先してネットワーク上で情報を移動する必要があるアプリケーションを指定できます。

スタティックラベルを使用した BGP/MPLS VPN の設定

ここでは、システムを MPLS-CE として設定し、スタティック MPLS ラベル機能を使用して PE と対話するために必要な手順について説明します。

以下で説明する設定手順を試す前に、本ガイドの「ルーティング」の章に記載されている基本設定を完了する必要があります。

重要 この章で説明されている機能は、ライセンス供与されたシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

重要 この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンドや、キーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

BGP/MPLS VPN に対応するようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 ルータで VRF を作成し、VRF 名を割り当てます。ルートターゲットを実行する前に、まずルート識別子を定義します。設定の詳細については、「route-distinguisher と route-target を使用した VRF の作成（1120 ページ）」の項を参照してください。

ステップ 2 「ネイバーの設定と VPNv4 ルート交換の有効化（1120 ページ）」の設定例を適用して、ルーティング情報を交換し、ピアルータとの BGP ピアリング接続を確立するようにネイバーとアドレスファミリを設定します。

ステップ 3 「アドレスファミリと接続済みルート再配布の設定（1120 ページ）」の設定例を適用して、アドレスファミリを設定し、接続されたルートドメインを BGP に再配布します。これにより、別のプロトコルからルートを取得し、BGP プロトコルを使用して BGP ネイバーにルートを再配布することができます。

ステップ 4 「MPLS ラベルを使用した IP プールの設定（1121 ページ）」の設定例を適用して、入出力用の MPLS ラベルを使用して IP プールを設定します。

ステップ 5 オプションです。「社内サーバー向けの DHCP サービスのバインド（1121 ページ）」の設定例を適用し、企業ネットワークの入出力で MPLS ラベルと連携するように DHCP サービスをバインドします。

ステップ 6 オプションです。「社内サーバー向けの AAA グループのバインド（1122 ページ）」の設定例を適用し、入出力で MPLS ラベルと連携するように企業ネットワークの AAA/RADIUS サーバーグループをバインドします。

ステップ 7 『*System Administration Guide*』[英語] の説明に従って、設定を保存します。

route-distinguisher と route-target を使用した VRF の作成

次の例を使用して、まずルータで VRF を作成し、VRF 名を割り当てます。2 番目の **ip vrf** コマンドにより、ルート識別子とルートターゲットを作成します。

```
configure
  context <context_name> -noconfirm
    ip vrf <vrf_name>
      router bgp <as_number>
        ip vrf <vrf_name>
          route-distinguisher {<as_value> | <ip_address>} <rt_value>
          route-target export {<as_value> | <ip_address>} <rt_value>
          end
```

ネイバーの設定と VPNv4 ルート交換の有効化

ピアルータと VPNv4 ルーティング情報を交換するネイバーおよびアドレスファミリを設定するには、次の例を使用します。

```
configure
  context <context_name>
    router bgp <as_number>
      neighbor <ip_address> remote-as <AS_num>
      address-family vpnv4
      neighbor <ip_address> activate
      neighbor <ip_address> send-community both
      exit
    interface <bind_intfc_name>
      ip address <ip_addr_mask_combo>
      end
```

アドレスファミリと接続済みルート再配布の設定

address-family を設定し、接続されたルートまたは IP プールを BGP に **redistribute** するには、次の例を使用します。これにより、別のプロトコルからルートを取得し、BGP プロトコルを使用してそれらを再配布します。

```
configure
   context <context_name>
     router bgp <as_number>
        address-family ipv4 <type> vrf <vrf_name>
          redistribute connected
          end
```

（注） StarOS は次のアドレス範囲を Martian と見なし、この範囲に該当する BGP アップデートを拒否します。

また、StarOS では BGP ネットワークコマンドによる以下の範囲からの設定は許可されません。

- 127.x.x.x
- 128.0.x.x
- 191.255.x.x
- 192.0.0.x
- 223.255.255.x

MPLS ラベルを使用した IP プールの設定

入力および出力用の MPLS ラベルを使用して IP プールを設定するには、この例を使用します。

```
configure
   context <context_name> -noconfirm
     ip pool <name> <ip_addr_mask_combo> private vrf <vrf_name> mpls-label input
 <in_label_value> output <out_label_value1> nexthop-forwarding-address
<ip_addr_bgp_neighbor>
      end
```

社内サーバー向けの DHCP サービスのバインド

この例を使用して、企業ネットワークでの入出力用に DHCP サービスを MPLS ラベルにバインドします。

```
configure
   context <dest_ctxt_name>
      interface <intfc_name> loopback
         ip vrf forwarding <vrf_name>
         ip address <bind_ip_address subnet_mask>
         exit
      dhcp-service <dhcp_svc_name>
         dhcp ip vrf <vrf_name>
         bind address <bind_ip_address> [ nexthop-forwarding-address
<nexthop_ip_address> [ mpls-label input <in_mpls_label_value> output
<out_mpls_label_value1> [ <out_mpls_label_value2> ]]]
```

```
dhcp server <ip_address>
end
```

注：

- 適切に動作させるには、DHCP機能を接続先コンテキスト内で設定する必要があります。
- オプションのキーワード **nexthop-forwarding-address** <*ip_address*> **mpls-label input** <*in_mpls_label_value*> **output <** <*out_mpls_label_value1*> により、MPLS トラフィックでの DHCP が適用されます。

社内サーバー向けの AAA グループのバインド

企業のネットワークの入出力用に AAA サーバーグループに MPLS ラベルをバインドするには、この例を使用します。

```
configure
  context <dest_ctxt_name>
    aaa group <aaa_grp_name>
      radius ip vrf <vrf_name>
      radius attribute nas-ip-address address <nas_address>
nexthop-forwarding-address <ip_address> mpls-label input <in_mpls_label_value>
 output < <out_mpls_label_value1>
     radius server <ip_address> encrypted key <encrypt_string> port <iport_num>

      end
```

注：

- *aaa_grp_name* は、コンテキスト コンフィギュレーション モードで設定されている事前設定済みの AAA サーバーグループです。AAA グループの設定の詳細については、『*AAA Interface Administration and Reference*』を参照してください。
- オプションのキーワード **nexthop-forwarding-address** <*ip_address*> **mpls-label input** <*in_mpls_label_value*> **output <** <*out_mpls_label_value1*> により、MPLS トラフィックの AAA グループを関連付けます。

ダイナミックラベルを使用した BGP/MPLS VPN の設定

このセクションでは、システムを MPLS-CE として設定し、ダイナミック MPLS ラベル機能を使用して PE と対話するために必要な手順について説明します。

以下で説明する設定手順を試す前に、本ガイドの「ルーティング」の章に記載されている基本設定を完了する必要があります。

重要 この章で説明する機能は拡張機能であり、拡張機能ライセンスが必要です。このサポートは、特定の機能サポートライセンスを購入し、シャーシにインストールした場合にのみ利用できます。

重要 このセクションの設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンドや、キーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

BGP/MPLS VPN に対応するようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 ルータでVRFを作成し、VRF名を割り当てます。ルーターゲットを実行する前に、まずルート識別子を定義します。設定の詳細については、「route-distinguisher と route-target を使用した VRF の作成 （1120 ページ）」のセクションを参照してください。

ステップ 2 「ネイバーの設定と VPNv4 ルート交換の有効化 （1124 ページ）」の設定例を適用して、ルーティング情報を交換し、ピアルータとのBGPピアリング接続を確立するようにネイバーとアドレスファミリを設定します。

ステップ 3 「アドレスファミリと接続済みルート再配布の設定 （1124 ページ）」の設定例を適用して、アドレスファミリを設定し、接続されたルートドメインをBGPに再配布します。これにより、別のプロトコルからルートを取得し、BGP プロトコルを使用して BGP ネイバーにルートを再配布することができます。

ステップ 4 「MPLS ラベルを使用した IP プールの設定 （1125 ページ）」の設定例を適用して、ダイナミック MPLS ラベルを使用して IP プールを設定します。

ステップ 5 オプションです。「社内サーバー向けの DHCP サービスのバインド （1125 ページ）」の設定例を適用して、企業ネットワークでダイナミック MPLS ラベルと連携するように DHCP サービスをバインドします。

ステップ 6 オプションです。「社内サーバー向けの AAA グループのバインド （1125 ページ）」の設定例を適用して、ダイナミック MPLS ラベルと連携するように企業ネットワークの AAA/RADIUS サーバーグループをバインドします。

ステップ 7 オプションです。「DSCP と EXP ビットのマッピング （1126 ページ）」の設定例を適用して、入力および出力トラフィックのMPLSヘッダーのDSCPビット値と試験的（EXP）ビット値間のマッピングのために、基本的な MPLS 機能をサポートするように設定されている、設定済みの IP VRF を変更します。

ステップ 8 『*System Administration Guide*』[英語] の説明に従って、設定を保存します。

route-distinguisher と route-target を使用した VRF の作成

次の例を使用して、まずルータで VRF を作成し、VRF 名を割り当てます。2 番目の **ip vrf** コマンドにより、ルート識別子とルートターゲットを作成します。

```
configure
  context <context_name> -noconfirm
    ip vrf <vrf_name>
    router bgp <as_number>
      ip vrf <vrf_name>
        route-distinguisher {<as_value> | <ip_address>} <rt_value>
        route-target export {<as_value> | <ip_address>} <rt_value>
        route-target import {<as_value> | <ip_address>} <rt_value>
        end
```

注：

- エクスポートルートターゲットとインポートルートターゲットが同じ場合は、**route-target import** および **route-target export** コマンドの代わりに、**route-target both** {*<as_value>* | *<ip_address>* } *<rt_value>* コマンドが使用できます。

ネイバーの設定と VPNv4 ルート交換の有効化

ピアルータと VPNv4 ルーティング情報を交換するネイバーおよびアドレスファミリを設定するには、次の例を使用します。

```
configure
  context <context_name>
    mpls bgp forwarding
    router bgp <as_number>
      neighbor <ip_address> remote-as <AS_num>
      address-family vpnv4
      neighbor <ip_address> activate
      neighbor <ip_address> send-community both
      exit
    interface <bind_intfc_name>
      ip address <ip_addr_mask_combo>
      end
```

アドレスファミリと接続済みルート再配布の設定

address-family を設定し、接続されたルートまたは IP プールを BGP に **redistribute** するには、次の例を使用します。これにより、別のプロトコルからルートを取得し、BGP プロトコルを使用してそれらを再配布します。

```
configure
  context <context_name>
    router bgp <as_number>
      address-family ipv4 <type> vrf <vrf_name>
```

```
redistribute connected
end
```

MPLS ラベルを使用した IP プールの設定

ダイナミック MPLS ラベルを使用して IP プールを設定するには、この例を使用します。

```
configure
  context <context_name> -noconfirm
    ip pool <name> <ip_addr_mask_combo> private vrf <vrf_name>
    end
```

社内サーバー向けの DHCP サービスのバインド

この例を使用して、企業ネットワークの DHCP サービスをダイナミック MPLS ラベルにバインドします。

```
configure
  context <dest_ctxt_name>
    interface <intfc_name> loopback
      ip vrf forwarding <vrf_name>
      ip address <bind_ip_address subnet_mask>
      exit
    dhcp-service <dhcp_svc_name>
      dhcp ip vrf <vrf_name>
      bind address <bind_ip_address>
      dhcp server <ip_address>
      end
```

注：

- 適切に動作させるには、DHCP機能を接続先コンテキスト内で設定する必要があります。

社内サーバー向けの AAA グループのバインド

この例を使用して、企業ネットワークの AAA サーバーグループをダイナミック MPLS ラベルにバインドします。

```
configure
  context <dest_ctxt_name>
    aaa group <aaa_grp_name>
      radius ip vrf <vrf_name>
      radius attribute nas-ip-address address <nas_address>
     radius server <ip_address> encrypted key <encrypt_string> port <iport_num>

      end
```

注：

- *aaa_grp_name* は、コンテキスト コンフィギュレーション モードで設定されている事前設定済みの AAA サーバーグループです。AAA グループの設定の詳細については、『*AAA Interface Administration and Reference*』を参照してください。

DSCP と EXP ビットのマッピング

QoS マッピングをサポートするように IP VRF の設定を変更するには、以下の例に示すコマンドを使用します。

```
configure
  context <context_name>
    ip vrf <vrf_name>
      mpls map-dscp-to-exp dscp <dscp_bit_value> exp <exp_bit_value>
      mpls map-exp-to-dscp exp <exp_bit_value> dscp <dscp_bit_value>
      end
```



第 66 章

複数のカスタマイズされた PCO のサポート

- 機能の概要と変更履歴 （1127 ページ）
- 機能説明 （1128 ページ）
- 機能の仕組み （1129 ページ）
- PCO の設定 （1130 ページ）
- モニタリングおよびトラブルシューティング （1132 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• GGSN • P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
追加のプロトコル設定オプションの Custom6 から Custom10 がサポートされるようになりました。	21.26
グローバル コンフィギュレーション モードで既存のコンテナ ID 値を削除または変更する前に、確認メッセージが表示されるようになりました。	21.24
拡張プロトコル設定オプション（ePCO）のサポートが、既存の新しい通信事業者定義の PCO で UWB インジケータで追加されました。	21.20.22
最初の導入。	21.20.16

機能説明

P-GW と GGSN はマルチ PCO サポート機能を使用して、カスタマイズされたプロトコル コンテナ オプション（PCO）を MS GTP メッセージに送信します。Custom1 は既存の PCO で、コンテナ ID の値は FF00H です。

P-GW と GGSN は、Custom1 から Custom10 までの PCO をサポートします。

グローバル PCO のコンテナ ID は実行時に変更されます。この変更は新しいサブスクライバ セッションにのみ影響し、既存のサブスクライバセッションには影響しません。FF03 から FFFF の範囲の PCO のコンテナ ID を設定できます。

超広帯域（UWB）インジケータの通信事業者定義の PCO

P-GW はセッション作成要求やベアラー変更要求で UE から受信した EPCOSI 通知ビットに基づき、プロトコル設定オプション（PCO）または拡張プロトコル設定オプション（ePCO）のいずれかをサポートします。

EPCOSI ビットが設定されている場合、P-GW は ePCO IE で PCO コンテナを送信します。EPCOSI ビットが設定されていない場合、P-GW は PCO IE で PCO コンテナを送信します。

（注） Gn または Gp モードをサポートするために、UE への 3G（UMTS）PCO 通知が追加されました。GGSN は ePCO IE をサポートしていません。

機能の仕組み

ここでは、Gx および Gy インターフェイスを使用して PCO 値を更新する方法について説明します。この章では、ゲートウェイ（GW）という用語は P-GW と GGSN に同じ意味で使用されています。

Gx インターフェイスを使用した PCO 値の更新

このセクションでは、Gx インターフェイスを使用して PCO 値を更新する手順について説明します。

- ポリシーおよび課金ルール機能（PCRF）は、事前定義済みルールをアクティブ化する要求を送信します。
- アクティブ化に成功し、課金アクションが PCO に対して設定されている場合は、取得された値が UE に送信されます。
- セッション作成（CCA）中に事前定義されたルールの作成が実行された場合、P-GW のセッション作成応答および GGSN の PDP コンテキスト作成応答で、取得された PCO が UE に送信されます。
- 事前定義されたルールのアクティブ化がセッションの途中で送信された場合（CCA-U）、取得された PCO が次のメッセージで UE に送信されます。
- PCRF は、事前定義されたルールを非アクティブにする要求を送信します。
- 事前定義されたルールが正常に削除されると、PCO が課金アクションに対して設定されている場合、APN で設定されている値が次のメッセージで UE に返されます。
- 複数の事前定義済みルールが有効になっている場合は、送信されたルールの順序で、PCO に設定された最後の課金アクションが有効と見なされ、その値を使用してセッションマネージャが更新されます。

（注） 最後に事前定義されたルールに、このシナリオの正しい PCO 値が含まれていることを確認します。要求された残りのルールは、通常の事前定義されたルールアクティブ化手順に従います。

Gy インターフェイスを使用した PCO 値の更新

この項では、Gy インターフェイスを使用して PCO 値を更新する手順について説明します。

- オンライン課金システム（OCS）は、フィルタ ID を送信して、対応する後処理のダイナミックルールを有効にします。

- ルールのアクティブ化が成功し、関連付けられた課金アクションが PCO に対して設定されている場合は、取得した値がセッション更新通知イベントを介してセッションマネージャに送信されます。
- GW は PCO 値を UE に送信します。
- OCS が複数のフィルタ ID を送信する場合、最後のフィルタ ID に関連付けられた課金アクションが PCO に使用されます。
- CRF は、事前定義されたルールを非アクティブにする要求を送信します。
- 事前定義済みルールが正常に削除されると、PCOに対して課金アクションが設定されている場合、APN のデフォルト PCO 値が次のメッセージで UE に返されます。

PCO の設定

この項では PCO の設定について説明します。APN コンフィギュレーション モードとグローバル コンフィギュレーション モードでコールがアクティブな場合、CLI の変更は許可されませんが、active-charging service の変更は許可されます。

課金アクションモードでの PCO の設定

ACS 課金アクション構成モードで複数の PCO を設定するには、次の設定例を使用します。

```
configure
   active-charging service service_name
      charging-action action_name
         { pco-custom1 | pco-custom2 | pco-custom3 | pco-custom4 |
pco-custom5 | pco-custom6 | pco-custom7 | pco-custom8 | pco-custom9 |
pco-custom10 } custom_value
         end
```

注：

- **pco-custom1 - pco-custom10** *custom_value*：複数の通信事業者に固有の PCO を設定します。custom_value には 0 ～ 255 の範囲の整数を指定します。

APN コンフィギュレーション モードでの Custom1 PCO の設定

APN コンフィギュレーション モードで Custom1 PCO を設定するには、次の設定例を使用します。

```
configure
   context context_name
      apn apn_name
         [ no ] pco-option custom1 [ ue-requested ]
         end
```

注：

- **pco-option custom1**：オペレータ定義の PCO コンテナ custom1 モードを設定します。デフォルトでは、コンテナ ID の値は 0 に固定されています。
- **ue-requested**：UE から要求された場合にのみ、カスタム PCO オプションを PCO IE に含めるように設定します。
- **no**：APN コンフィギュレーション モードで custom1 PCO 設定を削除します。

APN コンフィギュレーション モードで複数の PCO を設定する

APN コンフィギュレーション モードで複数の PCO を設定するには、次の設定例を使用します。

```
configure
  context context_name
    apn apn_name
      [ no ] pco-options { { custom1 | custom2 | custom3 | custom4 |
 custom5 | custom6 | custom7 | custom8 | custom9 | custom10 } [
ue-requested value custom_value | value custom_value ] }
      end
```

注：

- **custom1 - custom10**：PCO IE にカスタム PCO オプションを含めるように APN を設定します。
- **ue-requested**：UE から要求された場合にのみ、カスタム PCO オプションを PCO IE に含めるように設定します。
- **value** *custom_value* ：カスタム PCO のデフォルトコンテナ値を設定します。 custom_value は 0 ～ 255 の範囲の整数である必要があります。
- **no**：APN コンフィギュレーション モードで PCO 設定を削除します。

グローバル コンフィギュレーション モードでの PCO コンテナ ID の設定

グローバル コンフィギュレーション モードで複数の PCO を設定するには、次の設定例を使用します。

```
configure
  [ no ] pco-options { custom2 | custom3 | custom4 | custom5 | custom6
 | custom7 | custom8 | custom9 | custom10 } container-id container_id_value

  end
```

注：

- **pco-options { custom2 - custom10}**：PCO IE のカスタム PCO オプションを設定します。

- **container-id** *container_id_value*：オペレータ定義のコンテナ ID と、FF03 ～ FFFF の範囲の値を設定します。
- **no**：グローバル コンフィギュレーション モードでの PCO コンテナ ID の設定を削除します。

（注） custom1 コンテナ ID は、コンテナ値が FF00H に固定されているため、グローバル コンフィギュレーション モードでは設定できません。

（注） 進行中のセッションの既存のコンテナ ID 値を削除または変更した場合、新しいセッションにのみ影響し、進行中のセッションや既存のセッションには影響しません。

モニタリングおよびトラブルシューティング

ここでは、この機能をサポートする show コマンドを使ったモニタリングと障害対応の方法について説明します。

コマンドと出力の表示

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show active-charging charging-action all

このコマンドの出力が強化され、次のフィールドが表示されるようになりました。

表 *101 : show active-charging charging-action all* コマンド出力の説明

フィールド	説明
PCO-Custom1-10 value	複数の通信事業者固有の PCO のアクション値を示します。値の範囲は 1 ～ 10 です。

show active-charging sessions full all

このコマンドの出力が強化され、以下のフィールドが表示されるようになりました。

表 *102 : show active-charging sessions full all* コマンド出力の説明

フィールド	説明
custom	通信事業者固有のカスタムオプションを示します。

フィールド	説明
値	カスタム PCO コンテナでの送信に使用される値を示します。
Interface	次の条件に基づき、Gx、Gy または n/a などのインターフェイスを示します。 • Gx：課金ルールは、カスタム PCO 値を持つ Gx インターフェイスから適用されます。 • Gy：課金ルールは、カスタム PCO 値を持つ Gy インターフェイスから適用されます。 • n/a：APN プロファイルから適用される設定済みの PCO 値。

show apn all

このコマンドの出力が強化され、以下のフィールドが表示されるようになりました。

表 *103 : show apn all* コマンド出力の説明

フィールド	説明
Custom1 ～ 10 値	複数の通信事業者固有の PCO のアクション値を指定します。値の範囲は 1 ～ 10 です。
UE-Requested	新しい PCO オプションを要求した UE に対して PCO を指定します。



第 67 章

複数の IP バージョンのサポート

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （1135 ページ）
- 機能説明 （1136 ページ）
- 機能の仕組み （1136 ページ）
- 複数の IP バージョンのサポートの設定 （1139 ページ）
- モニタリングおよびトラブルシューティング （1139 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • S-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC - DI • VPC - SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *S-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

重要　リリース 21.2 および N5.1 よりも前に導入された機能の変更履歴の詳細は示されません。

改訂の詳細	リリース
この機能により、P-GW、S-GW、および SAEGW ノードは、セッションの設定中に交換される、すべてのトランスポートアドレスで受信した制御メッセージをサポートできます。	21.8
最初の導入。	21.2 よりも前

機能説明

この機能により、P-GW、S-GW、および SAEGW ノードは、セッションの設定中に交換される、すべてのトランスポートアドレスで受信した制御メッセージをサポートできます。

BRCmd、MBCmd、および DBCmd の各メッセージの動作を制御するために、egtp-service レベルで新しい CLI コマンドが導入されました。

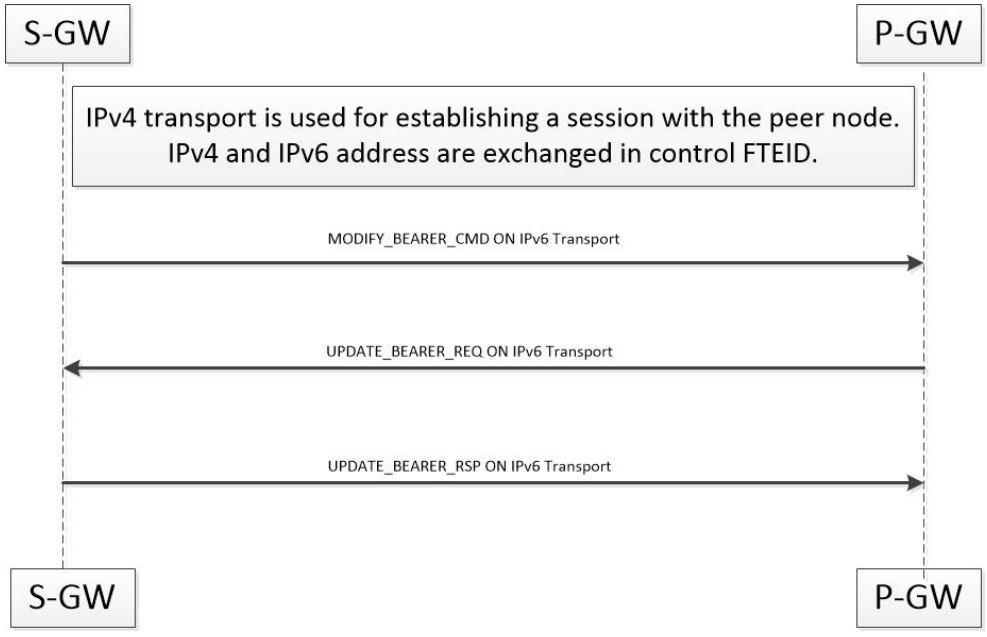
機能の仕組み

ここでは、この機能の動作を説明します。次に、MBCmd のコールフローの例を示します。

次の図は、 この機能が無効になっている場合のコールフローを示しています。



次の図は、この機能が有効になっている場合のコールフローを示しています。



セッションの確立中に、P-GW、S-GW、および SAEGW ノードはトランスポートとして IPv6 アドレスを使用します。このトランスポートは、ピアノードとのトンネルを確立するために使用されます。IPv4 アドレスと IPv6 アドレスが制御 FTEID で交換される場合、ノードはノード

によるIPv4トランスポートでMBCmd、BRCmd、およびDBCmdメッセージを処理する必要があります。

セッションの確立中に、IPv4アドレスがトランスポートとして使用され、ピアノードとのトンネルの確立に使用されている場合に、IPv4およびIPv6アドレスが制御FTEIDで交換される場合には、MBCmd、BRCmd、およびDBCmdメッセージも、ノードによってIPv6トランスポート上で処理されます。

セッションの確立中に、IPv4アドレスとIPv6アドレスが両方のピアによってデータF-TEIDで交換される場合、GTP-Uデータパケットは IPv6およびIPv4トランスポートの両方で処理されます。

ただし、セッションの確立中に、IPv4アドレスがトランスポートとして使用されている場合は、C-TEIDに IPv4アドレスが含まれず、そのメッセージはノードによって拒否されます。ノードは、IPv6アドレスに対して同様の動作を示します。

セッションの確立中に、IPv4アドレスとIPv6アドレスが両方のピアによってデータF-TEIDで交換される場合、GTP-Uデータパケットは IPv6およびIPV4トランスポートの両方で処理されます。

次の表に、さまざまなセッション確立シナリオでのメッセージ処理動作を示します。

表 *104* : さまざまなセッション確立シナリオでのメッセージ処理動作

メッセージ	セッションの確立に使用されるトランスポート	セッションの確立中に送信される C-FTEID	メッセージが送信されるトランスポート
MBR/DSR	IPv6	IPv4/IPv6	IPv4
MBC/DBC/BRC	IPv6	IPv4/IPv6	IPv4
Change Notification	IPv6	IPv4/IPv6	IPv4
一時停止/再開	IPv6	IPv4/IPv6	IPv4
MBR/DSR	IPv4	IPv4/IPv6	IPv6
MBC/DBC/BRC	IPv4	IPv4/IPv6	IPv6
Change Notification	IPv4	IPv4/IPv6	IPv6
一時停止/再開	IPv4	IPv4/IPv6	IPv6
MBR/DSR	IPv6	IPv6	IPv4
MBC/DBC/BRC	IPv6	IPv6	IPv4
Change Notification	IPv6	IPv6	IPv4
一時停止/再開	IPv6	IPv6	IPv4
MBR/DSR	IPv4	IPv4	IPv6

メッセージ	セッションの確立に使用されるトランスポート	セッションの確立中に送信される C-FTEID	メッセージが送信されるトランスポート
MBC/DBC/BRC	IPv4	IPv4	IPv6
Change Notification	IPv4	IPv4	IPv6
一時停止/再開	IPv4	IPv4	IPv6

複数の IP バージョンのサポートの設定

ここでは、この機能をサポートするために使用可能な CLI コマンドについて説明します。

デフォルトでは、この機能はイネーブルです。

```
configure
  context context_name
    egtp-service service_name
      [no] gtpc command-messages dual-ip-stack-support
      end
```

注：

- **no**：この機能を無効化します。
- **command-messages**：S-GW および P-GW での MBC、DBC、または BRC メッセージを設定します。
- **dual-ip-stack-support**：サポートされている場合は、P-GW、S-GW、SAEGW ノードが IPv4/IPv6 トランスポートの両方でコマンドメッセージを処理できるようにします。

モニタリングおよびトラブルシューティング

この項では、オーバーライド制御拡張機能のモニターとトラブルシューティングの方法について説明します。

コマンドと出力の表示

ここでは、オーバーライド制御拡張機能の show コマンドとコマンド出力について説明します。

show configuration

このコマンドの出力に、以下の新しいフィールドが追加されました。

- gtpc command-messages dual-ip-stack-support：サポートされている場合、IPv4 トランスポートと IPv6 トランスポートの両方でコマンドメッセージを指定します。

show egtp-service all

このコマンドの出力に、以下の新しいフィールドが追加されました。

- GTPC Command Messages Dual IP Support：IPv4/IPv6 トランスポートの両方でコマンドメッセージを指定します（サポートされている場合）。



第 68 章

NAT ポート チャンク ホールド タイマーのサポート

- 機能の概要と変更履歴 （1141 ページ）
- 機能説明 （1142 ページ）
- 機能の仕組み （1142 ページ）
- ポート チャンク ホールド タイマーの設定 （1144 ページ）
- ダウングレードプロセス （1146 ページ）
- モニタリングおよびトラブルシューティング （1146 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *P-GW* アドミニストレーション ガイド • *Command Line Interface Reference* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.28.m10

機能説明

P-GW での NAT ポート チャンク ホールド タイマー機能の可用性に応じて、ポート チャンク ホールド タイマーを多対 1 の NAT IP プールに設定できます。ポートチャンクからの最後のポートが解放されると、チャンクは **Used** から **Hold** 状態に移行し、ポート チャンク ホールド タイマーが開始されます。ポート チャンク ホールド タイマーの期限が切れると、ポートチャンクが解放され、新しいセッションで使用できるようになります。ポートチャンクが再利用されるパケットを、ポートチャンク ホールドタイマーが期限切れになる前に受信した場合、ポートチャンクタイマーが停止し、そのポートチャンクからのポートが割り当てられます。

ポートチャンクは、次の方法で解放できます。

- ポートチャンク内の最後のポートの最後のフローがタイムアウトでアイドル状態になると、ポート チャンク ホールド タイマーが開始し、ポート チャンク ホールド タイマーの期限切れ時にポートチャンクが解放されます。
- サブスクライバが切断されたとき。

NAT IP の解放は、NAT バインディングタイマーの期限切れ後に発生します。この動作は、ポート チャンク ホールド タイマー機能に関係なく同じ状態が維持されます。

機能の仕組み

次の表は、ポートチャンクを使用した単一の最後のフローに関するさまざまなタイマーのトリガーをまとめたものです。

表 *105 :* 対応するタイマー（秒単位）

秒	Timer
a	UDP アイドルタイムアウト
b	TCP アイドル タイムアウト
c	NAT バインドのタイムアウト
d	マッピングのタイムアウト
e	ポートチャンクホールドのタイムアウト

表 *106 : NAT* ポート、ポートチャンク、および *NAT IP* をリリースするトリガー

NAT ポートチャンクの最後のフロープロトコル	チャンクに対する NAT ポート（NAT マッピング）のリリース	ポートチャンクのリリース（ポートチャンク ホールド タイマーが有効である場合）	REALM からの NAT IP のリリース
UDP	a秒のアイドルタイムアウト＋「d」秒のマッピングタイムアウトの後にリリースされます。	「e」秒のポート チャンク ホールド タイムアウトの期限切れ後にリリースされます（ポート チャンク ホールド タイマーは、チャンクの最後の NAT ポート リリース後に開始されます）。 UDP フローが非アクティブになった時点からポートチャンクがリリースされるまでの合計時間は（a＋d＋e）秒です。	NAT バインド タイマーの期限切れ後にリリースされます。
TCP（グレースフル）	RST/FIN の受信時に TCP フローが終了した場合、フローがクリアされた後に NAT ポートがリリースされます。ただし、このポートは、設定された NAT 2MSL タイムアウトに再利用可能です。	「e」秒のポート チャンク ホールド タイムアウトの期限切れ後にリリースされます（ポート チャンク ホールド タイマーは、チャンクの最後の NAT ポート リリース後に開始されます）。 2 MSL とポートチャンクタイマーが並行して実行されます。2MSL の方がポート チャンク ホールド タイムアウトより長い場合、ポートは強制的に「フリー」状態になり、ポートチャンクがリリースされます。 最後の TCP フローがポート チャンク ホールド タイムアウトでクリアされた後にポートチャンクがリリースされるまでの合計時間は「e」秒です。	NAT バインド タイマーの期限切れ後にリリースされます。
TCP（オープン）	FIN/RST が送信されず、「b」秒のアイドルタイムアウト＋「d」秒のマッピングタイムアウトの期限切れ時に行われます。	「e」秒のポート チャンク ホールド タイムアウトの期限切れ後にリリースされます（ポート チャンク ホールド タイマーは、チャンクの最後の NAT ポート リリース後に開始されます）。 TCP フローが非アクティブになった時点からポートチャンクがリリースされるまでの合計時間は（b＋d＋e）秒です。	NAT バインド タイマーの期限切れ後にリリースされます。

ポート チャンク ホールド タイマーの設定

NAT バインディングタイマーとポート チャンク ホールド タイマーを個別に分離するには、次の設定を使用します。

ポート チャンク ホールド タイマーの設定は、NAT IP プール内のすべての NAT IP アドレスに適用されます。

```
configure
  context context_name
    ip pool nat_pool_name { ip_address subnet_mask | ip_address/mask> |
range from_ip_address to_ip_address  }
    napt-users-per-ip-address users [ alert-threshold [ { pool-free |
pool-hold | pool-release | pool-used } low_thresh [ clear high_thresh ] +
]
     [ max-chunks-per-user chunks] [ nat-binding-timer binding_timer [
port-chunk-hold-timer port-chunk-hold-timeout ] ]
    [ on-demand ] [ port-chunk-size size ] [ port-chunk-threshold threshold
 ] [ send-nat-binding-update ] [ srp-activate ] + ]
```

注：

- **port-chunk-hold-timer** *[port-chunk-hold-timeout]*：解放されたポートチャンクを NAPT IP プールで再利用できるようになるまでのタイムアウトを秒単位で表示します。値が 0 に設定されている、または値が設定されていない場合は、下位互換性を維持するために、ポートチャンクは**nat-binding-timer** に基づいて解放されます。最小値は 0 で、最大値は 31556926 です。デフォルトでは、ポート チャンク ホールド タイマーは無効です。NAT バインディングタイマー値より小さくゼロではない値を使用して、ポートチャンク ホールドタイマーを再度有効にすることができます。

（注）

- ポートチャンク ホールド タイマー機能を有効にしながら、NAT バインディングタイマー値を設定することを推奨します。
- **nat-binding-timer** を無効にして **port-chunk-hold timer** を設定すると、NAT IP アドレスは解放されず、**port-chunk-hold timer** の期限後にすべての NAT ポートチャンクが解放されます。
- **port-chunk-hold timer** には NAT バインドタイムアウト値よりも小さい値のみを指定します。ポートチャンクのホールドタイムアウト値が NAT バインドタイムアウトよりも高く設定されている場合、次の CLI エラーが表示されます。

```
「Failure: NAT port chunk hold timer must be less
than NAT binding timer.」
```

- ポート チャンク ホールド タイマーとして 2MSL 未満の値を設定しないでください。
- ポート チャンク ホールド タイマーの値は NAT バインディングタイマーよりも小さいため、この機能を使用すると、NAT バインディングレコード（NBR）の数が増加します。このタイマーの値を小さく設定しすぎると、NBR の数が多くなります。実際の値はサブスクライバのトラフィックプロファイルによって異なりますが、ほとんどの展開では、NAT バインディングタイマーが 1800 秒の場合にポート チャンク ホールド タイマーの値を 300 秒に保つことが許容されます。

ポート チャンク ホールド タイマーの変更

ポート チャンク ホールド タイマーを変更するには、次の設定を使用します。

```
configure
  context context_name
    ip pool nat_pool_name [ nat-binding-timer binding_timer
port-chunk-hold-timer port_chunk_hold_timeout ]
  exit
```

注：

- **nat-binding-timer** *binding_timer* **port-chunk-hold-timer** *port_chunk_hold_timeout* ：IP プールのポート チャンク ホールド タイマーを変更するためのポート チャンク ホールド タイムアウトを指定します。IP プールのポート チャンク ホールド タイマーが変更されると、新しいポートチャンクタイマーは、すべてのサブスクライバに対して変更された値を直ちに使用します。

設定例

次に設定の出力例を示します。

```
[local]qvpc-si# configure
[local]qvpc-si(config)# context egress
[egress]qvpc-si(config-ctx)# ip pool pgw_nat_ps_int01 97.36.232.0 255.255.255.252
napt-users-per-ip-address 2 group-name pgw_nat_ps_int alert-threshold pool-free 20 clear
 25 on-demand max-chunks-per-user 1 port-chunk-size 32256 nat-binding-timer 600
port-chunk-hold-timer 300
```

ダウングレードプロセス

port-chunk-hold-timer CLI キーワードを除外して ip pool CLI を再設定することをお勧めします。これは、**port-chunk-hold-timer** CLI キーワードを使用して設定を保存し、ダウングレードされたイメージで同じ設定ファイルを使用してリロードするときにダウングレードすると、ip pool CLI 全体が無視されるためです。

モニタリングおよびトラブルシューティング

ここでは、showコマンドとバルク統計を使用した、この機能のモニタリングとトラブルシューティングの方法について説明します。

show コマンドと出力

この項では、この機能をサポートするために使用可能な show CLI コマンドについて説明します。

show configuration

この **show configuration** CLI コマンドを使用して、多対 1 NAT 機能のポートチャンクタイマーの動作のサポートで使用可能な次のフィールドを表示します。

- **port-chunk-hold-timer** ：解放されたポートチャンクをNAPT IPプールで再利用できるようになるまでのタイムアウトを秒単位で表示します。

出力例

```
[local]qvpc-si# show configuration
Config
  context egress
    ip pool ipv4-private 10.0.0.1 255.255.0.0 private 0 srp-activate group-name int41
alert-threshold group-available 20 clear 25
    ip pool ipv4-static 11.0.0.1 255.255.0.0 static
    ip pool pgw_nat_ps_int01 97.36.232.0 255.255.255.252 napt-users-per-ip-address 2
group-name pgw_nat_ps_int alert-threshold pool-free 20 clear 25 on-demand port-chunk-size
 32256 nat-binding-timer 600 port-chunk-hold-timer 300
  exit
```

show ip pool nat-realm

この **show ip pool nat-realm** CLI コマンドを使用して、多対 1 NAT 機能のポートチャンクタイマーの動作のサポートで使用可能な次のフィールドを表示します。

- **Port-chunk-hold-Timer in seconds**：解放されたポートチャンクを NAPT IP プールで再利用できるようになるまでのタイムアウトを秒単位で表示します。

サンプル出力：

```
show ip pool nat-realm
      Group: pgw_nat_ps_int
           Pool: pgw_nat_ps_int01       97.36.232.0      255.255.255.252
           Pool Status:       Good
           Pool Id: 3
              Type:            NAPT                    Priority:   0
              Group:                                   pgw_nat_ps_int
                 Used:            0                    Free:       2

                 Hold:            0                    Released:   0
                 Limit Exceeded:  0                    Total Alloc Req: 0
                 Total Rel Req:   2
                    Recovered Alloc Req: 0          Alloc Req by Group:  2
        User-Plane Id: N/A
        Virtual-FE Id: N/A
        User-Plane Id: N/A
        Virtual-FE Id: N/A
        Vdu group name:
           Number of Users Per-IP: 2
           IP Sharing: Disabled
           Shared IP Size: n/a
           Allocation Mode: On-Demand
           Port Chunk Size: 32256
           Port Chunk Threshold: 100
           Maximum Number of Chunks per User: 1
           Minimum Number of Chunks per User: 0
           Nat-Binding-Timer: 600

           Send-Nat-Binding-Update: Disabled
           Nexthop Forwarding Address: Disabled
              Pool-Free Threshold:  20%                          Clear:  25%
              Pool-Used Threshold: Disabled                      Clear: Disabled
              Pool-Release Threshold: Disabled                   Clear: Disabled
              Pool-Hold Threshold: Disabled                      Clear: Disabled
              cip-local-pool-used Threshold: Disabled            Clear: Disabled
              cip-local-pool-in-use-addr Threshold: Disabled     Clear: Disabled
              Include-Network-Broadcast-Address: Disabled
              Port-chunk-hold-Timer in seconds: 300
                   Group Summary:
                   Group Used:                          0
                   Group Free:                          2
                   Group Hold:                          0
                   Group Quarantine:                    0
                   Group Released:                      0
                   Group Effective Alarm Threshold %: Disabled
                   Group Effective Clear Threshold %: Disabled
                   Group Current Usage %:             0.00%
                   Group Status:                      Good
```

show active-charging nat statistics

show active-charging nat statistics は、次の出力を表示します。

```
[local]qvpc-si# show active-charging nat statistics
Thursday March 09 23:30:21 EST 2023
NAT Realm Utilization:
---------------------
Realm Name:               pgw_nat_ps_int  Context:                        egress
Current IP Address-In-Use:           n/a  Total IP Address:                    2
Current Calls Using-Realm:           n/a  Current Port-Chunks Available:     n/a
Current Port-Chunks-In-Use:          n/a  Total Port-Chunks:                   4
Current Port-Chunks-On-hold     :    n/a
Port-Chunk size:                     n/a
Statistics:
  Total AAA alloc msgs sent:           0  Total AAA dealloc msgs sent:         0
  Total flows denied no IP:            0  Total flows denied no port:          0
  NAT44 flows denied no IP:            0  NAT44 flows denied no port:          0
  NAT64 flows denied no IP:            0  NAT64 flows denied no port:          0
  Total flows denied no memory:        0
  NAT44 flows denied no memory:        0  NAT64 flows denied no memory:        0
  Total bytes Transferred:             0  Total flows processed:               0
  NAT44 bytes Transferred:             0  NAT44 flows processed:               0
  NAT64 bytes Transferred:             0  NAT64 flows processed:               0
  Average TCP port usage:              0  Average UDP port usage:              0
  Average Others port usage:           0

Realm Name:             pgw_nat_ps_int01  Context:                        egress
Current IP Address-In-Use:           1  Total IP Address:                    2
Current Calls Using-Realm:           0  Current Port-Chunks Available:       3
Current Port-Chunks-In-Use:          0  Total Port-Chunks:                   4
Current Port-Chunks-On-hold     :    1
Total Reserved Port-Chunks:                                                  0
Current Reserved Port-Chunks-In-Use:                                         0
Current Available Reserved Port-Chunks:                                      0
Port-Chunk size:                 32256
Statistics:
  Total AAA alloc msgs sent:           0  Total AAA dealloc msgs sent:         0
  Total flows denied no IP:            0  Total flows denied no port:          0
  NAT44 flows denied no IP:            0  NAT44 flows denied no port:          0
  NAT64 flows denied no IP:            0  NAT64 flows denied no port:          0
  Total flows denied no memory:        0
  NAT44 flows denied no memory:        0  NAT64 flows denied no memory:        0
  Total bytes Transferred:            84  Total flows processed:               1
  NAT44 bytes Transferred:            84  NAT44 flows processed:               1
  NAT64 bytes Transferred:             0  NAT64 flows processed:               0
  Average TCP port usage:              0  Average UDP port usage:              1
  Average Others port usage:           0

Port-Chunks distribution:
Max no.of chunks used   Total no.of subscribers   Current no.of subscribers
---------------------   -----------------------   -------------------------
         1                        1                         1

Ports distribution:
Max no. of ports used   Total no. of subscribers
---------------------   -----------------------------------
         [0-8]                    1

Total Realms: 2
```

バルク統計

ここでは、バルク統計スキーマについて説明します。

NAT レルムスキーマ

NAT レルムスキーマは、NAT ポート チャンク ホールド タイマー機能のモニタリングと障害対応に使用できる動作統計情報を提供します。

表 *107 : NAT* レルムスキーマのバルク統計変数

変数	説明
nat-rlm-port-chunks-on-hold	コンテキストごとおよびレルムごとに収集される、保留中のポートチャンクの合計数



第 69 章

Wi-Fi EPC の NetLoc

この章では、P-GW および SAE-GW での「Wi-Fi EPC の NetLoc」機能の StarOS のサポートについて説明します。

- 機能説明 （1151 ページ）
- 機能の仕組み （1151 ページ）
- Wi-Fi EPC 機能向け NetLoc の設定 （1154 ページ）
- Wi-Fi EPC 機能の NetLoc のモニタリングと障害対応 （1155 ページ）

機能説明

この機能により、IMS ネットワークは WLAN アクセスネットワークから UE の位置情報を取得できます。これにより、通信事業者のための位置関連の機能が向上します。この機能は、位置情報に基づいてサブスクライバに課金する場合にも有用です。

LTE NetLoc は以前のリリースからすでサポートされていることに注意してください。このリリースでは、NetLoc のサポートが WLAN アクセスに拡張されています。SM、IMSA、および ECS などのさまざまな内部モジュールに、必要なパラメータを渡すための基本的な実装はすでにサポートされています。

機能の仕組み

アプリケーション機能（AF）が PCRF にアクセスネットワーク情報の報告を要求すると、PCRF は、要求されたアクセスネットワーク情報の通知（ユーザーの場所やユーザーのタイムゾーン情報）を Required-Access-Info AVP 内で PCEF に提供します。この AVP は、適切な PCC ルールの Charging-Rule-Definition AVP に含まれています。

PCRF は、Event-Trigger AVP 内の ACCESS_NETWORK_INFO_REPORT イベントトリガーも提供します。ACCESS_NETWORK_INFO_REPORT イベントトリガーが設定されている場合、Required-Access-Info AVP を含む PCC ルールのインストール、変更、および削除時に、P-GW は、使用される IP CAN タイプに必要なロケーション情報を取得できるかどうかを判断します。

ベアラー非アクティブ化または UE 切断処理中に、P-GW は、TWAN-Identifier AVP 内の PCRF にアクセスネットワーク情報を提供します。P-GW は、S2a/S2b インターフェイスに適用可能なものとして、User-Location-Info-Time AVP や UE-Local-IP-Address AVP 内の該当する場所に UE が存在することが最後に認識された時点に関する情報も提供します。

- 信頼できる WLAN の場合、ユーザーロケーション情報（ULI）が TWAN-Identifier AVP で提供されます。
- 信頼できない WLAN の場合、URI には TWAN 識別子、UE のローカル IP アドレスは、およびオプションで UDP 送信元ポート番号（NAT が検出された場合）が含められます。

ULI が PCRF によって要求されているものの、PCEF に提供されていない場合、PCEF は、3GPP-SGSN-MCC-MNC AVP 内でサービング PLMN 識別子を提供します。また、タイムゾーンが PCRF によって要求されると、PCEF は、3GPP-MS-TimeZone AVP 内でタイムゾーンを提供します。タイムゾーンは、信頼できる WLAN インターフェイスにのみ適用されることに注意してください。WLAN アクセスの場合、PCEF には、アクセスネットワーク情報のレポート中に、AN-Trusted AVP も含められます。

IP-CAN セッションの終了手順中に、PCEF は、ACCESS_NETWORK_INFO_REPORT イベントトリガーが設定されている場合、ULI（PCEF に提供された場合）、UE が最後に User-Location-Info-Time AVP 内の該当する場所に存在することが認識された場所（PCEFに提供された場合）、3GPP-SGSN-MCC-MNC AVP 内の PLMN 識別子（ユーザーロケーション情報が PCEF に提供されなかった場合））、および 3GPP-MS-TimeZone AVP内のタイムゾーン情報を含むアクセスネットワーク情報を提供します。

S2a/S2b インターフェイスから受信された WLAN ロケーション情報は、P-GW でサポートされているすべてのインターフェイス（Gx、Gy、および Gz）で報告されます。

アカウンティング要件

アカウンティング要件の一部として、次のディクショナリが使用されます。

- Gx：r8-gx-standard
- Gy：
  - S2a：custom-8 （Rel-11）
  - S2b：custom-8（Rel-13）
- Gx：
  - S2a：custom-48 および custom-52
  - S2b：custom-52

PGW-CDR の次のフィールドは、Gz 要件の一部として導入されました。

- custom-52 ディクショナリ（uWANUserLocationInfo の一部として）：
  - uELocalIPAddress

- uDPSourcePort
- sSID
- bSSID

custom-52 は新たに導入された標準ディクショナリであり、3GPP リリース 13 に準拠しています。

制限事項

この項では、この機能の既知の制限事項および制約事項を示します。

- S2b のユーザーロケーション情報（ULI）には、UE のローカル IP アドレスと、オプションで、UDP 送信元ポート番号（NAT が検出された場合）が含まれます。また、WLAN のロケーション情報（とその経過時間）も含まれます。UE ローカル IP アドレス、UDP ポート、または WLAN ロケーションのいずれかの情報が変更された場合に、ロケーションが変更されたと見なされます。
- Gz では、WLAN ロケーションの変更に対して ULI 変更トリガーが使用されます。
- Gy では、WLAN ロケーションの変更に対して location_any トリガーが使用されます。
- Rf および S2a RADIUS、および LI インターフェイスは、この機能の一部とは見なされません。
- S6b インターフェイスでは変更は行われません。
- TWAN/UWAN 識別子の SSID と BSSID のみがこの機能の一部と見なされます。
- UE ローカル IP アドレスのフィールドは、UWANUserLocationInfo の一部として Gz および Gy に必須です。
- S2b の場合、受信した UWANUserLocationInfo が以前の UWANUserLocationInfo と異なる場合、以下の限られたエラーケース処理が実行されます。
  - Gy の場合、受信したパラメータに IP アドレスが含まれていない場合、P-GW は ULI 変更レポートを生成しません。
  - Gz の場合、「ULI 変更」を含むコンテナは、コンテナに対応する UWANUserLocationInfo 値に IP アドレスが含まれている場合にのみ閉じられます。
- この機能は、NetLoc と Wi-Fi 統合ライセンスによって制御されています。
- S2b インターフェイスの場合、UE ローカル IP アドレスとポート、WLAN ID、および WLAN タイムスタンプは、CSReq/CBRsp/UBRsp/DBRsp で受信されない場合は 0 にリセットされます。
- 3GPP TS 32.298 に従い、TWAN 識別子は Gz のレコードレベルで存在します。
- WLAN タイムスタンプは、Gy および Gz インターフェイスでは送信されません。

- UE-location-IP-Address 変更イベントトリガーは、この機能には含まれません。
- EPC_Routed 機能（3GPP TS 29.212 を参照）はサポートされていません。

Wi-Fi EPC 機能向け NetLoc の設定

次の項では、この機能を有効にするための設定コマンドについて説明します。

Gx 用の NetLoc TWAN の設定

以下に示すコマンドで、Gx インターフェイスを介した NetLoc 信頼 WLAN 機能を設定します。

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        diameter encode-supported-features netloc-trusted-wlan
        end
```

注：

- **no diameter encode-supported-features**：この機能を無効化します。
- このコマンドは、S2b コールで Gx が有効になっている場合に有効です。
- デフォルトでは、この機能は無効になっており、Gx を介して TWAN 情報が送信されません。

Gx 用の NetLoc UWAN の設定

以下に示すコマンドで、Gx インターフェイスを介した NetLoc 非信頼 WLAN 機能を設定します。

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        diameter encode-supported-features netloc-untrusted-wlan
        end
```

注：

- **no diameter encode-supported-features**：この機能を無効化します。
- このコマンドは、S2b コールで Gx が有効になっている場合に有効です。
- デフォルトでは、この機能は無効になっており、Gx を介して UWAN 情報が送信されません。

Gy 用の NetLoc UWAN の設定

以下に示すコマンドは、3GPP Rel. 13 に基づいて追加する必要がある AVP のディクショナリ制御を設定します。

```
active-charging service service_name
  credit-control
    diameter update-dictionary-avps 3gpp-rel13
    end
```

注：

- **no diameter update-dictionary-avps**：この機能を無効化します。
- このコマンドは、S2b コールで Gy が有効になっている場合に有効です。
- デフォルトでは、この機能は無効になっており、Gy を介して UWAN 情報が送信されません。

Gz 用の NetLoc UWAN の設定

以下に示すコマンドで、Gz インターフェイスを介した NetLoc 非信頼 WLAN 機能を設定します。

```
configure
  context context_name
    gtpp group group_name
      gtpp attribute uwanuli
      end
```

注：

- **no gtpp attribute uwanuli**：この機能を無効化します。
- このコマンドは、S2b コールで Gz が有効になっている場合に有効です。
- デフォルトでは、この機能は無効になっており、Gz を介して UWAN 情報が送信されません。

Wi-Fi EPC 機能の NetLoc のモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

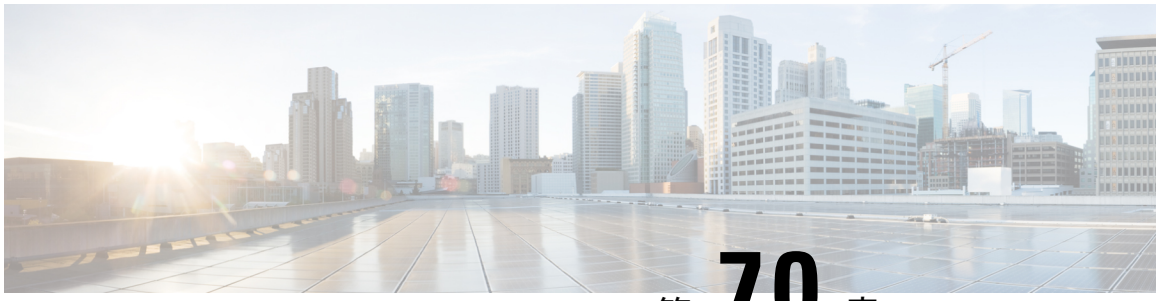
show コマンドと出力

次の表に、この機能のモニターやトラブルシュートに役立つ CLI コマンドを示します。

CLI コマンド	説明

show subscribers pgw-only full all
show subscriber saegw-only full all
	新しく導入された次のフィールドを表示します。これらは、S2a および S2b コールで値が入力されます。
	`TWAN User Location Information:`
	`SSID:`
	`BSSID:`
	`UWAN User Location Information:`
	`UE Local IP Address:`
	`UDP Port:`
	`SSID:`
	`BSSID:`

show ims-authorization service all verbose	新しく導入された次のフィールドを表示します。これらは、IMS承認サービス コンフィギュレーション モードで Supported Features AVP として設定されている場合に値が入力されます。 • **netloc-trusted-wlan** • **netloc-untrusted-wlan**
show gtpp group all	新しく導入された次のフィールドを表示します。これらは、GTPP サーバー グループ コンフィギュレーション モードで **gtpp attribute uwanuli** CLI コマンドが設定されている場合に値が入力されます。 • **UWAN ユーザーロケーション情報の有無**：



第 70 章

ネットワークモビリティ（NEMO）

この章では、NEMOのシステムサポートについて説明し、その設定方法を示します。製品アドミニストレーションガイドには、システム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、『*Cisco ASR 5500 Packet Data Network Gateway Administration Guide*』の説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

- NEMO の概要 （1157 ページ）
- NEMO 設定 （1165 ページ）

NEMO の概要

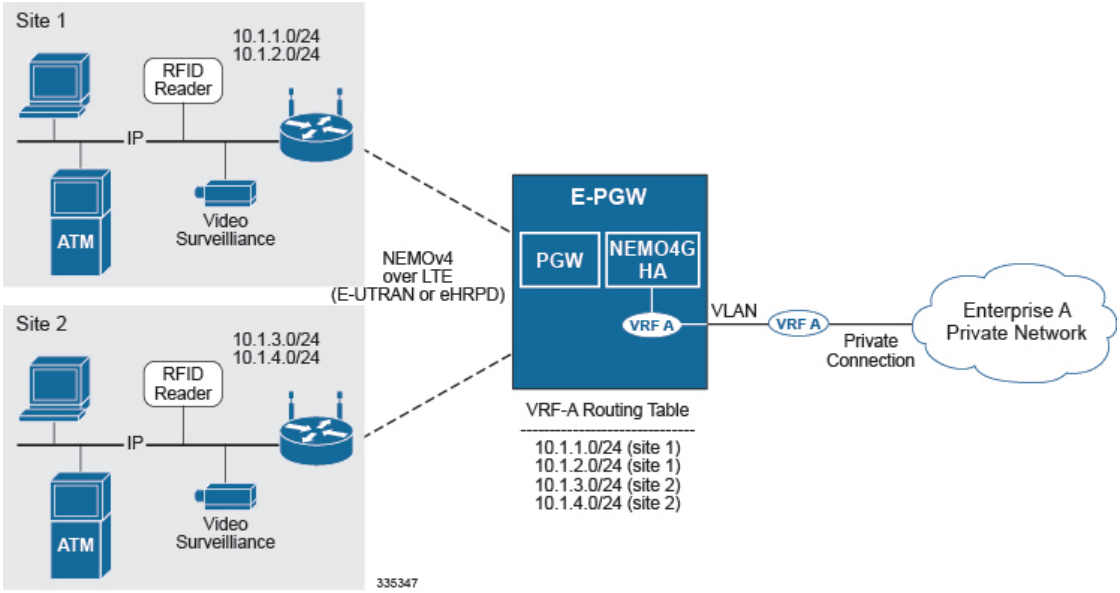
機能ライセンスキーを使用して有効にすると、システムには、P-GW プラットフォームにおけるモバイル IPv4 ネットワークモビリティ（NEMO-HA）の NEMO サポートが含められ、エンタープライズ PDN に接続するモバイルルータ（MR）からのモバイル IPv4 ベースの NEMO 接続が終端されます。NEMO 機能により、MR の背後にいるユーザーと固定ネットワークサイト上のユーザーまたはリソース間で、アプリケーションに依存しない双方向の通信が可能になります。

同じ NEMO4G-HA サービスとそのバインドされたループバック IP アドレスが、 NEMO 接続をサポートします。NEMO 接続の基盤となる PDN 接続は、GTP S5（4G アクセス）または PMIPv6 S2a（eHRPD アクセス）を介して行われます。

モバイルネットワークがマルチホームの場合、つまりモバイルネットワークとインターネットの間に複数のアタッチポイントがある場合は、複数 HA サービスの設定が必要です。

次の図は、LTE NEMOv4 アーキテクチャの概要を示しています。

図 *98 : NEMO* の概要



使用例

LTE の NEMO では、次のユースケースがサポートされています。

1. **固定**：モビリティを必要としないモバイルルータを使用する、分散拠点などのアプリケーション。
2. **移動**：サービス中には移動しないが、別の場所に移動してサービスを再開する可能性のある、モバイルルータを使用したアプリケーション（たとえば、ある日にモールに出店したキオスクが、翌日または翌月に別の場所に出店するなど）。
3. **移動可能**：公共安全車両など、移動および PDSN 境界の通過中に Dynamic Mobile Network Routing（DMNR）サービスの運用を維持する必要があるアプリケーション。サービスの持続性は、モビリティプロトコル（3G のモバイル IP や LTE の GTP）によって処理されます。

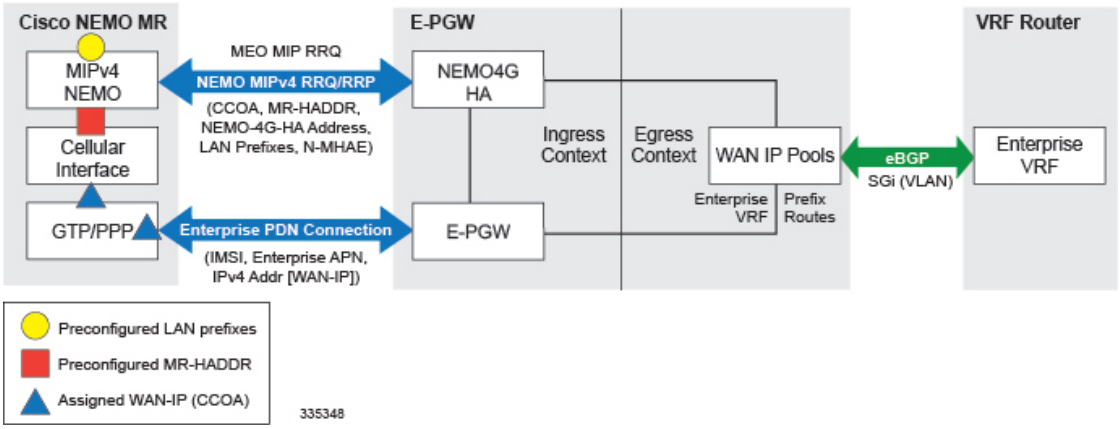
機能と利点

システムは、動的に学習された、重複した顧客プレフィックスの使用をサポートしています。これらのプレフィックスは BGP を介してアドバタイズされます。

MIPv4 ベース NEMO コントロールプレーン

次の図は、NEMO コントロールプレーンの概要を示しています。

図 *99 : NEMO* コントロールプレーン



NEMO には次の機能が含まれています。

- Collocated-Care-of-Address モード

  Cisco NEMO MR は、ユーザー トラフィック トランスポート用の NEMO GRE トンネルの IP エンドポイントの 1 つとして、NEMO4G-HA による NEMO MIPv4 セッションを確立するために、Collocated-Care-of-Address モードを使用することが想定されています。

- MR-HADDR

  NEMO4G-HA は、同じ企業内の、またはサービス対象となるすべての企業（同じ IP アドレス）内の全 MR で設定される、潜在的な「ダミー」の MR-HADDR アドレスをサポートしています。

- WAN-IP プールと学習済み LAN プレフィックスのダイナミック アドバタイズメント

  eBGP を使用して、エンタープライズ WAN-IP プール、および関連付けられた企業の NEMO を介して学習された LAN プレフィックスをアドバタイズします。

- N-MHAE ログイン情報

  NEMO4G-HA は、企業ごとに（同じ企業に属するすべての MR に対して 1 つの一意のセット）、またはグローバルベース（すべての企業に対して 1 つの一意のセット）で事前設定された N-MHAE-SPI/KEY 値に基づく NEMO MIPv4 RRQ のローカル認証をサポートします。

- LAN プレフィックス

  - NEMO4G-HA は、モバイルルータごとに最小 0 個の LAN プレフィックスと最大 8 個のプレフィックスを受け入れます。プレフィックスが 9 個以上のものはすべて、警告なしで破棄されます。

  - NEMO4G-HA は、任意のプレフィックス長（/32 を含む）をサポートします。

  - NEMO4G-HA は、動的なプレフィックス更新をサポートします。

    - NEMO4G-HA は、関連付けられたエンタープライズ VRF ルーティングテーブルから、特定の MR からのスケジュール済みまたはアドホック NEMO MIPv4 再登

録要求に含まれていないプレフィックスを削除します（これらのプレフィックスが以前のNEMO MIPv4 RRQに存在していたことを想定）。E-PGWは、次のeBGP更新で、このようなプレフィックスを削除された外部VRFルータを更新します。

- NEMO4G-HA は、スケジュール済みまたはアドホック NEMO MIPv4 再登録要求に含まれる新しいプレフィックスを承認し、MRごとにサポートされるプレフィックスの最大数（最大8）を超えない限り、関連付けられたエンタープライズVRFルーティングテーブルにインストールします。E-PGWは、次のeBGP更新で、新たにプレフィックスをインストールされた外部 VRF ルータを更新します。
  NEMO4G-HA は、最初の初期 RRQ でプレフィックスを含まない NEMO MIPv4 RRQ を受け入れ、後続の RRQ でアドバタイズされるプレフィックスを受け入れます。
- MR で IP アドレスまたはマスクが変更されたプレフィックスの場合、MR は古い IP アドレス/マスクを削除し、スケジュール済みまたはアドホック NEMO MIPv4 再登録要求で新しい IP アドレス/マスクプレフィックスを追加します。
  NEMO4G-HA は古いルートを削除し、新しいプレフィックスに対応する新しいルートをエンタープライズ VRF ルーティングテーブルに追加します。

- 重複 IP アドレッシング

  NEMO4G-HA は、WAN IP プール、MR-HADDR、および LAN プレフィックスについて、複数の企業間でのプライベートおよび重複 IP アドレッシングをサポートします。

NEMO MR 承認

NEMO4G-HAは、基礎となるPDN接続にNEMO権限が割り当てられている場合にのみ、NEMO MIPv4 セッションを承認します。NEMO 権限は、ローカル設定（APN パラメータ）を使用して、または PDN 承認中に 3GPP AAA によって割り当てられた NEMO permission AVP に基づいて、基礎となる PDN 接続に割り当てる必要があります。ローカル設定の場合、P-GW サービス内の APN/PDN レベルで NEMO 権限を有効にするために、新しい APN パラメータがサポートされます。

MIPv4 NEMO プロトコル

NEMO4G-HAは、MR NEMOクライアントから受信したモバイルIPv4 NEMO登録要求（RRQ）を処理します。

NEMO4G-HA は、MIPv4 NEMO RRQ に含まれる通常ベンダー/組織固有の拡張（NVSE）タイプの 3 つのシスコ固有 MIPv4 拡張の最初の処理を実行します。3 つのシスコ固有の NVSE は、MIPv4「識別」フィールドの後、必須 MIPv4「モバイルホーム認証拡張」の前に配置されます。NEMO4G-HA は、最初のシスコ固有の NVSE（ベンダータイプ = 9）でエンコードされた LAN プレフィックス（最大 8 つ）を受け入れます。NEMO4G-HA では、MR のローミングインターフェイスの内部インターフェイス ID と MR のローミングインターフェイス帯域幅をそれぞれ伝送する、ベンダータイプ = 49 である他の 2 つのシスコ固有 NVSE を処理することは想定されていません。

シスコ固有の NVSE は、RFC 3025「Mobile IP Vendor/Organization Specific Extensions」に準拠しています。

GRE のカプセル化

ユーザートラフィックは、MR NEMO クライアントと NEMO4G-HA 間の GRE トンネルでカプセル化する必要があります。GRE トンネルの IP エンドポイントは、エンタープライズ PDN 接続のセットアップ時に MR モデムに割り当てられた IPv4 と、E-PGW 上の NEMO4G-HA サービスの IPv4 アドレスである必要があります。

NEMO4G-HA は、関連付けられた SGi VLAN インターフェイスを介してエンタープライズ VPN に発信トラフィックを転送する前に、GRE カプセル化を解除する必要があります。同じ SGi VLAN インターフェイスを介して受信した着信トラフィックは、適切な GTP/PMIP トンネルを介して MR に転送するために E-PGW サービスに渡される前に、カプセル化してから GRE トンネルに送る必要があります。

セッションの相互作用

eHRPD または LTE アクセスを介して行われる、NEMO と基盤となる PDN の間の接続では、次のセッション相互作用シナリオがサポートされます。

次の状況では、NEMO4G-HA は関連付けられたプレフィックスルートをエンタープライズ VRF ルーティングテーブルから取り消し、eBGP ネイバーを更新し、基盤となる PDN 接続と NEMO セッションに割り当てられているすべての内部リソースを解放します。

- eHRPD が基盤となる PDN 接続を終了するとき（PPP-VSNCP-Term-Req が MR および PMIP-BU に送信され、lifetime = 0 が E-PGW に送信される）。
- MR が eHRPD を介してネットワークにアクセスしている状況で、PPP/PDN 接続を終了するとき。
- MR または MME によってeUTRAN（LTE）切断手順が開始された後。

NEMO MIPv4 RRQ（PMIPv6 または GTP）に関連付けられた基盤となる PDN 接続がない場合、NEMO4G-HA はこれらの RRQ を処理できません。つまり、NEMO MIPv4 RRQ は、モバイルルータによって E-PGW とエンタープライズ PDN の接続が確立されている場合にのみ受け入れられ、処理されます。

NEMO4G-HA は、各 NEMO MIPv4 RRQ に関連付けられている基盤となる PDN 接続に NEMO 許可が示されていない場合、NEMO MIPv4 RRQ をサイレントに無視します。これは、eHRPD と LTE の両方のアクセスに適用されます。

NEMO4G-HA は、ユーザーデータが NEMO4G-HA IP アドレスに宛てられていない場合、MIP または GRE トンネリング（それぞれ UDP/434 または IP プロトコル/47）を使用してこのようなデータを外部エンタープライズ VRF に転送します（ドロップしません）。これは、NEMO 許可が示されているかどうかにかかわらず、PDN 接続に適用されます。これは、eHRPD と LTE の両方のアクセスにも適用されます。

NEMO MIPv4 セッションの認証または承認のいずれかに障害が発生しても、eHRPD または LTE を介してモバイルルータと E-PGW の間で確立されている、基盤となる PDN 接続には影響を及

ぼしません。たとえば、MR NEMO クライアントと NEMO4G-HA の間でセキュリティクレデンシャルが一致しない場合、NEMO4G-HA は NEMO MIPv4 RRQ を拒否できますが、関連付けられた PDN 接続は終了しません。

NEMO セッションタイマー

MR が最大値（65534）を使用している場合でも、NEMO4G-HA はローカルに設定された登録ライフタイム値を使用します。

NEMO4G-HA は、アドホック NEMO RRQ メッセージを処理できます。

企業全体のルート制限制御

NEMO4G-HA は、特定の企業が登録できるプレフィックス/ルート（WAN IP 割り当て用のプールなど）の最大数を制限する制御メカニズムをサポートしています。

ルートの最大数に達すると、syslog メッセージが生成されます。ルート数が制限を下回ると、syslog メッセージが生成されて通知します。

強制フラグメンテーション

E-PGW は、DF ビットが設定された IP パケットであっても、IP パケットフラグメンテーションを強制します。

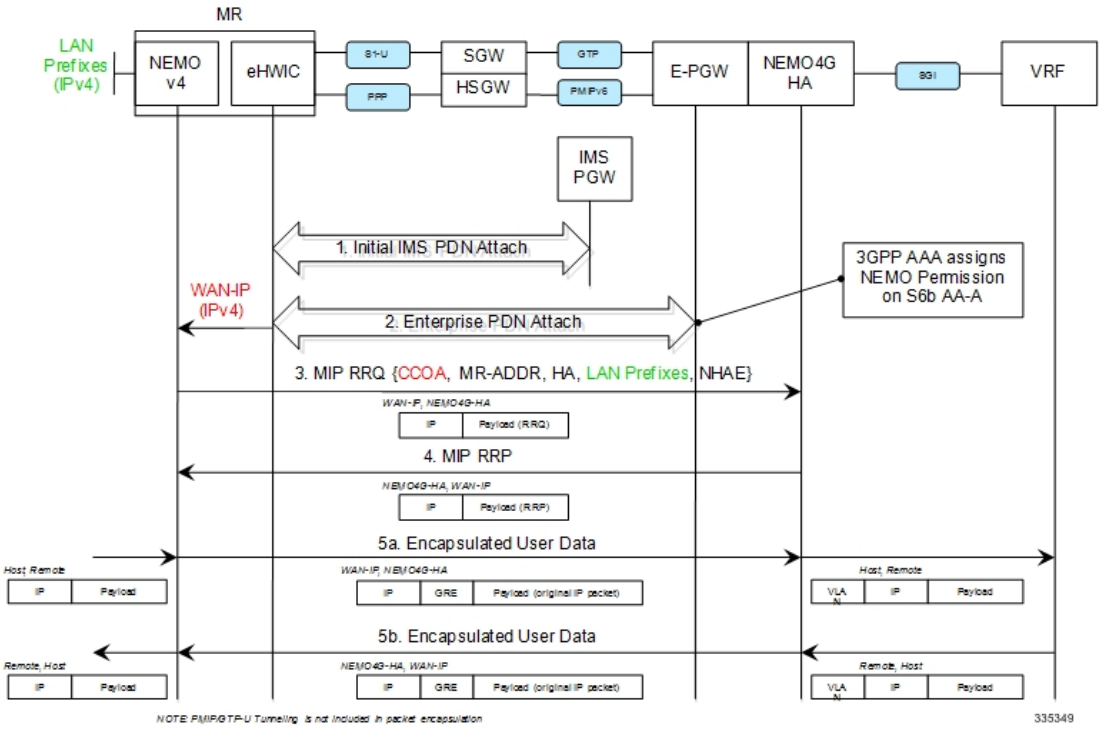
冗長性/信頼性

LTE NEMO ソリューションは、シャーシ内セッション冗長性（SR）およびシャーシ間セッション冗長性（ICSR）機能をサポートしています。

LTE NEMO コールフロー

次の図は、NEMOv4 ソリューションのコールフローを示しています。

図 *100 : NEMOv4* のコールフロー



1. Cisco MR eHWIC が、最初に IMS PDN への接続を確立して LTE ネットワークに登録します。正常に認証されるには、eHWIC のユーザー ID が HSS/SPR で適切にプロビジョニングされている必要があります。
2. Cisco MR eHWIC が、LTE ネットワークに登録され、IMS PDN への接続を確立した後に、ローカルに設定されたエンタープライズ APN に基づいて適切なエンタープライズ PDN に接続します。
   - S6b を使用した PDN 認証手順中に、3GPP AAA が、AVP を介して NEMO 権限を割り当てます。この AVP を E-PGW の APN パラメータとして使用して、PDN/エンタープライズレベルで NEMO サービスを許可することもできます。
   - E-PGW が、PDN 認証時に割り当てられたエンタープライズ IPv4 プールから、IPv4 アドレスを MR eHWIC に割り当てます。
   - E-PGW が、出力コンテキストの IPv4 プール設定を使用して、E-PGW プラットフォームの外部にある対応する VRF にパケットを転送するために、適切なフローを内部的に作成します。
   - MR eHWIC が、割り当てられた IPv4 アドレスで NEMO アプリケーションに渡されます（WAN-IPv4 アドレスとも呼ばれる）。
3. MR NEMO アプリケーションが、次のローカル設定と、エンタープライズ PDN アタッチ手順中に eHWIC に割り当てられた IPv4 アドレス（WAN-IP と呼ばれる）を使用して、モバイル IPv4 登録要求（RRQ）を開始します。NEMO MIPv4 RRQ が、モビリティ接続（LTE

の GTP、eHRPD の PPP/PMIPv6 のいずれか）を介して通常のユーザーパケットとして伝送されます。NEMO MIPv4 RRQ には、次の主要なパラメータが含まれます。

- CCOA：エンタープライズ PDN 接続のセットアップ（WAN-IP）中に eHWIC モデムに割り当てられる IPv4 アドレス。MR NEMO アプリケーションは、NEMO4G-HA に送信されるすべての NEMO パケット（制御およびトンネル ユーザー トラフィック）の送信元として CCOA/WAN-IP アドレスを使用します。
- MR-HADDR：MR NEMO アプリケーションで事前設定された必須の IPv4 アドレス。MR-HADDR は通常、NEMO4G-HA に送信されるすべての NEMO 制御パケットの送信元として使用されます。ただし、MR NEMO アプリケーションは、すべての NEMO パケット（制御およびトンネル ユーザー トラフィック）の送信元として CCOA を使用します。そのため、NEMO4G-HA は、RRQ に含まれる事前設定された MR-HADDR を無視しますが、NEMO MIPv4 RRP には引き続き含まれます。
- ホームエージェントアドレス：MR NEMO アプリケーションがすべての NEMO 制御および GRE トンネルユーザーデータの宛先として使用する事前設定された IPv4 アドレス（NEMO4G-HA の IPv4 アドレス）。
- 明示的な LAN プレフィックス：MR NEMO アプリケーションで事前設定された、ローカルにアタッチされる IPv4 ネットワーク。LAN プレフィックスは、3G 用の NEMO ソリューションで現在使用されているものと同じ Cisco NVSE 拡張機能でエンコードされます。NEMOv4 MIP RRQ に含まれる Cisco NVSE は、TLV の形式です。
- N-MHAE：事前共有キー（PSK）を使用して計算された SPI とオーセンティケータを含む、必須の NEMO MN-HA 認証拡張機能。SPI とキーの両方が、MR NEMO アプリケーションでも事前設定されています。
- NEMO トンネルフラグ。「Reverse Tunnel」、「Direct Termination」、「Tunnel Encapsulation」= GRE など（ただし、これらに限らない）。

4. NEMO4G-HA は、次のタスクを実行した後に、MR に MIP 登録応答（RRP）を送信します。
   - RRQ に含まれる N-MHAE 情報を使用して RRQ を認証します。
   - 関連するエンタープライズ PDN 接続に割り当てられた NEMO 権限属性に基づいて、NEMO サービスを承認します。
   - NEMO MIPv4 RRQ に含まれる Cisco NVSE 拡張機能でアドバタイズされたプレフィックスを受け入れます。
     - 学習されたプレフィックスは、有効なプールルートの現在のルールに従う必要があります。マスクの有効な最小長は /13 であり、プールルートに 0.0.0.0 または 255.255.255.255 を含めることはできません。
     - NEMO4G-HA は、最小 0 個のプレフィックス、最大 8 個のプレフィックスを受け入れます。プレフィックスが 9 個以上のものは、サイレントに破棄されます。
     - NEMO4G-HA は、結果として得られる新しいエンタープライズルート数（VRF ルートの合計数）が、特定のエンタープライズに対して設定されている可能性の

あるルート制限を超えないこともチェックします。事前設定されたルート制限を超えると、NEMO4G-HA は NEMO MIP RRQ を拒否します。それ以外の場合は、NEMO4G-HA が、受け入れられたプレフィックスを、エンタープライズ PDN に関連付けられた内部 VRF にインストールします。

- その後、eBGP は、次回の BGP 更新の一部として、新しい NEMO ルートを外部 VRF に伝達します。

5. NEMO MIP RRP を受信すると、MR は、ルーティングテーブルにデフォルトルート（0.0.0.0/0）をインストールして、LTE 接続を介してすべてのトラフィックをルーティングします。
   - アウトバウンドパケットは、トンネルの送信元として CCOA/WAN-IP アドレスを使用し、接続先として NEMO4G-HA-Service IPv4 アドレスを使用して、GRE を介してカプセル化されます。
   - NEMO4G-HA から MR NEMO アプリケーションのインバウンドパケットも、GRE を介してカプセル化されます。GRE トンネルの送信元は NEMO4G-HA-Service IPv4 アドレスであり、接続先は CCOA/WAN-IP アドレスです。

エンジニアリングルール

- BGP プロセスごとに複数の VRF にまたがる最大 5,000 のホストルート。シャーシあたり 6,000 のプールルートに制限されています。
- シャーシあたり最大 2,048 の VRF。

サポートされる標準

- IETF RFC 3025（2001 年 2 月）「Mobile IP Vendor/Organization Specific Extensions」
- IETF RFC 1191（1990 年 11 月）「Path MTU Discovery」

NEMO 設定



重要 この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンドや、キーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

NEMO に対応するようにシステムを設定するには、次の手順を実行します。

1. 「VRF の作成」の設定例を適用して、ルータで VRF を作成し、VRF-ID を割り当てます。VRF を作成します （1167 ページ）
2. 「ネイバーとアドレスファミリの設定 （1167ページ）」の設定例を適用して、ルーティング情報をピアルータと交換するようにネイバーとアドレスファミリを設定します。
3. 「接続済みルートの再配布 （1167ページ）」の設定例を適用して、接続済みのルートをルーティングドメイン間で再配布します。
4. 「APN プロファイルでの NEMO の設定と有効化 （1168 ページ）」の例を適用して、P-GW が NEMO サービスを使用できるようにします。
5. 「NEMO HA の作成 （1168 ページ）」の例を適用して、NEMO HA を作成します。
6. EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

設定例

```
configure
  context <egress_context_name>
  interface <interface_name_outbound>
    ip address <ipv4_address> <ipv4_mask>
    exit
  ip vrf <vrf_name>
  ip vrf-list first-list permit vrf <vrf_name>
  mpls bgp forwarding
  ip pool <pool_name> <pool_address> private vrf <vrf_name>
  nexthop-forwarding-address <ip_address> overlap vlanid <vlan_id>
  router bgp <as_number>
    neighbor <ip_address> remote-as <as_number>
    timers bgp keepalive-interval <seconds> holdtime-interval <seconds>
    address-family <type>
      redistribute connected
    #exit
    address-family <type>
      neighbor <ip_address> activate
      neighbor <ip_address> send-community both
    #exit
    ip vrf <vrf_name>
      route-distinguisher <asn_value> <rd_value>
      route-target both <asn_value> <rt_value>
    #exit
    address-family address-family ipv4 vrf <vrf_name>
      redistribute connected
    #exit
  #exit
  apn <apn_name>
```

```
    permission nemo
    ip context-name <egress_context_name>
    ip address pool name <pool_name>
    exit
  exit
  context <inress_context_name>
    interface <interface_name_inbound>
      ip address <ipv4_address> <ipv4_mask>
      exit
    ha-service <ha_service_name>
      mn-ha-spi spi-number <spi_number> encrypted secret <enc_secret>
      authentication mn-aaa noauth
      encapsulation allow keyless-gre
      bind address <ip_address>
      end
```

CLI およびキーワード/変数の詳細については、『*Command Line Interface Reference*』を参照してください。

VRF を作成します

最初にルータで VRF を作成し、VRF-ID を割り当てるには、次の例を使用します。

```
configure
  context <context_name> -noconfirm
    ip vrf <vrf_name>
    ip pool <pool_name> <pool_address> private vrf <vrf_name>
    nexthop-forwarding-address <ip_address> overlap vlanid <vlan_id>
    end
```

ネイバーとアドレスファミリの設定

ピアルータとルーティング情報を交換するネイバーおよびアドレスファミリを設定するには、次の例を使用します。

```
configure
  context <context_name>
    ip vrf <vrf_name>
      router bgp <as_number>
      ip vrf <vrf_name>
        neighbor <ip_address> remote-as <AS_num>
        address-family <type>
        neighbor <ip_address> activate
        end
```

接続済みルートの再配布

ルーティングドメイン間で接続されているルートを再配布するには、この例を使用します。

```
configure
  context <context_name>
    ip vrf <vrf_name>
      router bgp <as_number>
      ip vrf <vrf_name>
        address-family <type> vrf <vrf_name>
          redistribute connected
          end
```

APN プロファイルでの NEMO の設定と有効化

この例を使用して、APN プロファイルで NEMO を設定して有効にします。

```
configure
  context <context_name>
    apn <apn_name>
      permission nemo
      ip context-name <name>
      ip address pool name <pool_name>
      end
```

NEMO HA の作成

NEMO HA を作成するには、この例を使用します。

```
configure
  context <context_name>
    ha-service <ha_service_name>
      mn-ha-spi spi-number <number> encrypted secret <enc_secret>
      authentication mn-aaa noauth
      encapsulation allow keyless-gre
      bind address <ip_address>
      end
```

モニタリングおよびトラブルシューティング

ここでは、ネットワークモビリティのモニタリングと障害対応に使用できる CLI コマンドについて説明します。

モニタープロトコル

monitor protocol コマンドを使用する場合は、オプション 26 を有効にして、すべての NEMO メッセージを表示します。

show コマンドと出力

ここでは、ネットワークモビリティをサポートするために使用可能な show CLI コマンドについて説明します。

- **show ha-service all**：このコマンドを使用して、設定済みの HA サービスに関する情報を表示し、このサービス用に設定された CLI のすべての主要パラメータを使用してサービスが開始されていることを確認します。

（注） IP VRF 設定が行われているコンテキストから以下の show コマンド CLI を使用します。次の例では CLI はコンテキスト出力用です。

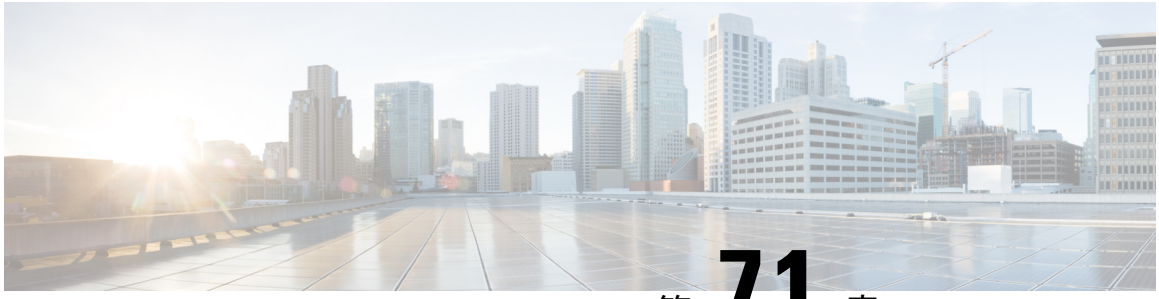
次の出力に示されているように、割り当てられたプレフィックスとルートに関する情報を表示するには、次のコマンドを使用します。

```
show ip bgp vpnv4 vrf <vrf-name>:
Network         Next Hop   Metric  LocPrf   Weight  Path
*> 15.1.1.0/32   0.0.0.0   0              32768  ?
*> 15.1.1.1/32   0.0.0.0   0              32768  ?
*> 15.1.1.2/32   0.0.0.0   0              32768  ?
*> 15.1.1.3/32   0.0.0.0   0              32768  ?
*> 15.1.1.4/32   0.0.0.0   0              32768  ?
*> 15.1.1.5/32   0.0.0.0   0              32768  ?
*> 15.1.1.6/32   0.0.0.0   0              32768  ?
*> 15.1.1.7/32   0.0.0.0   0              32768  ?
*> 80.240.0.0/20 0.0.0.0      0              32768  ?
*> 192.168.232.0/24 31.100.101.1    0        0     2000 ?

show ip route vrf <vrf-name>:
Destination   Nexthop  Protocol  Prec  Cost Interface
*15.1.1.0/32   0.0.0.0  connected   0        0
*15.1.1.1/32   0.0.0.0  connected   0        0
*15.1.1.2/32   0.0.0.0  connected   0        0
*15.1.1.3/32   0.0.0.0  connected   0        0
*15.1.1.4/32   0.0.0.0  connected   0        0
*15.1.1.5/32   0.0.0.0  connected   0        0
*15.1.1.6/32   0.0.0.0  connected   0        0
*15.1.1.7/32   0.0.0.0  connected   0        0
*80.240.0.0/20   0.0.0.0  connected   0       0 pool cust101-a
*192.168.232.0/24 31.100.101.1   bgp        20      0 19/1-sub101 (nhlfe-ix:8)

show mipha full all
MSID: -
Home Address: XX.XX.XX.XX  HA Address: XXX.XXX.XXX.X
Total Prefix: 16   Multi-VRF: NO
VRF #1: vrf-cust101   CtxtID: 0x43 GRE: 0x0
15.1.1.0/32    15.1.1.1/32
15.1.1.2/32    15.1.1.3/32
15.1.1.4/32    15.1.1.5/32
15.1.1.6/32    15.1.1.7/32
15.1.1.8/32    15.1.1.9/32
15.1.1.10/32    15.1.1.11/32
15.1.1.12/32    15.1.1.13/32
15.1.1.14/32    15.1.1.15/32
Send NAI Extension in Revocation Message: NO
Binding #1:  Care of Address: XX.XXX.X.XX
  FA Address/Port: XX.XXX.X.XX/XXX
  Lifetime: 00h01m15s   Remaining Life: 00h00m26s
  Reverse Tunneling: On   Encapsulation Type: Keyless-GRE
  GRE Key(Fwd): n/a   IPSec Required: No
  GRE Key(Rev): n/a
  IPSec Ctrl Tunnel Estab.:No  IPSec Data Tunnel Estab.: No
  Revocation Negotiated: NO  Rev I Bit Negotiated: NO
```

```
Colocated COA: YES   NAT Detected: NO
MN-HA-Key-Present: TRUE  MN-HA-SPI: 256
FA-HA-Key-Present: FALSE  FA-HA-SPI: n/a
HA-RK-KEY-Present: FALSE  HA-RK-SPI: n/a
HA-RK-Lifetime: n/a   HA-RK-Remaining-Lifetime: n/a
```



第 71 章

NEMO-LMA ハートビート

- 機能情報 （1171 ページ）
- 機能説明 （1172 ページ）
- 機能の仕組み （1172 ページ）
- NEMO-LMA ハートビートの設定 （1173 ページ）
- NEMO-LMA ハートビートのモニタリングと障害対応 （1173 ページ）

機能情報

要約データ

[ステータス（Status）]	新機能
導入されたリリース	21.2
変更されたリリース	該当なし
対象製品	P-GW
該当プラットフォーム	ASR 5500
デフォルト設定	無効
関連する CDETS ID	CSCuw08182
このリリースでの関連する変更点	LMA での NEMO PMIPv6 ハートビート（SAEGW）
関連資料	Command Line Interface Reference P-GW Administration Guide SAEGW Administration Guide

マニュアルの変更履歴

重要　リリース 21.2 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

機能説明

モバイルルータ（MR）とネットワークモビリティ-ローカルモビリティアンカー（NEMO-LMA）間のハートビートメッセージによる経路管理メカニズムは、ピアの可用性を認識し、障害を検出し、ノード障害から回復した場合にピアに迅速に通知し、ピアが適切なアクションを実行できるようにするために重要です。

機能の仕組み

MR と LMA は、定期的にハートビートメッセージを交換して、それらの間の可用性のステータスを検出します。NEMO-LMA は、ハートビート要求メッセージを送信して、MR とのハートビート交換を開始し、MR が到達可能かどうかを確認します。NEMO-LMA は、最後のハートビート要求メッセージのシーケンス番号を記録し、対応するハートビート応答との照合に使用します。NEMO-LMA は、対応するピアとの PMIPv6 セッションがあるかどうかに関係なく、ハートビート要求メッセージに対してハートビート応答メッセージで応答します。

バインドエラー

ハートビート要求メッセージへの応答で、ステータスが 2 に設定されたバインディングエラーメッセージを受信すると、以降 NEMO-LMA は、対応するピアとのハートビートメッセージを使用しません。

障害の検出

設定可能なパラメータ **max-heartbeat-retransmission** <*value*> **exceed-action drop-session** に対するハートビート応答を LMA ノードが受信しない場合、NEMO-LMA はピアが到達不能であると判断します。結果として、ピアへのハートビート要求は停止され、NEMO-LMA セッションがトラップなしでクリアされます。

再起動の検出

再起動カウンタの値が以前に受信した値と異なる場合は、ピアが一旦クラッシュし、その後回復したと見なされます。その結果、既存の NEMO-LMA セッションがクリアされます。

ライセンス要件

NEMOを使用するには、有効なライセンスキーがインストールされている必要があります。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

NEMO-LMA ハートビートの設定

トラップを生成せずにNEMO-LMAセッションをクリアするには、LMAサービス 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。

```
configure
  context context_name
    lma-service service_name
      heartbeat retransmission max number [ exceed-action drop-session
 ]
       end
```

注：

- **retransmission max**：ハートビート再送信の許容最大数。*number* は 0 ～ 15 の整数です。デフォルト：3
- **exceed-action**：ハートビート再送信の最大数に達した後に実行されるアクションを指定します。
- **drop-session**：経路障害が検出されたときにセッションをドロップするために使用されます。
- **exceed-action** および **drop-session** キーワードは NEMO-LMA セッションでのみ有効であり、ハートビート機能が有効になっている場合に機能します。

NEMO-LMA ハートビートのモニタリングと障害対応

以下では、機能をモニターまたはトラブルシュートするために使用できるコマンドを説明します。

monitor protocol コマンドを入力して、Exec モードでプロトコルモニターを起動します。

monitor protocol コマンドを使用する場合は、オプション **48** を有効にして、ハートビート要求とハートビート応答のメッセージをモニターしてください。

show lma-service statistics

ハートビートメッセージ関連の統計を表示するには、このコマンドを使用します。生成される出力は次のように表示されます。

```
Total Disconnects:          1
   Lifetime expiry:         0      Deregistrations:     0
      Admin Drops:          0      Path Failure Drops:  1
      Other Reasons:        0
```

show session disconnect-reasons

このコマンドを使用して、ハートビートパスの障害が原因で切断されたコールを確認します。生成される出力は次のように表示されます。

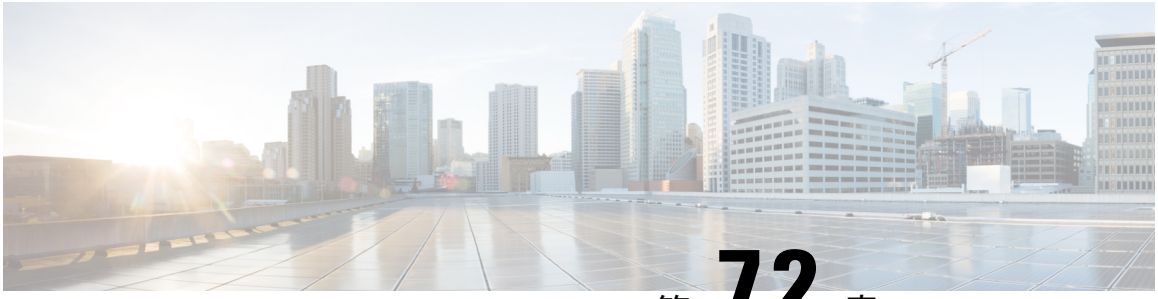
```
mme-guti_realloc_failed-detach(615)          0        0.00000
mme-pcscf-rest-detach(616)                   0        0.00000
Reject-ho-old-tun-path-failure(617)          0        0.00000
mip-path-failure(618)                        0        0.00000
```

バルク統計

LMA スキーマ

この機能をサポートするために、次の新しいバルク統計変数が LMA スキーマに追加されています。

- lma-pathfailsessionscleared：NEMO-LMA ハートビート機能のパス障害/再起動カウンタの値が変化した場合、セッション切断カウンタが増加します。



第 72 章

ネットワーク サービス ヘッダー（NSH）

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （1175 ページ）
- 機能説明 （1176 ページ）
- 機能の仕組み （1176 ページ）
- NSH フレームワークのサポートの設定 （1178 ページ）
- コマンドと出力の表示 （1185 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	有効、常時オン
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、トラフィックステアリングによる NSH ベースのトラフィック識別がサポートされています。	21.9
最初の導入。	21.4

機能説明

基盤となっているトランスポートプロトコルに依存しない専用のサービスプレーンを作成するために、新しいサービスチェーンプロトコルであるネットワーク サービス ヘッダー（NSH）が追加されています。一般に、NSH では、宛先アドレスに到達する前にパケットがルーティングされる一連のサービスノードを記述します。NSH には、IP パケット内のパケットとサービスチェーンに関するメタデータ情報が含まれます。NSH プロトコルにより、さまざまなサービス機能をゲートウェイの外部に展開するという増大する要件に対処できます。

この機能により、P-GW および SAEGW 製品に NSH プロトコルのサポートが導入され、次のものがサポートされます。

- P-GW/SAEGW での NSH 形式のエンコードおよび復号化。
- エンコードのために変数ヘッダーに含まれる設定可能なパラメータ。
- 設定に基づく選択的なトラフィックの NSH 処理。
- 変数ヘッダーに存在するパラメータのタグ値の設定。
- NSH で受信したデコードパラメータに基づいて機能するポリシーの選択的設定。
- フローのすべてのパケットで、またはフローごとに 1 回だけ、NSH 情報をエンコードするインテリジェンスの設定。
- トラフィックステアリングによる NSH ベースのトラフィック識別。

重要 このリリースでは、パラメータの選択的暗号化はサポートされていません。

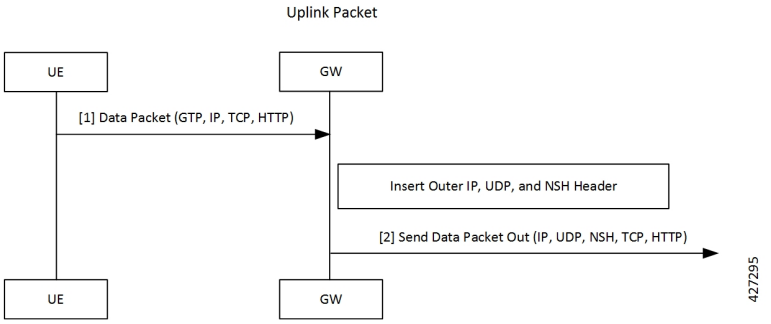
機能の仕組み

このセクションでは、シスコの P-GW/SAEGW 製品における NSH プロトコルサポートの仕組みについて説明します。

- **アップリンクパケット**

アップリンクパケットでは、指定された基準とフローが一致する場合、P-GW/SAEGW が NSH を追加します。NSH には可変長のコンテキストヘッダーも含まれています。

次のコールフローは、シスコの P-GW/SAEGW 製品におけるアップリンクパケットに対する NSH プロトコルのサポートを示しています。

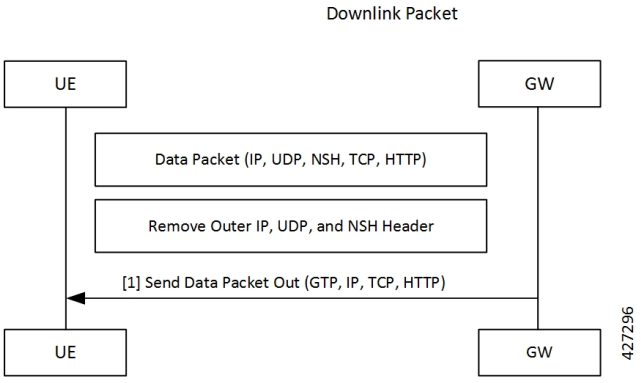


アップリンクパケットでは、コールフローが指定された基準に一致する場合、P-GW または SAEGW がデータパケットに NSH ヘッダーを追加します。NSH ヘッダーには、可変長のコンテキストヘッダーが含まれている場合があります。設定で指定されている場合は暗号化できます。

- **ダウンリンクパケット**

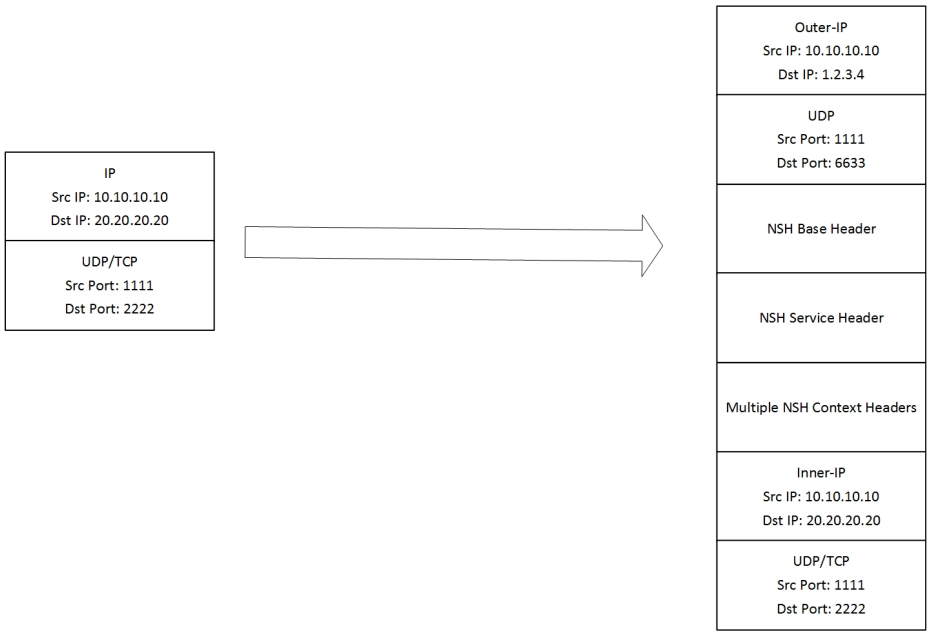
  ダウンリンクパケットの場合、P-GW/SAEGW は、NSH を処理して削除し、抽出された NSH パラメータに基づいてポリシーを適用します。

  次のコールフローは、シスコの P-GW/SAEGW 製品におけるダウンリンクパケットに対する NSH プロトコルのサポートを示しています。



  ダウンリンクパケットの場合、P-GW または SAEGW は NSH ヘッダーを処理して削除します。その後、P-GW または SAEGW は、抽出された NSH パラメータに基づいてポリシーを適用します。

- 外部 IP パケットの送信元および宛先 IP アドレスは、内部 IP パケットから取得されます。
- デフォルトでは、NSH カプセル化パケットはポート番号 6633 を使用します。



NSH フレームワークのサポートの設定

ここでは、NSHフレームワークのサポートを追加するためにこの機能で使用する設定手順について説明します。

課金アクションの関連付け

サービスチェーンは、次の方法で課金アクションに関連付けられます。

```
configure
  active-charging service service_name
    charging-action charging_action_name
      service-chain service_chain_name
      end
```

注：

- **charging-action**：課金アクションを定義します。

  charge_action_name：課金アクションの名前を指定します。1 ～ 64 文字の英数字で入力します。

- **service-chain**：サービスチェーンの関連付けを定義します。

  service_chain_name：サービスチェーンの名前を指定します。1 ～ 64 文字の英数字で入力します。

サービスチェーンの関連付け

サービスチェーンの関連付けのために、新しい CLI コマンド **nsh-format** が **service-chain** コマンドに追加されました。

```
configure
   service-chain <service_chain_name>
      nsh-format <nsh_format_name>
      end
```

注：

- **service-chain**：サービスチェーンの関連付けを定義します。

  service_chain_name：サービスチェーンの名前を指定します。1 ～ 64 文字の英数字で入力します。

- **nsh-format**：NSH 形式をサービスチェーンに関連付けます。

サービススキームの関連付け

ACS サービススキーム構成モードへの **trigger** コマンドに、新しい CLI コマンド **nsh-response-received** が加されました。

```
configure
  active-charging service service_name
     service-scheme service_scheme_name
        [ no ] trigger { bearer-creation | flow-create | loc-update |
nsh-response-received | sess-setup }
       end
```

注：

- **service-scheme**：サブスクライバクラスに基づいたサービススキームの関連付けを有効にします。

  service_scheme_name：サービススキームの名前を指定します。1 ～ 64 文字の英数字で入力します。

- **no**：service-scheme のトリガーアクションを無効にします。
- **trigger**：service-scheme のトリガーアクションを指定します。
- **Bearer-creation**：すべての新しいベアラーでトリガーします。
- **flow-create**：すべての新しいフローでトリガーします。
- **loc-update**：サブスクライバのロケーションが変更されるたびにトリガーします。
- **nsh-response-received**：NSH 応答パケットでトリガーします。
- **sess-setup**：セッションのセットアップでトリガーします。

NSH コンフィギュレーション モード

Network Services Header（NSH）コンフィギュレーション モードは、NSH コンフィギュレーション モードのサブモードです。この NSH モードは、NSH のエンコードまたは復号化に使用されます。

[Exec] > [Global Configuration] > [Network Service Entity - IP Configuration]

```
configure
   nsh
   end
```

上記のコマンドシーケンスを入力すると、次のプロンプトが表示されます。

[local]host_name(nsh)#

NSH フィールド コンフィギュレーション モード

NSH フィールド コンフィギュレーション モードは、NSH コンフィギュレーション モードのサブモードです。この NSH フィールド コンフィギュレーション モードは、NSH フィールドに値をタグ付けするために使用されます。

[Exec] > [Global Configuration] > [Network Service Header] > [Network Service Header - Fields Configuration]

```
configure
   nsh
     nsh-fields fields_name
     end
```

上記のコマンドシーケンスを入力すると、次のプロンプトが表示されます。

[local]host_name(nsh-nshfields)#

tag-value

NSH フィールド コンフィギュレーション モードに追加されたこの新しい CLI コマンドは、NSH フィールドにタグ値を関連付けるために使用できます。

```
configure
  nsh
    nsh-fields fields_name
       tag-value tag_value { content-type | enterprise-id | imei | imsi
 | msisdn | rating-group | rulebase | tdf-app-id }
       end
```

注：

- **nsh-fields**：NSH フィールドのタグ値を定義します。

  fields_name：*nsh-field* の名前を指定します。1 ～ 64 文字の英数字で入力します。

- **tag-value**：タグをフィールドに関連付けます。

  tag_value ：NSH フィールドのタグ値。

- **content-type**：コンテンツタイプを指定します。
- **enterprise-id**：NSH コンテキストヘッダーで送信する企業 ID を指定します。
- **imi**：サブスクライバの IMEI を指定します。
- **imsi**：サブスクライバの IMSI を指定します。
- **msisdn**：サブスクライバの電話番号を指定します。
- **rating-group**：トラフィックに適用する評価グループを指定します。
- **rulebase**：サブスクライバのルールベースを指定します。
- **tdf-app-id**：トラフィックに適用する TDF アプリケーション ID を指定します。

NSH 形式コンフィギュレーション モード

NSH 形式コンフィギュレーション モードは、NSH コンフィギュレーション モードのサブモードです。この NSH 形式モードは、NSH のエンコードまたはデコードに使用されます。

[Exec] > [Global Configuration] > [Network Service Header] > [Network Service Header - Format]

```
configure
   nsh
     nsh-format format_name
     end
```

上記のコマンドシーケンスを入力すると、次のプロンプトが表示されます。

[local]host_name(nsh-nshformat)#

encode

この新しいCLIコマンドは、NSH形式構成モードに追加されています。このコマンドは、NSH形式に関連付ける NSH エンコーディングフィールドを定義します。

```
configure
  nsh
    nsh-format format_name
      encode nsh-fields fields_name
      end
```

注：

- **nsh-format**：NSH ヘッダーの形式を定義します。

  format_name：NSH 形式の名前を指定します。1 ～ 64 文字の英数字で入力します。

- **encode**：エンコード用の nsh フィールドを関連付けます。

- **nsh-fields**：nsh フィールドのタグ値を定義します。

  fields_name：フィールドの名前を指定します。1 ～ 64 文字の英数字で入力します。

encoding-frequency

このコマンドは、NSH 形式に関連付ける NSH フィールドのエンコーディング頻度を定義します。

```
configure
  nsh
     nsh-format format_name
        encoding-frequency { always | once-per-flow }
        end
```

注：

- **encoding-frequency**：nsh-fields のエンコーディング頻度を定義します。
- **always**：ヒットするたびに NSH フィールドをエンコードします。
- **nce-per-flow**：フローごとに 1 回、NSH フィールドをエンコードします。

decode

このコマンドは、NSH 形式に関連付けられる NSH デコードフィールドを定義します。

```
configure
  nsh
     nsh-format format_name
        decode nsh-fields fields_name
        end
```

注：

- **nsh-format**：NSH ヘッダーの形式を定義します。

  format_name：*NSH* 形式の名前を指定します。1 ～ 64 文字の英数字で入力します。
- **decode**：デコード用の NSH フィールドを関連付けます。
- **nsh-fields**：nsh フィールドのタグ値を定義します。

  fields_name：フィールドの名前を指定します。1 ～ 64 文字の英数字で入力します。

トリガー条件コンフィギュレーション モード コマンド

content-type

このコマンドにより、照合するコンテンツタイプが指定されます。

```
configure
  active-charging service service_name
    trigger-condition trigger_condition_name
      content-type { operator condition }
      end
```

注：

- **trigger-condition**：ACS のトリガー条件を定義します。

  trigger_condition_name：トリガー条件の名前を指定します。1 ～ 64 文字の英数字で入力します。

- **content-type**：コンテンツタイプを指定します。
- **operator** ：照合方法を指定します。演算子は、次のいずれかにする必要があります。
  - **!=**：等しくない
  - **!contains**：含まない
  - **!ends-with**：次で終了しない
  - **!starts-with**：次で始まらない
  - **=**：等しい
  - **contains**：含む
  - **ends-with**：次で終了する
  - **started-with**：次で始まる
- **condition**：照合する条件を指定します。条件は次のいずれかにする必要があります。
  - FALSE
  - TRUE

tdf-app-id

このコマンドは、照合されるアプリケーションベースのルールの識別子を指定します。

```
configure
  active-charging service service_name
    trigger-condition trigger_condition_name
      tdf-app-id { operator condition }
      end
```

注：

- **trigger-condition**：ACS のトリガー条件を定義します。

trigger_condition_name：トリガー条件の名前を指定します。1 ～ 64 文字の英数字で入力します。

- **tdf-app-id**：アプリケーションベースのルールの識別子を指定します。
- **operator condition**：照合方法を指定します。演算子は、次のいずれかにする必要があります。
  - **!=**：等しくない
  - **!contains**：含まない
  - **!ends-with**：次で終了しない
  - **!starts-with**：次で始まらない
  - **=**：等しい
  - **contains**：含む
  - **ends-with**：次で終了する
  - **started-with**：次で始まる
- **condition**：照合する条件を指定します。条件は次のいずれかにする必要があります。
  - FALSE
  - TRUE

NSH 作成の設定例

次に、この NSH サービス作成の設定例を示します。

```
config
       nsh
         nsh-fields xyz
            tag-val 1 imei
            tag-val 2 imsi
        exit
         nsh-fields abc
            tag-val 4 content-type
        exit
        nsh-format format1
            encoding frequency always
            encode nsh-fields xyz
            decode nsh-fields abc
         exit
    exit
  traffic-steering
  appliance-group firewall
   nsh-format format1
   ip address 1.2.3.4
  #exit
 #exit
 service-chain sch1
```

```
  sfp direction uplink service-index 1 appliance firewall
 #exit
 exit
config
    active-charging service ACS
        trigger-action ta1
           throttle-suppress
        exit
        trigger-condition tc1
           content-type contains text
        exit
        service-scheme scheme1
            trigger nsh-response-received
                priority 1 trigger-condition tc1 trigger-action ta1
            exit
        exit
        subs-class class1
            any-match = TRUE
        exit
        subscriber-base base1
            priority 1 subs-class class1 bind service-scheme scheme1
        exit
       charging-action ca1
           service-chain xyz
       exit
    exit
exit
```

コマンドと出力の表示

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show nsh statistics

このリリースでは、nsh 統計を表示するためにこのコマンドが新たに追加されました。このコマンドを実行すると、次の出力が表示されます。

```
Total Encap Successful                :         0
Total Decap Successful                :         0

Total Encap Failed                    :         0
   Memory Allocation                  :         0
   Config Error                       :         0
   Encryption Failed                  :         0

Total Decap Failed                    :         0
   Config Error                       :         0
   Base Header
      Invalid Length                  :         0
      Unsupported Version             :         0
      Unsupported Next Protocol       :         0
      Next Protocol Mismatch          :         0
      Unsupported MD-Type             :         0
   Context Header
      Unsupported MD-Class            :         0
      Unsupported Type                :         0
```

```
OAM Packets
   Received                          :          0
   Dropped                           :          0

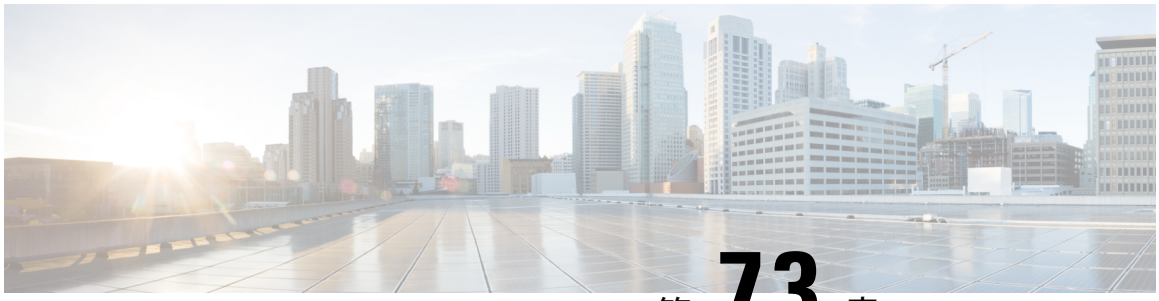
Unknown Context Header Type          :          0
```

show active-charging trigger-condition statistics

このコマンドの出力には、この機能の次のフィールドが含まれます。

- NSH-Rsp-Rcvd

このフィールドには、NSH 応答に基づくトリガー条件の一致が表示されます。



第 73 章

過課金保護のサポート

この章では、過課金保護サポート機能とその設定方法について説明します。製品アドミニストレーションガイドには、システム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、『*P-GW Administration Guide*』、『*S-GW Administration Guide*』、または『*SAEGW Administration Guide*』の説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

この章は、次の項で構成されています。

- 過課金保護機能の概要 （1187 ページ）
- ライセンス （1188 ページ）
- 過課金保護機能の設定 （1188 ページ）
- モニタリングおよびトラブルシューティング （1190 ページ）

過課金保護機能の概要

過課金保護は、UE がアイドルモードの間にドロップされたダウンリンクパケットのサブスクライバへの課金を回避するのに役立ちます。一部の国では、このような過課金を避けることが規制上の要件となっているため、そのような国の通信事業者には必須の機能となります。全体として、この機能は、サブスクライバがアイドルモードのときにサブスクライバが過課金にならないようにするのに役立ちます。



重要 この機能は、P-GW および S-GW でサポートされています。過課金保護は、SAEGW が Pure P または Pure S 機能用に設定されている場合にのみ SAEGW でサポートされます。

P-GW は UE の状態（アイドルまたは接続モード）を認識しません。ダウンリンクデータの課金は、UE がアイドルモードの場合でも、P-GW で適用されます。バッファオーバーフローまたはページングの遅延が原因で、UEがアイドルモードになっている場合、UEのダウンリンクデータが S-GW でドロップされることがあります。したがって、P-GW は、ドロップされたパケットの料金をサブスクライバに課金しますが、これは望ましくありません。この問題に対処するために、過課金保護機能を有効にすることで、S-GW は、S-GW でドロップされたパケッ

トおよびUEのアイドル状態からアクティブ状態への遷移に基づいて、課金を停止または再開するよう P-GW に通知します。

S-GW は、過課金保護機能をサポートしている場合、通知 IE で PDN Pause Support Indication フラグを 1 に設定した CSReq を P-GW に送信します。

P-GW は、過課金保護機能をサポートしている場合、通知 IE で PDN Pause Support Indication フラグを 1 に設定した CSRsp を P-GW に送信します。

「課金停止」をシグナリングする基準が満たされると、S-GWは、ベアラー変更要求（MBReq）を P-GW に送信します。PDN に対して MBReq が送信され、S-GW でドロップされるパケットが指定されます。MBReq には、「課金停止」および「課金開始」通知を P-GW に送信するための通知 IE および/または新しいプライベート拡張 IE があります。課金の一時停止/開始の手順（S-GW が MBReq を送信）では、P-GW からの MBRes には、過課金保護情報を含む通知 IE および/またはプライベート拡張 IE が含まれます。

PDN の S-GW から課金停止を含む MBReq を受信すると、P-GW はダウンリンクパケットの課金を停止しますが、S-GW へのパケットの送信は続行します。

P-GW は、次のいずれかの条件が満たされると、ダウンリンクパケットの課金を再開します。

- （以前に MBReq で「stopcharge」を送信していた）S-GW が、MBReq で「startcharge」を送信したとき。
- S-GW が変更された場合（これは、UE が新しい S-GW に再配置された可能性があることを示します）。

この機能は、3GPP TS 29.274：「3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C)」仕様に準拠しています。

重要 過課金保護機能が P-GW サービスと APN の両方で設定されている場合、APN での設定が優先されます。

ライセンス

過課金保護はライセンスが有効な機能です。P-GW 機能の過課金保護に新しいライセンスキーが導入されました。

重要 ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

過課金保護機能の設定

ここでは、P-GW および S-GW. で過課金保護サポートを設定する方法について説明します。

P-GW での過課金サポートの設定

このコマンドは、この APN プロファイルによって制御される APN の過課金保護を有効にし、無線カバレッジの損失中に一時的に課金しないことで過課金保護を設定します。各過課金保護オプションはスタンドアロンの設定であり、以前のオプションセット（存在する場合）をオーバーライドすることはありません。このコマンドを使用して、異常な S1 リリース、DDN 障害通知の発生時、またはドロップされたパケット数またはバイト数が設定された制限を超えた場合に、課金を一時停止するよう P-GW に指示します。



重要　この設定シーケンスは、P-GW でのみ有効です。

```
configure
   apn-profile apn_profile_name
      overcharge-protection { abnormal-s1-release | ddn-failure |
drop-limit drop_limit_value { packets | bytes } }
      [ remove ] overcharge-protection { abnormal-s1-release |
ddn-failure | drop-limit }
      end
```

注：

- **remove:**

  指定された設定を削除します。

- **abnormal-s1-release:**

  （将来の使用に備えて）過課金保護が異常な S1 リリースに対して有効になっている場合、S-GW は、無線リンク信号の異常なリリースが MME から発生した場合に、P-GW で課金が一時停止されるように MBR を送信します。

- **ddn-failure:**

  過課金保護が ddn-failure メッセージに対して有効になっている場合は、MME/S4-SGSN からの DDN 障害の受信時に課金が一時停止されるように、MBR が P-GW に送信されます。

- **drop-limit *drop_limit_value* { packets | bytes } }**

  PDN 接続で指定した数のパケット/バイトがドロップされた場合に、P-GW で課金が一時停止されるように MBR を送信します。

  drop_limit_value は、1 ～ 99999 の整数です。

  - **packets**：パケット単位でドロップ制限を設定します。
  - **bytes**：バイト単位でドロップ制限を設定します。

S-GW での過課金サポートの設定

S-GW で過課金をサポートするには、次の設定が必要です。

```
configure
   context context_name
      egtp-service service_name
         gtpc private-extension overcharge-protection
         end
```

注：

- このコマンドを有効にすることは、S-GW が、3GPP TS 29.274 リリース 12 – *3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3* をサポートしない過課金保護機能のためにリリース 15 P-GW と連携する必要があることを示しています。
- **gtpc private-extension overcharge-protection** コマンドが設定されている場合、S-GW はセッション作成要求（CSReq）およびベアラー変更要求（MBReq）メッセージにプライベート拡張を含めます。
- P-GW は、PDN Pause Support Indication フラグが 1 に設定された通知 IE を含む CSReq を受信するたびに、通知 IE でのみ応答します。
- CSReq に PDN Pause Support Indication フラグが 1 に設定された通知 IE がなく、P-GW が過課金保護をサポートしている場合、P-GW は通知 IE と プライベート拡張 IE の両方で応答します。

モニタリングおよびトラブルシューティング

P-GW スキーマ

過課金保護のために P-GW スキーマに次のバルク統計が追加されました。

これらの変数については、『*Statistics and Counters Reference* 』[英語] を参照してください。

- sessstat-ovrchrgprtctn-uplkpktdrop
- sessstat-ovrchrgprtctn-uplkbytedrop
- sessstat-ovrchrgprtctn-dnlkpktdrop
- sessstat-ovrchrgprtctn-dnlkbytedrop

show apn statistics all

次のカウンタには、この APN の過課金保護に関する統計が表示されます。

- UL 過課金保護バイトドロップ
- UL 過課金保護パケットドロップ
- DL 過課金保護バイトドロップ
- DL 過課金保護パケットドロップ

show pgw-service all

次のフィールドには、この P-GW サービスでの過課金保護の設定情報が表示されます。

- EGTP 過課金保護

show pgw-service statistics all

次のカウンタには、この P-GW ノードの過課金保護が表示されます。

- 過課金保護によるドロップ
  - パケット
  - Bytes

show sgw-service statistics name <sgw_service_name>

このコマンドの出力には、課金が一時停止された PDN の総数が表示されます。

- PDNs Total:
  - Paused Charging: <Total number of PDNs where charging was paused>

show subscribers full

次のカウンタには、すべてのサブスクライバの過課金保護が表示されます。

- in packet dropped overcharge protection
- in bytes dropped overcharge protection
- out packet dropped overcharge protection
- out bytes dropped overcharge protection



重要 セッションが過課金保護状態の場合、すべてのダウンリンクパケットがドロップされるわけではありません。ダウンリンクパケットはレート制限されます。現在の設定では、ダウンリンクパケットが P-GW に着信すると、S-GW への 1 分あたり 1 つのダウンリンクパケットが課金されることなく許可されます。P-GW は独自のパケットを生成しません。P-GW に別個のデバッグ統計が追加されました。

show subscribers pgw-only full all

次のフィールドとカウンタには、過課金保護が表示されます。

- Bearer State
  - in packet dropped overcharge protection
  - in bytes dropped overcharge protection
  - out packet dropped overcharge protection
  - out bytes dropped overcharge protection

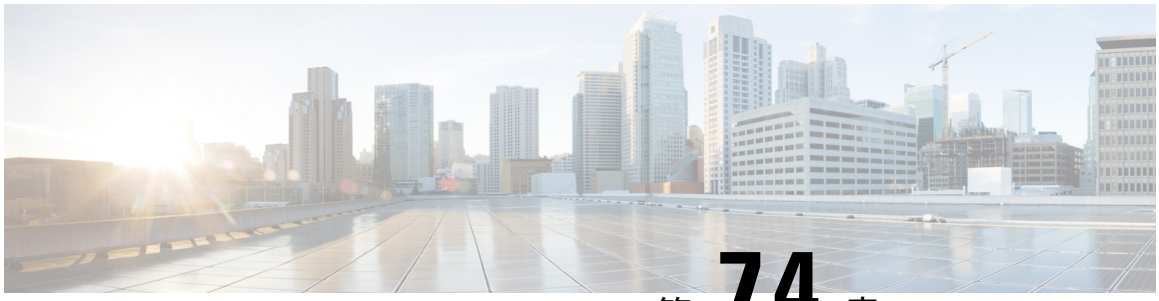
show subscribers summary

次のカウンタには、すべてのサブスクライバの過課金保護が表示されます。

- in bytes dropped ovrchrgPtn
- in packet dropped ovrchrgPtn
- out bytes dropped ovrchrgPtn
- out packet dropped ovrchrgPtn



重要 セッションが過課金保護状態の場合、すべてのダウンリンクパケットがドロップされるわけではありません。ダウンリンクパケットはレート制限されます。現在の設定では、ダウンリンクパケットが P-GW に着信すると、S-GW への 1 分あたり 1 つのダウンリンクパケットが課金されることなく許可されます。P-GW は独自のパケットを生成しません。P-GW に別個のデバッグ統計が追加されました。



第 74 章

クレジット制御応答を待たないオンライン課金サポート

- 機能の概要と変更履歴 （1193 ページ）
- 機能説明 （1194 ページ）
- 仕組み （1194 ページ）
- オンライン応答必須パラメータの設定 （1195 ページ）
- モニタリングおよびトラブルシューティング （1196 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC - SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、オンライン応答用の新しいCLIがAPNレベルで追加されました。この機能はこのリリースで完全に機能します。	21.20.3
最初の導入。	21.20

改訂の詳細	リリース
重要 この機能は、このリリースでは完全には機能しておらず、テスト目的でのみ使用できます。詳細については、シスコのアカウント担当者にお問い合わせください。	

機能説明

5G サブスクライバの場合、すべての料金設定グループとすべてのベアラーは、オンライン課金フラグを「yes」に設定し、請求レコードを作成するためのGyセッションを確立する必要があります。APN、ベアラー、料金設定の各グループのコールセットアップが遅延されたり、データフローがブロックされたりしないように、P-GW では、Gy を介して課金を実行できるようにして、セッションセットアップの遅延やデータ保留が発生しないようにする新機能をサポートしています。これにより、OCS を介した 5G-ChF（充電機能）の動作が模倣されます。

ポリシーおよび課金ルール機能（PCRF）は、次の 2 つの AVP を介して、上記の動作を必要とするベアラーを指示します。

- 課金レベル AVP –**Online-Response-Required** AVP は課金レベルで定義され、オンライン課金が有効な場合にのみ使用できます。この AVP は、セッション作成応答が CCA を「待機」する必要があるかどうかを制御します。
- オーバーライド制御 AVP–**Online-Response-Required** は、オーバーライド制御レベルで定義され、オンライン課金が有効な場合にのみ使用できます。この AVP は、ポリシーおよび課金ルール機能（PCRF）から受信した新しい課金 AVP を上書きします。

仕組み

次のコールフローと手順では、セッション作成中に CCR がどのようにトリガーされるのかを説明します。

表 *108 :* 手順

ステップ	説明
1	P-GW が、セッション作成要求を受信します。
2	PCRF から受信した課金 AVP をチェックします。

ステップ	説明
3	PCRF において、Gx インターフェイスで、**OnlineResponseRequired** または **Override-OnlineResponseRequired** AVP が、WAIT または DONT_WAIT のオプションにより、課金レベルまたはオーバーライドレベルでアクティブになります。ルールの選択に基づいて、次のアクションが発生します。 • セッション作成要求を、OnlineResponseRequired を示す WAIT ルールとともに受信した場合、セッション作成応答は、セッション作成応答を送信する前に、Gyインターフェイスを介した CCA-I を待ちます。 • セッション作成要求を、DONT_WAIT ルールとともに受信した場合、セッション作成応答は、CCA-I 応答を待ちません。
4	P-GW が、新しい AVP に基づいてセッション作成応答を送信します。

次のシナリオでは、データフローがどのように処理されるのかを説明します。

- クォータがない場合、P-GW は、そのフローについてポジティブと想定します。
- クォータがある場合は、次のようになります。
  - 課金レベルの AVP が DONT_WAIT を指定している場合、トラフィックはドロップされません。
  - クォータが期限切れになると、P-GW はポジティブと想定します。エラーコードがある場合（エラーコード 4012 を除く）、P-GW はポジティブ想定をトリガーします。

オンライン応答必須パラメータの設定

次のコマンドを使用して、APN コンフィギュレーションモードでオンライン応答が必要な AVP を設定します。

```
configure
  context context_name
    apn apn_name
       bearer-control-mode mixed
         use-gx-avp-online-response-required
         no  use-gx-avp-online-response-required
          end
```

注：

- **apn** ：アクセスポイント名を指定します。

- **bearer-control-mode mixed**：このキーワードは、ベアラーがユーザー機器（UE）とネットワーク側（GGSN）によっても制御されることを示します。デフォルトでは無効になっています。
- **use-gx-avp-online-response-required**：Gx AVP OnlineResponseRequired または override-OnlineResponseRequired で要求された動作に従って、P-GW が機能するようにします。
- **no**：指定した APN の OnlineResponseRequired 機能または override-OnlineResponseRequired 機能を無効にします。

モニタリングおよびトラブルシューティング

show コマンドと出力

show-active-charging subscribers

上記のコマンドの出力が拡張され、「Don't Wait」として選択される、オンライン応答必須ルール定義を示す新しいパラメータが表示されるようになりました。次に例を示します。

```
Override Control :
  Rule Name :
                      qci3
  Charging Parameters:
    Rating Group     : 555
    Service ID       : 333
    Online Enabled   : TRUE
    Offline Enabled  : TRUE
    Online Response Required: Don't Wait
  Policy Parameters:
    MBR UL           : 50000
    MBR DL           : 50000
```

show-active-charging-sessions-full-all

上記のコマンドの出力が拡張され、「Wait」として選択されたオンライン応答必須ルール定義を示す新しいパラメータが表示されるようになりました。

```
For example
Dynamic Charging Rule Definition(s) Configured:
Name                 Prior Content-Id Chrg-Type Rule Parameters
-------------------- ----- ---------- --------- --------------------------
       ruleName_Dean     5         55      Both Gate Status:      Allow All
                                                QoS Class Identifier:     1
                                                ARP Priority Level:       6
                                                Reporting Level: Rating Grp
                                                Metering Method:   Duration
                                                Uplink MBR:        40960000
                                                Downlink MBR:      40960000
                                                Uplink GBR:        40960000
                                                Downlink GBR:      40960000
                                                Filter 1:
                                                Direction:           Uplink
```

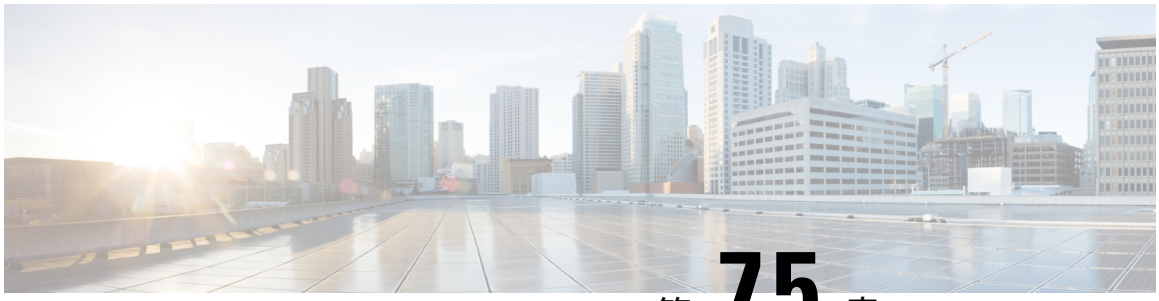
```
Dst Addr  0.0.0.0/0
Filter 2:
Direction:          Downlink
Src Addr  0.0.0.0/0
Filter 3:
Direction:            Uplink
Dst Addr  ::/0
Filter 4:
Direction:          Downlink
Src Addr  ::/0
Online Response Required: Wait
```

show apn-name

次の show apn name コマンド出力を使用して、コマンドエントリを確認します。

表 *109 :*

フィールド	説明
Access Point Name（APN; アクセスポイント名）	カウンタ表示の対象であるアクセスポイント名（APN）の名前を
認証コンテキスト（Authentication Context）	この APN の認証に使用されるシステムコンテキストの名前。
Pdp Type	PDP コンテキストのタイプを示します。PDP のタイプは次のとお • IPv4 • IPv6
緊急	**emergency-apn** オプションがこの APN に設定されているかどうか す。
Delay Tolerant	PDN 接続の遅延耐性動作が、省電力モードの UE で使用可能かど します。
PCO Options	ネットワーク内のどのカスタマイズされた PCO（プロトコル設定 ン）オプションがネットワーク内で MS GTP メッセージに送信さ 指定します。PCO オプションは次のとおりです。 • Custom1 • Mode • Link MTU • Nonlink MTU • ePDG Selection FQDN
Online Charging without Wait	APN レベルで定義されている待機なしのオンライン課金が無効に ことを示します。



第 75 章

G-CDR におけるパケットカウント

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （1199 ページ）
- 機能説明 （1200 ページ）
- 機能の仕組み （1200 ページ）
- G-CDR におけるパケットカウントの設定 （1200 ページ）
- モニタリングおよびトラブルシューティング （1201 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC - DI • VPC - SI
機能のデフォルト	有効、常時オン
このリリースでの関連する変更点	N/A
関連資料	*P-GW Administration Guide*

マニュアルの変更履歴



重要 リリース 21.2 および N5.1 よりも前に導入された機能の改訂履歴の詳細は示していません。

改訂の詳細	リリース
このリリースでは、P-GW は、ベアラーコンテキストを含まず、古い F-TEID を含むベアラー変更要求メッセージを受け入れます。	21.14
最初の導入。	21.2 よりも前

機能説明

IoT UE が接続されるとメッセージが送信され、必要に応じて次のメッセージの送信時間まで省電力モード（PSM）になります。IoT UE は、各メッセージの後に接続を解除（つまり、セッション終了）しません。通信事業者は IoT UE セッションで生成された CDR を介してこのようなメッセージの数を評価することで、オフラインの請求レコードにパケット数を含めて、IoT デバイス向けの課金システムを導入できます。

重要 この機能は、custom24 GTPP ディクショナリに適用されます。

機能の仕組み

この機能の一部として、datapacketsFBCDownlink と datapacketsFBCUplink というパケット数に関する 2 つの新しい属性が導入されました。これら 2 つの属性は CLI で制御され、CLI が有効になっている場合にのみ表示されます。既存の属性は変更または削除されません。

G-CDR におけるパケットカウントの設定

ここでは、この機能をサポートするために使用可能な CLI コマンドについて説明します。

G-CDR におけるパケット制御の有効化

GTPP サーバー グループ コンフィギュレーション モードで G-CDR のパケット数の送信を有効または無効にするには、次のコマンドを使用します。

```
configure
  context context_name
    gtpp group group_name
      [ no ] gtpp attribute packet-count
      end
```

注：

- **no**：G-CDR におけるアップリンクおよびダウンリンクのパケット数の送信を無効にします。
- **packet-count**：このオプションを指定すると、CDR にオプションフィールド「datapacketFBCUplink」と「datapacketFBCDownlink」が追加されます。
- デフォルトでは、この **gtpp attribute packet-count** CLI は無効になっています。

モニタリングおよびトラブルシューティング

このセクションでは、機能のモニタリングと障害対応に使用できる CLI コマンドについて説明します。

コマンドや出力の表示

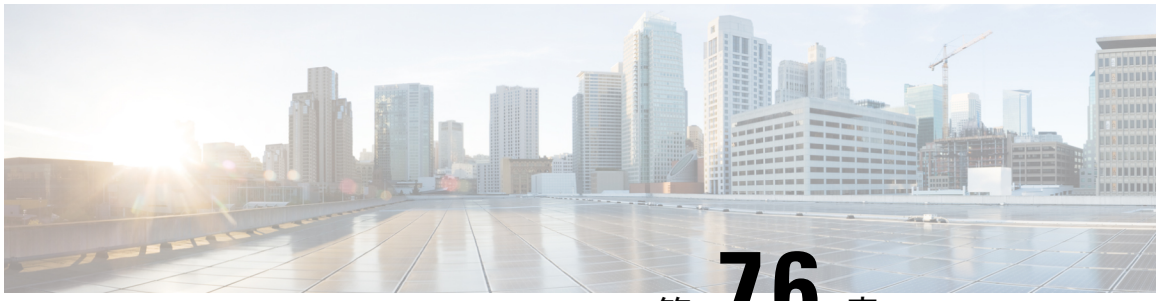
この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show configuration

この CLI コマンドの出力が拡張され、該当する機能が有効な場合、APN に関する次のフィールドが表示されるようになりました。gtpp attribute packet-count

show gtpp group name <name>

この CLI コマンドの出力が拡張され、該当する機能が有効な場合、Packet count present のフィールドが新たに表示されるようになりました。



第 76 章

ページングポリシー差別化

この章では、ページングポリシー差別化機能とその設定方法について説明します。製品アドミニストレーション ガイドには、システム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、『*P-GW Administration Guide*』、『*S-GW Administration Guide*』、または『*SAEGW Administration Guide*』の説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

この章は、次の項で構成されています。

- 機能説明 （1203 ページ）
- 機能の仕組み （1205 ページ）
- ページングポリシー差別化機能の設定 （1206 ページ）
- ページングポリシー差別化のモニタリングと障害対応 （1207 ページ）

機能説明

S-GW/P-GW は、ユーザーデータグラム パケットと外部 IP パケット（GTP-U トンネル IP ヘッダー）の DSCP 値を変更するための設定制御を提供します。DSCP マーキングは、設定に応じてさまざまなレベルで実行されます。ただし、ページングポリシー差別化（PPD）機能が有効になっている場合、ユーザーデータグラム パケット DSCP（トンネル化 IP パケット）のマーキングは変更されません。

現在、標準規格では、外部 GTP-U ヘッダーの QCI から DSCP へのマーキングのみが規定されています。ユーザーデータグラム パケットの DSCP 値を変更する ECS、P-GW、および S-GW のすべての設定は非標準です。標準ベースの PPD 機能では、P-CSCF または同様の Gi エンティティによって、ユーザーデータグラム パケットの DSCP がマーキングされます。このユーザーデータグラム パケットの DSCP 値は、S-GW によって MME/S4-SGSN に DDN メッセージで送信されます。MME/S4-SGSN は、この DSCP 値を使用してページング優先順位を付けます。

重要 P-GW と S-GW は、デフォルトと専用の両方のベアラーに PPD 機能を適用する必要があります。仕様に従って、P-GW はユーザーデータグラム パケットを透過的に S-GW に渡します。つまり、PPD 機能が有効になっている場合、通信事業者はデフォルトベアラーと専用ベアラーに異なる動作を適用できません。

関係

P-GW/S-GW は非標準ベースの DSCP マーキングをサポートしているため、標準ベースの PPD 機能と非標準ベースのユーザーデータグラムパケットの DSCP 設定がどちらも有効になっている場合、競合が発生します。この競合を回避するために、次の点に注意してください。

- PPD 機能が有効になっている場合、APN およびサービスレベルの設定は無視されます。
- S-GW/P-GW は、PPD 機能が有効になっている場合でも、外部 GTP-U ヘッダーの DSCP 値を変更できます。
- ユーザーデータグラムパケットの DSCP 値は、PPD 機能が有効になっている場合、ECS、P-GW、および S-GW によって変更されません。
- P-GW では、PPD 機能を有効または無効にするための APN レベルの設定が追加されています。
- S-GW では、PPD 機能を有効または無効にするためのサービスレベルの設定が追加されています。これにより、IMS-PDN や Internet-PDN などによってトリガーされたすべての DDN メッセージのページングおよびサービス情報 IE で DSCP が送信されます。

重要 DDN メッセージのページングおよびサービス情報 IE は MME/S4-SGSN によって使用されます。

- システムには分離ページング機能と PPD 機能が共存しています。つまり、両方の機能が有効になっている場合、ページングおよびサービス情報 IE と個別ページング IE の両方が DDN で送信されます。
- 現在、P-GW では、コールセットアップ時間中に DSCP 設定がサブセッションレベルで適用されます。そのため、P-GW に対して PPD CLI が有効になっている場合、それが新しいコールに適用されます。
- 現在、S-GW では、DSCP 設定が S-GW サービスレベルで適用されます。そのため、S-GW サービスで PPD CLI が有効になっている場合は、それが新しいコールと既存のコールの両方に適用されます。
- PPD CLI は、有効になると、セッションリカバリと ICSR のスイッチオーバーの後にも存在します。
- ページングおよびサービス情報 IE は、ベアラーごとのページングおよびサービス情報を伝送するために使用されます。

ライセンス

PPD はライセンスにより有効となる機能です。P-GW、S-GW、および SAEGW の PPD 機能を有効にするには、S-GW ページング プロファイル ライセンス キーが必要です。

重要　ライセンスの入手方法の詳細については、シスコのアカウント担当者にお問い合わせください。

機能の仕組み

アーキテクチャ

S-GW

S-GW が PPD 機能をサポートする場合には、S-GW でのダウンリンクデータパケットの到着によってトリガーされるダウンリンクデータ通知メッセージに、新しいページングおよびサービス情報 IE を含める必要があります。この IE 内のページングポリシーの表示値には、P-GW から GTP-U パケットの IP ペイロードで受信した TOS（IPv4）または TC（IPv6）情報の DSCP 値が含まれます。

S-GW では、サービスレベルの設定により PPD 機能が有効化または無効化されます。PPD を設定すると、この機能が有効になり、既存のコールと新しいコールの両方に適用されます。

P-GW

ユーザーデータグラム パケットの DSCP 値は、ダウンリンクデータの P-GW によって変更されることはありません。PPD 機能は、S5 と S8 インターフェイスでのみサポートされています。他のインターフェイスから S5 または S8 インターフェイスにハンドオフするすべてのシナリオでは、APN が PPD 機能に対応している場合、そのインターフェイスでのコールセットアップ時間中に PPD 機能が有効になります。

P-GW では、APN レベルの設定により PPD 機能が有効化または無効化されます。コールに対して PPD 機能が有効になっていて、S5 または S8 インターフェイスから他のインターフェイスへのハンドオフが発生した場合、PPD 機能は無効になります。ハンドオフが発生し、このコールが S5 または S8 インターフェイスに戻れば、PPD 機能は有効になります。

SAEGW

SAEGW で PPD 機能をサポートするには、S-GW と P-GW の両方の設定が必要です。

他の機能との関係

- PPD 機能は、S-GW ページングプロファイルのライセンスの下でライセンスが管理されます。ライセンスを有効にすると、両方の機能が共存し、独立して動作します。つまり、DDN メッセージは、PPD 機能によって指定された DSCP マーキングと、S-GW ページングプロファイル機能によって指定された優先順位の DDN 値の両方を伝送する可能性があります。
- S-GW では、ユーザーデータグラム パケットの DSCP 値が DDN での送信に使用されます。S-GW は、ローカル設定（APN プロファイルまたはサービスレベル）に従って DSCP を変

更することはできません。eNodeB では、パケットのスケジューリングは DSCP ではなく QCI に基づいていますが、EPC ノードは内部 DSCP 値を変更/修正することはできません。

- PPD 機能が有効になっている場合、EPS ノードがユーザーデータグラム パケットの DSCP 値を変更することはありません。したがって、PPD が有効になっている場合、ECS ではユーザーデータグラムパケットの DSCP 値が上書きされないようにする必要があります。

標準準拠

PPD 機能は、次の標準規格に準拠しています。

- 29.274、CR-1565、「Paging Policy Indication in Downlink Data Notification Message」
- 23.401、CR-2731「Paging policy differentiation for IMS voice」

ページングポリシー差別化機能の設定

PPD 機能を動作させるには、P-GW と S-GW で有効にする必要があります。

P-GW と S-GW の両方のサービスに PPD 設定を個別に適用します。したがって、APN からのダウンリンクデータパケットでは、P-GW に PPD 設定がないが、S-GW には PPD 設定がある場合があります。このような競合を回避するには、P-GW（APN レベル）と S-GW（サービスレベル）の両方で PPD 機能を設定する必要があります。

設定

PPD 機能を管理するには、次の CLI コマンドを使用します。

P-GW での有効化

次のコマンドを使用すると、APN レベルで P-GW の PPD 機能が有効になります。

```
configure
     context context_name
        apn apn_name
               paging-policy-differentiation
               end
```

S-GW での有効化

次のコマンドを使用すると、サービスレベルで S-GW の PPD 機能が有効になります。

```
configure
     context context_name
        sgw-service service_name
               paging-policy-differentiation
               end
```

注：

- これにより、IMS-PDN や Internet-PDN などによってトリガーされたすべての DDN メッセージのページングおよびサービス情報 IE で DSCP が送信されます。
- DDN メッセージのページングおよびサービス情報 IE は MME/S4-SGSN によって使用されます。
- S-GW サービスで PPD 機能が有効になっている場合、APN プロファイルに関係なく、すべてのコールに適用されます。

P-GW での無効化

次のコマンドを使用すると、APN レベルで P-GW の PPD 機能が無効になります。

```
configure
     context context_name
        apn apn_name
               no paging-policy-differentiation
               end
```

S-GW での無効化

次のコマンドを使用すると、サービスレベルで S-GW の PPD 機能が無効になります。

```
configure
     context context_name
        sgw-service service_name
               no paging-policy-differentiation
               end
```

ページングポリシー差別化のモニタリングと障害対応

この項では、PPD 機能のサポートに使用できる show コマンドについて説明します。

P-GW show コマンド

ここでは、PPD 機能をサポートする P-GW show コマンドとその出力について説明します。

show apn name<apn_name>

PPD 機能を表示するために、次のカウンタが追加されました。

```
Paging Policy Differentiation : Enabled
```

show subscribers pgw-only full all

PPD 機能を表示するために、次のカウンタが追加されました。

```
Paging Policy Differentiation : Enabled
```

SAEGW show コマンド

このセクションでは、PPD 機能をサポートする SAEGW show コマンドとその出力について説明します。

show subscribers saegw-only full all

PPD 機能を表示するために、次のカウンタが追加されました。

```
Paging Policy Differentiation : Enabled
```

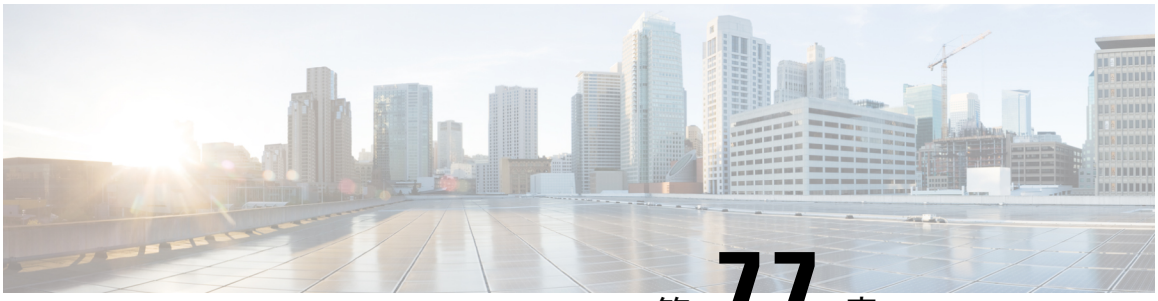
S-GW show コマンド

ここでは、PPD 機能をサポートする S-GW show コマンドとその出力について説明します。

show sgw-service name <service_name>

PPD 機能を表示するために、次のカウンタが追加されました。

```
Paging Policy Differentiation : Enabled
```



第 77 章

P-GW バッファリングメカニズム

- 機能の概要と変更履歴 （1209 ページ）
- 機能説明 （1210 ページ）
- 機能の仕組み （1210 ページ）
- P-GW バッファリングメカニズム機能の設定 （1210 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC - DI • VPC - SI
機能のデフォルト	有効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、P-GW によるバッファリングメカニズム機能がサポートされています。	21.23
最初の導入。	21.14

機能説明

Default-Bearer-QoS の変更が保留状態の場合、P-GW は最大 2 つのポリシー（PCRF）メッセージをバッファに保存できます。Presence Reporting Area（PRA）関連のコールフローでは、ベアラー更新応答（UBResp）が保留状態のときに 2 つ以上のメッセージを受信できます。

P-GW バッファリングメカニズム機能により、P-GW は UBResp を待機中に、PCRF から受信した RAR や CCA-U をスムーズに処理できます。UBResp が受信されると、保留中のメッセージが P-GW のバッファキューから取得され、後続処理が実行されます。

機能の仕組み

アクティブ課金サービス（ACS）モードでは、バッファサイズを増やすために CLI コマンド **pending-buffer-size** が追加されました。デフォルトベアラー QoS の変更が保留状態の間は、P-GW が UBResp メッセージを受信するまで、PCRF メッセージがバッファされます。

P-GW バッファリングメカニズム機能の設定

デフォルトベアラー QoS の変更ステータスが保留中の場合に、PCRF メッセージを保存するバッファサイズを大きくするには、次の設定を使用します。

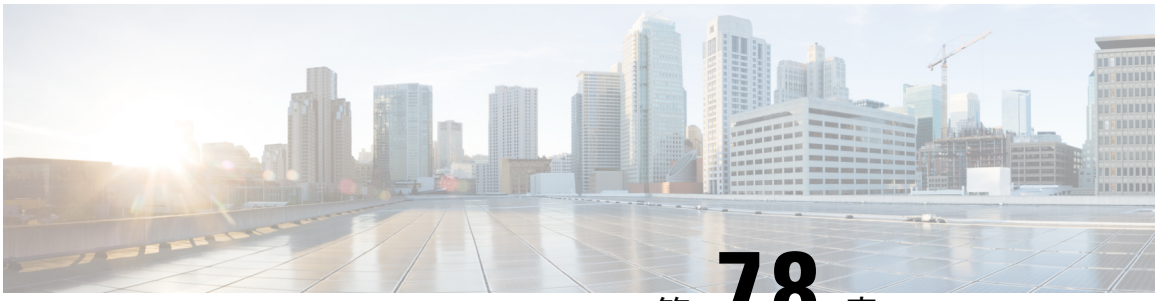
```
configure
  active-charging service service_name
    policy control def-bearer-qos-change pending-buffer-size buffer_size

    end
```

注：

- **def-bearer-qos-change**：デフォルトベアラー QoS 変更パラメータを設定します。
- **pending-buffer-size** *buffer_size*：デフォルトベアラー QoS の変更が保留中の場合に、PCRF メッセージを保存するバッファサイズを指定します。buffer_size は 2 ～ 4 の整数です。

  設定されている最小値は 2、最大値は 4 です。
- **no policy control def-bearer-qos-change** により、コマンドがデフォルト値に設定されます。デフォルトは 2 です。
- ほとんどの使用例では、デフォルト値で十分です。ただし、使用例に基づいて、メモリ使用量を考慮し、それよりも高い値を設定する必要があります。
- CLI コマンドは、新しいコールに対して有効になります。



第 78 章

P-GW のバッファリングの最適化

- 機能の概要と変更履歴 （1211 ページ）
- 機能説明 （1212 ページ）
- 他の機能との関係性 （1212 ページ）
- 機能の仕組み （1212 ページ）
- P-GW バッファリング最適化の設定 （1212 ページ）
- モニタリングおよびトラブルシューティング （1213 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC- DI • VPC- SI
機能のデフォルト	有効、常時オン
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、P-GW は、PRA メッセージを効率的に処理するためのバッファリング最適化をサポートしています。	21.23

改訂の詳細	リリース
最初の導入	21.22.3

機能説明

P-GW のバッファリングの最適化により、P-GW は、Presence Reporting Area（PRA）メッセージを効率的に処理できます。UBResp がまだ保留されている間に、2 つ以上の PRA が受信されると、P-GW バッファキューがいっぱいになったり、メッセージドロップが発生したりする可能性があります。この機能拡張により、メッセージがドロップされる可能性が小さくなるため、ポリシーおよび課金ルール機能（PCRF）からの PRA 応答を効率的に処理できます。

新しいメッセージを受信すると、P-GW は、そのメッセージをキュー内にある既存の類似タイプのメッセージとマージします。これにより、P-GW は、キューサイズを増やしたり、メッセージドロップ率を減らしたりせずに、類似タイプのメッセージを同時に処理できます。メッセージがキューから読み取られると、Gx Rule Level 属性値ペア（AVP）で定義されたアクションがトリガーされます。メッセージがバッファリングされている場合、Rule Level AVP の有効性はチェックされません。

他の機能との関係性

P-GWバッファリング最適化機能は、P-GWバッファリングメカニズム機能に関連しています。詳細については、『*P-GW Administration Guide*』の「*P-GW*バッファリングメカニズム」の章を参照してください。

機能の仕組み

アクティブ課金サービス（ACS）モードでは、CLI コマンドの **optimze-update** を有効または無効にして、バッファリングメカニズムを有効または無効にします。

P-GW バッファリング最適化の設定

次の設定を使用して、キュー内の同様のタイプのメッセージを処理するためのP-GWバッファの最適化を有効または無効にします。

```
configure
         active-charging service service_name
           [ no ] policy control optimze-update pra-change
        end
```

注：

- **optimize-update**：以前の応答が保留中の場合に、PCRF から受信した複数のポリシーの最適化を有効にします。デフォルトは、[Disabled] です。
- **no**：複数のポリシーの最適化を無効にします。
- **pra-change**：プレゼンスレポートエリア（PRA）の変更時にのみ、ポリシーの最適化を有効にします。

モニタリングおよびトラブルシューティング

この項では、この機能をサポートするために show コマンドを使用して監視およびトラブルシューティングする方法について説明します。

コマンドと出力の表示

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show Active-Charging Sessions Full All

show Active-Charging Sessions Full All の出力です。

表 *110 : show active-charging sessions full all* コマンド出力の説明

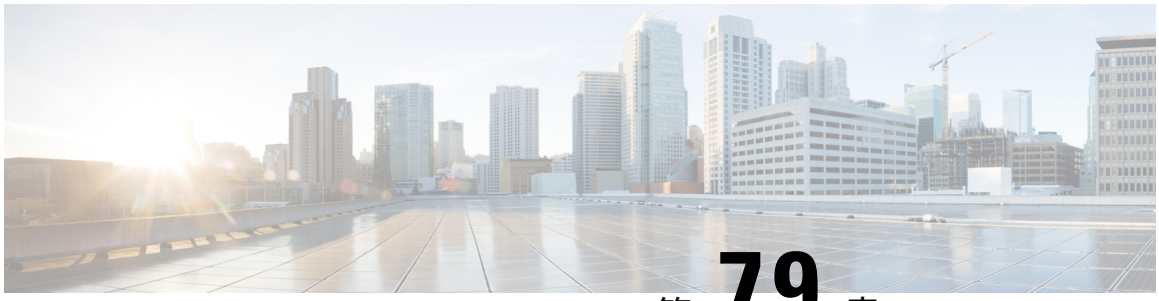
フィールド	説明
現在の P-GW バッファのキュー長	現在使用されているキューの長さを表示します。
P-GW バッファマージ合計数	PRA メッセージのマージ数を表示します。

show Active-Charging Service All

show Active-Charging Service All の出力です。

表 *111 : show active-charging service all* コマンド出力の説明

フィールド	説明
optimize-update	複数のポリシー最適化を有効にします。
pra-change	PRA 変更に対する最適化ポリシーを有効にします。



第 79 章

VoWiFi の P-GW ハンドオフ KPI

• VoWiFi の P-GW ハンドオフ KPI （1215 ページ）

VoWiFi の P-GW ハンドオフ KPI

変更された機能

現在、特定の RAT テクノロジーで開始された新しいセッションの数を判断し、APN ごとのテクノロジー間ハンドオーバーをモニターするための統計はありません。

この機能により、以下をモニターするために、新しいセッション/ハンドオフ KPI と P-GW VoWifi 固有の KPI が導入されます。

- 特定の RAT テクノロジーで開始された新しいセッションの数
- すべてのアクセステクノロジーとの間での、APN ごとの、テクノロジー間ハンドオーバー
- ネットワークプランニングのためのサブスクライバのアクティビティ

統計情報は、APN ごとと、P-GW/SAEGW サービスタイプごとに維持されます。CLI は、P-GW および SAEGW 製品にのみ適用されます。eHRPD/PMIP/GGSN サービスが P-GW/SAEGW サービスに関連付けられている場合、これらのサービスに関連するカウンタが、P-GW/SAEGW サービス統計の CLI 出力の下に反映されます。

利点

この機能の導入により、通信事業者は、RAT が開始したセッションおよびテクノロジー間ハンドオーバーごとに KPI を監視でき、2G、3G、4G、Wi-Fi、および eHRPD のカバレッジを測定できます。

通信事業者では次も可能です。

- 以下を報告する統計の取得
  - ePDG を使用する Wi-Fi などの新しいアクセス技術

- セッションの開始方法
- 実行されたハンドオフの数

- ネットワーク内のサブスクライバのアクティビティの追跡
- 以上を踏まえたネットワークの計画

制限事項

- APN レベルで開始されたセッション統計とハンドオーバー統計は、メモリと CPU の制約により、デマルチプレクサで維持または増分されません。たとえば、輻輳シナリオ中、一部のコールはデマルチプレクサで拒否されるため、この数はAPN レベルで開始されたセッションカウンタには表示されません。
- eHRPD および S2b-PMIP のバルク統計は、SAEGW スキーマではサポートされていません。

VoWiFi の P-GW ハンドオフ KPI のモニタリングと障害対応

ここでは、VoWiFi の P-GW ハンドオフ KPI のモニタリングに使用できるコマンドについて説明します。

VoWiFi のハンドオフ KPI の show コマンド

ここでは、VoWiFi のハンドオフ KPI のモニタリングに使用できるコマンドについて説明します。

show apn statistics [all | name *apn_name* | verbose]

このコマンドを実行すると、次の出力が表示されます。

```
Initiated Sessions per RAT Type:
    EUTRAN:    0    UTRAN:       0
    GERAN:     0    EHRPD:       0
    S2A GTP:   0    S2B GTP:     0
    S2B PMIP:  0

Inter Technology handover:
  GNGP-to-LTE handover:          LTE-to-GNGP handover:
    Attempted:         0          Attempted:          0
    Succeeded:         0          Succeeded:          0
    Failed:            0          Failed:             0

GNGP-to-S4SGSN handover:       S4SGSN-to-GNGP handover:
    Attempted:         0          Attempted:          0
    Succeeded:         0          Succeeded:          0
    Failed:            0          Failed:             0

S4SGSN-to-LTE handover:        LTE-to-S4SGSN handover:
    Attempted:         0          Attempted:          0
    Succeeded:         0          Succeeded:          0
    Failed:            0          Failed:             0
```

```
LTE-to-eHRPD handover:          eHRPD-to-LTE handover:
    Attempted:        0             Attempted:           0
    Succeeded:        0             Succeeded:           0
    Failed:           0             Failed:              0

LTE-to-S2bPMIP handover:        S2bPMIP-to-LTE handover:
    Attempted:        0             Attempted:           0
    Succeeded:        0             Succeeded:           0
    Failed:           0             Failed:              0

eHRPD-to-S2bPMIP handover:      S2bPMIP-to-eHRPD handover:
    Attempted:        0             Attempted:           0
    Succeeded:        0             Succeeded:           0
    Failed:           0             Failed:              0

S2bGTP-to-LTE handover:         LTE-to-S2bGTP handover:
    Attempted:        0             Attempted:           0
    Succeeded:        0             Succeeded:           0
    Failed:           0             Failed:              0

S2bGTP-to-eHRPD handover:       eHRPD-to-S2bGTP handover:
    Attempted:        0             Attempted:           0
    Succeeded:        0             Succeeded:           0
    Failed:           0             Failed:              0

S2aGTP-to-LTE handover:         LTE-to-S2aGTP handover:
    Attempted:        0             Attempted:           0
    Succeeded:        0             Succeeded:           0
    Failed:           0             Failed:              0
```

show pgw-service statistics { all | name *service_name* }

このコマンドを実行すると、次の出力が表示されます。

```
Initiated PDNs By RAT-Type:
    EUTRAN:            0          UTRAN:       0
    GERAN:             0          EHRPD:       0
    S2A GTP:           0          S2B GTP:     0
    S2B PMIP:          0
```

show saegw-service statistics { all | name *service_name* } function pgw

このコマンドを実行すると、次の出力が表示されます。

```
Initiated PDNs By RAT-Type:
  EUTRAN:                     0       UTRAN:                     0
  GERAN:                      0       EHRPD:                     0
  S2A GTP:                    0       S2B GTP:                   0
  S2B PMIP:                   0
```

VoWifi 用の P-GW ハンドオフ KPI のスキーマ

この項では、VoWifi 機能用の P-GW ハンドオフ KPI に追加されたスキーマを示します。

APN スキーマ

RAT テクノロジーに基づく開始されたセッションの統計情報：

この機能強化では、サービス/APN ごと、RAT タイプごとに開始されたセッションの数を表示するための、次の新しいカウンタが追加されました。

- initiated-eutran-sessions
- initiated-utran-sessions
- initiated-geran-sessions
- initiated-ehrpd-sessions
- initiated-s2a-gtp-sessions
- initiated-s2b-gtp-sessions
- initiated-s2b-pmip-sessions

テクノロジー間ハンドオーバーの統計情報：

この機能強化により、APN/サービスごとのテクノロジー間ハンドオーバー数の統計情報を表示するための、次の新しいカウンタが追加されました。

- apn-handoverstat-gngptolteatt
- apn-handoverstat-gngptoltesucc
- apn-handoverstat-gngptoltefail
- apn-handoverstat-ltetogngpatt
- apn-handoverstat-ltetogngpsucc
- apn-handoverstat-ltetogngpfail
- apn-handoverstat-gngptos4sgsnatt
- apn-handoverstat-gngptos4sgsnsucc
- apn-handoverstat-gngptos4sgsnfail
- apn-handoverstat-s4sgsntogngpatt
- apn-handoverstat-s4sgsntogngpsucc
- apn-handoverstat-s4sgsntogngpfail
- apn-handoverstat-s4sgsntolteatt
- apn-handoverstat-s4sgsntoltesucc
- apn-handoverstat-s4sgsntoltefail
- apn-handoverstat-ltetos4sgsnatt
- apn-handoverstat-ltetos4sgsnsucc
- apn-handoverstat-ltetos4sgsnfail
- apn-handoverstat-ltetoehrpdatt
- apn-handoverstat-ltetoehrpdsucc

- apn-handoverstat-ltetoehrpdfail
- apn-handoverstat-ehrpdtolteatt
- apn-handoverstat-ehrpdtoltesucc
- apn-handoverstat-ehrpdtoltefail
- apn-handoverstat-ltetos2bpmipatt
- apn-handoverstat-ltetos2bpmipsucc
- apn-handoverstat-ltetos2bpmipfail
- apn-handoverstat-s2bpmiptolteatt
- apn-handoverstat-s2bpmiptoltesucc
- apn-handoverstat-s2bpmiptoltefail
- apn-handoverstat-ehrpdtos2bpmipatt
- apn-handoverstat-ehrpdtos2bpmipsucc
- apn-handoverstat-ehrpdtos2bpmipfail
- apn-handoverstat-s2bpmiptoehrpdatt
- apn-handoverstat-s2bpmiptoehrpdsucc
- apn-handoverstat-s2bpmiptoehrpdfail
- apn-handoverstat-s2bgtptolteatt
- apn-handoverstat-s2bgtptoltesucc
- apn-handoverstat-s2bgtptoltefail
- apn-handoverstat-ltetos2bgtpatt
- apn-handoverstat-ltetos2bgtpsucc
- apn-handoverstat-ltetos2bgtpfail
- apn-handoverstat-s2bgtptoehrpdatt
- apn-handoverstat-s2bgtptoehrpdsucc
- apn-handoverstat-s2bgtptoehrpdfail
- apn-handoverstat-ehrpdtos2bgtpatt
- apn-handoverstat-ehrpdtos2bgtpsucc
- apn-handoverstat-ehrpdtos2bgtpfail
- apn-handoverstat-s2agtptolteatt
- apn-handoverstat-s2agtptoltesucc
- apn-handoverstat-s2agtptoltefail
- apn-handoverstat-ltetos2agtpatt

- apn-handoverstat-ltetos2agtpsucc
- apn-handoverstat-ltetos2agtpfail

P-GW スキーマ

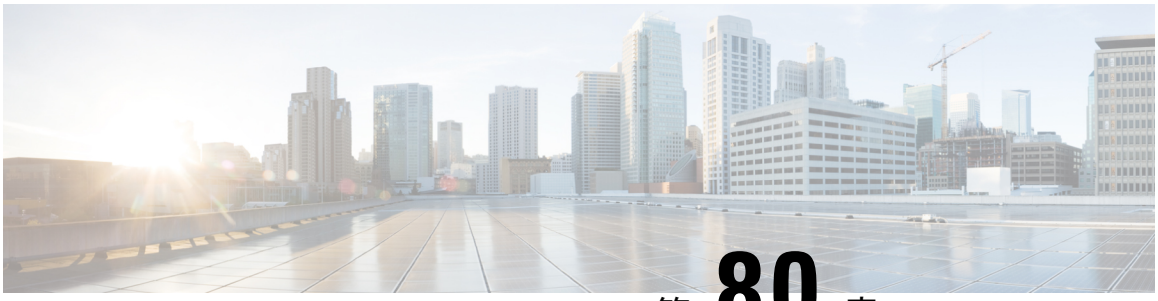
RAT テクノロジーに基づく開始されたセッションの統計情報：この機能強化では、RAT タイプごと、サービス/APN ごとに開始されたセッションの数を表示するために、次のカウンタが追加されました。

- sessstat-rat-init-eutran
- sessstat-rat-init-utran
- sessstat-rat-init-geran
- sessstat-rat-init-ehrpd
- sessstat-rat-init-s2a-gtp
- sessstat-rat-init-s2b-gtp
- sessstat-rat-init-s2b-pmip

SAEGW スキーマ

RAT テクノロジーに基づく開始されたセッションの統計情報：この機能強化では、RAT タイプごと、サービス/APN ごとに開始されたセッションの数を表示するために、次のカウンタが追加されました。

- pgw-sessstat-pdn-rat-init-eutran
- pgw-sessstat-pdn-rat-init-utran
- pgw-sessstat-pdn-rat-init-geran
- pgw-sessstat-pdn-rat-init-s2a-gtp
- pgw-sessstat-pdn-rat-init-s2b-gtp



第 80 章

Presence Reporting Area

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （1221 ページ）
- 機能説明 （1222 ページ）
- 機能の仕組み （1222 ページ）
- Multiple Presence Reporting Area （1225 ページ）
- Presence Reporting Area の設定 （1227 ページ）
- モニタリングおよびトラブルシューティング （1228 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW • S-GW
該当プラットフォーム	ASR 5500
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *S-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.4

機能説明

この機能により、3GPP 標準規格に準拠するためのプレゼンスレポートエリア（PRA）機能のサポートが追加されます。

プレゼンスレポートエリアは、エリア内の UE のプレゼンスをレポートするために、3GPP パケットドメイン内で定義されたエリアです。これはポリシー制御と課金シナリオに必要です。E-UTRAN では、PRA は、ネイバーまたは非ネイバーのトラッキングエリア、または eNB、またはセルのセットで構成できます。プレゼンスレポートエリアには、「UE 専用プレゼンスレポートエリア」と、MME プールに適用される「コアネットワーク事前設定プレゼンスレポートエリア」の 2 つのタイプがあります。

この機能には次のような特長があります。

- この機能は、LTE/S4-SGSN 関連の RAT タイプでサポートされています。他の RAT タイプの場合、P-GW は PCRF から受信した PRA 情報を無視します。
- 現在、仕様に準拠して、セッションごとに 1 つの PRA-ID がサポートされています。
- 現在、P-GW では、コアネットワーク事前設定プレゼンスレポートエリアがサポートされています。
- ICSR から N-1 へのリリースの場合、PRA 機能はサポートされていません。
- PRA-ID は、CDR インターフェイス、つまり Gz、Gy、および Rf ではサポートされていません。

機能の仕組み

IP-CAN セッション中、PCRF は、PRA での UE プレゼンス変更に関するレポートが IP-CAN セッションに必要かどうかを判断します。この判断は、サブスクライバのプロファイル設定とサポートされている AVP 機能に基づいて行われます。パラメータ CNO-ULI も同様に設定されます。IP-CAN セッションのレポートが必要である場合は、PCRF が Presence-Reporting-Area-Information AVP を PCEF に提供します。この AVP には、Presence-Reporting-Area-Identifier AVP 内の PRA 識別子が含まれています。UE 専用 PRA の場合、PCRF は、Presence-Reporting-Area-Elements-List AVP 内の PRA で構成される要素のリストを PCEF に提供します。PCRF は、IP-CAN セッション全体の任意の時点で、PCEF での CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT イベントトリガーをサブスクライブすることにより、PRA での UE プレゼンス変更に関するレポートをアクティブにする場合があります。

UE が PRA に入るか PRA から出ると、PCEF は、CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_ARE_REPORT イベントを報告します。また、PCEF は、Presence-Reporting-Area-Status AVP 内の PRA ステータスと、Presence-Area-Information AVP に含まれる Presence-Reporting-Area-Identifier AVP 内の PRA 識別子も報告します。

次の表では、このシナリオと、それに関連する動作について説明します。

シナリオ	動作
PCRF が初期コールセットアップとは異なる新しい PRA ID を送信する場合。	• P-GW は、初期コールセットアップ中に新しい PRA ID を受信し、PRA ID 情報を保存します。 • RAR では、PRA_EVENT_TRIGGER が登録されます。 • P-GW は、PRA_ACTION PRA ID="A", ACTION=start を送信します。 • CCA-U では、新しい PRA ID を受信します。 • P-GW は、新しい PRA ID 情報を保存します。 • P-GW は、PRA_ACTION PRA ID = "B", Action=start を送信しますが、以前の PRA に関する Action=stop は送信しません。 **重要** 理想的には、上記の条件の場合、PCRF は、最初にイベントトリガーを無効にして、新しい PRA-ID=B を送信し、後続のメッセージでイベントトリガーを有効にします。
PCRF が初期コールセットアップと同じである新しい PRA ID を送信する場合。	PRA ID は、S-GW に対して PRA アクションを送信せず、P-GW は、これを無視します。
PRA ID 復号化の動作	受信した PRA ID が「コアネットワーク事前設定 Presence Reporting Area」である場合、P-GW は PCRF からの「要素リスト」を無視します。それ以外の場合、PRA ID が「UE 専用 Presence Reporting Area」であれば、P-GW は「要素リスト」を解析し、アクセス側に転送します。

シナリオ	動作
PCRF からの PRA ID 値が 1 オクテット、2 オクテット、および 3 オクテットの場合。	PCRF から受信した値の MSB が評価されることで PRA タイプが確認されます。エンコード中に、GTPC 側のゼロが先頭に追加され、3 オクテットになります。 たとえば、PRA ID = FC (1111 1100) が PCRF から受信された場合、それは UE 専用 PRA と見なされ、復号化中に 00 00 FC として復号化されます。 P-GW は、PRA 情報を PCRF または UE から受信した場合、それをローミングサブスクライバに転送します。 **重要** Presence Reporting Area での UE プレゼンス変更に関するレポートは、ローミングシナリオには適用されません。
ローミングシナリオ	Presence Reporting Area での UE プレゼンス変更に関するレポートは、ローミングシナリオには適用されません。 サービング EPC ノード（MME、S4-SGSN）が変更されると、モビリティ手順中に、すべての PDN 接続の Presence Reporting Area 識別子が、MM コンテキスト情報の一部として、ターゲットのサービングノードに転送されます。Presence Reporting Area の要素のリストも、それらが P-GW によって提供される場合には転送されます。
ハンドオーバーの動作：PRA 識別子が送信元 MME/S4-SGSN からターゲット MME/S4-SGSN に通信される方法。	MME/S4-SGSN は、PRA 識別子を MM コンテキスト情報の一部として送信元 MME/S4-SGSN から取得します。 サービング EPC ノード（MME、S4-SGSN）が変更されると、モビリティ手順中に、すべての PDN 接続の Presence Reporting Area 識別子が、MM コンテキスト情報の一部として、ターゲットのサービングノードに転送されます。Presence Reporting Area の要素のリストも、それらが P-GW によって提供される場合には転送されます。
ハンドオフの動作：新しいアクセスタイプが PRA をサポートしていない場合に PRA を無効にする方法。	新しいアクセス PRA がサポートされていない場合、アクセスタイプと内部設定に応じて、PCRF は、PRA を非アクティブにします。 IP-CAN セッション中、P-GW は、UE があるアクセスタイプに位置することを PCRF に通知します。このアクセスタイプでは、ローカル PCRF 設定において、PRA での UE プレゼンス変更に関するレポートがサポートされません。PCRF は、PRA での UE プレゼンス変更のサブスクライブを解除します（以前にアクティブ化されている場合）。

シナリオ	動作
E-UTRAN で一部のノードが PRA をサポートしていない場合の動作。	PRA が PCRF から有効になっている場合、EPC ノードは、それをサポートします。すべてのノードがサポートされていない場合、PRA PCRF は、ロケーション変更レポートをアクティブにします。 **重要** E-UTRAN アクセスでは、ネットワーク内の Presence Reporting Area での UE プレゼンス変更に関するレポートの同種サポートが想定されています。PRA での UE プレゼンス変更に関するレポートが E-UTRAN でサポートされていることを PCRF 設定が示している場合、これは、すべての P-GW、すべての MME、およびすべての S-GW（ネットワーク共有モードで動作する MME と S-GW を含む）がそれをサポートしていることを意味します。PRA での UE プレゼンス変更に関するレポートがサポートされていない場合、PCRF は、代わりにセルまたはサービングエリアレベルでロケーション変更レポートをアクティブにすることができます。
アクセス側手順の失敗または衝突が発生した場合（ベアラーの作成または更新手順）。	PRA アクションが要求メッセージで送信された、ベアラーの更新または作成手順が失敗し、PRA 情報が応答メッセージで受信されなかった場合、P-GW は、次回の制御手順でリモートピアへの PRA アクションの送信を試みます。 PRA アクションが要求メッセージで送信された、ベアラーの更新または作成手順が失敗し、PRA 情報が応答メッセージで受信されなかった場合、P-GW は、PRA アクションがリモートピアに正常に伝達されたと見なします。 PRA アクションが要求メッセージで送信され、更新または作成手順が中止された、ベアラー更新または作成の衝突シナリオでは、P-GW は、次回の制御手順でリモートピアへの PRA アクションの送信を試みます。

Multiple Presence Reporting Area

重要 この機能はリリース 21.9.1 で導入されました。

P-GW は、PCRF を使用する Gx インターフェイスを介した Feature-List-ID 2 の Multiple-Presence Reporting Area 機能のネゴシエーションをサポートします。CNO-ULI 機能は、P-GW や PCRF が Multiple-PRA をサポートしておらず、P-GW と PCRF の両方が CNO-ULI をサポートしている場合にのみ使用されます。

IP-CAN セッションのライフタイム中に Multiple-PRA 機能がサポートされている場合、P-GW は、Presence-Reporting-Area-Information AVP（それぞれは Presence-Reporting-Area-Identifier AVP 内にプレゼンスレポートエリア識別子を含みます）を含む PRA-Install AVP の PCRF からのレポートエリア要求内にある UE プレゼンスの変更を処理します。

P-GW によるイベントトリガーの処理

プレゼンスレポートエリアでの UE プレゼンスの変更レポートのアクティブ化のための、PCRF からの CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT。

P-GW は、上記のように PRA-Install AVP 内の新しい PRA を使用して、または PRA-Remove AVP 内の既存の PRA を削除することにより、PCRF からの PRA 識別子変更要求を処理します。この場合、削除された PRA の Presence-Reporting-Area-Identifier AVP を Presence-Reporting-Area-Information AVP 内に含める必要があります。

P-GW は、次のメッセージで PCRF からの PRA-Install および PRA-Remove AVP をサポートしています。

- CC-Answer（CCA）コマンド
- Re-Auth-Request（RAR）コマンド

P-GW は、プレゼンスレポートエリアの UE プレゼンスの変更への登録を解除するための PCRF からの要求を処理します。PCRF は、以前にアクティブ化された場合に、値 CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT（48）が削除された Event-Trigger AVP を提供します。

P-GW は、任意の時点での IP-CAN セッションに対して最大 4 つの PRA をサポートします。PRA の最大数は PCRF で設定でき、4 つまでに制限する必要があります。P-GW は、4 つを超えるプレゼンスレポートエリア識別子エントリを無視します。

P-GW が、S5 または S8 インターフェイスを介してサービングノードからプレゼンスレポートエリア情報を受信し、UE が 1 つ以上のプレゼンスレポートエリアの内部または外部にある、またはいずれかのプレゼンスレポートエリアが非アクティブに設定されていることが通知された場合、P-GW は、報告されたプレゼンスレポートエリア識別子が、PCRF に関連するプレゼンスレポートエリアに対応するかどうかをチェックします。この場合、P-GW はさらに、Event-Trigger AVP で CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT イベントを報告します。また、P-GW は、Presence-Reporting-Area-Status AVP 内でプレゼンスレポートエリアのステータスを、また Presence-Reporting-Area-Identifier AVP 内でプレゼンスレポートエリア識別子を報告します（これらは、サービングノードにより報告される各プレゼンスレポートエリアの Presence-Reporting-Area-Information AVP に含まれます）。

P-GW は、PCRF および OCS がプレゼンスレポートエリアでの UE プレゼンスの変更をサブスクライブしていない場合に、プレゼンスレポートエリアの UE プレゼンスの変更を報告するための関連する IP-CAN 固有の手順を非アクティブにします。

PRA-Install AVP（3GPP-EPS アクセスタイプ）の定義

PRA-Install AVP（AVP コード 2845）はグループ化されたタイプであり、IP-CAN セッション用の新規または更新されたプレゼンスレポートエリアのリストをプロビジョニングするために使用されます。

AVP の形式

```
PRA-Install ::= < AVP Header: 2845 >
 *[ Presence-Reporting-Area-Information ]
 *[ AVP ]
```

PRA-Remove AVP（3GPP-EPS アクセスタイプ）の定義

PRA-Remove AVP（AVP コード 2846）はグループ化されたタイプであり、IP-CAN セッション用のプレゼンスレポートエリアリストの報告を停止するために使用されます。

AVP の形式

```
PRA-Remove ::= < AVP Header: 2846 >
 *[ Presence-Reporting-Area-Identifier ]
 *[ AVP ]
```

Presence Reporting Area の設定

PRA の設定

PRA を有効にするには、次の設定を使用します。

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        diameter encode-supported-features cno-uli
        { default | no } diameter encode-supported-features
        end
```

注：

- **diameterencode-supported-features**：Supported-Features AVP のエンコーディングと送信を有効または無効にします。
- **cno-uri**：Presence Reporting Area 情報レポート機能を有効にします。
- **no**：以前に設定されたサポート対象機能を削除します。
- **default**：このコマンドのデフォルト設定を適用します。

Multiple-PRA の設定

Multiple Presence Reporting Area（Multiple-PRA）機能を有効にするには、次の設定コマンドを使用します。

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        diameter encode-supported-features multiple-pra
```

```
{ default | no } diameter encode-supported-features
end
```

注：

- **ims-auth-service** *service_name*：IMS 認証サービスを作成します。*service_name* は 1 ～ 63 文字の英数字の文字列にする必要があります。
- **policy-control**：IMS 承認用の Diameter 承認とポリシー制御パラメータを設定します。
- **diameter encode-supported-features**：Supported-Features AVP のエンコードと送信を有効にします。
- **multiple-pra**：Multiple Presence Reporting 情報レポート機能を有効にします。
- **no**：以前に設定されたサポート対象機能を削除します。
- **default**：このコマンドのデフォルト設定を適用します。

モニタリングおよびトラブルシューティング

以下の章では、機能をモニターするために使用できるコマンドを説明します。

コマンドと出力の表示

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show ims-authorization service name *<service-name>*

上記のコマンドの出力が変更され、ネゴシエートされた条件付きポリシー機能に関連する情報が表示されるようになりました。変更された出力は次のとおりです。

```
Context: ha
  IMS Authorization Service name: imsa-Gx
                  ……
  Diameter Policy Control:
    Endpoint: gx.st16.starentnetworks.com
    Origin-Realm: starentnetworks.com
    Dictionary: r8-gx-standard
    Supported Features:
      mission-critical-qcis
      conditional-policy-info-default-qos
cno-uli
    Request Timeout:
        Initial Request   : 100 deciseconds
        Update Request    : 100 deciseconds
        Terminate Request : 100 deciseconds
    Endpoint Peer Select: Not Enabled
    Reauth Trigger: All
    Custom Reauth Trigger:
      QoS-Change
```

show ims-authorization sessions full all

このコマンドの出力には、次のフィールドが含まれています。

```
CallId: 00004e26            Service Name: imsa-Gx
  IMSI:  123456789012349
  Session ID: gx.st16.starentnetworks.com;20006;2305;598ab8cf-102
  Bearer Type: GTP
  SGSN IP-Addr: 192.168.23.4
  APN: starent.com
  Bearer Control Mode: UE/NW
  State: Connected
  Negotiated Supported Features:
    3gpp-r8
    conditional-policy-info-default-qos
    cno-uli
  Auth Decision:
    Event Triggers:
      QoS-Change
      RAT-Change
      Change-Of-UE-Presence-In-PRA
      Usage-Report
      Resource-Modification-Request
    multiple-pra
```

show ims-authorization service statistics

上記のコマンドの出力が変更され、PRA機能の統計が表示されるようになりました。変更された出力は次のとおりです。

```
IMS Auth Service Statistics Summary:
Total Services:      2
Auth Session:
  Current Active:               1
  Current Fallback Session:     0             Current PCRF Session:          1
  Total Attempted:              1             Total Setup:                   1
  Total Failed:                 0             Total Released:                0
  Total Fallback:               0
Re-Authorization Triggers:
  SGSN Change:                  0             PLMN Change:                   0
  RAT Change:                   0             TFT Change:                    0
  Bearer Recovery:              0             Bearer Loss:                   0
  QoS Change:                   0             Policy Failure:                0
  IP-CAN Change:                0             Resources Limitation:          0
  Max Num of Bearers Rchd:      0             QoS Chng Exceeding Auth:       0
  RAI Change:                   0             User Location Change:          0
  TAI Change:                   0             ECGI Change:                   0
  PCRF Triggered ReAuth:        0             Preservation Changed:          0
  Reactivation Changed:         0             Revalidation Timeout:          0
  AN GW Changed:                0             Out Of Credit Reauth:          0
  Reallocation Of Credit:       0             Def EPS Bearer QoS Chng:       0
  Successful Resource Alloc:    0             Usage Report:                  0
  Service Flow Detection:       0             UE Timezone Change:            0
UE IP Address Allocate:         0             UE IP Address Release:         0
  Resource Modification Req:    0             APN AMBR Mod Failure:          0
  Def Bearer QOS Mod Failure:   0             Tethering Flow Detected:       0
  Chrg Correlation Exchange:    0             Subnet Change:                 0
  Session Recovery:             0             Session Sync:                  0
  Access Nw Info Report:        0             DCCA Failure Report:           0
  Application Start:            0             Application Stop:              0
  Change Of UE Presence In PRA: 1
```

```
Local Fallback:
CCRU sent:                      0
```

show subscribers pgw-only full all

このコマンドの出力には、次のフィールドが含まれています。

```
Username        : xyz
Subscriber Type : Visitor
Status          : Online/Active
State           : Connected
Connect Time    : Mon Aug 28 07:32:13 2017
Auto Delete     : No
Idle time       : 00h00m06s
MS TimeZone     : n/a                   Daylight Saving Time: n/a
Access Type: gtp-pdn-type-ipv4          Network Type: IP
Access Tech: eUTRAN                     pgw-service-name: pgw1
Callid: 00004e23                        IMSI: 123456789012349
MSISDN: 9326737733
Interface Type: S5S8GTP                 Low Access Priority: N/A
TWAN Mode: N/A
eMPS Bearer: No
Emergency Bearer Type: N/A
IMS-media Bearer: No
S6b Auth Status: Enabled
Access Peer Profile: default
Acct-session-id (C1): C0A8170100000003
ThreeGPP2-correlation-id (C2): 00500660 / 002shwI-
Card/Cpu: 2/0                           Sessmgr Instance: 1
ULI:
 TAI-ID:
  MCC: 214  MNC: 365
  TAC: 0x6789
 ECGI-ID:
  MCC: 214 MNC: 365
  ECI: 0x1234567
PRA Information:
 PRA-ID: 0x801204      Action: Start           Status: In
PRA Information:
 PRA-ID: 0xA11202      Action: Start           Status: N/A
```

show subs saegw-only full all

上記のコマンドの出力が変更され、PRA-ID、PRA ステータス、PRA アクションなどの PRA 情報が含まれるようになりました。変更された出力は次のとおりです。

```
Username          : xyz
SAEGW Call mode   : Co-located
Subscriber Type   : Visitor
Status            : Online/Active
State             : Connected
Bearer State      : Active
Connect Time      : Mon Aug 28 08:21:45 2017

SAEGW UID         : 10001
Idle time         : 00h00m19s
Auto Delete       : No
Callid            : 4e25                        IMSI                : 241460144418770
Card/Cpu          : 2/0                         Sessmgr Instance    : 1
Source context    : ingress                     Destination context : egress
Bearer Type       : Default                     Bearer-Id           : 5
```

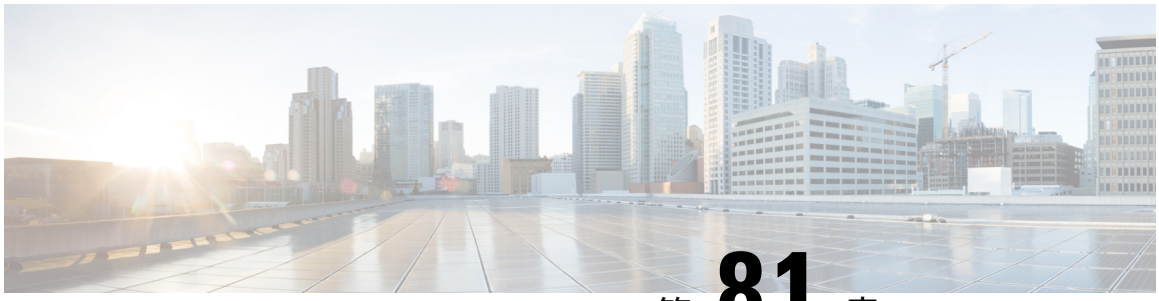
```
Access Type       : gtp-pdn-type-ipv4          Network Type        : IP
Access Tech       : eUTRAN                     saegw-service-name  : saegw
MSISDN            : 9326737733
TWAN Mode         : N/A
eMPS Bearer       : No
IPv6 alloc type   : n/a
ECS Rulebase      : prepaid
Chrg Char Sel Mod : Peer Supplied
Restoration priority level : n/a
HLCOM Session     : No
IP Address        : 10.0.0.5
Bearer capable for restoration: No
UE P-CSCF Restoration Support : No

Peer Profile      :
  PGW Access      : default
  SGW Access      : default
  SGW Network     : default

ULI               : TAI-ID
  MCC             : 214                        MNC             : 365
  LAC             : n/a                        TAC             : 0x6789
  SAC             : n/a                        RAC             : n/a
  CI              : n/a                        ECI             : 0x1234567

PRA Information   :
  PRA-ID: 0xFC0104     Action: Start          Status: In

Bearer QoS        :
 QCI              : 5
 ARP              : 0x08
 PCI              : 0 (Enabled)
 PL               : 2
 PVI              : 0 (Enabled)
 MBR Uplink(bps)  : 0                          MBR Downlink(bps)   : 0
 GBR Uplink(bps)  : 0                          GBR Downlink(bps)   : 0
```



第 81 章

プロキシモバイル IP

この章では、プロキシモバイル IP のシステムサポートについて説明し、その設定方法を示します。製品アドミニストレーションガイドには、システム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、お使いのサービスモデルに最適な設定例を選択することを推奨します。

プロキシモバイル IP は、簡易 IP のみをサポートできるモバイルノード（MN）を持つサブスクライバにモビリティソリューションを提供します。

この章は、次の項で構成されています。

- 概要 （1233 ページ）
- 3GPP2 ネットワークにおけるプロキシモバイル IP の仕組み （1237 ページ）
- 3GPP ネットワークにおけるプロキシモバイル IP の仕組み （1243 ページ）
- WiMAX ネットワークにおけるプロキシモバイル IP の仕組み （1246 ページ）
- 複数認証がある Wi-Fi ネットワークにおけるプロキシモバイル IP の仕組み （1251 ページ）
- プロキシモバイル IP サポートの設定 （1256 ページ）

概要

プロキシモバイル IP は、モバイル IP プロトコルスタックをサポートしていない MN を持つサブスクライバにモビリティを提供します。

重要 プロキシモバイル IP は、シスコのライセンス機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

プロキシモバイル IP 機能は、さまざまな製品でサポートされています。この機能がサポートされている製品と、その製品に関連する章の参照先を次の表にを示します。

表 *112 :* 対象製品と関連するセクション

対象製品	参照先
PDSN	• 3GPP2 サービスのプロキシモバイル IP （1235 ページ） • 3GPP2 ネットワークにおけるプロキシモバイル IP の仕組み （1237 ペ • FA サービスの設定 （1257 ページ） • プロキシ MIP HA フェールオーバーの設定 （1258 ページ） • *HA* サービスの設定 • サブスクライバプロファイル RADIUS 属性の設定 （1259 ページ） • プロキシモバイル IP に必要な RADIUS 属性 （1259 ページ） • PDSN でのプロキシ MIP のローカル サブスクライバ プロファイルの （1261 ページ） • ホーム エージェント コンテキストでのデフォルト サブスクライバ タの設定 （1262 ページ）
GGSN	• 3GPP サービスのプロキシモバイル IP （1236 ページ） • 3GPP ネットワークにおけるプロキシモバイル IP の仕組み （1243 ペ • FA サービスの設定 （1257 ページ） • プロキシ MIP HA フェールオーバーの設定 （1258 ページ） • *HA* サービスの設定 • サブスクライバプロファイル RADIUS 属性の設定 （1259 ページ） • プロキシモバイル IP に必要な RADIUS 属性 （1259 ページ） • ホーム エージェント コンテキストでのデフォルト サブスクライバ タの設定 （1262 ページ） • APN パラメータの設定 （1262 ページ）

対象製品	参照先
ASN GW	• WiMAX サービスのプロキシモバイル IP （1236 ページ） • WiMAX ネットワークにおけるプロキシモバイル IP の仕組み （124 • FA サービスの設定 （1257 ページ） • プロキシ MIP HA フェールオーバーの設定 （1258 ページ） • *HA* サービスの設定 • サブスクライバプロファイル RADIUS 属性の設定 （1259 ページ） • プロキシモバイル IP に必要な RADIUS 属性 （1259 ページ） • ホーム エージェント コンテキストでのデフォルト サブスクライバ タの設定 （1262 ページ）
PDIF	• 複数認証がある Wi-Fi ネットワークにおけるプロキシモバイル IP （1251 ページ） • FA サービスの設定 （1257 ページ） • プロキシ MIP HA フェールオーバーの設定 （1258 ページ） • *HA* サービスの設定 • サブスクライバプロファイル RADIUS 属性の設定 （1259 ページ） • プロキシモバイル IP に必要な RADIUS 属性 （1259 ページ） • ホーム エージェント コンテキストでのデフォルト サブスクライバ タの設定 （1262 ページ）

3GPP2 サービスのプロキシモバイル IP

プロキシモバイル IP を使用したサブスクライバセッションの場合、RP および PPP セッションは、簡易 IP セッションの場合と同様に、MN と PDSN の間で確立されます。ただし、PDSN/FA は、MN に代わって HA（サブスクライバのプロファイルに保存されている情報で識別）とモバイル IP 操作を実行します（つまり、MN は PDSN との簡易 IP PPP セッションを維持する役割のみを担います）。

MN には、PDSN/FA または HA によって IP アドレスが割り当てられます。送信元と関係なく、アドレスは HA に保存されているモバイル バインディング レコード（MBR）に保存されます。したがって、MN がサービスプロバイダーのネットワークを介してローミングするとき、ハンドオフが発生するたびに、MN は HA 上の MBR に保存されているのと同じ IP アドレスを使用し続けます。

単一の PPP リンクを介して複数のセッションを実行できるモバイル IP 対応 MN とは異なり、プロキシモバイル IP は PPP リンクを介した単一のセッションだけを許可することに注意して

ください。さらに、モバイル IP および簡易 IP の同時セッションについては、現在 MN のプロキシモバイル IP セッションを可能にしている FA が MN に対してサポートすることはありません。

MN には、HA、AAA サーバー、または静的のいずれかによって IP アドレスが割り当てられます。このアドレスは HA に格納されているモバイル バインディング レコード（MBR）に格納されます。したがって、MN がサービスプロバイダーのネットワークを介してローミングするとき、ハンドオフが発生するたびに、MN は HA 上の MBR に保存されているのと同じ IP アドレスを使用し続けます。

3GPP サービスのプロキシモバイル IP

プロキシモバイル IP を使用する IP PDP コンテキストの場合、MN は通常どおり GGSN とのセッションを確立します。ただし、GGSN/FA は、MN に代わって HA（サブスクライバのプロファイルに保存されている情報で識別）とモバイル IP 操作を実行します（つまり、MN は GGSN との簡易 IP PDP コンテキストを維持する役割のみを担い、MN との間でエージェント アドバタイズメント メッセージのやり取りはありません）。

MN には、HA、AAA サーバー、または静的のいずれかによって IP アドレスが割り当てられます。このアドレスは HA に格納されているモバイル バインディング レコード（MBR）に格納されます。したがって、MN がサービスプロバイダーのネットワークを介してローミングするとき、ハンドオフが発生するたびに、MN は HA 上の MBR に保存されているのと同じ IP アドレスを使用し続けます。

プロキシモバイル IP は、サブスクライバのユーザープロファイルに含まれている情報に基づいてサブスクライバごとに個別に実行することも、特定の APN で有効なすべてのサブスクライバに対して実行することもできます。非トランスペアレント IP PDP コンテキストの場合、サブスクライバのプロファイルから返された属性が APN の設定よりも優先されます。

WiMAX サービスのプロキシモバイル IP

プロキシモバイル IP を使用したサブスクライバセッションの場合、サブスクライバセッションは、簡易 IP セッションの場合と同様に、MN と ASN GW の間で確立されます。ただし、ASN GW/FA は、MN に代わって HA（サブスクライバのプロファイルに保存されている情報で識別）を使用してモバイル IP 操作を実行します（つまり、MN は ASN GW との簡易 IP サブスクライバセッションを維持する役割のみを担います）。

MN には、ASN GW/FA または HA によって IP アドレスが割り当てられます。送信元と関係なく、アドレスは HA に保存されているモバイル バインディング レコード（MBR）に保存されます。したがって、MN がサービスプロバイダーのネットワークを介してローミングするとき、ハンドオフが発生するたびに、MN は HA 上の MBR に保存されているのと同じ IP アドレスを使用し続けます。

単一のセッションリンクを介して複数のセッションを実行できるモバイル IP 対応 MN とは異なり、プロキシモバイル IP は、セッションリンクを介した単一のセッションだけを許可することに注意してください。さらに、モバイル IP および簡易 IP の同時セッションについては、

現在 MN のプロキシモバイル IP セッションを可能にしている FA が MN に対してサポートすることはありません。

3GPP2 ネットワークにおけるプロキシモバイル IP の仕組み

このセクションには、成功したプロキシモバイル IP セッションのセットアップシナリオを示すコールフローが含まれています。MN で IP アドレスを受信する方法に応じた複数のシナリオが存在します。以下のシナリオについて説明します。

- **シナリオ 1**：PDSN で MN を認証する AAA サーバーが MN に IP アドレスを割り当てます。PDSN がそれ自体の IP プールからアドレスを割り当てることはない点に注意してください。
- **シナリオ 2**：HA が、ローカルに設定されたダイナミックプールの 1 つから MN に IP アドレスを割り当てます。

シナリオ 1：AAA サーバーと PDSN/FA が IP アドレスを割り当てる

MN が AAA サーバーと PDSN/FA から IP アドレスを受け取る場合のコールフローの図と説明を以下に示します。

図 *101 : AAA* と *PDSN* が割り当てた *IP* アドレスプロキシのモバイル *IP* コールフロー

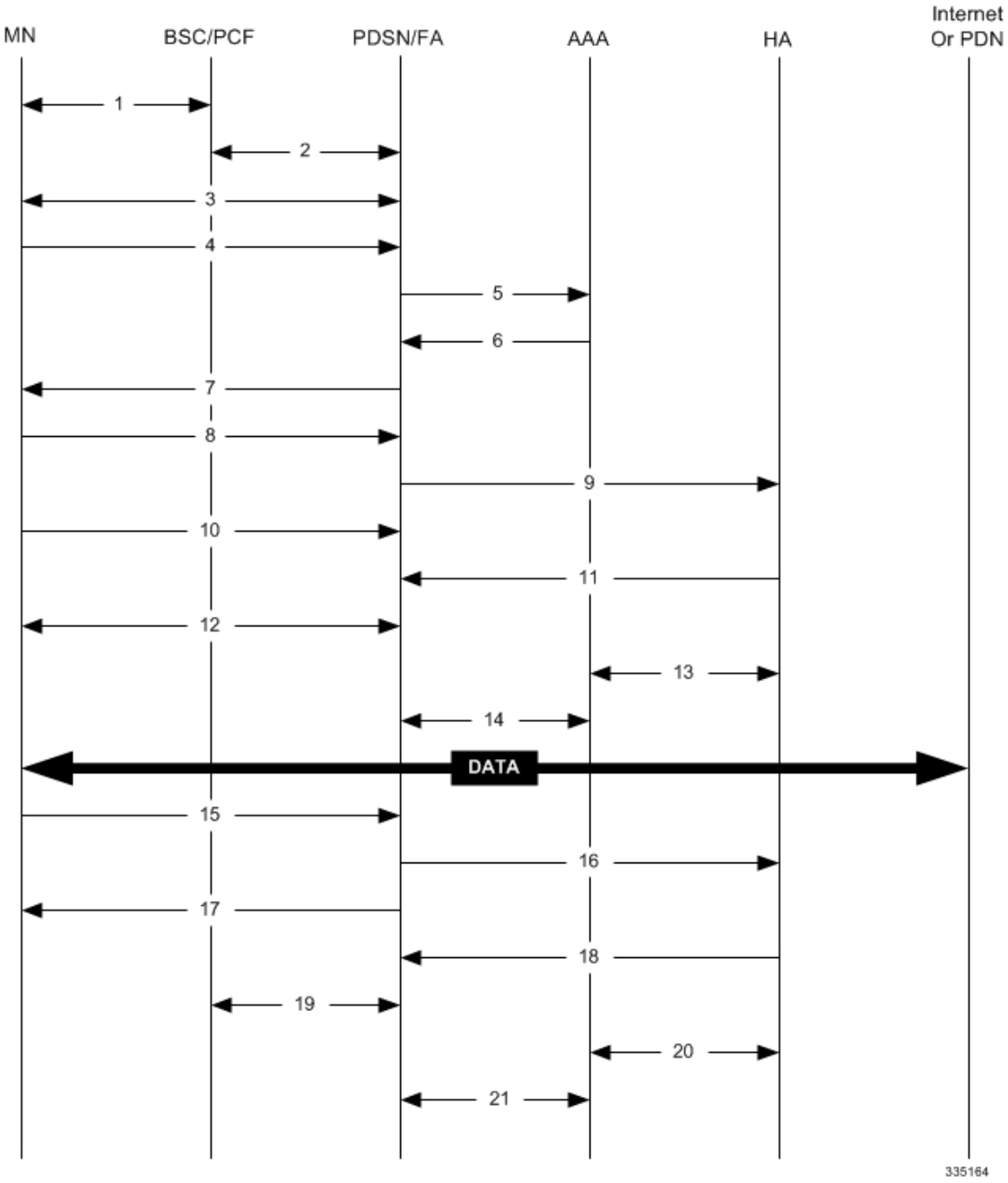


表 *113 : AAA* と *PDSN* が割り当てた *IP* アドレスプロキシのモバイル *IP* コールフローの説明

ステップ	説明
1	モバイルノード（MN）は、BSC/PCF を介して RAN とのエアリンク上のトラフィックチャネ します。
2	PCF と PDSN/FA が、セッションの R-P インターフェイスを確立します。
3	PDSN/FA と MN が、リンク制御プロトコル（LCP）をネゴシエートします。
4	LCP のネゴシエーションが成功すると、MN は PPP 認証要求メッセージを PDSN/FA に送信し
5	PDSN/FA は、アクセス要求メッセージを RADIUS AAA サーバーに送信します。
6	RADIUS AAA サーバーは、サブスクライバを正常に認証すると、PDSN/FA に Access Accept を返します。この Accept メッセージには、MN のホームアドレス（IP アドレス）や使用する アドレスなど、MN に割り当てられるさまざまな属性が含まれる場合があります。
7	PDSN/FA は、PPP 認証応答メッセージを MN に送信します。
8	MN は、インターネットプロトコル制御プロトコル（IPCP）設定要求メッセージを、MN アド を使用して PDSN/FA に送信します。
9	PDSN/FA は、プロキシモバイル IP 登録要求メッセージを HA に転送します。このメッセージ のホームアドレス、FA の IP アドレス（care-of-address）、FA-HA 拡張（セキュリティ パラメ デックス（SPI））などのフィールドが含まれます。
10	FA が HA と通信している間に、MN が追加の IPCP 設定要求メッセージを送信する場合があ
11	HA は、ホームアドレスをそのプールに対して検証した後、プロキシモバイル IP 登録応答で す。また、HA は、サブスクライバセッションのモバイル バインディング レコード（MBR） ます。
12	MN と PDSN/FA が IPCP をネゴシエートします。その結果、MN には AAA サーバーで元々指 いたホームアドレスが割り当てられます。
13	MN および PDSN/FA が IPCP をネゴシエートしている間に、HA と AAA サーバーがアカウン を開始します。
14	IPCP ネゴシエーションが完了すると、PDSN/FA と AAA サーバーはアカウンティングを開始 PDN 間でデータの送受信が可能なセッションを完全に確立します。
15	セッションが完了すると、MN は LCP 終了要求メッセージを PDSN に送信し、PPP セッショ ます。
16	PDSN/FA は、プロキシモバイル IP 登録解除要求メッセージを HA に送信します。
17	PDSN/FA は、PPP セッションを終了する MN に LCP 終了確認応答メッセージを送信します。

ステップ	説明
18	HA は、Pi インターフェイスを終了する FA にプロキシモバイル IP 登録解除応答メッセージを送す。
19	PDSN/FA と PCF が R-P セッションを終了させます。
20	HA と AAA サーバーが、セッションのアカウンティングを停止します。
21	PDSN と AAA サーバーが、セッションのアカウンティングを停止します。

シナリオ 2：HA が IP アドレスを割り当てる

MN が HA から IP アドレスを受け取る場合のコールフローの図と説明を以下に示します。

図 *102 : HA* が割り当てた *IP* アドレスのプロキシモバイル *IP* コールフロー

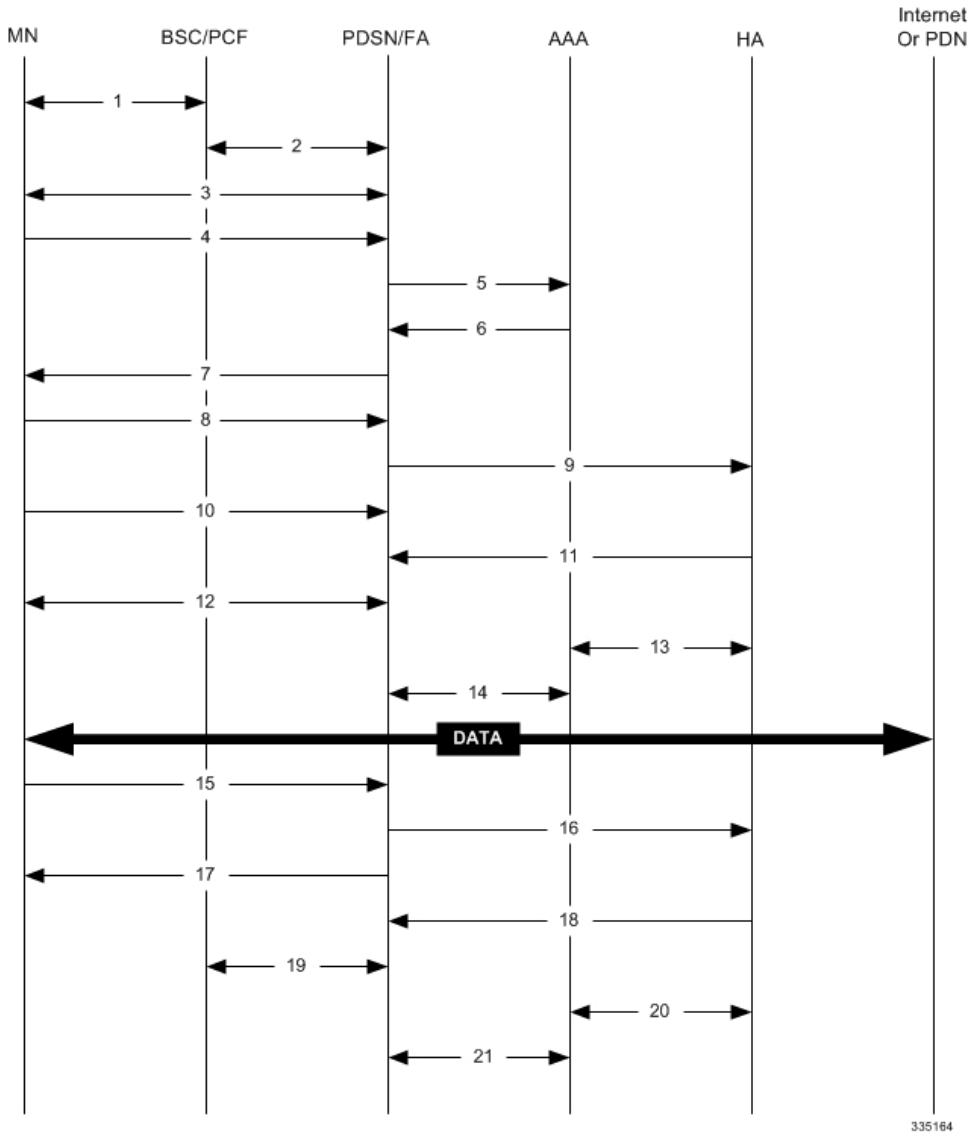


表 *114 : HA* が割り当てた *IP* アドレスのプロキシモバイル *IP* コールフローの説明

ステップ	説明
1	モバイルノード（MN）は、BSC/PCF を介して RAN とのエアリンク上のトラフィックチャネ します。
2	PCF と PDSN/FA が、セッションの R-P インターフェイスを確立します。
3	PDSN/FA と MN が、リンク制御プロトコル（LCP）をネゴシエートします。
4	LCP のネゴシエーションが成功すると、MN は PPP 認証要求メッセージを PDSN/FA に送信し

ステップ	説明
5	PDSN/FA は、アクセス要求メッセージを RADIUS AAA サーバーに送信します。
6	RADIUS AAA サーバーは、サブスクライバを正常に認証すると、PDSN/FA に Access Accept メッ を返します。この Accept メッセージには、使用する HA の IP アドレスなど、MN に割り当てら まざまな属性が含まれる場合があります。
7	PDSN/FA は、PPP 認証応答メッセージを MN に送信します。
8	MN は、インターネットプロトコル制御プロトコル（IPCP）設定要求メッセージを、MN アドレス を使用して PDSN/FA に送信します。
9	PDSN/FA は、プロキシモバイル IP 登録要求メッセージを HA に転送します。このメッセージに 0.0.0.0 のホームアドレスインジケータ、FA の IP アドレス（care-of-address）、および FA-HA 拡 キュリティ パラメータ インデックス（SPI））などのフィールドが含まれます。
10	FA が HA と通信している間に、MN が追加の IPCP 設定要求メッセージを送信する場合があり
11	HA が、プロキシモバイル IP 登録応答で応答します。この応答には、MN に割り当てるために に設定されたプールの 1 つからの IP アドレス（ホームアドレス）が含まれます。また、HA は、 クライバセッションのモバイル バインディング レコード（MBR）も作成します。
12	MN と PDSN/FA が IPCP をネゴシエートします。その結果、MN には AAA サーバーで元々指定 いたホームアドレスが割り当てられます。
13	MN および PDSN/FA が IPCP をネゴシエートしている間に、HA と AAA サーバーがアカウンテ を開始します。
14	IPCP ネゴシエーションが完了すると、PDSN/FA と AAA サーバーはアカウンティングを開始し、 PDN 間でデータの送受信が可能なセッションを完全に確立します。
15	セッションが完了すると、MN は LCP 終了要求メッセージを PDSN に送信し、PPP セッションを ます。
16	PDSN/FA は、プロキシモバイル IP 登録解除要求メッセージを HA に送信します。
17	PDSN/FA は、PPP セッションを終了する MN に LCP 終了確認応答メッセージを送信します。
18	HA は、Pi インターフェイスを終了する FA にプロキシモバイル IP 登録解除応答メッセージを送 す。
19	PDSN/FA と PCF が R-P セッションを終了させます。
20	HA と AAA サーバーが、セッションのアカウンティングを停止します。
21	PDSN と AAA サーバーが、セッションのアカウンティングを停止します。

3GPP ネットワークにおけるプロキシモバイル IP の仕組み

このセクションには、3GPP ネットワークでの成功したプロキシモバイル IP セッションのセットアップのシナリオを示すコールフローが含まれています。

次の図とその後のテキストで、3GGP サービスでの成功したプロキシモバイル IP セッションのセットアップのコールフロー例について説明します。

図 *103 : 3GPP* でのプロキシモバイル *IP* コールフロー

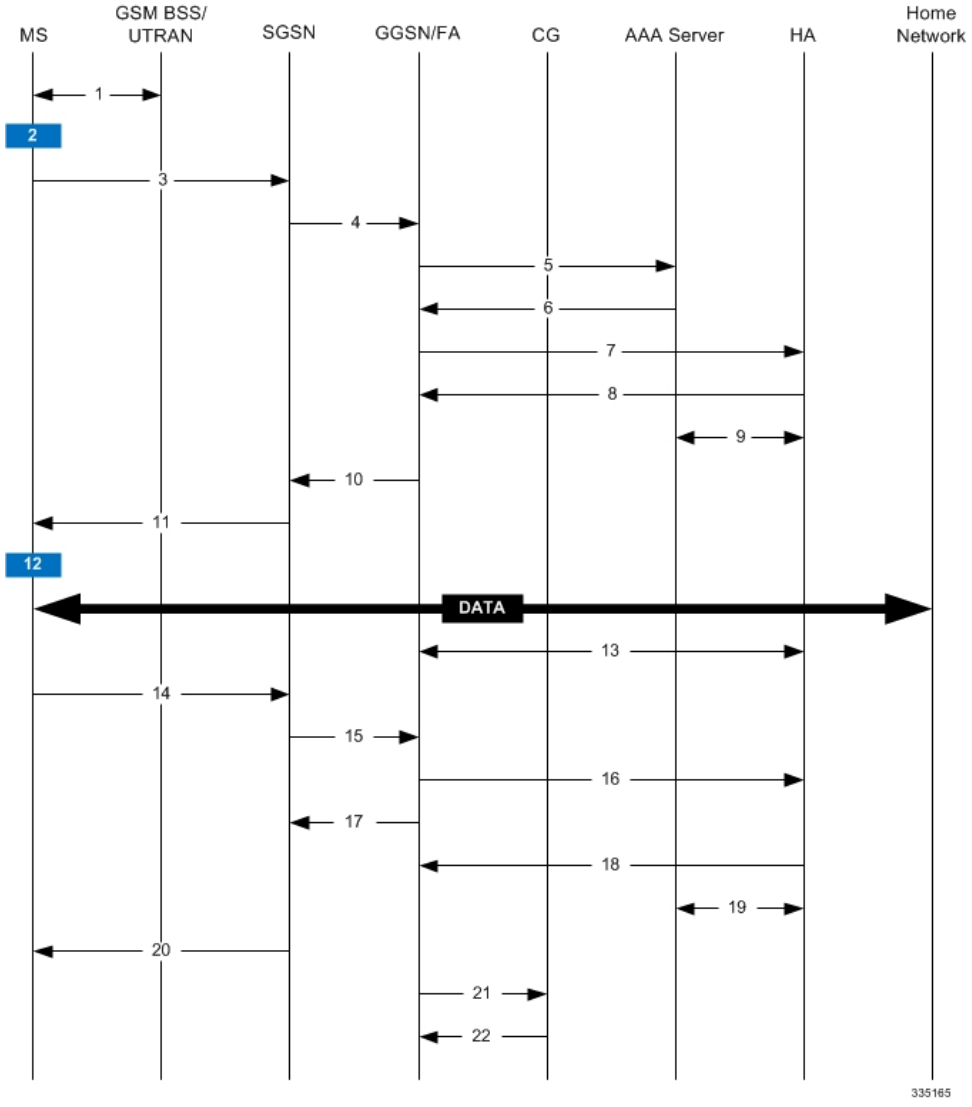


表 *115 : 3GPP* でのプロキシモバイル *IP* コールフローの説明

ステップ	説明
1	モバイルステーション（MS）が、GPRS/UMTS ネットワークに自身をアタッチするプロセスを実す。
2	MS の端末装置（TE）部分が、MS のモバイル端末（MT）部分に AT コマンドを送信して PPP モします。 その後、Link Control Protocol（LCP）を使用して、最大受信ユニットサイズと認証プロトコル（Challenge-Handshake Authentication Protocol（CHAP）、Password Authentication Protocol（PAP）はなし）を設定します。CHAP または PAP が使用される場合は、TE が MT に対して自身を認証の後 MT が認証情報を格納します。 認証が成功すると、TE が Internet Protocol Control Protocol（IPCP）設定要求メッセージを MT にます。このメッセージは、使用する静的 IP アドレスを含むか、IP アドレスが動的に割り当てらとを要求します。
3	MS が PDP コンテキストアクティブ化要求メッセージを送信し、SGSN がそれを受信します。このセージには、ネットワーク層サービスアクセスポイント識別子（NSAPI）、PDP タイプ、PDP アス、アクセスポイント名（APN）、要求された Quality of Service（QoS）、PDP 設定オプションサブスクライバに関する情報が含まれます。
4	SGSN が、要求メッセージを認証し、GPRS トンネリングプロトコル（GTPC、「C」はこのプロの制御シグナリング部分を示す）を使用して GGSN に PDP コンテキスト作成要求メッセージをます。受信側の GGSN は、MS の要求に基づいて選択されるか、SGSN によって自動的に選択されこのメッセージは、PDP タイプ、PDP アドレス、APN、課金特性、トンネルエンドポイント識別子アドレスが静的な場合は TEID）などのさまざまな情報要素で構成されます。
5	GGSN は、（メモリまたは CPU リソース、設定などの観点で）セッションを促進できるかどう断し、PDP コンテキストリストに新しいエントリを作成して、セッションの課金 ID を提供しま GGSN は、メッセージで指定された APN から、サブスクライバの認証されるかどうかと、プロバイル IP がサブスクライバでサポートされるかどうかを判断し、サポートされる場合は、接続の IP アドレスを判断します。 プロキシモバイル IP のサポートは、ユーザーのプロファイルの属性でも判断できることに注意ださい。APN 設定よりも、ユーザーのプロファイルの属性が優先されます。 認証が必要な場合、GGSN は、メモリ内に格納されているプロファイルに対してサブスクライバカルに認証するか、RADIUS Access-Request メッセージを AAA サーバーに送信することを試み
6	GGSN がサブスクライバを AAA サーバーに対して認証した場合、AAA サーバーは、認証の成功RADIUS Access-Accept メッセージと、サブスクライバ PDP コンテキストを処理するための属性ます。

ステップ	説明
7	APN またはサブスクライバのプロファイルのいずれかでプロキシモバイル IP サポートが有効 いる場合は、GGSN/FA が、指定された HA にプロキシモバイル IP 登録要求メッセージを転送 このメッセージには、MS のホームアドレス、FA の IP アドレス（care-of-address）、FA-HA セ キュリティ パラメータ インデックス（SPI））などが含まれます。
8	HA が、プロキシモバイル IP 登録応答で応答します。この応答には、MS に割り当てるために に設定されたプールの 1 つからの IP アドレス（ホームアドレス）が含まれます。また、HA は クライバセッションのモバイル バインディング レコード（MBR）も作成します。
9	HA が RADIUS アカウンティング開始要求を AAA サーバーに送信し、AAA サーバーが応答
10	GGSN が、GTPC を使用して肯定的な PDP コンテキスト作成応答で応答します。この応答に よって要求された静的アドレスまたは GGSN によって割り当てられたアドレスのいずれかを アドレス、PDP アドレスを参照するために使用される TEID、GGSN によって指定された PD ションなどの情報要素が含まれます。
11	SGSN が、MS に PDP コンテキストアクティブ化承認メッセージを返します。このメッセー 初の要求で送信された設定パラメータへの応答が含まれます。
12	MT が、TE の IPCP 設定要求に対して IPCP 設定 ACK メッセージで応答します。 これで、MS は、セッションが終了するかタイムアウトになるまで、PDN との間でデータを送 ます。モバイル IP の場合、MS に対して 1 つの PDP コンテキストのみがサポートされること てください。
13	FA が、プロキシモバイル IP 登録要求更新メッセージを HA に定期的に送信します。HA は、 に応答を送信します。
14	MSは、いつでもデータセッションを終了させることができます。セッションを終了するため PDP コンテキスト非アクティブ化要求メッセージを送信し、SGSN がそれを受信します。
15	SGSNが、データセッションを促進するPDPコンテキスト削除要求メッセージをGGSNに送信 このメッセージには、PDP コンテキストを識別するために必要な情報要素（TEID、NSAPI な まれます。
16	GGSN がメモリから PDP コンテキストを削除し、FA がプロキシモバイル IP 登録解除要求メ HA に送信します。
17	GGSN が、SGSN に PDP コンテキスト削除応答メッセージを返します。
18	HA が、プロキシモバイル IP 登録解除要求応答で FA に応答します。
19	HA が、RADIUS アカウンティング停止要求を AAA サーバーに送信し、AAA サーバーが応答
20	SGSN が、MS に PDP コンテキスト非アクティブ化承認メッセージを返します。

ステップ	説明
21	GGSN が、GTP プライム（GTPP）を使用して、GGSN 課金詳細レコード（G-CDR）を課金ゲイ（CG）に配信します。この例では示されていませんが、PDP コンテキストがアクティブであに部分的な CDR を送信するように GGSN をオプションで設定できることに注意してください。
22	GGSN から受信した各アカウンティングメッセージに対して、CG が確認応答で応答します。

WiMAX ネットワークにおけるプロキシモバイル IP の仕組み

このセクションには、成功したプロキシモバイル IP セッションのセットアップシナリオを示すコールフローが含まれています。MN で IP アドレスを受信する方法に応じた複数のシナリオが存在します。以下のシナリオについて説明します。

- **シナリオ 1**：ASN GW で MN を認証する AAA サーバーが MN に IP アドレスを割り当てます。ASN GW がそれ自体の IP プールからアドレスを割り当てることはない点に注意してください。
- **シナリオ 2**：HA が、ローカルに設定されたダイナミックプールの 1 つから MN に IP アドレスを割り当てます。

シナリオ 1：AAA サーバーと ASN GW/FA が IP アドレスを割り当てる

MN が AAA サーバーと ASN GW/FA から IP アドレスを受け取る場合のコールフローの図と説明を以下に示します。

図 *104 : AAA/ASN GW* が割り当てた *IP* アドレスプロキシのモバイル *IP* コールフロー

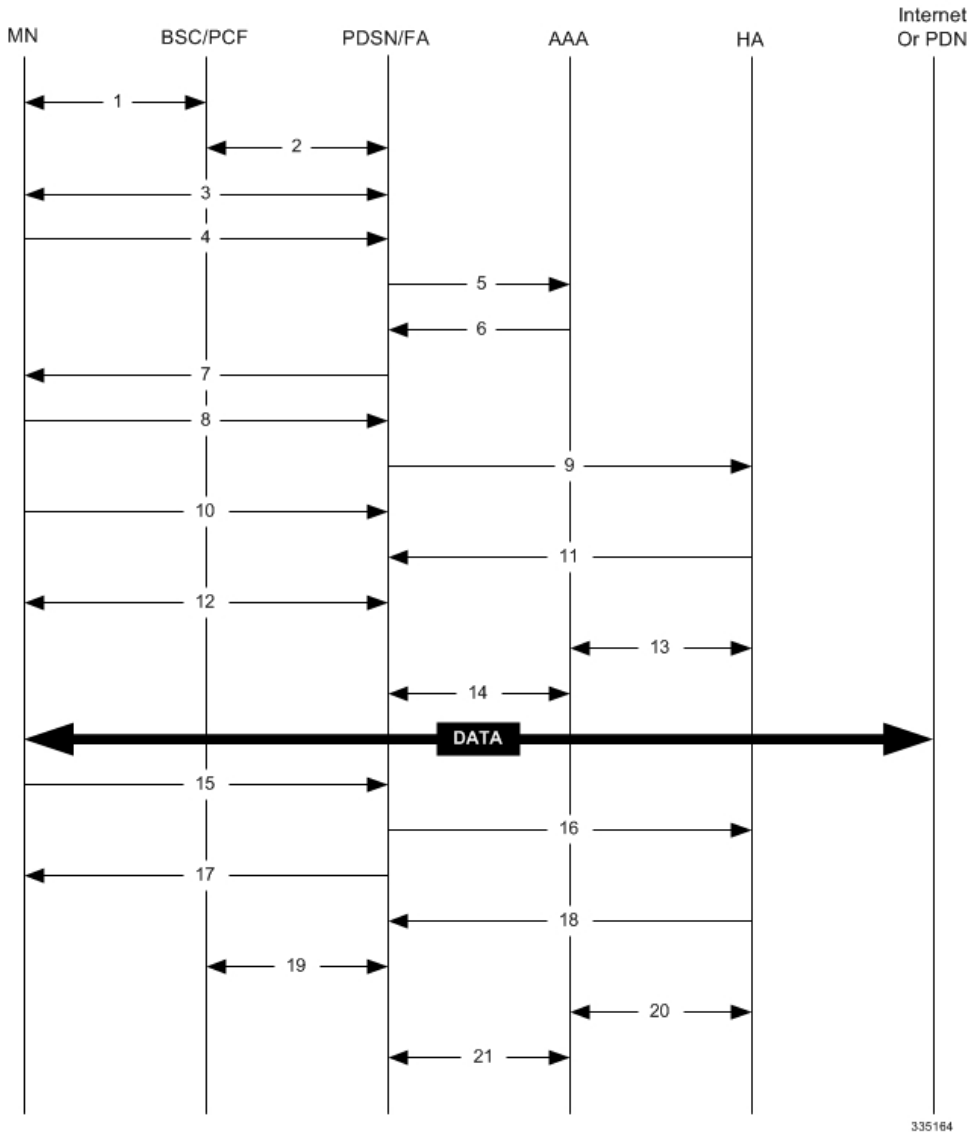


表 *116 : AAA/ASN GW* が割り当てた *IP* アドレスプロキシのモバイル *IP* コールフローの説明

ステップ	説明
1	モバイルノード（MN）は、BS とのエアリンク上のトラフィックチャネルを保護します。
2	BS と ASN GW/FA が、セッションの R6 インターフェイスを確立します。
3	ASN GW/FA と MN が、リンク制御プロトコル（LCP）をネゴシエートします。
4	LCP のネゴシエーションが成功すると、MN は PPP 認証要求メッセージを ASN GW/FA に送信

ステップ	説明
5	ASN GW/FA は、アクセス要求メッセージを RADIUS AAA サーバーに送信します。
6	RADIUS AAA サーバーは、サブスクライバを正常に認証すると、ASN GW/FA に Access Accept メッセージを返します。この Accept メッセージには、MN のホームアドレス（IP アドレス）や使用する IP アドレスなど、MN に割り当てられるさまざまな属性が含まれる場合があります。
7	ASN GW/FA は、EAP 認証応答メッセージを MN に送信します。
8	MN は、インターネットプロトコル制御プロトコル（IPCP）設定要求メッセージを、MN アドレスを使用して ASN GW/FA に送信します。
9	ASN GW/FA は、プロキシモバイル IP 登録要求メッセージを HA に転送します。このメッセージ MN のホームアドレス、FA の IP アドレス（care-of-address）、FA-HA 拡張（セキュリティ パラインデックス（SPI））などのフィールドが含まれます。
10	FA が HA と通信している間に、MN が追加の IPCP 設定要求メッセージを送信する場合があります
11	HA は、ホームアドレスをそのプールに対して検証した後、プロキシモバイル IP 登録応答で応答す。また、HA は、サブスクライバセッションのモバイル バインディング レコード（MBR）もます。
12	MN と ASN GW/FA が IPCP をネゴシエートします。その結果、MN には AAA サーバーで元々指ていたホームアドレスが割り当てられます。
13	MN および ASN GW/FA が IPCP をネゴシエートしている間に、HA と AAA サーバーがアカウングを開始します。
14	IPCP ネゴシエーションが完了すると、ASN GW/FA と AAA サーバーはアカウンティングを開始と PDN 間でデータの送受信が可能なセッションを完全に確立します。
15	セッションが完了すると、MN は LCP 終了要求メッセージを ASN GW に送信し、サブスクライションを終了します。
16	PDSN/FA は、プロキシモバイル IP 登録解除要求メッセージを HA に送信します。
17	ASN GW/FA は、サブスクライバセッションを終了する MN に LCP 終了確認応答メッセージを送す。
18	HA は、R3 インターフェイスを終了する FA にプロキシモバイル IP 登録解除応答メッセージを送す。
19	ASN GW/FA と BS が R6 セッションを終了させます。
20	HA と AAA サーバーが、セッションのアカウンティングを停止します。
21	ASN GW と AAA サーバーが、セッションのアカウンティングを停止します。

シナリオ 2：HA が IP アドレスを割り当てる

MN が HA から IP アドレスを受け取る場合のコールフローの図と説明を以下に示します。

図 *105 : HA* が割り当てた *IP* アドレスのプロキシモバイル *IP* コールフロー

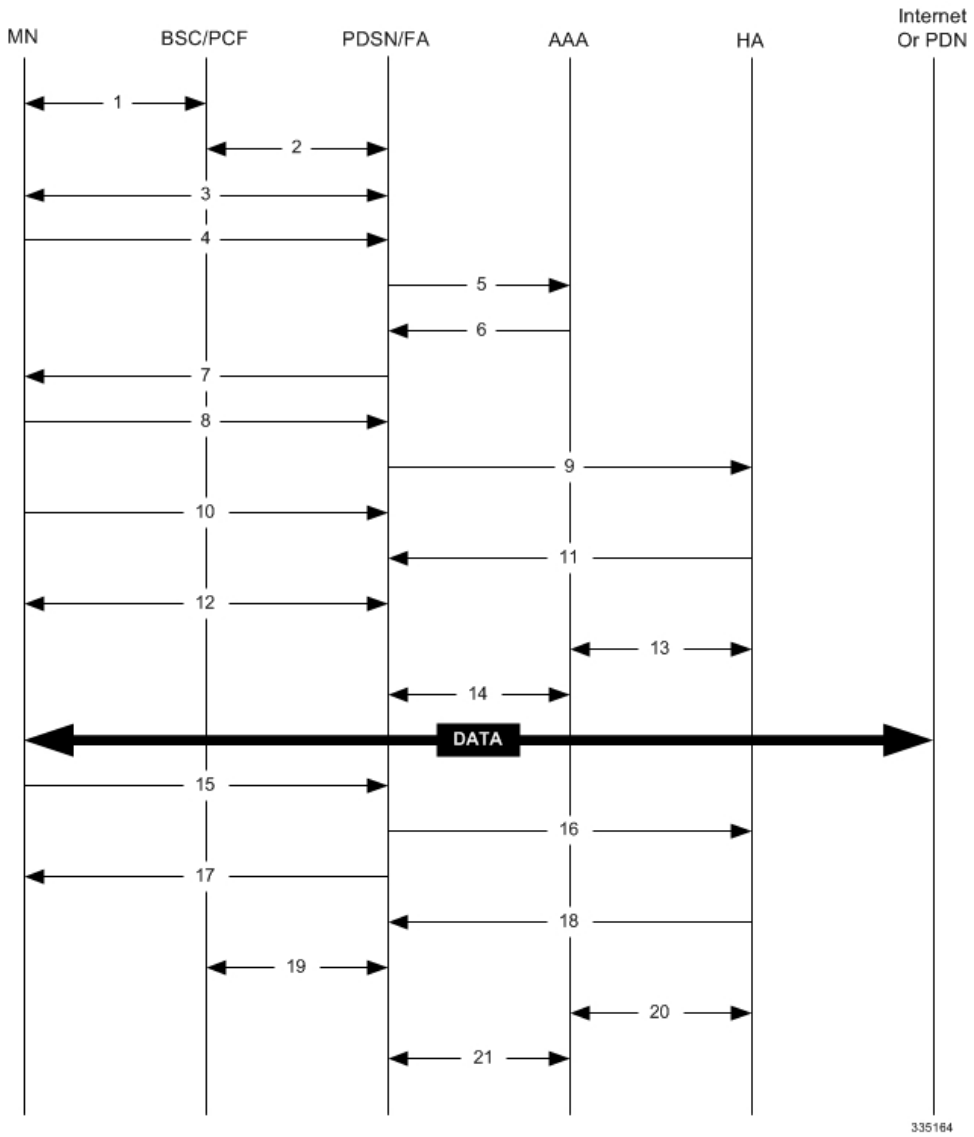


表 *117 : HA* が割り当てた *IP* アドレスのプロキシモバイル *IP* コールフローの説明

ステップ	説明
1	モバイルノード（MN）は、BS とのエアリンク上のトラフィックチャネルを保護します。
2	BS と ASN GW/FA が、セッションの R6 インターフェイスを確立します。

ステップ	説明
3	ASN GW/FA と MN が、リンク制御プロトコル（LCP）をネゴシエートします。
4	LCP のネゴシエーションが成功すると、MN は EAP 認証要求メッセージを ASN GW/FA に送信し
5	ASN GW/FA は、アクセス要求メッセージを RADIUS AAA サーバーに送信します。
6	RADIUS AAA サーバーは、サブスクライバを正常に認証すると、ASN GW/FA に Access Accept メ ジを返します。この Accept メッセージには、使用する HA の IP アドレスなど、MN に割り当て さまざまな属性が含まれる場合があります。
7	ASN GW/FA は、EAP 認証応答メッセージを MN に送信します。
8	MN は、インターネットプロトコル制御プロトコル（IPCP）設定要求メッセージを、MN アドレス を使用して ASN GW/FA に送信します。
9	ASN GW/FA は、プロキシモバイル IP 登録要求メッセージを HA に転送します。このメッセージ 0.0.0.0 のホームアドレスインジケータ、FA の IP アドレス（care-of-address）、および FA-HA 拡 キュリティ パラメータ インデックス（SPI））などのフィールドが含まれます。
10	FA が HA と通信している間に、MN が追加の IPCP 設定要求メッセージを送信する場合があり
11	HA が、プロキシモバイル IP 登録応答で応答します。この応答には、MN に割り当てるために に設定されたプールの 1 つからの IP アドレス（ホームアドレス）が含まれます。また、HA は、 クライバセッションのモバイル バインディング レコード（MBR）も作成します。
12	MN と ASN GW/FA が IPCP をネゴシエートします。その結果、MN には AAA サーバーで元々指 ていたホームアドレスが割り当てられます。
13	MN および ASN GW/FA が IPCP をネゴシエートしている間に、HA と AAA サーバーがアカウン グを開始します。
14	IPCP ネゴシエーションが完了すると、ASN GW/FA と AAA サーバーはアカウンティングを開始 と PDN 間でデータの送受信が可能なセッションを完全に確立します。
15	セッションが完了すると、MN は LCP 終了要求メッセージを ASN GW に送信し、サブスクライ ションを終了します。
16	ASN GW/FA は、プロキシモバイル IP 登録解除要求メッセージを HA に送信します。
17	ASN GW/FA は、PPP セッションを終了する MN に LCP 終了確認応答メッセージを送信します。
18	HA は、R3 インターフェイスを終了する FA にプロキシモバイル IP 登録解除応答メッセージを送 す。
19	ASN GW/FA と BS が R6 セッションを終了させます。
20	HA と AAA サーバーが、セッションのアカウンティングを停止します。

ステップ	説明
21	ASN GW と AAA サーバーが、セッションのアカウンティングを停止します。

複数認証がある Wi-Fi ネットワークにおけるプロキシモバイル IP の仕組み

プロキシモバイル IP は、モバイル IP を運用できないモバイルサブスクライバ（MS）のネットワークの結果として開発されました。このシナリオでは、PDIF がモバイル IP クライアントとして機能するため、プロキシ MIP サポートが実装されます。

プロキシ MIP ネットワークにおいて必須ではありませんが、この実装では「マルチ認証」と呼ばれる手法が使用されます。マルチ認証方式では、デバイスは、最初に HSS サーバーを使用して認証されます。デバイスが認証されると、サブスクライバは、RADIUS インターフェイスを介して AAA サーバーに認証されます。これは、ネットワーク内の既存の EV-DO サーバーをサポートしています。

MS は、最初に PDIF との IKEv2 セッションを確立しようとします。MS は、HSS サーバーと通信するために、SCTP over IPv6 を介した Diameter による最初のデバイス認証に EAP-AKA 認証方式を使用します。最初の Diameter EAP 認証の後に、MS は続いて EAP MD5/GTC 認証を行います。

デバイス認証が成功すると、PDIF は、サブスクライバ認証のために、RADIUS を使用して AAA サーバーと通信します。RADIUS AAA サーバーが EAP 方式を使用せず、そのために RADIUS メッセージには EAP 属性が含まれないことが前提となっています。

RADIUS 認証が成功した場合、PDIF は、制御トラフィックのみを渡すために、トンネル内部アドレス（TIA）を使用して IPSec 子 SA トンネルをセットアップします。PDIF は、ホームエージェントから MS アドレスを受信し、IKEv2 交換で最終認証応答を通して MS アドレスを MS に渡します。

IPSec ネゴシエーションが完了すると、PDIF は、ホームアドレスを MS に割り当て、データを渡すための子 SA を確立します。初期 TIA トンネルが破棄され、IP アドレスがアドレスプールに返されます。その後、PDIF が、RADIUS アカウンティングの START メッセージを生成します。

セッションが切断されると、PDIF は、RADIUS アカウンティングの STOP メッセージを生成します。

次の図では、CHAP 認証（EAP-MD5）を使用したプロキシ MIP セッションのセットアップが示されていますが、EAP-MD5 が PDIF または MS によってサポートされていない場合は、EAP-GTC を使用した PAP 認証のセットアップにも対応しています。

図 *106 : CHAP* 認証を使用したプロキシ *MIP* コールのセットアップ

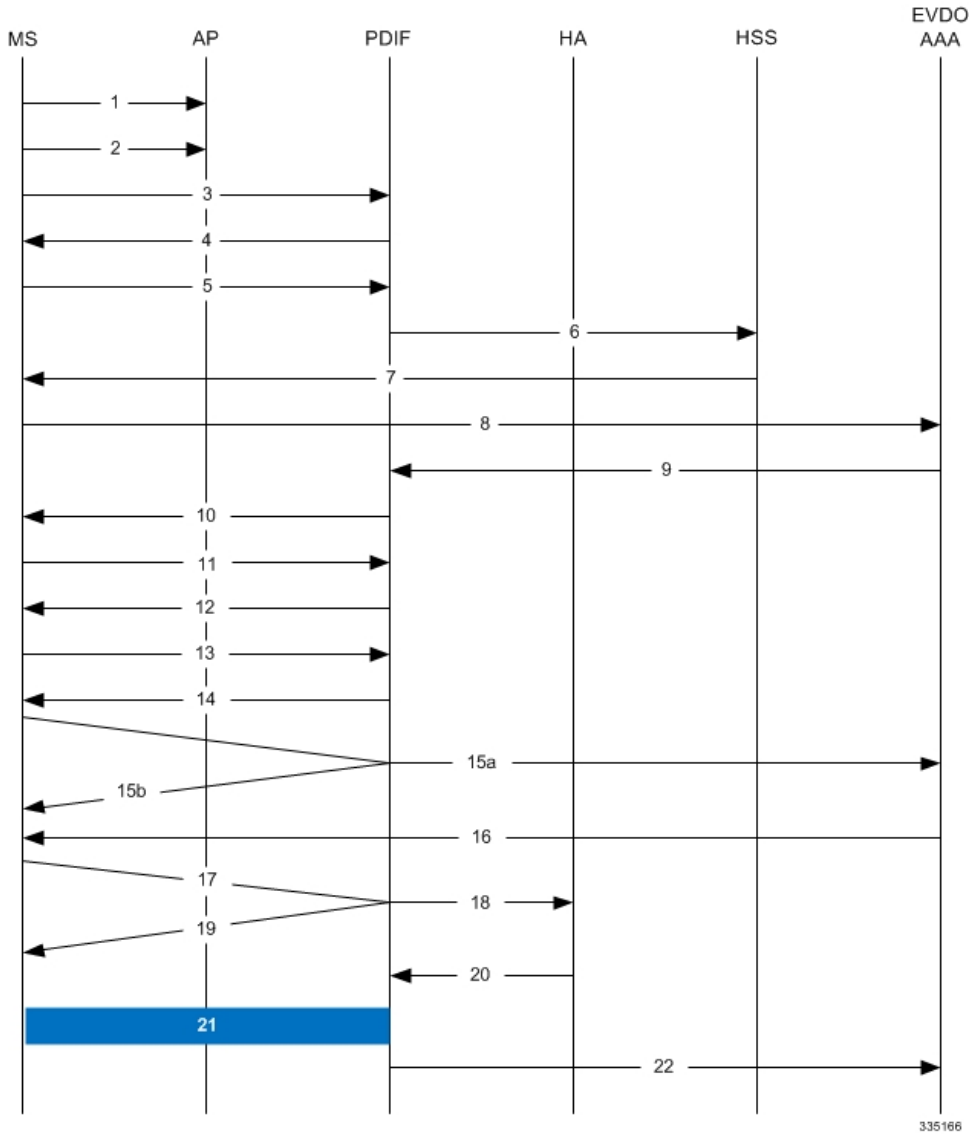


表 *118 : CHAP* 認証を使用したプロキシ *MIP* コールのセットアップ

ステップ	説明
1	Wi-Fi ネットワークに接続すると、MS が、最初に DNS クエリを送信して PDIF IP アドレスを ます。
2	MS が、DNS から PDIF アドレスを受信します。
3	MS が、IKE_SA_INIT 要求を PDIF に送信することにより、IKEv2/IPSec トンネルをセットア ます。MS は、IKEv2 交換に SA、KE、Ni、NAT-DETECTION 通知ペイロードを含めます。

ステップ	説明
4	PDIF が、（IKEv2 INIT 要求の宛先 IP アドレスによってバインドされた）適切な PDIF サ IKE_SA_INIT 要求を処理します。PDIF は、SA、KE、Nr ペイロードおよび NAT-DETECT ペイロードを含む IKE_SA_INIT 応答で応答します。PDIF サービスでマルチ認証サポート なるように設定されている場合、PDIF は、IKE_SA_INIT 応答に MULTIPLE_AUTH_SUPP 知ペイロードを含めます。PDIF は、IKE_SA_INIT 応答の送信後に、IKEv2 セットアップ 開始します。
5	PDIF から正常な IKE_SA_INIT 応答を受信すると、MS が、最初の EAP-AKA 認証のために、 要求を送信します。MS は、マルチ認証を実行できる場合、IKE_AUTH 要求に MULTI_AUTH_SUPPORTED 通知ペイロードを含めます。MS は、NAI、SA、TSi、TSr、 側の IP アドレスと DNS アドレス）ペイロードを含む IDi ペイロードも含めます。MSは、 ソッドを使用することを示す AUTH ペイロードは含めません。
6	MS から IKE_AUTH 要求を受信すると、PDIF が、Diameter AAA サーバーに DER メッセ します。AAA サーバーは、ドメインプロファイル、デフォルトのサブスクライバテンプ たはデフォルトのドメイン設定に基づいて選択されます。PDIF は、DER に、Multiple-Au AVP、EAP-Payload AVP を EAP-Response/Identity とともに含めます。正確な詳細については メッセージの項を参照してください。PDIF は、MS から IKE_AUTH 要求を受信すると、 セットアップ タイマーを開始します。
7	PDIF が、EAP 認証を続行するように指定する Result-Code AVP を含む DEA を受信します。 EAP-Payload AVP の値を取得し、EAP ペイロードで MS に IKE_AUTH 応答を送信します。 PDIF サービスでの IDr および CERT 設定を可能にし、オプションで（設定に応じて）IDr CERT ペイロードを含めることができます。PDIF サービスがそのように設定されている場 はオプションで IKE_AUTH 応答に AUTH ペイロードを含めます。
8	MS が、PDIF から IKE_AUTH 応答を受信します。MS は、交換を処理し、EAP ペイロー しい IKE_AUTH 要求を送信します。PDIF は、MS から新しい IKE_AUTH 要求を受信し、 AAA サーバーに送信します。この DER メッセージには、MS から受信した EAP-AKA チ 答およびチャレンジを含む EAP-Payload AVP が含まれます。
9	AAA サーバーが、「success」の Result-Code AVP を含む DEA を PDIF に返信します。EA AVP メッセージには、「success」を含む EAP 結果コードも含まれます。DEA には、ユー も含まれます。これは Callback-Id AVP に含まれています。PDIF は、この IMSI を、後続 セッション管理機能（重複セッション検出など）に使用します。また、PDIF は、AAA か 受信します。これは、追加のキー計算に使用されます。
10	PDIF が、EAP ペイロードを含む IKE_AUTH 応答を MS に返信します。
11	MS が、キーから計算された AUTH ペイロードを含む、最初の認証のための最終 IKE_AU 送信します。MS は、2 つ目の認証を実行する予定である場合、ANOTHER_AUTH_FOLL ペイロードも含めます。

ステップ	説明
12	PDIF が、AUTH 要求を処理し、MSK から計算された AUTH ペイロードを含む IKE_AUTH 応答します。PDIF は、2 つ目の認証を保留中の MS に IP アドレスを割り当てません。また、PD設定ペイロードも含めません。 a. PDIF サービスがマルチ認証をサポートしておらず、ANOTHER_AUTH_FOLLOWS 通知ペードを受信した場合、PDIF は、適切なエラーを含む IKE_AUTH 応答を送信し、INFORMATION除）要求を送信して IKEv2 セッションを終了します。b. IKE_AUTH 要求に ANOTHER_AUTH_FOLLOWS 通知ペイロードが含まれていない場合、PDIF は、ローカルにれたプールから IP アドレスを割り当てます。ただし、**proxy-mip-required** が有効になっている PDIF は、P-MIP RRQ を送信することにより、HA へのプロキシ MIP セットアップを開始しPDIF は、プロキシ MIP RRP を受信すると、ホームアドレスを（DNS アドレスがある場合はそ取得し、ホームアドレスと DNS アドレスを含む CP ペイロードを含めた IKE_AUTH 応答を M信します。いずれの場合も、IKEv2 のセットアップはこの段階で終了し、IPSec トンネルは内部アドレス（TIA）で確立されます。
13	MS が、NAI を含む IDi ペイロードを含めた IKE_AUTH 要求を送信することにより、2 つ目の実行します。この NAI は、最初の認証で使用された NAI とはまったく異なる場合がありま
14	2 つ目の認証の IKE_AUTH 要求を受信すると、PDIF が、設定されている 2 つ目の認証方式をクします。2 つ目の認証は、EAP-MD5（デフォルト）または EAP-GTC のいずれかです。EA式は、EAP-Passthru または EAP-Terminated のいずれかです。 a. 設定された方式が EAP-MD5 である場合、PDIF は、チャレンジを含む EAP ペイロードを含IKE_AUTH 応答を送信します。b. 設定された方式が EAP-GTC である場合、PDIF は、EAP-C含む IKE_AUTH 応答を送信します。c. MS は、IKE_AUTH 応答を処理します。 • MS が EAP-MD5 をサポートしており、受信した方式が EAP-MD5 である場合、MS は、ンジを実行し、応答を計算して、チャレンジと応答を含む EAP ペイロードを含めた IKE要求を送信します。 • MS が EAP-MD5 ではなく EAP-GTC をサポートしており、受信した方式が EAP-MD5 で合、MS は、EAP-GTC を含む従来の Nak を送信します。
15(a)	PDIF が、MS から新しい IKE_AUTH 要求を受信します。 元の方式が EAP-MD5 であり、MD5 チャレンジおよび応答が受信された場合、PDIF は、対応性（チャレンジ、チャレンジ応答、NAI、IMSI など）を持つ RADIUS アクセス要求を送信し
15(b)	元の方式が EAP-MD5 であり、GTC を含む従来の Nak が受信された場合、PDIF が、EAP-GTむ IKE_AUTH 応答を送信します。
16	PDIF が、RADIUS からアクセス承認を受信し、EAP 成功を含む IKE_AUTH 応答を送信しま
17	PDIF が、AUTH ペイロードを含む最終 IKE_AUTH 要求を受信します。

ステップ	説明
18	PDIF が、AUTH ペイロードの有効性をチェックし、**proxy-mip-required** が有効になってい ホームエージェントへのプロキシ MIP セットアップ要求を開始します。HA アドレスは、 承認（ステップ 16）で RADIUS サーバーから受信することも、ローカルに設定すること す。PDIF は、最終 DEA メッセージで受信した最初の認証の HA アドレスも記憶してい ります。
19	**proxy-mip-required** が無効になっている場合、PDIF が、ローカルプールから IP アドレス ます。
20	PDIF が、プロキシ MIP RRP を受信し、IP アドレスと DNS アドレスを取得します。
21	PDIF が、ホームアドレスを使用して IPSec トンネルをセットアップします。IKE_AUTH すると、MS も、受信した IP アドレスを使用して IPSec トンネルをセットアップします。 IP アドレスと、オプションで DNS アドレスを含む CP ペイロードを含めることにより、 応答を MS 返信します。これでセットアップは完了です。
22	PDIF が、RADIUS アカウンティング開始メッセージを送信します。

重要 PAP を使用したプロキシ MIP コールセットアップの場合、最初の 14 ステップは、CHAP 認証と同じです。ただし、MS は EAP-MD5 認証ではなく EAP-GTC をサポートしているため、ここではそれらが異なります。EAP-MD5 チャレンジへの応答では、MS は代わりに、EAP-GTC を含む従来の Nak で応答します。次の図はこの時点での動作を示しています。

図 *107 : PAP* 認証を使用したプロキシ *MIP* コールのセットアップ

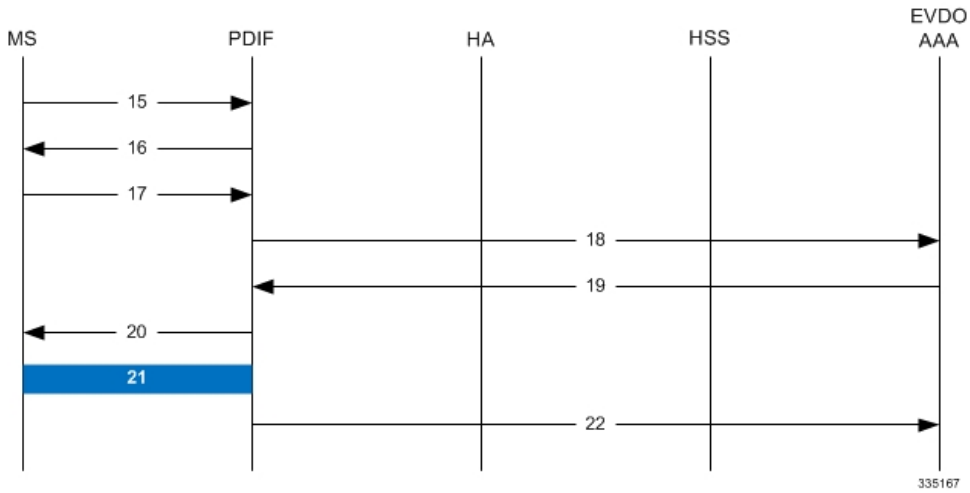


表 *119 : PAP* 認証を使用したプロキシ *MIP* コールのセットアップ

ステップ	説明
15	MS ではCHAP 認証ではなく PAP 認証が可能であり、MS が、EAP ペイロードを返信して、EA 認証が必要であることを示します。
16	PDIF が、EAP-GTC 手順を開始し、MS にパスワードを要求します。
17	MS が、PDIF への EAP ペイロードに認証パスワードを含めます。
18	パスワードを受信すると、PDIF が、User-Name 属性と PAP-password に NAI を含む RADIUS ス要求を送信します。
19	認証に成功すると、AAA サーバーが、RADIUS Access Accept メッセージを返します。このメ ジには、Framed-IP-Address 属性を含めることができます。
20	PDIF が MS に IKE_AUTH 応答を送信するときに、Access Accept メッセージの属性コンテン EAP 成功を含む EAP ペイロードとしてエンコードされます。
21	これで、MS と PDIF が、通信のためのセキュアな IPSec トンネルを確立します。
22	Pdif が、アカウンティング START メッセージを送信します。

プロキシモバイル IP サポートの設定

プロキシモバイル IP をサポートするには、次の設定を行う必要があります。

重要 すべてのコマンドとキーワード/変数がサポートされているわけではありません。これは、プラットフォームのタイプとインストールされているライセンスによって異なります。

- **FA サービス**：プロキシモバイル IP を有効にし、動作パラメータを設定し、FA-HA セキュリティ アソシエーションを指定する必要があります。
- **HA サービス**：FA-HA セキュリティ アソシエーションを指定する必要があります。
- **サブスクライバプロファイル**：サブスクライバがプロキシモバイル IP を使用できるように属性を設定する必要があります。これらの属性は、システム上にローカルで、または RADIUS サーバー上にリモートで保存されているサブスクライバプロファイルにおいて設定できます。
- **APN テンプレート**：プロキシモバイル IP は、APN の設定に基づく特定の APN テンプレートによって支援される、すべてのサブスクライバ IP PDP コンテキストでサポートできます。

重要　これらの説明は、それぞれの製品のアドミニストレーションガイドに記載されている手順に従って、サブスクライバ データ セッションをコアネットワークサービスや HA としてサポートするようシステムがあらかじめ設定されていることを前提としています。

FA サービスの設定

次の例を使用して、プロキシモバイル IP をサポートするように FA サービスを設定します。

```
configure
 context <context_name>
 fa-service <fa_service_name>
 proxy-mip allow
 proxy-mip max-retransmissions <integer>
 proxy-mip retransmission-timeout <seconds>
 proxy-mip renew-percent-time percentage
 fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number
number { encrypted secret enc_secret | secret secret } [ description string ][
hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | replay-protection {
timestamp | nonce } | timestamp-tolerance tolerance ]
authentication mn-ha allow-noauth
 end
```

注：

- **proxy-mip max-retransmissions** コマンドは、プロキシモバイル IP 登録要求を HA に送信するときに FA サービスが行うことができる最大再試行回数を設定します。
- **proxy-mip retransmission-timeout** は、プロキシモバイル IP 登録要求メッセージを再送信する前に、HA からの応答を待機する、FA によって許可される最大時間を設定します。
- **proxy-mip renew-percent-time** は、FA がプロキシモバイル IP 登録更新要求を送信するまでの経過時間を設定します。

例

FA サービスに設定されているアドバタイズメント登録の有効期間が 900 秒に設定されており、更新時間が 50 に設定されている場合、FA はプロキシ MIP 登録要求で 900 秒の有効期間を要求します。HA により **600** 秒の有効期間が与えられた場合、FA は **300** 秒が経過した後にプロキシモバイル IP 登録更新要求メッセージを送信します。

- **fa-ha-spi remote-address** コマンドを使用して、プロキシモバイル IP をサポートするように設定済みの FA-HA SPI を変更します。完全なコマンドシンタックスについては、『*Command Line Interface Reference*』を参照してください。



重要　プロキシ MIP 機能を動作させるには FA-HA SPI の設定が**必須**ですが、通常の MIP ではオプションであることに注意してください。

- **authentication mn-ha allow-noauth** コマンドを使用して、HA を認証せずに HA から通信できるように FA サービスを設定します。

FA サービス設定の確認

次のコマンドを使用して、FA サービスの設定を確認します。

show fa-service name *<fa_service_name>*

注：

- プロキシ MIP をサポートするように追加の FA サービスを設定するには、必要に応じてこの例を繰り返します。
- Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

オプションのプロキシ MIP HA フェールオーバーの設定 （1258 ページ） に進んでプロキシ MIP HA フェールオーバーのサポートを設定するか、「*HA* サービスの設定」に進み、プロキシモバイル IP の HA サービスのサポートを設定します。

プロキシ MIP HA フェールオーバーの設定

次の例を使用して、プロキシモバイル IP HA フェールオーバーを設定します。



重要　このセクションの設定はオプションです。

プロキシ MIP HA フェールオーバーが設定されている場合、プライマリ HA が使用できないときに、サブスクライバセッションに指定された代替ホームエージェントを使用するメカニズムを使用できます。プロキシ MIP HA フェールオーバーを設定するには、次の設定例を使用します。

```
configure
 context <context_name>
 fa-service <fa_service_name>
 proxy-mip ha-failover [ max-attempts <max_attempts> |
num-attempts-before-switching <num_attempts> | timeout <seconds> ]
```

注：

- Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイスやネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

サブスクライバプロファイル RADIUS 属性の設定

サブスクライバがプロキシモバイル IP を使用するには、サブスクライバのユーザープロファイル、または 3GPP サービスの APN で属性を設定する必要があります。前述のように、サブスクライバプロファイルは、システム上にローカルに配置することも、RADIUS AAA サーバー上にリモートに配置することもできます。

この項では、プロキシモバイル IP をサポートするために、使用する必要がある RADIUS 属性、およびローカルに保存されたプロファイル/APN の設定手順について説明します。

重要 このドキュメントでは、RADIUS ベースのサブスクライバプロファイルの設定手順は説明していません。詳細については、ご使用のサーバーに関するドキュメントを参照してください。

サブスクライバプロファイル RADIUS 属性の設定

サブスクライバがプロキシモバイル IP を使用するには、サブスクライバのユーザープロファイル、または 3GPP サービスの APN で属性を設定する必要があります。前述のように、サブスクライバプロファイルは、システム上にローカルに配置することも、RADIUS AAA サーバー上にリモートに配置することもできます。

この項では、プロキシモバイル IP をサポートするために、使用する必要がある RADIUS 属性、およびローカルに保存されたプロファイル/APN の設定手順について説明します。

重要 このドキュメントでは、RADIUS ベースのサブスクライバプロファイルの設定手順は説明していません。詳細については、ご使用のサーバーに関するドキュメントを参照してください。

プロキシモバイル IP に必要な RADIUS 属性

次の表に、サブスクライバがプロキシモバイル IP を使用するために、RADIUS AAA サーバーに保存されているプロファイルで設定する必要がある属性を示します。

表 *120 :* プロキシモバイル *IP* に必要な *RADIUS* 属性

属性	説明	値
SN-Subscriber- Permission または SN1-Subscriber-Permission	サブスクライバに配信可能なサービスを示します。 プロキシモバイル IP の場合は、この属性を簡易 IP に**必ず**設定します。	• なし（0） • 簡易 IP（0x01） • モバイル IP（0x02） • ホームエージェント バイル IP（0x04）
SN-Proxy-MIP または SN1-Proxy-MIP	設定されたサービスが、簡易 IP サブスクライバに対して強制プロキシ MIP トンネリングを実行するかどうかを指定します。 プロキシモバイル IP をサポートするには、この属性を**必ず**有効にします。	• 無効：強制プロキシ 実行しない（0） • 有効：強制プロキシ 実行する（1）
SN-Simultaneous-SIP-MIP または SN1-Simultaneous-SIP-MIP	サブスクライバが簡易 IP サービスとモバイル IP サービスの両方に同時にアクセスできるかどうかを示します。 （注） この属性の設定に関係なく、プロキシモバイル IP セッションを促進する FA は、MN の簡易 IP セッションとモバイル IP セッションの同時発生を許可**しません**。	• 無効（0） • 有効（1）
SN-PDSN-Handoff-Req-IP-Addr または SN1-PDSN-Handoff-Req-IP-Addr	モバイルによって IPCP 内で提示されたアドレスが、シャーシ間ハンドオフ中にシャーシによって付与された既存のアドレスと一致しない場合に、システムがサブスクライバセッションを拒否して終了するかどうかを指定します。 この属性は、シャーシ間ハンドオフ中に発生する IPCP ネゴシエーションの間に MN によって提示された IP アドレスとしての 0.0.0.0 の受け入れを無効にするために使用できます。 この属性はデフォルトでは無効（拒否しない）になっています。	• 無効：拒否しない • 有効：拒否する（1）
3GPP2-MIP-HA-Address	アクセス許可メッセージで送信されるこの属性は、HA の IP アドレスを指定します。 アクセス許可では複数の属性を送信できます。ただし、最初の 2 つのみが処理の対象として考慮されます。1 つ目はプライマリ HA で、2 つ目は HA フェールオーバーに使用されるセカンダリ（代替）HA です。	IPv4 アドレス

PDSN でのプロキシ MIP のローカル サブスクライバ プロファイルの設定

ここでは、PDSN でプロキシモバイル IP をサポートするように、ローカル サブスクライバ プロファイルをシステムで設定する手順について説明します。

```
configure
 context <context_name>
 subscriber name <subscriber_name>
 permission pdsn-simple-ip
 proxy-mip allow
 inter-pdsn-handoff require ip-address
 mobile-ip home-agent <ha_address>
 <optional> mobile-ip home-agent <ha_address> alternate
 ip context-name <context_name>
 end
```

サブスクライバが正しく設定されたかを確認します。

```
show subscribers configuration username <subscriber_name>
```

注：

- PDSN 間のハンドオフによる IPCP ネゴシエーション中に MN に割り当てられた IP アドレスを強制的に使用するようにシステムを設定します。IPCP を再ネゴシエートするセッションに、PDSN によって付与されたアドレス（0.0.0.0）以外のアドレスが含まれる場合、そのセッションは拒否されます。このルールを有効にするには、**inter-pdsn-handoff require ip-address** コマンドを入力します。
- 任意：プロキシ MIP の HA フェールオーバー機能を有効にしている場合は、**mobile-ip home-agent** *ha_address* alternate コマンドを使用して、セカンダリまたは代替 HA を指定します。
- プロキシ MIP をサポートするように追加の FA サービスを設定するには、必要に応じてこの例を繰り返します。
- EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

PDIF でのプロキシ MIP のローカル サブスクライバ プロファイルの設定

このセクションでは、PDIF でプロキシモバイル IP をサポートするように、ローカル サブスクライバ プロファイルをシステムで設定する手順について説明します。

```
configure
 context <context-name>
 subscriber name <subscriber_name>
 proxy-mip require
```

注記

subscriber_name はサブスクライバの名前です。1 ～ 127 文字の英字や数字を使用でき、大文字と小文字が区別されます。

ホーム エージェント コンテキストでのデフォルト サブスクライバ パラメータの設定

HA サービスと同じコンテキストで設定されたデフォルトサブスクライバに、接続先コンテキストの名前が設定されていることは非常に重要です。次の設定例を使用します。

```
configure
 context <context_name>
 ip context-name <context_name>
 end
```

EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイスや、ネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

APN パラメータの設定

この項では、APN テンプレートによって促進されるすべての IP PDP コンテキストでプロキシモバイル IP をサポートするように、APN テンプレートを設定する手順について説明します。

重要 この設定は、オプションです。さらに、非透過 IP PDP コンテキストでサブスクライバのプロファイルから返された属性は、APN の設定よりも優先されます。

次の手順では、Exec モードのルートプロンプトが表示されていることを前提としています。

```
[local]host_name
```

手順

ステップ 1 次のコマンドを入力して、コンフィギュレーション モードを開始します。

```
configure
```

次のプロンプトが表示されます。

```
[local]host_name(config)
```

ステップ 2 次のコマンドを入力してコンテキスト コンフィギュレーション モードを開始します。

```
context <context_name>
```

context_name は、APN 設定専用のシステム接続先コンテキストの名前です。名前は 1 ～ 79 文字の英数字で指定する必要があり、大文字と小文字が区別されます。次のプロンプトが表示されます。

```
[<context_name>]host_name(config-ctx)
```

ステップ 3 次のコマンドを入力して、目的の APN のコンフィギュレーションモードを開始します。

apn <*apn_name*>

apn_name は、設定する APN の名前です。名前は 1 ～ 62 文字の英数字で指定する必要があり、大文字と小文字は区別されません。ドット（.）やダッシュ（-）を含めることもできます。次のプロンプトが表示されます。

[<*context_name*>]*host_name*(config-apn)

ステップ 4 次のコマンドを入力して、APN のプロキシモバイル IP を有効にします。

proxy-mip required

このコマンドにより、APN によって促進されるすべての IP PDP コンテキストでプロキシモバイル IP がサポートされるようになります。

ステップ 5 オプションです。次のコマンドを入力すると、MIP 登録要求で GGSN/FA MN-NAI 拡張機能をスキップできます。

proxy-mip null-username static-homeaddr

このコマンドにより、この APN で NAI 拡張機能を使用せずに MIP 登録要求を受け入れることができます。

ステップ 6 次のコマンドを入力して、ルートプロンプトに戻ります。

end

次のプロンプトが表示されます。

[local]*host_name*

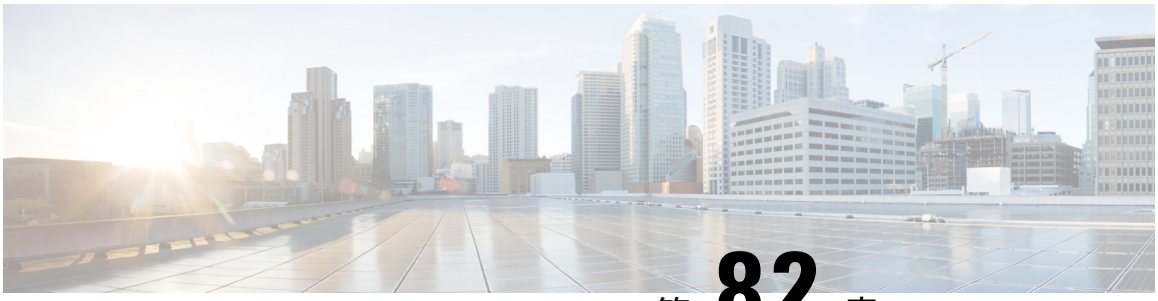
ステップ 7 必要に応じてステップ *1* からステップ *6* を繰り返し、追加の APN を設定します。

ステップ 8 次のコマンドを入力して、APN が正しく設定されていることを確認します。

show apn { all | name <*apn_name*> }

出力は、設定済みの APN パラメータ設定の詳細なリストです。

ステップ 9 Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。



第 82 章

セカンダリ RAT 使用状況 CDR レコード処理中の Sessmgr の再起動

- 機能の概要と変更履歴 （1265 ページ）
- 変更された機能 （1266 ページ）
- コマンドの変更 （1266 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	有効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• P-GW Administration Guide • Command Line Interface Reference

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、CDR の RAT 使用状況レポートを制限するために、新しい CLI コマンド *limit-secondary-rat-usage* が導入されました。	21.23

改訂の詳細	リリース
このリリースでは、CDR の RAT 使用状況レポートを制限するために、新しい CLI コマンド *limit-secondary-rat-usage* が導入されました。	21.21.3
最初の導入	21.19.7

変更された機能

以前の動作：課金データレコード（CDR）プロセスがトリガーされている間に、セッションマネージャ（SessMgr）が再起動されます。異なるスタックでバッファが 64K バイトに達すると、再起動が発生します。

新しい動作：このStarOS 21.21.3 リリースと StarOS 21.23 リリースでは、CDR 内のセカンダリ無線アクセス技術（RAT）の使用状況レポートの数を最大 32 レコードに制限することで、SessMgr の再起動を回避できます。CDR のセカンダリ RAT 使用状況レポートを制限するために、新しい CLI コマンド limit-secondary-rat-usage が導入されました。

（注） デフォルトでは、limit-secondary-rat-usage は無効になっています。この CLI は、CUSTOM38 ディクショナリには適用されません。

コマンドの変更

次の CLI 設定を使用して、CDR のセカンダリ RAT 使用状況を制限します。

```
configure
  context context_name
  gtpp group group_name
    [no] limit-secondary-rat-usage
    end
```

注：

- **limit-secondary-rat-usage**：CDR のセカンダリ RAT 使用状況レポート数の制限を有効にします。
- **no**：CDR のセカンダリ RAT 使用状況レポート数の制限を無効にします。



第 83 章

WPS セッションの APN、QCI、および ARP ベースの DSCP マッピング

- 機能の概要と変更履歴 （1267 ページ）
- 機能説明 （1268 ページ）
- 機能の仕組み （1270 ページ）
- WPS 用の IMS 承認サービスの設定 （1275 ページ）
- DSCP マッピングの設定 （1276 ページ）
- モニタリングおよびトラブルシューティング （1280 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • S-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	N/A

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。 **重要** この機能は、すべてのお客様の展開シナリオでは検証されていません。詳細については、シスコのアカウント担当者にお問い合わせください。	21.23

機能説明

WPS セッションの APN、QCI、ARP ベースの DSCP マッピング機能により、P-GW と S-GW で、ワイヤレス プライオリティ サービス サブスクライバの APN、QCI、ARP 機能に基づく DSCP マーキングをサポートできます。

コントロール プレーン トラフィックの優先順位付け：WPS ユーザーのコントロール プレーン トラフィックは、LTE コアのさまざまなネットワーク機能間で他のサブスクライバよりも優先されます。

優先順位レベル：P1、P2、P3 は、WPS ユーザーが使用できる 3 つの優先順位レベルです。

- P1 と P2 のユーザーは HSS/PCRF で識別され、GW はデフォルトおよび専用のベアラーの作成、変更、更新、削除時にそれぞれの優先順位（APN、QCI、ARP）を使用します。
- P1 および P2 の WPS ユーザーは、高い優先順位で扱われます。
- 優先順位付けされたユーザーのコントロールプレーン IP パケットの DSCP マーキングは DSCP＝47 でマークされ、他のすべてのユーザー制御パケット IP パケットは DSCP＝32 でマークされます。
- 非 WPS ユーザーと P3 WPS ユーザー（たとえば QCI=5 と ARP PL＝5）には、発信されるコールに基づいて高い優先順位が動的に割り当てられます。例：WPS-P1 ユーザーが非 WPS ユーザーを呼び出す場合 。
- LTE コアでは、MPS-Identifier-AVP の有無と Rx-AAR 内の Service-Info-Status-AVP の値に基づいて、ユーザーに対して示される高い優先順位が Rx よりも優先されます。PCRF は適切なアクションを実行し、適切な QCI、ARP 値を Gx セッションで P-GW に伝達します。

Diameter インターフェイス：

- P-GW、Policy Change Rule Function（PCRF）、および Diameter ルーティングエージェント (DRA) は、Gx インターフェイスや Rx インターフェイスなどの Diameter インターフェイスの設定を使用して、サブスクライバのポリシー制御や課金制御をサポートします。

非 Diameter インターフェイス：P-GW および S-GW は、それぞれのピアとの間で S5、S8、S11、S1U などの非 Diameter インターフェイスを使用します。

Diameter ベースインターフェイスの低および高優先順位チャネルの特性

低優先順位チャネルは WPS 以外のユーザーセッションに使用され、高優先順位チャネルは WPS ユーザーセッションに使用されます。これらのチャネルは、異なる Differentiated Services Code Point（DSCP）マーキングによって識別されます。PGW（Gx）の DRA へのピア接続を図に示します。

図 *108 : Gx* インターフェイスを介した低優先順位チャネルおよび高優先順位チャネルの概要

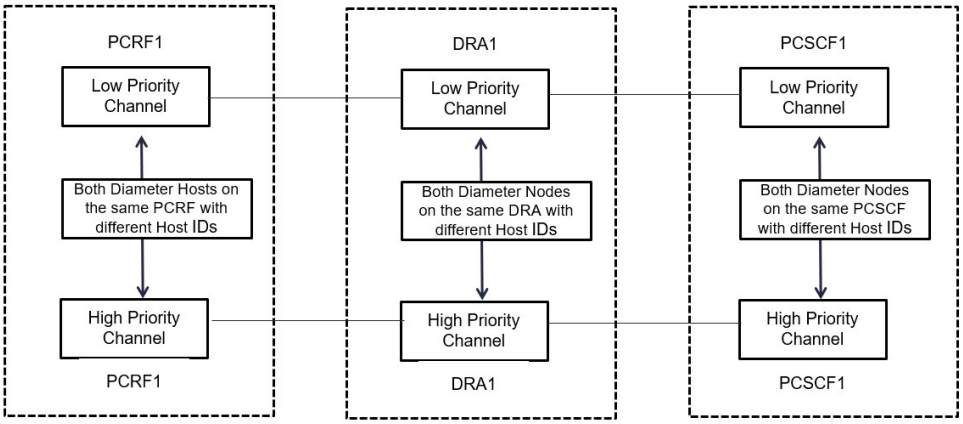


表 *121 : Gx* インターフェイスの低優先順位チャネルと高優先順位チャネル

優先順位チャネル	Diameter インターフェイス	IP レイヤ DSCP	IP レイヤを介した TCP 接続	Diameter ホスト FQDN
低優先順位	Gx	32 と等しい	32 （注） このチャネルは非 WPS Diameter メッセージ用ですが、すべてのレッドピアがダウンしている場合などのエラーシナリオで WPS Diameter メッセージを伝送する可能性があります。	未変更 例：0 0 0 1-diamproxy. PGW-Gx', 'dra1', 'pcrf1
高優先順位	Gx	47 と等しい	47	高い優先順位に固有 例：0001-diamproxy. PGW-Gx-wps', ' dra1-wps', 'pcrf1-wps'.

S11、S5、または S8 インターフェイスの低優先順位チャネルと高優先順位チャネルの特性

S5 インターフェイスと S11 インターフェイスは GTPv2 ベース（トランスポートプロトコルとして UDP を使用）で、低優先順位チャネルと高優先順位チャネルに次の特性があります。

表 *122 :* 他のインターフェイスの低優先順位チャネルと高優先順位チャネル

優先順位チャネル	Diameter インターフェイス	IP レイヤ DSCP	IP レイヤを介した TCP 接続	Diameter ホスト FQDN
低優先順位	S11 または S5 または S8	32	—	—
高優先順位	S11 または S5 または S8	47	—	—

機能の仕組み

この機能の動作の概要を以下で説明します。

P-GW/S-GW は、WPS プロファイルに基づいて、高い優先順位または低い優先順位のいずれかのチャネルを選択します。次の表に、デフォルトで、またはセッションの専用ベアラーのいずれかで設定済みの APN 名、QCI 値、および ARP PL に基づく DSCP マーキングルールを示します。WPS セッションの検出は、デフォルトまたはセッションの専用ベアラーで設定済みの APN 名、QCI、および ARP PL 値に基づいて行われます。S5、S8、および S11 インターフェイスには、表に示すように、APN、QCI、および ARP PL パラメータに基づいて、DSCP=47 IP でマークされた IP パケットが含まれます。他の IP パケットは、DSCP=32 でマークされます。

表 *123 : APN*、*QCI*、および *ARP* の優先順位レベルに基づく *WPS* メッセージの優先順位付け

APN 名	QCI	ARP PL	DSCP
APN-x/APN-y/*	66,69	*	47
APN-x/APN-y/*	*	1、2	47
APN-x/APN-y/*	8	3	47
APN-x/APN-y/*	9	5	47
APN-x/APN-y/*	2	4	47

次の表では、トランザクションまたは発信元ホストに基づく動的なトランスポート選択のプロセスについて説明します。

表 *124* : 手順

プロセス	説明
WPS ユーザーと非 WPS ユーザーの識別	• WPS ユーザーを有効または無効にするには、Diameter のエンドポイントで CLI コマンド **priority-select** を使用します。この CLI コマンドは、IMS 承認サービスのポリシー制御設定にあります。 • P-GW は、APN 名、QCI、および ARP PL 値がタグ付けされたすべての WPS セッションでセッション作成要求を受信します。 • P-GW は、その APN 名、QCI、および ARP PL 値が WPS と一致しているかどうかを確認します。 • セッションマネージャは、受信した ARP PL 値が WPS セッションと一致しているかどうかを確認します。 • WPS セッションの一致と有効な優先順位選択という上記の基準が満たされている場合、ユーザーは WPS ユーザーと呼ばれます。それ以外の場合、ユーザーは通常ユーザーと呼ばれます。
セッションの優先順位付け	ポリシー変更ルール機能（PCRF）では、非 WPS ユーザー向けの低い優先順位のセッションと WPS ユーザー向けの高い優先順位のセッションといった 2 つの優先順位レベルを定義できます。 • **WPS セッション時に常時**：WPS ユーザーに属する GTPv2-S5、GTPv2-S11、GTPv2-S8、および Gx セッションは、常に高い優先順位として扱われます。 • **オンデマンド WPS セッション**：非 WPS ユーザーに属する GTPv2-S5、GTPv2-S11、GTPv2-S8、および Gx セッションを、より高い優先順位（より低い ARP PL 値）に動的に昇格できます。この最も一般的な例は、WPS ユーザーが非 WPS ユーザーに WPS コール（*272 で始まるコールをダイヤルすることにより開始）を発信する場合です。このようなタイプのセッションは、オンデマンド WPS セッションと呼ばれます。 • 高い優先順位のセッションに属するコントロールプレーン Gx メッセージは、高い優先順位のチャネルを使用する必要があります。 • 高くない優先順位のセッションに属するコントロールプレーン Gx メッセージは、低い優先順位のチャネルを使用する必要があります。

プロセス	説明
通常ユーザーと WPS ユーザー間のパスの差別化	Gx インターフェイスでは、CLI レベルで 2 番目のパスを形成するためにさまざまな接続が行われます。 • P-GW は 2 セットの DRA ピア接続を作成します。1 つは高い優先順位に設定され、もう 1 つは通常の優先順位のメッセージに設定されます。 • P-GW は、セッションのタイプ（WPS セッションまたは非 WPS セッション）に応じて、特定の接続ペアで CCR-Initial および CCR-Update Gx メッセージを送信します。 • ピアに priority-select フラグを設定すると、WPS セッションのすべての CCR メッセージが、高い優先順位のピアで開始されます。P-GW がユーザーを WPS ユーザーとして識別すると、DSCP を 47 にマーキングして優先順位の高いピアにバインドします。ただし、非 WPS サブスクライバの Diameter メッセージは低い優先順位のピアで開始され、DSCP は 32 に設定されます。 （注） ピアの DSCP 設定が指定されていない場合は、Diameter エンドポイントに設定されたグローバル DSCP 値が使用されます。Diameter エンドポイントにグローバル DSCP 値が設定されていない場合は、DSCP 値「0」が使用されます。 WPS ユーザーに関しては、CCR-I メッセージをトリガーする前次のアクションが実行されます。 • 高い優先順位のピアの選択。 • 既存の AVP 文字列がピア設定で設定されている場合、発信元ホスト ID に文字列が追加されます。文字列が設定されていない場合、デフォルトの **-wps** 文字列が発信元ホスト ID に追加されます。 • DRA または PCRF は、CCR-I の受信時に高い優先順位のチャネルを介して CCA-I で応答します。その後のメッセージは、高い優先順位のチャネルに従います。

通話フロー

この機能の主なコールフローには、非 WPS セッションから WPS セッションへの移行と、PCRF によって開始されたベアラー削除が含まれます。

CSR（セッション作成要求）に 1 つのベアラーがあり、ARP PL、QCI が、対応する APN の WPS プロファイルで定義された ARP PL、QCI と一致しない場合、セッションは非 WPS セッ

ションとして扱われます。すべての Gx メッセージは、PCRF への低い優先順位のチャネルに従います。ただし、モバイルによってトリガーされた専用ベアラーの ARP PL、QCI が、対応する APN の WPS プロファイルで定義された ARP PL、QCI と一致する場合、低い優先順位のセッションは WPS セッションに移行されます。



（注） 「グリーンピア」は「低い優先順位のチャネル」です。「レッドピア」は「高い優先順位のチャネル」です。

図 *109* : 非 *WPS* セッションと *WPS* セッション相互の移行

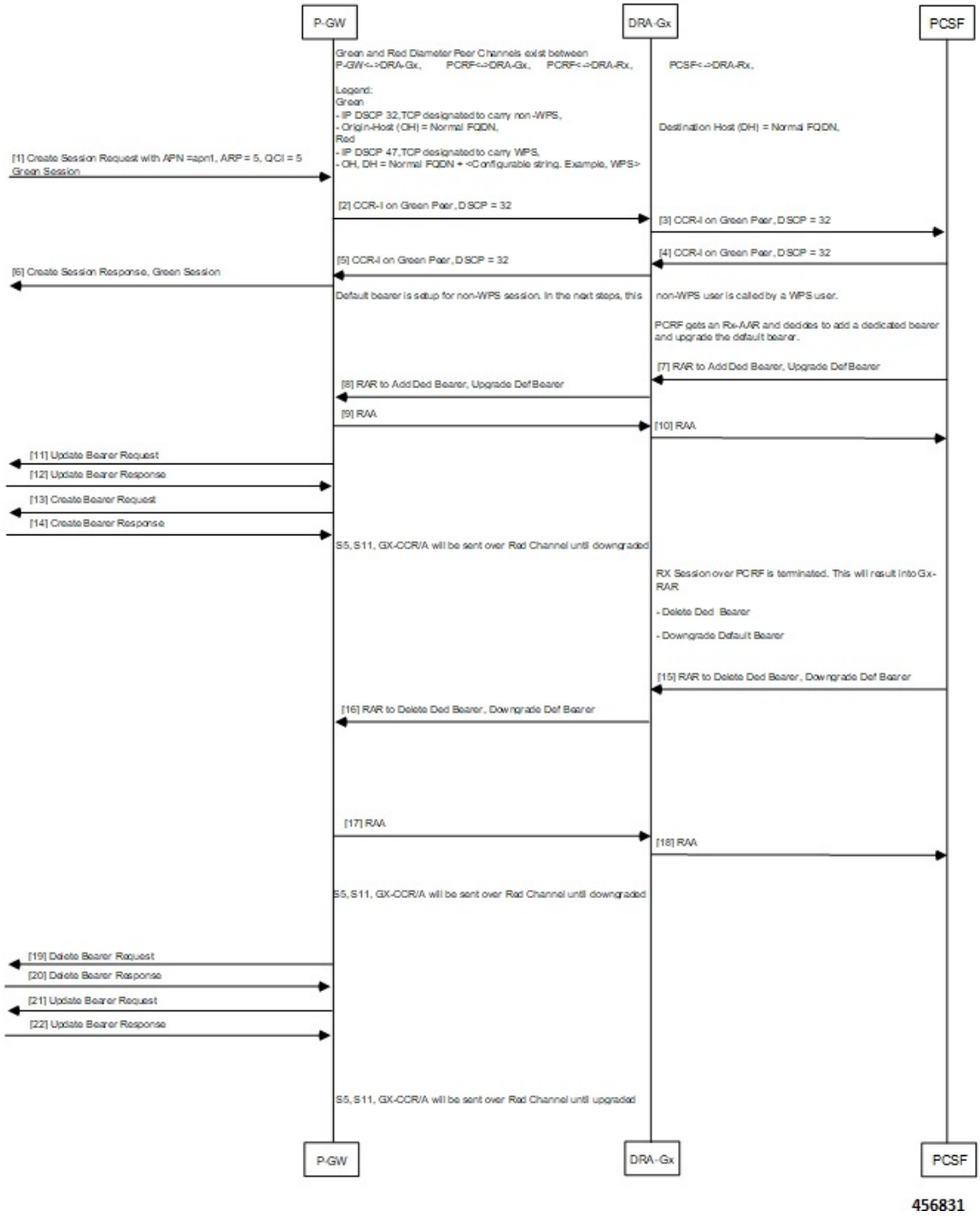


表 *125 :* 手順

ステップ	説明
1 ～ 6	低い優先順位のチャネルは、非WPSセッションに使用されます。
7 ～ 14	P-GW が、WPS APN プロファイルの ARP PL と一致する APN、ARP PL、QCI を持つ専用ベアラーを受信し、次の操作が実行され、CCR-U が DRA/PCRF に送信されます。 • 非 WPS セッションが WPS セッションに移行します。CLP が WPS セッションとして更新されます。 • P-GW が、高い優先順位のピアを識別します。 • 文字列「-wps」または設定された origin-host-suffix 文字列を発信元ホスト ID に追加します。 Gx、S5、S11、またはS8での後続の発信メッセージは、セッションが再度ダウングレードされるまで、高い優先順位のチャネルに従います。
15 ～ 22	P-GW が、WPS APN プロファイルで定義されていない QCI または ARP PL を含む RAR を受信すると、セッションが WPS セッションから非 WPS にダウングレードされます。

WPS 用の IMS 承認サービスの設定

IMS サブスクライバの IMSA サービスをコンテキストレベルで設定するには、次の設定例を使用します。

```
configure
   context context_name
      ims-auth-service imsa_service_name
        policy-control
           diameter origin endpoint endpoint_name priority-select
           diameter dictionary dictionary
           no event-report-indication
           custom-reauth-trigger  qos-change default-bearer-qos-change
ue-ip-addr-allocate resource-modification-request  ue-ip-addr-release
apn-ambr-mod-failure default-bearer-qos-mod-failure
           diameter host-select table { 1 | 2 } algorithm round-robin
           diameter host-select row-precedence  precedence_value  table { 1
 | 2 } host  primary_host_name  [ realm  primary_realm_id  ] [ secondary host
  secondary_host_name  [ realm  secondary_realm_id  ] ] priority-host [ -noconfirm
 ]
           exit
        exit
```

注：

- *context_name* は、IMSA サービスを有効にするコンテキストの名前です。
- *imsa_service_name* は、Rel. 8 Gx インターフェイス認証用に設定する IMSA サービスの名前です。
- Rel. 8 Gx インターフェイスのサポートを有効にするには、関連する Diameter ディクショナリを設定する必要があります。使用する具体的な Diameter ディクショナリの詳細については、シスコのアカウント担当者にお問い合わせください。
- PCRF 選択のためのラウンドロビンアルゴリズムは、多数の PCRF を選択する場合にのみ効果的であり、細かいレベルでの効果は薄いです。
- **priority-select**：サブスクライバのワイヤレス プライオリティ サービス（WPS）を有効にします。これは、ピアをレッドピアとして定義するための必須パラメータです。

（注） **priority-select** キーワードは、IMSA だけでなく、「Diameter エンドポイント」の設定でも使用されます。現在の機能を動作させるには、両方を有効にする必要があります。

- **priority-host**：ホストをレッドホストとして設定します。1 つの行で priority-host キーワードが設定されていると、プライマリピアとセカンダリピアの両方がレッドホストとして扱われます。

（注） このキーワードを削除するには、**no-priority-host** を設定します。

DSCP マッピングの設定

ここでは、DSCP マッピングを設定する方法について説明します。

- WPS APNプロファイルの設定
- WPS プロファイルと P-GW および S-GW サービスとの関連付け
- WPS セッションの Gx 優先順位付けの有効化
- 低優先度ピアと高優先度ピアの区別

WPS APN プロファイルの設定

WPS APN プロファイルを設定するには、次のコマンドを使用します。このプロファイルは、ベアラーまたはセッションを WPS ベアラーまたはセッションとして識別するために使用されます。

```
configure
     wps-apn-profile  wps_apn_name
    [ no ] wps-apn-row row_number qci qci_value earp arp_pl_value dscp dscp_value
end
```

注：

- **wps-apn-profile** *wps_apn_name*：APN の WPS プロファイルを設定します。この APN 名は、WPS セッションの検出に使用されます。**wps-apn-profile all** は、この WPS APN プロファイルをすべての APN に適用する場合に使用されます。



重要　APN ごとに異なる **wps-apn-profile** を定義する必要があります。

- **wps-apn-row**：この設定は、ベアラー/PDN を WPS としてマークするために使用されます。QCI および eARP PL は、WPS セッションの検出に使用されます。最大 16 行までの設定が可能で、1 ～ 16 の整数値を設定できます。

  qci and earp の場合、**all** はワイルドカード一致を意味します。

- **dscp**：この設定は、設定済み DSCP マーキングによって WPS PDN に関連付けられたさまざまな発信 GTP-C および Gx メッセージをマークするために、S-GW または P-GW で使用されます。DSCP 値は、1 ～ 63 の整数です。

WPS APN プロファイルと P-GW および S-GW サービスとの関連付け

ここでは、WPS APN プロファイルを P-GW や S-GW サービスに関連付ける方法について説明します。

```
configure
  context  context_name
    [ no ] pgw-service service_name
      [ no ] associate wps-apn
      end
```

注：

- **no**：WPS APN プロファイルと P-GW サービスの関連付けを無効にします。
- **associate wps-apn**：WPS APN プロファイルを P-GW サービスに関連付けます。

```
configure
  context context_name
    [ no ] sgw-service  service_name
```

```
[ no ] associate wps-apn
end
```

注：

- **no**：WPS APN プロファイルと S-GW サービスの関連付けを無効にします。
- **associate wps-apn**：WPS APN プロファイルを S-GW サービスに関連付けます。

WPS セッションの Gx 優先順位付けの有効化

ここでは、WPS セッションの Gx 優先順位付けレベルを有効にする方法について説明します

```
configure
  context context_name
    [ no ]ims-auth-service service_name
      [ no ] policy control
        [ no ] diameter origin endpoint  endpoint_name  priority-select

        [ no ] diameter session-prioritization
        diameter host-select row-precedence precedence_value table { 1
| 2 } host primary_host_name [ realm primary_realm_id ] [ secondary host
secondary_host_name [ realm secondary_realm_id  ] ]  priority-host [ -noconfirm
 ]
      end
```

注：

- **priority-select**：選択したIMS承認サービスの ワイヤレス プライオリティ サービス（WPS）を有効にします。

（注） WPS 機能では、**priority-select** キーワードは必須です。

- **no diameter session-prioritization**：WPS セッションの Gx シグナリングの優先順位付けを有効または無効にします。
  - デフォルトでは、**diameter session-prioritization** CLI コマンドは無効になっており、Gx メッセージは WPS 値に基づいて優先順位付けされません。
  - 以前に設定されている場合は、**no diameter session-prioritization** CLI コマンドを使用してデフォルトの動作を設定します。
  - **diameter session-prioritization** CLI は、Gx が WPS APN プロファイルとともに設定で有効になっている場合に有効になります。
  - **diameter session-prioritization** 設定コマンドは、高優先順位チャネルを通過する Diameter メッセージに DRMP-0 AVP をアタッチします。DRA/PCRF は、P-GW から DRA または DRA から PCRF Gx のリンクで高優先順位チャネルから低優先順位チャネルへのフォールバックが発生した場合、DRMP-0 に基づいて適切なアクションを実行します。

（注） diameter session-prioritization は既存の CLI であり、WPS 機能の必須設定ではありません。

- **priority-host**：ホストをレッドホストとして設定します。1 つの行で priority-host キーワードが設定されていると、プライマリピアとセカンダリピアの両方がレッドホストとして扱われます。

低優先度ピアと高優先度ピアの区別

ここでは、低優先度ピアと高優先度ピアを区別する方法について説明します。ポリシー制御の下の優先度エンドポイントの設定により、WPS 機能は、ポリシー制御領域の IMS 承認サービスにのみ適用されるようになります。Gx インターフェイスに適用されます。

```
configure
   context context_name
      [ no ] diameter endpoint pgw-gx
        peer  primary_peer_name [ realm primary_realm_name ] address ip_address
[ port port_number ]
          peer  secondary_peer_name [ realm secondary_realm_name ] address
ip_address [ port port_number ] priority-select dscp dscp_value
origin-host-suffix suffix_name
          end
```

注：

- **priority-select**：ピアを高優先度の WPS ピアとして定義します。両方のパラメータを設定することはオプションです。ピアを設定するときは、次の条件が適用されます。
  - **priority-select** が設定されていない場合、ピアは高優先度の **WPS** ピアとして扱われません。
  - ピアで DSCP が設定されていない場合、エンドポイントレベルの DSCP が、DRA/PCRF への IP パケットに書き込まれます。それ以外の場合は、設定された DSCP が IP パケットに書き込まれます。
  - priority-select が設定され、**origin-host-suffix** がピアで設定されている場合、設定された文字列が発信元ホスト ID に追加されます。それ以外の場合は、デフォルトの「-wps」文字列が発信元ホスト ID に追加されます（例：pgw-gx-wps）。
  - **dscp**：DSCP は低優先度ピアでも設定できます。dscp 値は、1 ～ 63 の整数です。

モニタリングおよびトラブルシューティング

ここでは、障害対応情報、show コマンドと出力、IMSA レベルの統計、eGTPC 統計、およびバルク統計について説明します。

コマンドと出力の表示

show ims-authorization policy-control statistics

この CLI コマンドを使用して、`Rule Installation Failure` 統計、優先順位付けされた DRMP メッセージの数、WPS および非 WPS セッションの統計の詳細に関する出力フィールドを表示します。

フィールド	説明
DPCA WPS Session Stats	
Total Current Sessions	このシステムで現在実行されている DPCA WPS セッションの総数
Switched from Priority Chnl	ワイヤレスプライオリティから通常に移動されたサブスクライバの合計を示します
Switched to Priority Chnl	通常からワイヤレスプライオリティに移動したサブスクライバの合計を示します
DPCA WPS Message Stats	
Priority Channel 高優先度チャネルで送受信された WPS セッションのメッセージの統計を示します。	
Total messages Received	IMS 承認ポリシー制御のために受信したポリシー制御メッセージの合計。
Total Messages Sent	IMS 承認ポリシー制御サーバーに送信されたメッセージの合計。
Total CCR	受信したクレジット制御リクエスト（CCR）メッセージの合計。
Total CCA	CCR への応答として送信されたクレジット制御応答（CCA）メッセージの合計。
CCR-Initial	受信した初期 CCR メッセージの総数。
CCA-Initial	初期 CCR メッセージへの応答として送信された初期 CCA メッセージの合計数。

フィールド	説明
CCA-Initial Accept	初期 CCR メッセージへの応答として受信した初期 CCA メッセージの合計数。
CCA-Initial Reject	初期の CCR メッセージに対する応答として拒否された初期 CCA メッセージの合計数。
CCA-Initial Dropped	S-GW 復元、DPCA がオフであるか存在しない、または IMSA セッションが保持モードであるためにドロップされた CCA-I メッセージの合計数。
CCA-Initial Timeouts	初期 CCR メッセージへの応答がタイムアウトした初期 CCA メッセージの合計数。
CCR-Update	更新のための初期 CCR 後に受信したクレジット制御要求（CCR）メッセージの総数。
CCA-Update	CCR を更新するために応答として送信されたクレジット制御応答（CCA）メッセージの合計。
CCA-Update Timeouts	CCR を更新するために応答として送信されたがタイムアウトしたクレジット制御応答（CCA）メッセージの合計。
CCA-Update Errors	CCA-Update メッセージの解析中に発生したエラーの合計数。
CCA-Update Dropped	S-GW 復元、DPCA がオフであるか存在しない、または IMSA セッションが保持モードであるためにドロップされた CCA-U メッセージの合計数。
CCR-Final	アプリケーションを終了するために受信した最終 CCR メッセージの合計数。
CCA-Final	セッションを終了するための最終 CCR メッセージへの応答として送信された最終 CCA メッセージの合計数。
CCA-Final Timeouts	セッションを終了するための最終 CCR メッセージへの応答として送信されたがタイムアウトした最終 CCA メッセージの合計数。
CCA-Final Errors	CCA-Terminate メッセージの解析中に発生したエラーの合計数。
CCA-Final Dropped	S-GW 復元、DPCA がオフであるか存在しない、または IMSA セッションが保持モードであるためにドロップされた CCA-T メッセージの合計数。
ASR	受信したセッション中止要求（ASR）の合計数。

フィールド	説明
ASA	セッション中止要求（ASR）への応答として送信されたセッション中止承諾（ASA）メッセージの合計数。
RAR	再承認のために受信した Re-Auth-Requests（RAR）の合計数。
RAA	再承認応答（RAA）メッセージ応答がある再承認要求（RAR）の合計数。
RAR-CCR collision	未処理のクレジット制御要求（CCR）メッセージがある場合に、PCRFから受信した再承認要求（RAR）メッセージの合計数。
Non-Priority Channel	**プライオリティチャネルで送受信されることが想定されるが、非プライオリティチャネルで送受信された WPS セッションのメッセージの統計を示します。**
Total messages Received	IMS 承認ポリシー制御のために受信したポリシー制御メッセージの合計。
Total Messages Sent	IMS承認ポリシー制御サーバーに送信されたメッセージの合計。
Total CCR	受信したクレジット制御リクエスト（CCR）メッセージの合計。
CCR-Initial	受信した初期 CCR メッセージの総数。
CCA-Initial	初期 CCR メッセージへの応答として送信された初期 CCA メッセージの合計数。
CCA-Initial Accept	初期CCRメッセージへの応答として受信した初期CCAメッセージの合計数。
CCA-Initial Reject	初期の CCR メッセージに対する応答として拒否された初期 CCA メッセージの合計数。
CCA-Initial Dropped	S-GW復元、DPCAがオフであるか存在しない、またはIMSAセッションが保持モードであるためにドロップされたCCA-Iメッセージの合計数。
CCA-Initial Timeouts	初期CCRメッセージへの応答がタイムアウトした初期CCAメッセージの合計数。
CCR-Update	更新のための初期 CCR 後に受信したクレジット制御要求（CCR）メッセージの総数。

フィールド	説明
CCA-Update	CCR を更新するために応答として送信されたクレジット制御応答（CCA）メッセージの合計。
CCA-Update Timeouts	CCR を更新するために応答として送信されたがタイムアウトしたクレジット制御応答（CCA）メッセージの合計。
CCA-Update Errors	CCA-Update メッセージの解析中に発生したエラーの合計数。
CCA-Update Dropped	S-GW 復元、DPCA がオフであるか存在しない、または IMSA セッションが保持モードであるためにドロップされた CCA-U メッセージの合計数。
CCR-Final	アプリケーションを終了するために受信した最終 CCR メッセージの合計数。
CCA-Final	最終 CCR メッセージに応答してセッションを終了するために送信された最終 CCA メッセージの合計数。
CCA-Final Timeouts	セッションを終了するための最終 CCR メッセージへの応答として送信されたがタイムアウトした最終 CCA メッセージの合計数。
CCA-Final Errors	CCA-Terminate メッセージの解析中に発生したエラーの合計数。
CCA-Final Dropped	S-GW 復元、DPCA がオフであるか存在しない、または IMSA セッションが保持モードであるためにドロップされた CCA-T メッセージの合計数。
ASR	受信したセッション中止要求（ASR）の合計数。
ASA	セッション中止要求（ASR）への応答として送信されたセッション中止承諾（ASA）メッセージの合計数。
RAR	再承認のために受信した Re-Auth-Requests（RAR）の合計数。
RAA	再承認応答（RAA）メッセージ応答がある再承認要求（RAR）の合計数。
RAR-CCR collision	未処理のクレジット制御要求（CCR）メッセージがある場合に、PCRF から受信した再承認要求（RAR）メッセージの合計数。

show diameter peers full all

この CLI コマンドを使用して、ピアの詳細を表示します。

カウンタ	説明
優先順位チャネル	ピアの優先順位が高いかどうかを示します。次のオプションがあります。 • Yes：ピアが WPS であることを示します。 • No：ピアが非 WPS であることを示します。

show wps-apn-profile{all | name wps_apn_profile_name}

関連する属性で設定された特定またはすべての WPS APN プロファイルを表示します。

show pgw-service { name <name> | all }

フィールド	説明
WPS APN Profile(s) Associated	**wps apn プロファイル**が P-GW サービスに関連付けられているかどうかを示します。Yes または No で示されます。

show sgw-service { name <name> | all } コマンドの場合と同様の出力フィールド情報を表示できます。

show pgw-service { name_*name* | all }

このコマンドの出力は、P-GW サービスに関連付けられた WPS APN プロファイルに応じて変わります。

フィールド	説明
WPS APN Profile(s) Associated	**wps apn** プロファイルが P-GW サービスに関連付けられているかどうかを示します。**Yes** または **No** で示されます。

show sgw-service { name_*name* | all }

このコマンドの出力は、S-GW サービスに関連付けられた WPS APN プロファイルに応じて変わります。

フィールド	説明
WPS APN Profile(s) Associated	**wps apn** プロファイルが SGW サービスに関連付けられているかどうかを示します。**Yes** または **No** で示されます。

show subscribers pgw-only full all

このコマンドの出力は、セッションが WPS かどうかを反映するように変更されます。

フィールド	説明
WPS Bearer	ベアラーが WPS か非 WPS かを示します。**Yes** または **No** で示されます。

show sgw-service statistics all

このコマンドの出力が変更され、WPS PDN 統計情報が表示されるようになりました。

フィールド	説明
WPS PDNs	
Current Active	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。WPS PDN がリリースされている場合、または非 WPS PDN にデグレードされている場合に減分されます。
Cumulative Activated	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。
Cumulative De-activated	WPS PDN がリリースされている場合、または非 WPS PDN にデグレードされている場合に増分されます。

show subscribers sgw-only full all

このコマンドの出力が変更され、セッションが WPS かどうかが反映されるようになりました。

フィールド	説明
WPS Bearer	ベアラーが WPS か非 WPS かを示します。**Yes** または **No** で示されます。

show subscribers saegw-only full all

このコマンドの出力は、セッションが WPS かどうかを反映するように変更されます。

フィールド	説明
WPS Bearer	ベアラーが WPS か非 WPS かを示します。**Yes** または **No** で示されます。

show pgw-service statistics all

このコマンドの出力が変更され、WPS PDN 統計情報が表示されるようになりました。

フィールド	説明
WPS PDNs	
Current Active	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。WPS PDN がリリースされている場合、または非 WPS PDN にデグレードされている場合に減分されます。
Cumulative Activated	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。
Cumulative De-activated	WPS PDN がリリースされている場合、または非 WPS PDN にデグレードされている場合に増分されます。

show sgw-service statistics all

このコマンドの出力が変更され、WPS PDN 統計情報が表示されるようになりました。

フィールド	説明
WPS PDNs	
Current Active	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。WPS PDN がリリースされている場合、または非 WPS PDN にデグレードされている場合に減分されます。
Cumulative Activated	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。
Cumulative De-activated	WPS PDN がリリースされている場合、または非 WPS PDN にデグレードされている場合に増分されます。

show saegw-service statistics all

このコマンドの出力が変更され、WPS PDN 統計情報が表示されるようになりました。

フィールド	説明
WPS PDNs	
Colocated PDNs	Collapsed PDN の WPS PDN 統計情報を表示します。

フィールド	説明
Current Active	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。WPS PDN がリリースされている場合、または非 WPS PDN にデグレードされている場合に減分されます。
Cumulative Activated	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。
Cumulative De-activated	WPS PDN がリリースされている場合、または非 WPS PDN PGW アンカー WPS PDN にデグレードされている場合に増分されます。P-GW アンカー PDN の WPS PDN 統計情報を表示します。
PGW-Anchor WPS PDNs：P-GW アンカー PDN の WPS PDN 統計情報を表示します。	
Current Active	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。WPS PDN がリリースされている場合、または非 WPS PDN にデグレードされている場合に減分されます。
Cumulative Activated	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。
Cumulative De-activated	WPS PDN がリリースされている場合、または非 WPS PDN PGW アンカー WPS PDN にデグレードされている場合に増分されます。P-GW アンカー PDN の WPS PDN 統計情報を表示します。
SGW-Anchor WPS PDNs：SGW アンカー PDN の WPS PDN 統計情報を表示します。	
Current Active	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。WPS PDN がリリースされている場合、または非 WPS PDN にデグレードされている場合に減分されます。
Cumulative Activated	いずれかの PDN が WPS PDN としてセットアップされている場合、または WPS PDN にアップグレードされている場合に増分されます。
Cumulative De-activated	WPS PDN がリリースされている場合、または非 WPS PDN にデグレードされている場合に増分されます。

show egtpc statistics interface pgw-ingress interface-type S5/S8

以下の CLI コマンドは、P-GW 入力の S5 または S8 インターフェイスの WPS セッション関連 GTP-C メッセージ統計を表示するように変更されています。

カウンタ	説明
合計 WPS 統計：WPS セッションで送受信されたメッセージの累積 GTP-C メッセージ統計を表示します。	
セッション作成要求（合計RX）	このカウンタは、セッションを WPS にする S5 または S8 インターフェイスで P-GW がセッション作成要求メッセージを受信したときに、P-GW によって増加されます。
セッション作成応答（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がセッション作成応答メッセージを送信したときに、P-GW によって増加されます。
ベアラー変更要求（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー変更要求メッセージを受信したときに、P-GW によって増加されます。
ベアラー変更応答（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー変更応答メッセージを送信したときに、P-GW によって増加されます。
ベアラー作成要求（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー作成要求メッセージを受信したときに、P-GW によって増加されます。
ベアラー作成応答（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー作成応答メッセージを受信したときに、P-GW によって増加されます。
ベアラー更新要求（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー更新要求メッセージを送信したときに、P-GW によって増加されます。
ベアラー更新応答（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー更新応答メッセージを受信したときに、P-GW によって増加されます。
現在の間隔 WPS 統計： 現在の統計収集間隔で、WPS セッションで送受信されたメッセージの GTP-C メッセージ統計。統計の収集間隔は、バルク統計の収集間隔と同じになります。バルク統計の収集が設定されていない場合、現在の WPS 統計は合計 WPS 統計と同様に表示されます。	

カウンタ	説明
セッション作成要求（合計RX）	このカウンタは、セッションを WPS にする S5 または S8 インターフェイスで P-GW がセッション作成要求メッセージを受信したときに、P-GW によって増加されます。
セッション作成応答（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がセッション作成応答メッセージを送信したときに、P-GW によって増加されます。
ベアラー変更要求（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー変更要求メッセージを受信したときに、P-GW によって増加されます。
ベアラー変更応答（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー変更応答メッセージを送信したときに、P-GW によって増加されます。
ベアラー作成要求（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー作成要求メッセージを受信したときに、P-GW によって増加されます。
ベアラー作成応答（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー作成応答メッセージを受信したときに、P-GW によって増加されます。
ベアラー更新要求（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー更新要求メッセージを送信したときに、P-GW によって増加されます。
ベアラー更新応答（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで P-GW がベアラー更新応答メッセージを受信したときに、P-GW によって増加されます。

show egtpc statistics interface sgw-egress interface-type S5/S8

次の CLI コマンドは、S-GW 出力の S5/S8 インターフェイスの WPS セッション関連 GTP-C メッセージ統計を表示するように変更されています。

カウンタ	説明
合計 WPS 統計：WPS セッションで送受信されたメッセージの累積 GTP-C メッセージ統計を表示します。	
セッション作成要求（合計RX）	このカウンタは、セッションを WPS にする S5 または S8 インターフェイスで S-GW がセッション作成要求メッセージを受信したときに、S-GW によって増分されます。

カウンタ	説明
セッション作成応答（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がセッション作成応答メッセージを送信したときに、S-GW によって増分されます。
ベアラー変更要求（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がベアラー変更要求メッセージを受信したときに、S-GW によって増分されます。
ベアラー変更応答（合計 TX）	セッションが WPS の場合、このカウンタは、S5/S8 インターフェイスで S-GW がベアラー応答メッセージの変更を送信したときに、S-GW によって増分されます。
ベアラー作成要求（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がベアラー作成要求メッセージを受信したときに、S-GW によって増分されます。
ベアラー作成応答（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がベアラー作成応答メッセージを受信したときに、S-GW によって増分されます。
ベアラー更新要求（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がベアラー更新要求メッセージを送信したときに、S-GW によって増分されます。
ベアラー更新応答（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がベアラー更新応答メッセージを受信したときに、S-GW によって増分されます。
現在の間隔 WPS 統計： 現在の統計収集間隔で、WPS セッションで送受信されたメッセージの GTP-C メッセージ統計。統計の収集間隔は、バルク統計の収集間隔と同じになります。バルク統計の収集が設定されていない場合、現在の WPS 統計は合計 WPS 統計と同様に表示されます。	
セッション作成要求（合計RX）	このカウンタは、セッションを WPS にする S5 または S8 インターフェイスで S-GW がセッション作成要求メッセージを受信したときに、S-GW によって増分されます。
セッション作成応答（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がセッション作成応答メッセージを送信したときに、S-GW によって増分されます。
ベアラー変更要求（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がベアラー変更要求メッセージを受信したときに、S-GW によって増分されます。

カウンタ	説明
ベアラー変更応答（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がベアラー変更応答メッセージを送信したときに、S-GW によって増分されます。
ベアラー作成要求（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がベアラー作成要求メッセージを受信したときに、S-GW によって増分されます。
ベアラー作成応答（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がベアラー作成応答メッセージを受信したときに、S-GW によって増分されます。
ベアラー更新要求（合計 TX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がベアラー更新要求メッセージを送信したときに、S-GW によって増分されます。
ベアラー更新応答（合計 RX）	セッションが WPS の場合、このカウンタは、S5 または S8 インターフェイスで S-GW がベアラー更新応答メッセージを受信したときに、S-GW によって増分されます。

show egtpc statistics interface sgw-ingress interface-type s11

次の CLI コマンドが変更され、S-GW 入力の S11 インターフェイスの WPS セッション関連 GTP-C メッセージ統計が表示されるようになりました。

カウンタ	説明
合計 WPS 統計：WPS セッションで送受信されたメッセージの累積 GTP-C メッセージ統計を表示します。	
セッション作成要求（合計RX）	このカウンタは、セッションを WPS にする S11 インターフェイスで S-GW がセッション作成要求メッセージを受信したときに、S-GW によって増分されます。
セッション作成応答（合計 TX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がセッション作成応答メッセージを送信したときに、S-GW によって増分されます。
ベアラー変更要求（合計 TX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がベアラー変更要求メッセージを受信したときに、S-GW によって増分されます。
ベアラー変更応答（合計 TX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がベアラー応答メッセージの変更を送信したときに、S-GW によって増分されます。

カウンタ	説明
ベアラー作成要求（合計 TX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がベアラー作成要求メッセージを受信したときに、S-GW によって増分されます。
ベアラー作成応答（合計 RX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がベアラー作成応答メッセージを受信したときに、S-GW によって増分されます。
ベアラー更新要求（合計 TX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がベアラー更新要求メッセージを送信したときに、S-GW によって増分されます。
ベアラー更新応答（合計 RX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がベアラー更新応答メッセージを受信したときに、S-GW によって増分されます。
現在の間隔 WPS 統計： 現在の統計収集間隔で、WPS セッションで送受信されたメッセージの GTP-C メッセージ統計。統計の収集間隔は、バルク統計の収集間隔と同じになります。バルク統計の収集が設定されていない場合、現在の WPS 統計は合計 WPS 統計と同様に表示されます。	
セッション作成要求（合計RX）	このカウンタは、セッションを WPS にする S11 インターフェイスで S-GW がセッション作成要求メッセージを受信したときに、S-GW によって増分されます。
セッション作成応答（合計 TX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がセッション作成応答メッセージを送信したときに、S-GW によって増分されます。
ベアラー変更要求（合計 TX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がベアラー変更要求メッセージを受信したときに、S-GW によって増分されます。
ベアラー変更応答（合計 TX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がベアラー変更応答メッセージを送信したときに、S-GW によって増分されます。
ベアラー作成要求（合計 TX）	セッションが WPS の場合、このカウンタは、11 インターフェイスで S-GW がベアラー作成要求メッセージを受信したときに、S-GW によって増分されます。
ベアラー作成応答（合計 RX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がベアラー作成応答メッセージを受信したときに、S-GW によって増分されます。

カウンタ	説明
ベアラー更新要求（合計 TX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がベアラー更新要求メッセージを送信したときに、S-GW によって増分されます。
ベアラー更新応答（合計 RX）	セッションが WPS の場合、このカウンタは、S11 インターフェイスで S-GW がベアラー更新応答メッセージを受信したときに、S-GW によって増分されます。

clear egtpc

インターフェイスレベルおよび eGTP-C サービスレベルで WPS 統計をクリアするために、以下の CLI コマンドが変更されました。

- **clear egtpc statistics interface-type interface-pgw-ingress interface s5s8**：P-GW 入力タイプと S5/S8 インターフェイスのすべての eGTP-C サービスについて、インターフェイス統計と WPS 統計をクリアします。
- **clear egtpc statistics interface-type [interface-sgw-ingress | interface-sgw-egress] interface [s11 | sgw-s5s8]**：S-GW 入力タイプと S11 インターフェイス、または S-GW 出力タイプと S5/S8 インターフェイスのすべての eGTP-C サービスについて、インターフェイス統計と WPS 統計をクリアします。
- **clear egtpc statistics egtp-service pgw_egtpc_service_name interface [s5s8]**：すべての P-GW eGTP-C サービスおよび S5/S8 インターフェイスについて、インターフェイス統計と WPS 統計をクリアします。
- **clear egtpc statistics egtp-service sgw_egptc_service_name interface [s11 | sgw-s5s8]**：すべての S-GW eGTP-C サービスおよび S11 または S5/S8 インターフェイスについて、インターフェイス統計と WPS 統計をクリアします。

バルク統計

この項では、QCI および ARP ベースの DSCP マッピング機能のサポートに使用できる、バルク統計について説明します。

IMSA スキーマ

WPS と非 WPS のユーザーの高優先順位および低優先順位カテゴリを追跡するために、IMSA スキーマには次のバルク統計が含まれています。

カウンタ	説明
dpca-imsa-total-session-priority-channel	ワイヤレス優先サブスクライバの累積数を表示します。
dpca-imsa-total-sessions-switched-from-priority-channel	ワイヤレス優先から通常に移行したサブスクライバの累積数を示します。

カウンタ	説明
dpca-imsa-total-sessions-switched-to-priority-channel	通常からワイヤレス優先に移行したサブスクライバの累積数を示します。

PGW スキーマ

P-GW スキーマには、次のバルク統計が含まれています。

カウンタ	説明
sessstat-pdn-wps-cumulative-activated	WPS PDN として設定されているか、WPS PDN にアップグレードされている P-GW PDN の総数を示します。
sessstat-pdn-wps-cumulative-deactivated	リリースされた、または非 WPS PDN へとデグレードされた P-GW PDN の総数。

SGW スキーマ

S-GW スキーマには次のバルク統計が含まれています。

カウンタ	説明
sessstat-pdn-wps-cumulative-activated	WPS PDN として設定されているか、WPS PDN にアップグレードされている S-GW PDN の総数を示します。
sessstat-pdn-wps-cumulative-deactivated	リリースされた、または非 WPS PDN へとディグレードされた S-GW PDN の総数。

SAEGW スキーマ

バルク統計変数をサポートするために、次のバルク統計が SAEGW スキーマに追加されました。

カウンタ	説明
pgw-anchor-pdns-wps-cumulative-activated	WPS PDN として設定されているか、WPS PDN にアップグレードされた、P-GW アンカー PDN の総数を示します。
pgw-anchor-pdns-wps-cumulative-deactivated	リリースされた、または非 WPS PDN へとデグレードされた、P-GW アンカー PDN の総数を示します。
saegw-colocated-pdns-wps-cumulative-activated	WPS PDN として設定されているか、WPS PDN にアップグレードされた、SAE-GW Collapsed PDN の総数を示します。
saegw-colocated-pdns-wps-cumulative-deactivated	リリースされた、または非 WPS PDN にデグレードされた、SAE-GW Collapsed PDN の総数を示します。

カウンタ	説明
sgw-anchor-pdns-wps-cumulative-activated	WPS PDN として設定されているか、WPS PDN にアップグレードされた、S-GW アンカー PDN の総数を示します。
sgw-anchor-pdns-wps-cumulative-deactivated	リリースされた、または非 WPS PDN にデグレードされた、S-GW アンカー PDN の総数を示します。

eGTP-C スキーマ

この機能をサポートするために、次の新しいバルク統計変数が eGTP-C スキーマに追加されています。これらの統計は、現在のバルク統計間隔についてのみ表示されます。

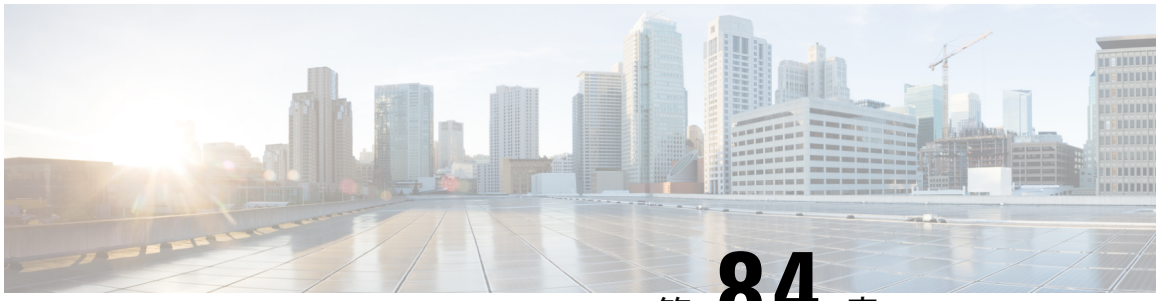
カウンタ	説明
s11-tun-recv-modbearerreq-wps	s11 インターフェイスで WPS サブスクライバに対してシステムが受信したトンネルベアラー変更要求メッセージの総数を示します。
s11-tun-sent-modbearerresp-wps	s11 インターフェイスで WPS サブスクライバに対してシステムによって送信されたトンネルベアラー変更応答メッセージの総数を示します。
s11-tun-sent-crebearerreq-wps	s11 インターフェイスで WPS サブスクライバに対してシステムによって送信されたトンネルベアラー作成要求メッセージの総数を示します。
s11-tun-recv-crebearerresp-wps	s11 インターフェイスで WPS サブスクライバに対してシステムが受信したトンネルベアラー作成応答メッセージの総数を示します。
s11-tun-sent-updbearerreq-wps	s11 インターフェイス s11 で WPS サブスクライバに対してシステムによって送信されたトンネルベアラー更新要求メッセージの総数を示します。
s11-tun-recv-updbearerresp-wps	s11 インターフェイスで WPS サブスクライバに対してシステムが受信したトンネルベアラー更新応答メッセージの総数を示します。
tun-sent-cresessreq-wps	s5 または s8 インターフェイスで WPS サブスクライバに対してシステムによって送信されたトンネルセッション作成要求メッセージの総数を示します。
tun-recv-updbearerresp-wps	s5 または s8 インターフェイスで WPS サブスクライバに対してシステムが受信したトンネルベアラー更新応答メッセージの総数を示します。

カウンタ	説明
tun-sent-updbearerresp-wps	s5 または s8 インターフェイスで WPS サブスクライバに対してシステムによって送信されたトンネルベアラー更新応答メッセージの総数を示します。

P-GW eGTP-C S5/S8 スキーマ

この機能をサポートするために、次のバルク統計が P-GW eGTP-C S5/S8 スキーマに追加されています。これらの統計は、現在のバルク統計間隔についてのみ表示されます。

カウンタ	説明
tun-recv-cresessreq-wps	S5 または S8 インターフェイスで WPS サブスクライバに対してシステムが受信したトンネルセッション作成要求メッセージの総数を示します。
tun-sent-cresessresp-wps	S5 または S8 インターフェイスで WPS サブスクライバに対してシステムが送信したトンネルセッション作成応答メッセージの総数を示します。
tun-recv-modbearerreq-wps	S5 または S8 インターフェイスで WPS サブスクライバに対してシステムが受信したトンネルベアラー変更要求メッセージの総数を示します。
tun-sent-modbearerresp-wps	S5 または S8 インターフェイスでシステムが送信した WPS サブスクライバに対するトンネルベアラー変更応答メッセージの総数を示します。
tun-sent-crebearerreq-wps	S5 または S8 インターフェイスでシステムが送信した WPS サブスクライバに対するトンネルベアラー作成要求メッセージの総数を示します。
tun-recv-crebearerresp-wps	S5 または S8 インターフェイスでシステムが受信した WPS サブスクライバに対するトンネルベアラー更新応答メッセージの総数を示します。
tun-sent-updbearerreq-wps	S5 または S8 インターフェイスでシステムが送信した WPS サブスクライバに対するトンネルベアラー更新要求メッセージの総数を示します。
tun-recv-updbearerresp-wps	S5 または S8 インターフェイスで WPS サブスクライバに対してシステムが受信したトンネルベアラー更新応答メッセージの総数を示します。



第 84 章

S6b から MDN を取得する

- 変更された機能 （1297 ページ）
- コマンドの変更 （1298 ページ）
- パフォーマンス指標の変更 （1298 ページ）

変更された機能

現在の実装では、最初のアタッチの際に、P-GW は、モバイルディレクトリ番号（MDN）またはモバイルステーション国際サブスクライバディレクトリ番号（MSISDN）を S6b インターフェイスから選択します。その後、コールが P-GW から eHRPD/信頼 Wi-Fi/非信頼 WiFi などの他のサービスにハンドオフされるか、これらのサービスから P-GW へのハンドオフが実行されると、セッション作成（CS）要求から MDN/MSISDN が選択され、S6b で承認された MDN/MSISDN が失われます。その結果、異なる値の MDN/MSISDN が Rf レコードで送信されます。通常、オペレータは MDN を使用してサブスクライバに請求するため、収益の損失が発生します。

この機能では、最初のアタッチの際に、また P-GW と eHRPD/信頼 Wi-Fi/非信頼 Wi-Fi 間のハンドオフでも、S6b インターフェイスまたは CS 要求からの MDN/MSISDN 値が保持されます。MDN/MSISDN の値は、コールの有効期間中は変更されません。そのため、セッションのすべての Rf レコードには同じ MDN/MSISDN の値が含められます。

新しいキーワード **retain-mdn** が CLI コマンド **authorize-with-hss** に追加されました。この CLI コマンドキーワードを設定すると、MDN/MSISDN 値が保持されます。この CLI コマンドキーワードが設定されていない場合、MDN/MSISDN 値は S6b インターフェイスから受信されません。この場合、CS 要求で受信した MDN/MSISDN の値が使用されます。

重要 この機能は、GnGp ハンドオフには適用されません。

以前の動作：P-GW と eHRPD/信頼/非信頼 Wi-Fi などのサービス間のハンドオフ中に、MSISDN の値が上書きされました。

新しい動作：MSISDN の値がコールの存続期間中保持されます。この期間には P-GW と eHRPD/信頼/非信頼 Wi-Fi などのサービスとのハンドオフが含まれます。

コマンドの変更

retain-mdn

S6b インターフェイスからの、またはセッション作成要求からの MDN/MSISDN 値を保持するために、この CLI コマンドのキーワードが追加されました。

ハンドオフ手順の実行中にこの CLI コマンドが無効になった場合、MDN/MSISDN 値は保持されません。たとえば、次の CLI コマンドが設定され、MDN/MSISDN 値が S6b によって許可されている場合、同じ値がコールに使用されます。ただし、ハンドオフ前に CLI コマンドが無効になっている場合は、セッション作成要求で受信した MDN/MSISDN 値が使用されます。この値は、初期接続中に S6b インターフェイスから受信した値とは異なる場合があります。

この CLI コマンドが設定されていない場合、MDN/MSISDN 値は S6b インターフェイスから受信されません。この場合、セッション作成（CS）要求で受信した MDN/MSISDN 値が使用されます。

```
configure
     context context_name
       pgw-service service_name
          authorize-with-hss retain-mdn
          { no | default } authorize-with-hss
          end
```

注：

- **no:** 初期接続またはハンドオフ後に S6b 承認を無効にします。
- **default: authorize-with-hss** のデフォルト設定を設定します。初期接続中にこれが S6b から受信されると、ハンドオフ後に MDN を強制しません。
- **authorize-with-hss:**S6b Diameter インターフェイス上でのホームサブスクライバサーバー（HSS）を介したサブスクライバセッション許可を有効または無効にします。
- **retain-mdn:** コールの存続期間中（ハンドオフを含む）、コールのセットアップ時にネゴシエートされた値（S6b で取得した MDN または CS Request の MDN）で MSISDN/MDN 値が保持されることを有効化します。

パフォーマンス指標の変更

show pgw-service all

このコマンドを実行すると、次の出力が表示されます。

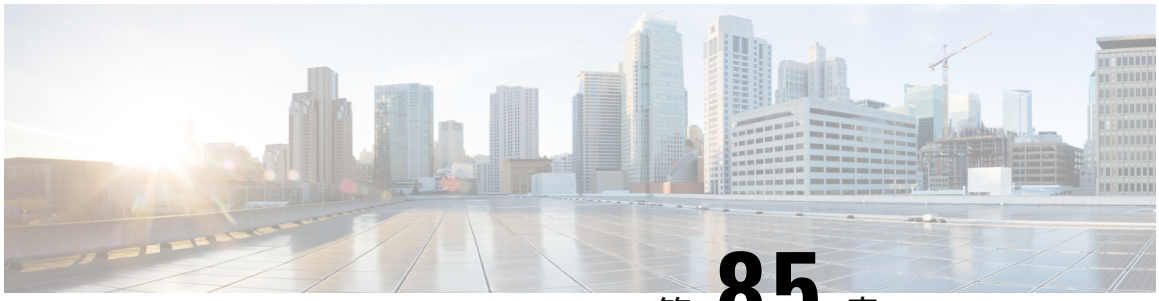
```
S6b IPv6 Reporting:     Disabled
Retain MDN :     Enabled
```

show pgw-service name *<service_name>*

このコマンドを実行すると、次の出力が表示されます。

```
S6b IPv6 Reporting:     Disabled
Retain MDN :        Enabled
```

show pgw-service name <service_name>



第 85 章

サブスクライバトラフィックの変更マーキング

- 機能の概要と変更履歴 （1301 ページ）
- 機能説明 （1302 ページ）
- 機能の仕組み （1303 ページ）
- サブスクライバトラフィックの変更マーキングの設定 （1304 ページ）
- ユーザーデータトラフィックの 802.1p および MPLS EXP マーキングの設定 （1305 ページ）
- サブスクライバトラフィックの変更済みマーキングのモニタリングと障害対応 （1308 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	• 無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
P-GW は、ユーザーデータトラフィック用の 802.1p および MPLS Experimental（EXP）ビットマーキングの設定をサポートします。この機能は、このリリースで完全に機能するようになりました。	21.20.2
このリリースでは、P-GW は、ユーザーデータトラフィック用の 802.1p および MPLS Experimental（EXP）ビットマーキングの設定をサポートします。 **重要** この機能は、このリリースでは完全には機能しておらず、テスト目的でのみ使用できます。詳細については、シスコのアカウント担当者にお問い合わせください。	21.20

機能説明

802.1p/MPLS EXP マーキングは、L2 レベルでトラフィックに優先順位を付けることにより、QoS 処理を実行するのに役立ちます。

現在、GGSN、eHRPD、P-GW、S-GW などのさまざまなアクセスタイプのデータトラフィックで、QCI-QoS テーブルが参照され、特定の行に関連付けられた internal-qos 値に基づいて、適切な 802.1p または MPLS-EXP（L2 QoS）マーキングが設定されます。ただし、QCI-QoS テーブルからの internal-qos の使用は設定できず、デフォルト値が使用されます。さらに、L2 QoS（802.1p/MPLS EXP）マーキングは、P-GW での GGSN コール、SAEGW コール、および GTPv1/eHRPD コールではサポートされません。

この機能を使用すると、次のことが可能になります。

- GGSN コール、GTPv1 P-GW コール、および SAEGW コールの QCI マッピングテーブルでの内部優先順位を設定できます。
- 802.1p または MPLS-EXP のいずれかでサブスクライバトラフィックをマークして、L2 マーキングを有効または無効にできます。サブスクライバトラフィックをマークするサービス固有の設定をサポートするために、新しい CLI コマンドが導入されました。この L2 マーキングは、QCI と DSCP のマーキングの組み合わせに基づいて、または DSCP マーキングのみに基づいて決定できます。

制限事項

- この機能は、制御パケットの動作を制御しません。制御パケット（GTP-C）は、DSCP 派生 L2 マーキングに基づいて、継続して L2 マーキングされます。
- この機能は、スタンドアロンの GGSN ではサポートされていません。GnGp-GGSN ノードでサポートされます。

機能の仕組み

GGSN コール、GTPv1 P-GW コール、および SAEGW コールの QCI マッピングテーブル内部での優先順位を設定できます。また、802.1p または MPLS-EXP のいずれかでサブスクライバトラフィックをマークして、L2 マーキングを有効または無効にすることもできます。これを行うには、CLI コマンドを使用して、サブスクライバトラフィックをマーク付けするサービス固有の設定を行います。この L2 マーキングは、QCI と DSCP のマーキングの組み合わせに基づいて、または DSCP マーキングのみに基づいて決定できます。

さまざまなサービスに対する動作の変更

ここでは、さまざまなサービスに対するこの機能の動作について説明します。CLI コマンドオプションとその動作の詳細については、「コマンドの変更」を参照してください。

GGSN/P-GW GTPv1 コール：

以前の動作：以前は、トラフィックがデータパス用にマークされていませんでした。これは GGSN に対するデフォルトの動作でした。

新しい動作：次に基づいてトラフィックをマークするために、新しい CLI コマンドが導入されました。

- QCI 派生
- DSCP 派生
- なし（None）

CLI コマンドの no または default オプションが使用された場合、トラフィックはマークされません。機能が有効になっていない場合、トラフィックはマークされません。

P-GW GTPv2、S-GW、SAEGW コール：

以前の動作：QCI-QoS マッピング機能では L2 マーキングに内部 QoS が使用され、データトラフィックに QCI 派生マーキングが使用されていました。これは、P-GW、S-GW、および SAEGW コールのデフォルトの動作でした。

新しい動作：この機能を使用すると、次に基づいてトラフィックがマークされます。

- QCI 派生
- DSCP 派生
- なし（None）

CLI コマンドの no または default オプションが使用された場合、トラフィックはマークされず、デフォルトの動作が実行されます。機能が有効になっていない場合、トラフィックはマークされません。

サブスクライバトラフィックの変更マーキングの設定

デフォルトでは、トラフィックデータパスはGGSNでサポートされています。内部での優先順位は、GGSN、GTPv1 P-GW、およびSAEGWコールのQCIマッピングテーブルで設定できます。サブスクライバトラフィックを802.1pまたはMPLS-EXPでマーク付けして、L2マーキングを有効または無効にすることもできます。これを行うには、CLIコマンドを使用して、サブスクライバトラフィックをマーク付けするサービス固有の設定を行います。このL2マーキングは、QCIとDSCPのマーキングの組み合わせに基づいて、またはDSCPマーキングのみに基づいて決定できます。

内部優先順位の設定

GGSN、GTPv1 P-GW、およびSAEGWコールのQCIマッピングテーブルで内部優先順位を設定するには、次のサービス固有の設定を使用します。GGSNサービスコンフィギュレーションのこのコマンドは、データパケット専用のQCI - QoSマッピングの動作をオーバーライドします。

```
configure
     context context_name
       ggsn-service service_name
          internal-qos data { dscp-derived | none | qci-derived }
          { no | default } internal-qos data { dscp-derived | none |
qci-derived }
          end
```

注：

- **no:** ：指定された機能を無効にします。
- **default:** ：機能を無効にします。
- **dscp-derived:** ：データパケットは、QCI - QoSマッピングテーブルで設定されたDSCPに基づいてレイヤ2でマーキングされます。DSCPがQCI - QoSマッピングテーブルで設定されていない場合、データパケットはマーキングされません。
- **none:** ：データパケットは、レイヤ2（MPLS EXP/802.1P）マーキングでマーキングされません。
- **qci-derived:** ：データパケットは、QCI - QoSマッピングテーブルで設定されたinternal-qos-priorityに基づいてレイヤ2でマーキングされます。internal-qos-priorityがQCI - QoSマッピングテーブルで設定されていない場合、データパケットはマーキングされません。

設定の確認

この機能の設定は、EXECモードで次のコマンドを使用して確認できます。

- **show configuration**
- **show** *service-type* **{ all | name** *service_name* **}**

コマンド出力については、「サブスクライバトラフィックの変更マーキングのモニタリングと障害対応」の項を参照してください。

ユーザーデータトラフィックの 802.1p および MPLS EXP マーキングの設定

このセクションでは、ユーザーデータトラフィック用に802.1pおよびMPLS実験（EXP）ビットを設定する方法について説明します。この機能の設定は、次のタスクで構成されています。

1. ip-dscp-iphb-mapping を設定します。
2. L2 マッピングの設定
3. qci-qos-mapping を設定します。
4. 出力コンテキストで l2-mapping を関連付けます。
5. 入力コンテキストで l2-mapping を関連付けます。
6. P-GW サービスと S-GW サービスでの内部 QoS データの関連付け

ip-dscp-iphb-mapping の設定

QOS プロファイル コンフィギュレーション モードにアクセスし、ip-dscp-ipphb-mapping を設定するには、次の例を使用します。

```
configure
  qos ip-dscp-iphb-mapping dscp Value  internal-priority cos  value
  end
```

注：

- *qos ip-dscp-iphb-mapping dscp*：QOS プロファイルを作成します。
- **dscp** ：0x0 ～ 0x3F の 16 進数値で DSCP マッピングを指定します。
- **internal-priority cos** ：サービスクラス（cos）の値を 0x0 ～ 0x7 の範囲で定義します。

L2 マッピングの設定

QOS L2 マッピング コンフィギュレーション モードにアクセスして L2 マッピングを設定するには、次の例を使用します。

```
configure
  qos l2-mapping-table name  { name map_table_name | system-default }
```

```
    internal-priority cos class_of_service_value color color_value [
802.1p-value 802.1p_value ] [ mpls-tc mpls_tc_value ]
     end
```

注：

- **qos l2-mapping-table name** ：QoS を内部 QoS から l2 値にマッピングします。
- **internal-priority cos** ：内部 QoS の優先順位をサービスクラス（CoS）値にマッピングします。
  - *class_of_service_value*：0x0 ～ 0x7 の 16 進数を指定します。
  - **802.1p-value** ：802.1p 値にマッピングします。*802.1p_value* は、0x0 ～ 0xF の 16 進数である必要があります。
  - **mpls-tc** *mpls_tc_value*：MPLS トラフィッククラスにマッピングします。*mpls_tc_value* は、0x0 ～ 0x7 の 16 進数である必要があります。

QCI-QoS の設定

QCI-QoS マッピングを設定するには、次のコマンドを使用します。

```
Configure
  qci-qos-mapping name
   qci  num [ arp-priority-level arp_value ] [ downlink [ encaps-header
 { copy-inner | dscp-marking  dscp-marking-value } ] [ internal-qos
priority  priority ] [ user-datagram dscp-marking  dscp-marking-value
 ] ]  [ uplink [ downlink] [ encaps-header { copy-inner | dscp-marking
  dscp-marking-value } ] [ internal-qos priority  priority ]  [
user-datagram dscp-marking  dscp-marking-value  ] ]
     end
```

注：

- **qci-qos-mapping** ：内部 QoS の優先順位をサービスクラス（CoS）値にマッピングします。
- **quci num**：有効にする通信事業者定義の QCI 値を指定します。
- **arp-priority-level** ：Address Retention Priority（ARP）の優先順位レベルを指定します。
- **downlink**：ダウンリンクトラフィックのパラメータを設定します。
- **encaps-header { copy-inner | dscp-marking** *dscp-marking-value}*：IP-in-IP、GRE、または GTP カプセル化のヘッダーで DSCP マーキングを設定する必要があることを記述します。
  - **copy-inner**：DSCP マーキングがカプセル化内の UDP ヘッダーから取得されるように記述します。
  - **dscp-marking** *dscp-marking-value*：このキーワードで DSCP マーキングが定義されるように記述します。

    dscp-marking-value は、0x00 から 0x3F までの 16 進数で表されます。

- **uplink**：アップリンクトラフィックのパラメータを設定します。
- **internal-qos priority** *priority* ：内部 QoS を設定します。これらは L2 値で解決されます。
- **user-datagram dscp-marking** *dscp-marking-value*：このキーワードで IP DSCP マーキングを定義することを記述します。*dscp-marking-value* は、0x00 から 0x3F までの 16 進数で表されます。

L2 マッピングテーブルの関連付け

出力コンテキストと入力コンテキストで L2 マッピングテーブルを関連付けるには、次のコマンドを使用します。

```
configure
  context egress context_name | ingress context_name
  associate l2-mapping-table { name table_name
  exit
  context ingress context_name
  associate l2-mapping-table { name table_name
  end
```

- **associate l2-mapping-table**：QoS を内部 QoS から l2 値にマッピングします。
- **{ name** *table_name*：QoS を内部 QoS から l2 値にマッピングするテーブルの名前を指定します。*table_name* は、1 ～ 80 文字の英数字にする必要があります。

P-GW サービスと S-GW サービスでの内部 QoS データの関連付け

P-GW および S-GW サービスで内部 QoS データを関連付けるには、次のコマンドを使用します。

```
configure
     context context_name
       pgw-service service_name
          internal-qos data { qci-derived | dscp-derived | none }
          { no | default } internal-qos data { dscp-derived | none |
qci-derived }
          exit
       sgw-service service_name
          internal-qos data { qci-derived | dscp-derived | none }
          { no | default } internal-qos data { dscp-derived | none |
qci-derived }
          end
```

注：

- **no:** ：指定された機能を無効にします。
- **default** ：機能を無効にします。

- **dscp-derived:** ：データパケットは、QCI - QoS マッピングテーブルで設定された DSCP に基づいてレイヤ 2 でマーキングされます。DSCP が QCI - QoS マッピングテーブルで設定されていない場合、データパケットはマーキングされません。
- **none:** ：データパケットは、レイヤ 2（MPLS EXP/802.1P）マーキングでマーキングされません。
- **qci-derived:** ：データパケットは、QCI - QoS マッピングテーブルで設定された internal-qos-priority に基づいてレイヤ 2 でマーキングされます。internal-qos-priority が QCI - QoS マッピングテーブルで設定されていない場合、データパケットはマーキングされません。

サブスクライバトラフィックの変更済みマーキングのモニタリングと障害対応

続くセクションでは、サブスクライバトラフィックの変更済みマーキングをモニターするために使用できるコマンドについて説明します。

内部優先順位表示コマンド

以下では、内部優先順位のモニターに使用できるコマンドについて説明します。

show configuration

このコマンドを実行すると、次の出力が表示されます。

- **internal-qos data** が **none** に設定されている場合：

```
internal-qos data none
```

- **internal-qos data** が **qci-derived** に設定されている場合：

```
internal-qos data qci-derived
```

- **internal-qos data** が **dscp-derived** に設定されている場合：

```
internal-qos data dscp-ds-derived
```

- **internal-qos data** が **not configured** に設定されている場合：

```
no internal-qos data
```

show *service-type* { all | name *service_name* }

このコマンドを実行すると、次の出力が表示されます。

- **internal-qos data** が **none** に設定されている場合：

```
Internal QOS Application:    Enabled
Internal QoS Policy:         None
```

- **internal-qos data** が **qci-derived** に設定されている場合：

```
Internal QOS Application:   Enabled
Internal QOS Policy:        QCI Derived
```

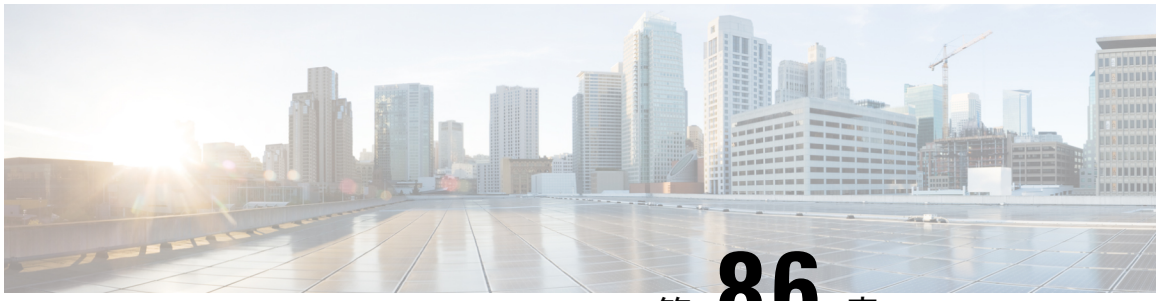
- **internal-qos data** が **dscp-derived** に設定されている場合：

```
 Internal QOS Application:    Enabled
 Internal QOS Policy:         DSCP Derived
```

- **internal-qos data** が **not configured** に設定されている場合：

```
Internal QOS Application:     Backward-compatible
```

show service-type { all | name service_name }



第 86 章

Rf インターフェイスのサポート

この章では、Diameter Rf インターフェイスの概要と、Rf インターフェイスの設定方法について説明します。

次の製品のシスコシステムで Rf インターフェイスがサポートされています。

- Gateway GPRS Support Node（GGSN）
- プロキシコールセッション制御機能（P-CSCF）
- Packet Data Network Gateway（P-GW）
- サービングコールセッション制御機能（S-CSCF）

重要 Rf インターフェイスは、S-GW ではサポートされていません。

この章に記載する手順を実行する前に、展開する製品のアドミニストレーション ガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

この章では、次の事項について説明します。

- はじめに （1311 ページ）
- 機能の概要と変更履歴 （1315 ページ）
- 機能と用語 （1316 ページ）
- 機能の仕組み （1331 ページ）
- Rf インターフェイスサポートの設定 （1333 ページ）

はじめに

Rf インターフェイスは、課金トリガー機能（CTF）（例：P-GW、P-CSCF）と課金収集機能（CCF）間のオフライン課金インターフェイスです。LTE/GPRS/eHRPD オフライン課金の Rf インターフェイス仕様は、3GPP TS 32.299 V8.6.0、3GPP TS 32.251 V8.5.0、およびその他の 3GPP 仕様に基づいています。IP マルチメディアサブシステム（IMS）オフライン課金の Rf インターフェイス仕様は、3GPP TS 32.260 V8.12.0 および 3GPP TS 32.299 V8.13.0 に基づいています。

オフライン課金は、定期的に支払うネットワーク サービスに使用されます。たとえば、あるユーザーが、月単位で支払う音声通話のサブスクリプションを持っているとします。Rfプロトコルを使用すると、CTF（Diameterクライアント）は、課金データ機能（CDF）（Diameterサーバー）にオフライン課金イベントを発行できます。課金イベントは、1回限りのイベントか、セッションベースにすることができます。

システムは、展開されたアプリケーションがRfプロトコルに基づく課金イベントを生成するために使用できる、Diameterオフライン課金アプリケーションを提供します。オフライン課金アプリケーションは、基本的なDiameterプロトコルの実装を使用して、シャーシ上に展開された任意のアプリケーションが、設定済みのCDFに対するCTFとして機能できるようにします。

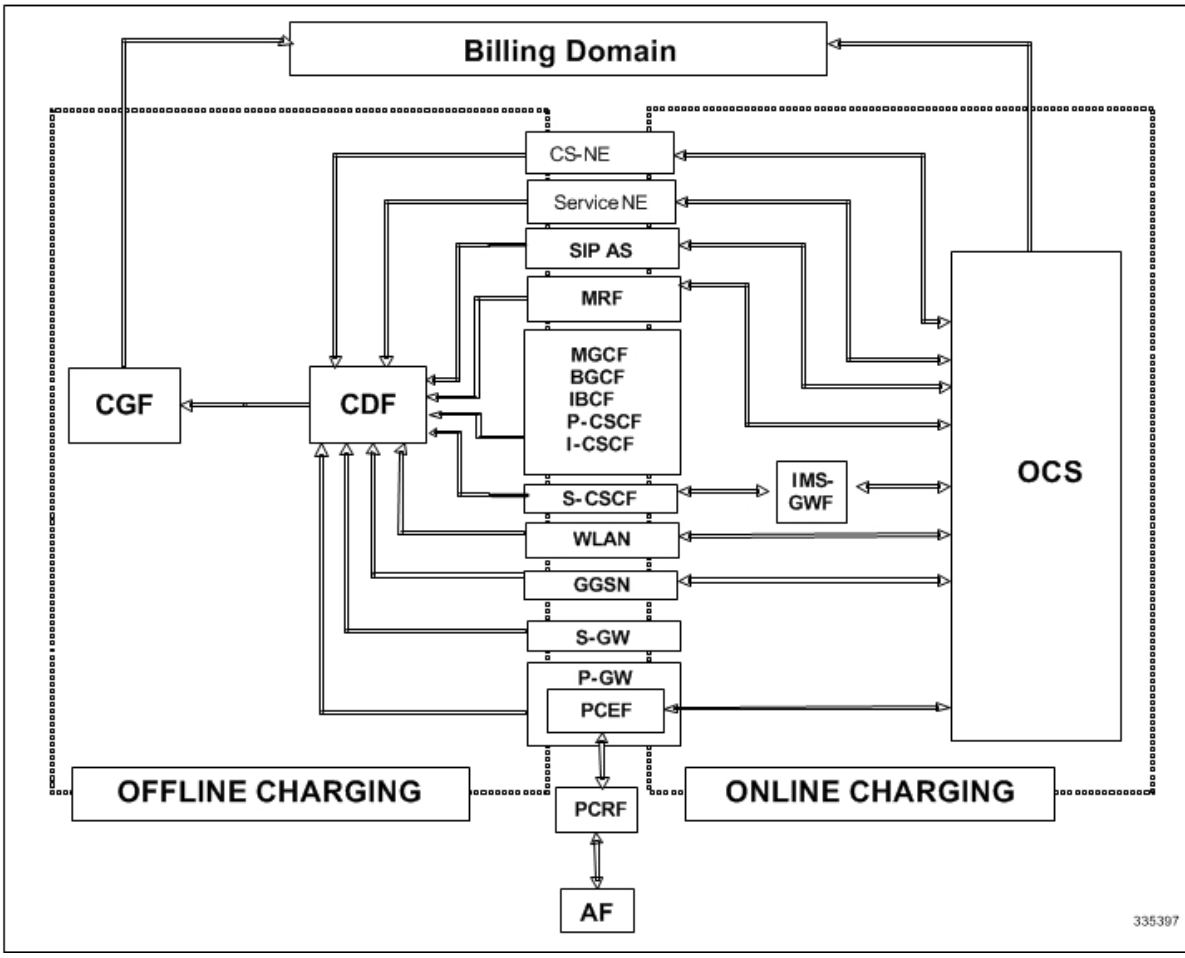
一般に、課金システムが、提供される各サービスについて統合レコードを生成できるようにするために、コアネットワーク要素からアカウント情報を収集する必要があります。

CDFおよび課金ゲートウェイ機能（CGF）を備えたCCFは、コア ネットワーク アプリケーションの一部として実装されます。CDF機能はさまざまなCTFからRfメッセージを収集して集約し、CDRを作成します。CGFはCDFからCDRを収集し、請求用のデータ仲介/請求システムの課金データレコードファイルを生成します。

オフライン課金アーキテクチャ

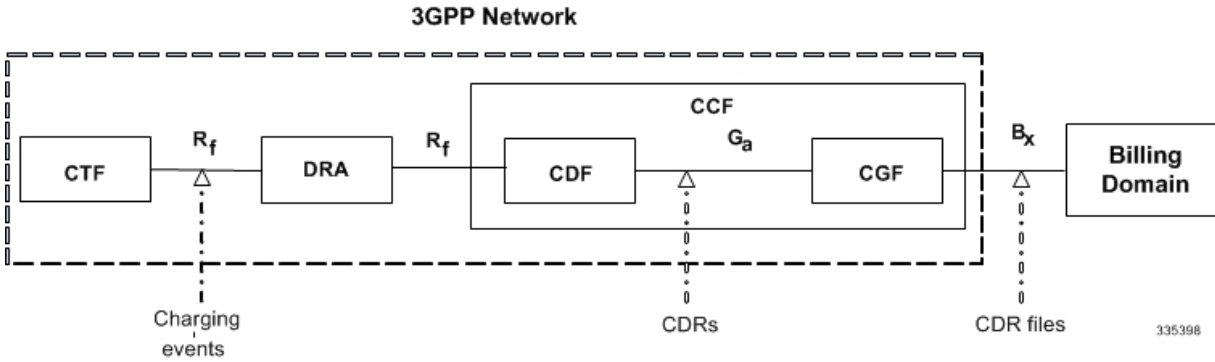
次の図は、3GPP 32.240で指定されている課金アーキテクチャの概要を示しています。CCFを使用したCSCF、P-GW、およびGGSN間のインターフェイスはRfインターフェイスです。EPCドメインのRFインターフェイスは、PSドメインに適用される3GPP標準規格（32.240、32.251、32.299など）に準拠しています。

図 *110 :* 課金アーキテクチャ



次の図は、CTF と CDF 間の Rf インターフェイスを示しています。

図 *111 :* 論理オフライン課金アーキテクチャ



Rfオフライン課金アーキテクチャは主に3つのネットワーク要素（CCF、CTF、およびDiameter ダイナミック ルーティング エージェント（DRA））で構成されます。

課金収集機能

CCF は CDF と CGF を実装します。CCF は、Rf インターフェイスの Diameter サーバーとして機能します。CTF 機能をサポートするすべてのネットワーク要素は、DRA への TCP 接続で、Diameter ベースの Rf インターフェイスを確立する必要があります。DRA 機能は、TCF への TCP 接続で Rf インターフェイス接続を確立します。

CCF は主に、定義されたインターフェイスを介してすべてのアカウンティング情報を受信し、ローカルストレージ内にある CDR（別名 UDR と FDR）レコードを生成する役割を担います。このデータは、他のインターフェイスを使用して請求システムに転送されます。また、CCF には、そのような CDR の形式が請求システムの要件と一致していることを保証する役割もあります。CCF 内の CDF 機能が CDR を生成し、CGF が CDR を請求システムに転送します。

CCF の CDF 機能は、課金情報を収集し、3GPP 標準に従った GTP ベースのインターフェイスを介して適切な CGF に渡します。CGF は SCP を介して課金中間システムに CDR ファイルを渡します。

課金トリガー機能（CTF）

CTF は CDR レコードを生成し、それを CCF に渡します。P-GW サービスが CTF として設定されている場合、PCRF を介して示されているとおりに、フローデータレコード（FDR）情報が生成されます。P-GW は、PDN セッションごとに Rf メッセージを生成します。P-GW によって、 UE ごと、またはベアラーごとに生成される課金メッセージはありません。

IP-CAN ベアラーデータトラフィック内のサービスデータフローは、複数のキーフィールド（Rating Group、Rating Group および Service -Identifier）の組み合わせに基づいて分類されます。各 Service-Data-Container は、Rating Group または Rating Group と Service-Identifier によって定義された単一の双方向フローまたは単一双方向フローのグループをキャプチャします。

ダイナミック ルーティング エージェント（DRA）

DRA により、CTF から CCF への Rf トラフィックについて、セッション単位で負荷が分散されます。DRA は、ゲートウェイに対しては Diameter サーバーのように機能します。DRA は、CCF に対しては Diameter クライアントのように機能します。DRA は、CTF には CCF のように、CCF には CTF のように見えます。

DRA により、Diameter の課金セッションごとに Rf トラフィックがルーティングされます。DRA では、負荷分散アルゴリズム（ラウンドロビン、重み付け分散など）を設定できます。1 つの Diameter 課金セッションにおけるすべてのアカウンティングレコード（ACR）が、DRA によって同じ CCF にルーティングされます。1 つの CCF に障害が発生すると、DRA は、CCF のプールから代替 CCF を選択します。

ライセンス要件

Rfインターフェイスのサポートは、ライセンス供与されたシスコの機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、

『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

サポートされる標準

RF インターフェイスのサポートは次の標準に基づいています。

- IETF RFC 4006：Diameter Credit Control Application（2005 年 8 月）
- 3GPP TS 32.299 V9.6.0 (2010-12) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release9)

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• 5G Non Standalone Solution Guide • AAA Interface Administration and Reference • Command Line Interface Reference • 『eDRX Support on the MME』機能の章を • Statistics and Counters Reference

マニュアルの変更履歴

改訂の詳細	リリース
StarOS 21.22 では、既存のユーザーロケーション情報（ULI）が GGSN、P-GW、および SAEGW のオフライン課金（RF）インターフェイスでアカウンティングレコード（ACR）停止メッセージに送信されます。	21.22

機能と用語

ここでは、Rf 機能に関連する機能と用語について説明します。

オフライン課金シナリオ

CTF と CDF 間のイベントとセッションのオフライン課金は共に、3GPP TS 32.240 で定義されている Rf 参照ポイントを使用して実行されます。

基本原則

Diameter クライアントとサーバーは、RFC 3588 Diameter 基本プロトコルで定義されているように、Diameter アカウンティングの基本機能を実装する必要があります。

オフライン課金の場合、CTF は RFC 3588 に記載されているアカウンティング ステート マシンを実装します。CDF サーバーは、RFC 3588 で規定されているアカウンティング ステート マシン「SERVER, STATELESS ACCOUNTING」を実装しています。つまり、サーバーが想定しているアカウンティング情報の受信順序はありません。

CDF へのオフライン課金イベントのレポートは、Diameter アカウンティング要求（ACR）メッセージによって管理されます。Rf は次の ACR イベントタイプをサポートします。

表 *126 : Rf ACR* イベントタイプ

要求	説明
START	アカウンティングセッションを開始します
INTERIM	アカウンティングセッションを更新します
STOP	アカウンティングセッションを停止します
EVENT	1 回限りのアカウンティングイベントを示します

ACR タイプの START、INTERIM、および STOP は、成功したセッションに関連するアカウンティングデータに使用されます。対照的に、EVENT アカウンティングデータはセッションとは無関係であり、たとえば、ネットワーク要素によってトリガーされた単純な登録または問い合わせと成功したサービスイベントに使用されます。また、EVENT アカウンティングデータは、失敗したセッション確立試行にも使用されます。

重要 ACR イベントタイプ「EVENT」は、IMS 固有の Rf 実装の場合にのみ Rf CDR でサポートされます。

次の表で、IMS ノード、つまり P-CSCF および S-CSCF から送信される可能性のあるすべての ACR について説明します。

表 *127*: *P-CSCF* および *S-CSCF* の *SIP* メソッドまたは *ISUP* メッセージによってトリガーされるアカウンティング要求メッセージ

Diameter メッセージ	トリガーする SIP メソッドおよび ISUP メッセージ
ACR（Start）	初期 SIP INVITE への確認応答 SIP 200 OK
	ISUP：ANM（MGCF に適用可能）
ACR（Interim）	SIP への確認応答 SIP 200 OK
	RE-INVITE または SIP UPDATE（例：メディアコンポーネントの変更）
	AVP の期限切れ（Acct-Interim-Interval）
	SIP 応答（4xx、5xx、または 6xx）。SIP RE-INVITE または SIP UPDATE が失敗したことを示します。
ACR（Stop）	SIP BYE メッセージ（通常のセッション終了と異常なセッション終了の両方）
	ISUP：REL（MGCF に適用可能）
ACR（Event）	以下の非セッション関連 SIP メッセージへの確認応答 SIP 200 OK • SIP NOTIFY • SIP MESSAGE • SIP REGISTER • SIP SUBSCRIBE • SIP PUBLISH
	初期 SIP INVITE への確認応答 SIP 200 OK
	SIP REFER またはその他の方法への確認応答 SIP 202 Accepted
	SIP 最終応答 2xx（SIP 200 OK を除く）
	SIP 最終またはリダイレクション応答 3xx
	SIP 最終応答（4xx、5xx、または 6xx）。SIP セッションのセットアップが失敗したことを示します。
	SIP 最終応答（4xx、5xx、または 6xx）。セッションとは無関係のプロシージャが失敗したことを示します。
	SIP CANCEL。SIP セッションのセットアップの中止を示します

イベントベースの課金

イベントベースの課金の場合、ネットワークは、使用状況、またはレンダリングされたサービス（提供されるサービスが 1 回の操作でレンダリングされる場合）を報告します。これは、ACR EVENT を使用して報告されます。

このシナリオでは、CTF は CDF にイベント関連の課金データを保存するように指示します。

セッションベースの課金

セッションベースの課金は、セッションの使用状況レポートを報告するプロセスであり、START、INTERIM、および STOP のアカウンティングデータを使用します。セッション中、ネットワーク要素は、セッションの進行状況に応じて複数の ACR Interim を送信する場合があります。

このシナリオでは、CTF は CDF に、セッション関連の課金データを保存するように要求します。

Diameter 基本プロトコル

Diameter 基本プロトコルは、Diameter クライアントと Diameter サーバー間の基礎となる接続を維持します。クライアントとサーバー間の接続は TCP ベースです。

アプリケーションを仕様に準拠させるために、ステートマシンが実装内の何らかのレベルで導入される必要があります。

Diameter Base は、アプリケーション内で使用できる次の Rf メッセージコマンドをサポートしています。

表 *128 : Diameter Rf* メッセージ

コマンド名	送信元	接続先	省略形
Accounting-Request	CTF	CDF	ACR
Accounting-Answer	CDF	CTF	ACA

接続と機能のステータスを確認するために、他の一連の Diameter メッセージが交換されます。

- 機能交換メッセージ：機能交換メッセージは、互いの機能と互いのアイデンティティを認識するために、Diameter ピア間で交換されます。
  - 機能交換要求（CER）：このメッセージは、サーバーの機能を認識するためにクライアントからサーバーに送信されます。
  - 機能交換応答（CEA）：このメッセージは、CER メッセージへの応答としてサーバーからクライアントに送信されます。
- デバイスウォッチドッグ要求（DWR）：CER/CEA メッセージが交換された後、しばらくの間ピア間のトラフィックがなくなった場合、接続の正常性をモニターするために、DWR メッセージがクライアントから送信されます。デバイス ウォッチドッグ タイマー（Tw）

が設定可能で、6～30秒の範囲で設定できます。値を小さくすると、メッセージの重複が発生します。デフォルト値は 30 秒です。DWA なしで Tw が 2 回連続して期限切れになると、ピアはダウンしていると見なされます。



重要 DWR は、サーバーから最後のメッセージ受信した後、Tw の期限切れ後にのみ送信されます。たとえば、ピア間で継続的にメッセージが交換される場合、サーバーからの最後のメッセージ受信時刻から現在時刻までの経過時間が Tw よりも小さい場合、DWR は送信されない可能性があります。

- デバイスウォッチドッグ応答（DWA）：これは、サーバーからの DWR メッセージに対する応答です。接続状態のモニタリングに使用されます。
- ピア切断要求（DPR）：このメッセージは、接続をシャットダウンするように通知するためにピアに送信されます。現在、Diameter サーバーにメッセージを送信する機能はありません。
- ピア切断応答（DPA）：このメッセージは、ピアからの DPR 要求に対する応答です。DPR を受信すると、ピアは DPA を送信し、接続状態を「DO NOT WANT TO TALK TO YOU」状態にします。ピアを再度設定する以外、接続を元に戻す方法はありません。

  切断されたピアを再試行するためのタイムアウト値を指定する必要があります。

タイマーの有効期限切れの動作

Diameter 接続の確立時に、中間アカウンティングタイマー（AII）を使用して、Diameter アカウンティングセッションの有効期限が示されます。これは、CTF で設定できます。CTF は、Acct-Interim-Interval AVP の ACR-Start のタイマー値を示します。CDF は（DRA を介して）独自の AII 値で応答します。この AII 値は CTF がタイマーを開始するために使用され、期限が切れた場合には ACR INTERIM メッセージを送信する必要があります。AII タイマーのインスタンスは、アカウンティングセッションの開始時に CCF で開始され、ACR-Interim の受信時にリセットされ、ACR-Stop の受信時に停止されます。AII タイマーの期限が切れた後、ACR INTERIM メッセージが生成され、タイマーがリセットされ、アカウンティングセッションが続行されます。

Rf インターフェイスの障害/エラー条件

現在のアーキテクチャでは、CDF 要素を使用した各ネットワーク要素のプライマリ接続およびセカンダリ接続またはアクティブ-アクティブ接続が可能です。

DRA/CCF 接続失敗

CCF のプライマリ/アクティブ DRA の 1 つへの接続が使用できなくなると、CTF は、セカンダリ/アクティブ IP アドレスを選択し、それをプライマリとして使用し始めます。

DRA（やCCF）が到達不能の場合、ネットワーク要素は、生成されたアカウンティングデータを不揮発性メモリにバッファする必要があります。DRA 接続がアップ状態になると、すべてのアカウンティングメッセージは、オフラインファイル転送を介して CDF によって取得される必要があります。

CCF からの応答なし

CTF/DRA が ACR の応答として ACA を受信しない場合、ACR メッセージを再送信する場合があります。通信事業者は、再送信までの待機時間と最大再送信回数の両方を設定できます。最大再送信回数に達しても、ACA 応答を受信していない場合、CTF/DRA はセカンダリ/代替 DRA/CCF に ACR を送信します。

メッセージの重複検出

RFC 3588 で説明されているように、Diameter クライアントは重複の可能性がある要求メッセージ（リンクのフェールオーバープロセスによる再送信など）を T フラグでマークします。

CDF が受信したメッセージに再送信済みのマークが付いており、このメッセージをすでに受信している場合、その重複メッセージは破棄されます。ただし、再送信されたメッセージの元のメッセージがまだ受信されていない場合、マークされたメッセージ内の情報は CDR の生成時に考慮されます。重複したメッセージの情報が使用された CDR にはマークが付けられます。

CCF が障害を検出した場合

CCF は、特定のセッションで想定される Diameter ACR が一定期間受信されなかったことを検出すると、CDR を終了します。CCF のこの動作は、オペレータが設定できます。

Rf-Gy 同期拡張機能

サブスクライバの使用状況および課金レポートには、Rf（OFCS）インターフェイスと Gy（OCS）インターフェイスの両方が使用されます。各インターフェイスはサブスクライバの使用状況を個別に更新するため、報告される情報が同一でないシナリオがあり得ます。クォータの適用とは別に、OCS がリアルタイムレポート（RTR）に使用されます。これにより、現在の使用状況を追跡し、特定のしきい値に達したときに通知を受け取る方法がユーザーに提供されます。

Rf（OFCS）と Gy（OCS）でサブスクライバセッションの使用状況情報が異なるシナリオでは、課金されるまでサブスクライバが潜在的な超過に気付かない可能性（Rf が Gy より大きいシナリオ）や、サブスクライバはクォータをすでに使い果たしたと信じているのに実際の課金がそれより少ない可能性（Gy が Rf より大きいシナリオ）があります。Rf と Gy の両方で報告される使用状況の値を揃える試みとして、両方のインターフェイスで報告される値をできるだけ一致させる方法を提供する機能が、リリース 12.3 で導入されました。ただし、一部の機能が延期されていたため、この機能によって追加の拡張機能が実装されます。

Gy インターフェイスの時間/ボリュームクォータが使い果たされると、Gy は、「サービスデータのボリューム制限」と「サービスデータの時間制限」をトリガーします。この機能により、16.0 では、この動作が CLI で制御されるようになりました。CLI コマンド「**trigger-type { gy-sdf-time-limit { cache | immediate } | gy-sdf-unit-limit { cache | immediate } | gy-sdf-volume-limit**

{ cache | immediate } }」に基づいて、ACR-Interim をすぐに送信するか、将来のトランザクションのためにコンテナをキャッシュするかの動作が決定されます。Gy を介して受信されたイベントトリガーに関して CLI が設定されていない場合、それらの ACR-Interim はドロップされます。

この機能での同期のためにトリガーされるさまざまな Rf メッセージ（ACR）を制御するための CLI 設定オプションが、ポリシーアカウンティング設定で提供されます。

このリリースでは、次の拡張機能がサポートされています。

- ACR-I を OFCS に送信および報告できなかったシナリオでコンテナをキャッシュします。
- OCS からの CCA を待機する現在の実装の代わりに、OCS への CCR が送信されたときに OFCS への ACR がトリガーされます。

ACR-I を OFCS に送信できなかった場合、PCEF は、コンテナレコードをキャッシュし、それを次のトランザクションで OFCS に送信します。

CCR-U が Gy インターフェイスを介して送信されると、コンテナは、CCA-U を正常に受信した後にのみ閉じられます。つまり、Rf トリガーは、CCA-U メッセージを受信した後にのみ送信されます。

この機能に関連するコマンドの詳細については、『*Command Line Interface Reference*』の「*Accounting Policy Configuration Mode Commands*」の章 [英語] を参照してください。

Rf と Gy の同期のために、共通タイマーベースのアプローチが実装されています。新しい設計の一部として、Gy と Rf は、定期的チェックポイントだけでなくフルチェックポイントでも、同じ時点でチェックポイントされます。そのため、ICSR スイッチオーバーイベント、内部イベント、セッションマネージャのクラッシュ、非アクティブな Rf/Gy リンクなどの発生とは関係なく、課金レコードが常に同期されます。これにより、課金の不一致が回避されます。

UE が IDLE の場合の Rf レコードの中止

UE が IDLE 状態であると識別され、データを送信していない場合、P-GW は Rf レコードを生成しません。新しい CLI コンフィギュレーション コマンド「**session idle-mode suppress-interim**」は、ACR レベルで機能を有効または無効にして、UE がアイドル状態でデータが転送されない場合に、ACR-I を生成する必要があるかどうかの決定を制御するために用意されています。

つまり、この CLI 設定は、UE がアイドルモードになっていてレポートするデータがない場合に、ACR-I レコードの送信を制御するために使用されます。

このコマンドの詳細については、『*Command Line Interface Reference*』の「*Accounting Policy Configuration Mode Commands*」の章 [英語] を参照してください。

QoS 変更シナリオ

eHRPD-LTE ハンドオフ中の Rf レコードでの QOS_CHANGE トリガー

生成された Rf レコードの SDC には、eHRPD から LTE へのハンドオフ中の QOS_CHANGE トリガーが含まれません。

デフォルトベアラーの QoS の変更

デフォルトのベアラーの QoS が変更された場合、対応するベアラーが切断されない限り、NR SDV コンテナは表示されません。QoS 変更が行われたベアラー、つまりデフォルトのベアラーに対して、QoS 変更コンテナだけがクローズ/リリースされます。

Diameter Rf 重複レコードの生成

この項では、Rf 重複レコード生成機能の概要と実装について説明します。

このセクションでは、この機能に関する次のトピックについて説明します。

- 機能説明 （1322 ページ）
- Rf 重複レコード生成の設定 （1324 ページ）
- Rf 重複レコード生成のモニタリングと障害対応 （1326 ページ）

機能説明

この機能は、重複する Rf レコードの作成と、その Rf インターフェイスに設定されたセカンダリ AAA グループサーバーへの通信をサポートするために導入されました。

この機能を実現するには、次の設定を有効にする必要があります。

- APN で **aaa group** CLI コマンドを使用すると、最大 2 つの AAA グループ（プライマリおよびセカンダリ AAA グループ）、または Rf Diameter アカウンティングサーバー用の 2 つの異なるエンドポイントを設定できます。
- AAA グループで **diameter accounting duplicate-record** を使用すると、Rf 重複レコードの作成が許可されます。

diameter accounting duplicate-record は、 Rf START、INTERIM、および STOP アカウンティングレコードを複製するためにこのリリースで導入された新しい CLI コマンドです。



重要 これはライセンスで制御される CLI コマンドです。詳細については、シスコのアカウント担当者にお問い合わせください。

21 より前のリリースでは、ゲートウェイで Rf アカウンティングの APN ごとに 1 つの AAA グループ設定のみが許可されます。AAA グループは複数のサーバー間でロードバランシングを

行って Rf トラフィックを通過させ、アカウンティング応答も予期できるように設定されています。セカンダリ AAA グループの設定は現在許可されていますが、RADIUS アカウンティングのみに制限されていることに注意してください。

リリース 21 以降では、Rf インターフェイスで APN ごとにセカンダリ AAA グループを設定し、重複する Diameter Rf アカウンティングレコードをセカンダリ AAA グループサーバーに送信する機能がゲートウェイに搭載されています。セカンダリ AAA グループは、請求以外の目的にのみ使用されます。



重要 複製に失敗したレコードは、HDD に書き込まれず、アーカイブリストに追加されません。

プライマリ AAA グループのメッセージの現在の動作に変更はありません。プライマリ AAA グループは、セカンダリ AAA グループから独立しており、複数の RF サーバーが設定されています。該当する設定に従って複数回再試行しても Rf サーバーが応答しない場合、Rf レコードはアーカイブされて HDD に保存されます。セカンダリ AAA グループの設定に関係なく、この動作はそのまま続行されます。

セカンダリ AAAA グループの設定は、プライマリ AAAA グループと非常によく似ていますが、セカンダリ AAAA グループを設定するための新しい CLI コマンド **diameter accounting duplicate-record** が追加で含まれている点のみ異なります。また、プライマリとセカンダリの AAA グループには、異なる Diameter エンドポイントと個別の Rf サーバーのセットをプロビジョニングする必要があることにも注意する必要があります。

設定されているすべてのサーバーがダウンした場合、要求メッセージは HDD に書き込まれず、aaamgr にアーカイブされることなく破棄されます。

元の Rf メッセージと複製された Rf メッセージでは、2 つの異なる AAA グループと 2 つの異なる Diameter エンドポイントが使用されます。したがって、Session-ID AVP の値は異なります。プライマリおよびセカンダリエンドポイントの設定によって、Origin-Host、Origin-Realm、Destination-Realm、Destination-Host の AVP の値が異なる場合があります。また、セカンダリグループの仮想/Gn APN 名を含むためのポリシーアカウンティングの設定に基づいて、Called-Station-ID AVP が変更される場合もあります。他のすべての AVP は、プライマリ AAA グループの Rf メッセージと同じ値になります。

AAA サーバーのセカンダリグループから ACA で受信した Acct-Interim-Interval（AII）間隔などの値は無視されることにも注意してください。

他の機能との関係

この機能を仮想 APN の切り捨て機能と組み合わせて使用することで、目的の結果を得ることができます。

仮想 APN の切り捨て機能は、リリース 21 の新機能です。この機能の詳細については、展開している製品のアドミニストレーション ガイドを参照してください。

制限事項

この機能には次の制限があります。

- APN ごとに設定できるセカンダリ AAA グループは 1 つのみです。
- セカンダリ AAAA グループの下位にあるすべての Rf ピアがダウンし、重複する Start レコードが送信されない場合は、重複する Interim および Stop レコードが後で到着しても、セカンダリ AAAA グループサーバーのいずれにも送信されません。ただし、サーバーが稼働していて重複する Start レコードが送信されたのにサーバーが応答しなかった場合、重複する Start レコードはすべての再試行後にドロップされます。この場合、重複する Interim レコードと Stop レコードがサーバーに送信される可能性があります。
- 重複する Start レコードが送信されたが、重複するInterim/Stopレコードの生成中にピアが応答/ダウンしなかった場合、すべての再試行の後、重複する Interim および Stop レコードはドロップされ、HDD に書き込まれません。
- すべてのプライマリ Rf レコードで重複レコードが生成されるため、メモリと CPU への若干の影響が予想されます。

Rf 重複レコード生成の設定

以下では、Rf 重複レコード生成を有効にするための設定コマンドについて説明します。

セカンダリ AAA グループの設定

重複 Rf レコードを受信するようにセカンダリ AAA グループを設定するには、次の設定コマンドを使用します。

```
configure
   context context_name
      apn apn_name
         aaa group group_name
         aaa secondary-group group_name
         exit
```

注：

- **aaa group** *group_name*：APN の AAA サーバーグループを指定します。*group_name* は、1 ～ 63 文字の英数字の文字列である必要があります。
- **secondary group** *group_name*：APN のセカンダリ AAA サーバーグループを指定します。*group_name* は、1 ～ 63 文字の英数字の文字列である必要があります。

Rf レコードの重複の設定

Rf レコードのセカンダリフィードを作成し、それをセカンダリ AAA グループに送信するようにシステムを構成するには、次の設定コマンドを使用します。

```
configure
   context context_name
      aaa group group_name
         diameter accounting duplicate-record
         exit
```

注：

- **duplicate-record**：設定されたセカンダリ AAA グループに重複 Rf レコードを送信します。このキーワードはライセンスによって異なります。詳細については、シスコのアカウント担当者にお問い合わせください。
- デフォルトの設定は、**no diameter accounting duplicate-record** です。デフォルトでは、この機能は無効になっています。
- **diameter accounting duplicate-record** CLI コマンドを有効にする前に、セカンダリ AAA グループを APN 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。

Rf 重複レコード生成の設定確認

次のコマンドを使用して、この機能の設定ステータスを確認するには、次のコマンドを使用します。

show configuration

show aaa group all

または

show aaa group *group_name*

group_name は、設定時に指定した AAA グループの名前にする必要があります。

このコマンドを実行すると、指定した AAA グループ内で有効になっている設定がすべて表示されます。

この機能の設定例を以下に示します。

```
configure
   context source
      apn domainname.com
         associate accounting-policy policy_accounting_name
         aaa group group1
         aaa secondary-group group2
         exit
      aaa group group1
         diameter accounting dictionary aaa-custom4
         diameter accounting endpoint rf_endpoint1
         diameter accounting server rf_server1 priority 1
         diameter accounting server rf_server2 priority 2
         exit
      aaa group group2
         diameter accounting dictionary aaa-custom4
         diameter accounting endpoint rf_endpoint2
         diameter accounting duplicate-record
         diameter accounting server rf_server3 priority 3
         diameter accounting server rf_server4 priority 4
         exit
      diameter endpoint rf-endpoint1
         use-proxy
         origin host rf-endpoint1.carrier.com address 192.50.50.3
         no watchdog-timeout
```

```
            response-timeout 20
            connection retry-timeout 5
            peer rf_server1 realm domainname.com address 192.50.50.4 port 4872
            peer rf_server2 realm domainname.com address 192.50.50.4 port 4873
            exit
        diameter endpoint rf-endpoint2
            use-proxy
            origin host rf-endpoint2.carrier.com address 192.50.50.2
            no watchdog-timeout
            response-timeout 20
            connection retry-timeout 5
            peer rf_server3 realm domainname.com address 192.50.50.5 port 4892
            peer rf_server4 realm domainname.com address 192.50.50.5 port 4893
end
```

注：

- **diameter accounting duplicate-record** CLI はライセンス固有です。そのため、CLI コマンドを設定するには、対応するライセンスを有効にする必要があります。
- プライマリとセカンダリの両方の AAA グループに、異なるアカウンティング エンドポイント名を割り当てることができます。

Rf 重複レコード生成のモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

次の操作を実行して、この機能に関連する障害をトラブルシュートできます。

- **show configuration** または **show aaa group all** CLI コマンドを使用して、この機能が有効になっているかどうかを確認します。有効になっていない場合は、diameter accounting duplicate-record CLI コマンドを設定して、この機能が動作するかどうかを確認します。
- **show diameter aaa statistics** コマンドの出力を収集し、デバッグ統計を分析します。また、報告されたログを確認します（存在する場合）。詳細な分析が必要な場合は、シスコのアカウント担当者にご連絡ください。

show diameter aaa-statistics

アカウンティングレコードを HDD またはアーカイブリストに追加する代わりに送信しようとして、失敗したためにドロップされた重複 Rf レコードについて、この show コマンドの出力には次の統計が追加されます。

- 重複アカウンティングレコード統計
  - ドロップされた ACR-Start
  - ドロップされた ACR-Interim
  - ドロップされた ACR-Stop

これらの統計は、aaamgrインスタンスレベルごとに保持されます。これらの統計の詳細については、『*Statistics and Counters Reference*』を参照してください。

これらの統計は、重複レコードのグループベースまたはサーバーベースごとに収集することもできます。これには、**show diameter aaa-statistics group** <*group_name*> および **show diameter aaa-statistics server** <*server_name*> CLI コマンドを使用します。

Rf レコードの仮想 APN の切り捨て

この機能により、S6b サーバーから返された仮想 APN（VAPN）の切り捨てを Gx、Gy、および Rf インターフェイスに送信できます。

機能説明

現在、ネットワーク内のすべてのノードに到達することなく、各ノードで仮想 APN をプロビジョニングすることもなく、仮想 APN（S6b-VAPN）ごとにデータ ストリーミング サービス（DSS）サーバーへの Rf アカウンティングを迅速にオンにする方法はありません。この機能は、S6b サーバーによって返される仮想 APN 名を、設定済みの標準デリミタで切り捨てるために実装されています。この方法により、ノードごとに 1 つの設定を仮想 APN に基づくすべての企業に対して利用できます。このアプローチにより、要求された機能を新しい企業向けにプロビジョニングする際の作業の規模と時間が大幅に削減されます。

この機能を実現するには、APN ごとに設定を追加して、S6b-VAPN の切り捨てを有効にし、APN 名を切り捨てるデリミタも設定します。（.）や（-）などの標準のデリミタを使用します。APN 名では英数字以外にこれらの 2 文字しかサポートされないためです。

AAA サーバーがハイフンデリミタとドットデリミタの両方を返す場合や、同じデリミタを仮想 APN として 2 回以上返す場合、最初のデリミタは区切り文字と見なされます。たとえば、AAA サーバーが仮想 APN として xyz-cisco.com を返す場合、ハイフンは区切り文字です。

AAA マネージャは、APN 設定に基づいて仮想 APN 名の切り捨てを実行し、切り捨てられた APN 名に対応する正しい APN プロファイルを提供します。切り捨てに成功した場合、完全な仮想 APN 名が Gx、Gy、および Rf インターフェイスに送信されます。

リアルタイム使用状況通知とデバイス管理機能をサポートするには、アカウンティングレコードが必要です。そのため、**apn-name-to-be-included** CLI コマンドが拡張され、実際の APN（Gn-APN）名または仮想 APN（S6b から返された仮想 APN）名を有効にして、ポリシーアカウンティング設定のセカンダリ Rfアカウンティングレコード（セカンダリサーバーグループ）の Called-Station-ID AVP に含めることができるようになりました。現在、ポリシーアカウンティング設定は、プライマリ Rf サーバーの Called-Station-ID での Gn-APN/S6b-VAPN の送信をサポートしています。この CLI コマンドを使用すると、この機能がセカンダリ Rf サーバーまで拡張されます。

新しい AAA 属性「Secondary-Called-Station-ID」が追加され、セカンダリグループ Rf サーバーに送信される重複 Rf レコードの Called-Station-ID AVP での Gn/仮想 APN 名の送信がサポートされるようになりました。

Rf レコードの仮想 APN 切り捨ての設定

以下では、Rf レコードの仮想 APN 切り捨て機能を有効にするための設定コマンドについて説明します。

Rf アカウンティング用の Gn-APN/VAPN の設定

次の設定コマンドを使用して、Rfアカウンティング用の実際のAPNまたは仮想APN（VAPN）を設定します。

```
configure
  context context_name
    policy accounting policy_name
      apn-name-to-be-included { gn | virtual } [ secondary-group { gn
 | virtual } ]
      end
```

注：

- **apn-name-to-be-included**：プライマリサーバーグループの Rf メッセージに含める APN 名を設定します。
- **secondary-group { gn | virtual }**：セカンダリサーバーグループの Rf メッセージに含める APN 名を設定します。
- **gn**：Rf メッセージに含める Gn APN 名を設定します。
- **virtual**：Rf メッセージに含める仮想 APN 名を設定します。
- デフォルトでは、プライマリおよびセカンダリ RF サーバーグループの両方で、Called-Station-ID AVP に含まれる APN 名は Gn-APN です。
- セカンダリグループの設定を使用できない場合、デフォルトの動作では、セカンダリ RF グループの重複レコードに対して Gn APN が設定されます。

仮想 APN の切り捨ての設定

次の設定コマンドを使用して、S6b インターフェイスから返された APN 名が切り捨てられるようにゲートウェイを設定します。

```
configure
  context context_name
    apn apn_name
      virtual-apn { gcdr apn-name-to-be-included { gn | virtual } |
truncate-s6b-vapn delimiter { dot [ hyphen ] | hyphen [ dot ] } }
      end
```

注：

- 既存のキーワードの詳細については、『*Command Line Interface Reference*』のガイドを参照してください。
- **truncate-s6b-vapn**：S6bから受信した仮想APNを、設定したデリミタ文字で切り捨てられるようにします。

- **delimiter { dot [hyphen] | hyphen [dot] }**：S6b から受信した仮想 APN を切り捨てる際のデリミタを設定します。この CLI コマンドが設定されている場合、S6b から返された仮想 APN は設定したデリミタで切り捨てられます。
  - **dot**：S6b-VAPN の切り捨てに使用するデリミタをドット（.）に設定します。
  - **hyphen**：S6b-VAPN の切り捨てに使用するデリミタをハイフン（-）に設定します。
- ドットとハイフンの両方のデリミタを同じ行または新しい行に設定できます。
- **no virtual-apn truncate-s6b-vapn**：仮想 APN 名の切り捨てを無効にします。両方のデリミタを一度に無効にする必要がある場合は、**no virtual-apn truncate-s6b-vapn** CLI コマンドを使用します。

  特定のデリミタを無効にする必要がある場合は、明示的に指定する必要があります。たとえば、ドットのデリミタを無効にする場合は、**no virtual-apn truncate-s6b-vapn delimiter dot** CLI コマンドを使用します。
- デフォルトでは、この機能は無効になっており、デリミタは設定されていません。
- この CLI コマンドは、S6b サーバーが認証承認受諾（AAA）メッセージで仮想 APN 名を返す場合にのみ有効です。
- 受信した S6b 仮想 APN 名に区切り文字がない場合は、仮想 APN 名全体が設定時に考慮されます。

仮想 APN の切り捨て設定の確認

次のコマンドを使用して、この機能の設定ステータスを確認します。

show configuration apn *apn_name*

apn_name は、機能の設定中に指定された APN の名前である必要があります。

このコマンドを実行すると、指定した APN 名内で有効になっている設定がすべて表示されます。次に、この show コマンドの出力例を示します。

```
[local]st40# show configuration apn intershat
configure
   context ingress
      apn intershat
         pdp-type ipv4 ipv6
         bearer-control-mode mixed
         virtual-apn truncate-s6b-vapn delimiter hyphen
         end
```

仮想 APN 切り捨てのモニタリングと障害対応

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

次の操作を実行して、この機能に関連する障害をトラブルシュートできます。

- **show configuration apn** *apn_name* CLI コマンドを使用して、機能が有効になっているかどうかを確認します。有効になっていない場合は、**virtual-apn truncate-s6b-vapn delimiter {**

dot [hyphen] | hyphen [dot] } } CLI コマンドを設定して、この機能が動作するかどうかを確認します。

- **show apn statistics** CLI コマンドの出力を収集し、デバッグ統計を分析します。サポートが必要な場合は、シスコのアカウント担当者にご連絡ください。



重要 P-GW、GGSN、および SAEGW サービスでは、S6b から返された仮想 APN 名の切り捨てが失敗し、仮想 APN 名が設定されていない場合、「unknown-apn-name」を原因としてコールが拒否されます。

show apn statistics

この機能が有効になっている場合、この show コマンドは、既存の APN 統計を使用して、切り捨てられた仮想 APN 名を入力します。

show subscribers ggsn-only full all

この機能が有効になっている場合、この show コマンドの出力に新たに追加された次のフィールドには、S6b から返された完全な仮想 APN 名が表示されます。有効になっていない場合は、「n/a」と表示されます。

- S6b Returned Virtual APN

show subscribers pgw-only full all

この機能が有効になっている場合、この show コマンドの出力に新たに追加された次のフィールドには、S6b から返された完全な仮想 APN 名が表示されます。有効になっていない場合は、「n/a」と表示されます。

- S6b が返した仮想 APN

show subscribers saegw-only full all

この機能が有効になっている場合、この show コマンドの出力に新たに追加された次のフィールドには、S6b から返された完全な仮想 APN 名が表示されます。有効になっていない場合は、「n/a」と表示されます。

- S6b Returned Virtual APN

アカウンティングレコード停止ロケーションレポート

以前の動作：P-GW または S-GW が ACR 停止メッセージで新しいユーザーロケーション情報（ULI）メッセージを Rf インターフェイスを介してオフライン課金システム（OFCS）に送信すると、セッションの終了時に報告された場所と、想定されるロケーションレポートの内容が一致しませんでした。アカウンティング停止レコード（ACR 停止）で使用されている場所に不整合があり、ロケーションレポート中に、（ACR が送信される前の場所を示していない）ACR 停止暫定メッセージが発生していました。

新しい動作：StarOS 21.22 以降のリリースでは、セッション削除要求が新しいユーザーロケーション情報（ULI）とともに受信されるときに、既存のULIが、GGSN、P-GW、およびSAEGWのオフライン課金（RF）インターフェイスでアカウンティングレコード（ACR）停止メッセージに送信されます。

機能の仕組み

ここでは、GPRS/eHRPD/LTE/IMS ネットワークでの Rf インターフェイスのサポートにより、サブスクライバのオフライン課金がどのように機能するのかを説明します。

次の図と表で、イベントベース課金を実行するために Diameter Rf インターフェイスで必要なトランザクションについて説明します。この操作は、サービス/コンテンツの配信前、配信中、または配信後に実行することもできます。

図 *112*：イベントベース課金の *Rf* コールフロー

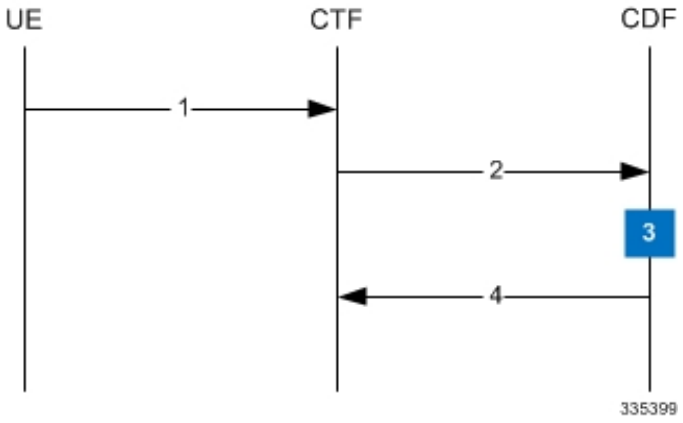


表 *129*：イベントベース課金の *RF* コールフローの説明

ステップ	説明
1	ネットワーク要素（CTF）が、サービスが使用または配信されたことを示す通知を受信します。
2	CTF（Diameter クライアントとして機能）が、サービス固有の情報を CDF（Diameter サーバとして機能）に示すために、EVENT_RECORD に設定された Accounting-Record-Type AVP を含むアカウンティング要求（ACR）を送信します。
3	CDF が、関連するサービス課金パラメータを受信して、アカウンティング要求を処理します。
4	CDF が、課金情報を受信したことを通知するために、EVENT_RECORD に設定された Accounting-Record-Type AVP を含むアカウンティング応答（ACA）メッセージを CTF に返します。

次の図と表で、セッションベース課金の単純な Rf コールフローについて説明します。

図 *113 :* セッションベース課金の *Rf* コールフロー

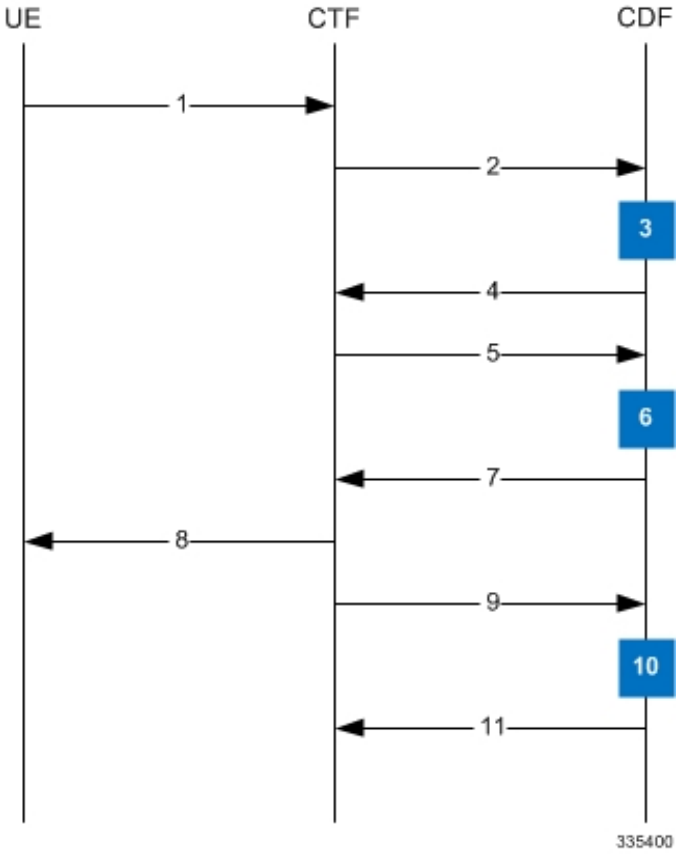


表 *130 :* セッションベース課金の *Rf* コールフローの説明

ステップ	説明
1	CTF が、サービス要求を受信します。サービス要求は、ユーザーまたは他のネットワーク要素によって開始される可能性があります。
2	アカウンティングセッションを開始するために、CTF が、START_RECORD に設定された Accounting-Record-Type AVP を含むアカウンティング要求（ACR）を CDF に送信します。
3	セッションが開始され、CDF が、現在のセッションの CDR を開きます。
4	CDF が、START_RECORD に設定された Accounting-Record-Type と、場合によっては目的の中間課金間隔を示すゼロ以外の値に設定された Acct-Interim-Interval AVP（AII）を含むアカウンティング応答（ACA）メッセージを CTF に返します。
5	AII が経過するか、課金条件の変更が CTF で認識されると、CTF が、INTERIM_RECORD に設定された Accounting-Record-Type AVP を含むアカウンティング要求（ACR）を CDF に送信します。

ステップ	説明
6	CDF が、問題の CDR を更新します。
7	CDF が、INTERIM_RECORD に設定された Accounting-Record-Type を含むアカウンティング応答（ACA）メッセージを CTF に返します。
8	サービスが終了します。
9	CTF が、STOP_RECORD に設定された Accounting-Record-Type AVP を含むアカウンティング要求（ACR）を CDF に送信します。
10	CDF が、それに応じて CDR を更新し、CDR を閉じます。
11	CDF が、STOP_RECORD に設定された Accounting-Record-Type を含むアカウンティング応答（ACA）メッセージを CTF に返します。

Rf インターフェイスサポートの設定

Rf インターフェイスのサポートを設定するには、次の手順を実行します。

1. このアドミニストレーションガイドの説明に従って、コアネットワークサービスを設定します。
2. アクティブ課金サービス（ACS）を有効にして、『*Enhanced Charging Services Administration Guide*』[英語] の説明に従って ACS を作成します。



重要 このセクションの手順では、『*Enhanced Charging Services Administration Guide*』[英語] に記載されている ECS のインストールと設定を含めて、シャーシの設置と設定が完了していることを前提としています。

3. 「アクティブ課金サービスでの RF インターフェイスの有効化（1334 ページ）」の説明に従い、ACS で Rf アカウンティングを有効にします。
4. 関連するセクションの説明に従って、Rf インターフェイスのサポートを設定します。
   - GGSN/P-GW Rf インターフェイスサポートの設定 （1334 ページ）
   - P-CSCF/S-CSCF Rf インターフェイスサポートの設定 （1344 ページ）



重要 StarOS バージョン 19 以降では、Rf インターフェイスは S-GW でサポートされていません。

5. EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存

する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

重要 この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンド、および/またはキーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

アクティブ課金サービスでの RF インターフェイスの有効化

課金レコード生成と Rf アカウンティングを有効にするには、次の設定を使用します。

```
configure
   active-charging service <service_name>
      rulebase <rulebase_name>
         billing-records rf
        active-charging rf { rating-group-override | service-id-override
 }
         end
```

注：

- アクティブ課金サービス（ACS）を作成する前に、**require active-charging** コマンドを設定して ACS 機能を有効にする必要があります。
- **billing-records rf** コマンドは、サブスクライバセッションに対して実行される課金の Rf レコードタイプを設定します。Rf アカウンティングは、ダイナミック ACS ルールおよび事前定義済みの ACS ルールにのみ適用されます。

  ルールとその設定の詳細については、『*Command Line Interface Reference*』の「*ACS Charging Action Configuration Mode Commands*」の章 [英語] を参照してください。
- **active-charging rf** コマンドは、RF ベースのアカウンティングに関するすべての PCC ルール、事前定義された ACS ルール、および静的 ACS ルールに特定の評価グループ/サービス識別子を適用するために使用されます。この CLI 設定はルールベースレベルで適用されるため、現在のルールベースが定義されているすべての APN でこの設定が継承されます。

  このコマンドの詳細については、『*Command Line Interface Reference*』の「*ACS Rulebase Configuration Mode Commands*」の章 [英語] を参照してください。

GGSN/P-GW Rf インターフェイスサポートの設定

GGSN/P-GW の標準 Rf インターフェイスサポートを設定するには、次の設定を使用します。

```
configure
   context <context_name>
```

```
apn <apn_name>
   associate accounting-policy <policy_name>
   exit
policy accounting <policy_name>
   accounting-event-trigger { cgi-sai-change | ecgi-change |
flow-information-change | interim-timeout | location-change | rai-change
 | tai-change } action { interim | stop-start }
   accounting-keys qci
accounting-level { flow | pdn | pdn-qci | qci | sdf | subscriber }
   cc profile index { buckets num | interval seconds | sdf-interval
 seconds | sdf-volume { downlink octets { uplink octets } | total octets |
uplink octets { downlink octets } }  | serving-nodes num | tariff time1
min hrs [ time2 min hrs...time4 min hrs ] | volume { downlink octets { uplink
 octets } | total octets | uplink octets { downlink octets } } }
   max-containers { containers | fill-buffer }
   end
```

注：

- ポリシーは、任意のコンテキストで設定できます。
- アカウンティングレベル/ポリシー/モード/イベントトリガーの設定の詳細については、『*Command Line Interface Reference*』の「*Accounting Policy Configuration Mode Commands*」の章を参照してください。
- 設定されているトリガーに応じて、コンテナはキャッシュまたはリリースされます。GGSN/P-GW の場合、イベントトリガーが次のいずれかであると、コンテナはキャッシュされます。
  - QOS_CHANGE
  - FLOW_INFORMATION_CHANGE
  - LOCATION_CHANGE
  - SERVING_NODE_CHANGE
  - SERVICE_IDLE
  - SERVICE_DATA_VOLUME_LIMIT
  - SERVICE_DATA_TIME_LIMIT
  - IP_FLOW_TERMINATION
  - TARIFF_CHANGE

  イベントトリガーが次のいずれかであると、コンテナはリリースされます。
  - VOLUME_LIMIT
  - TIME_LIMIT
  - RAT_CHANGE
  - TIMEZONE_CHANGE
  - PLMN_CHANGE



重要 現在、P-GW では、SDF およびフロー レベル アカウンティングがサポートされています。

次の前提条件により、Change-Condition トリガーに対する P-GW、GGSN、および CCF の動作が決まります。

- 変更条件による ACR メッセージのデータには、以前の ACR メッセージからフロー/セッションの間隔に適用されるすべてのデータのスナップショットが含まれます。これには、すでに送信されており、変更されていないすべてのデータ（SGSN-Address など）が含まれます。
- Change-Condition トリガー時点までの PDN セッション/フローに含まれるすべての情報は、ACR-Interim メッセージでキャプチャ（スナップショット）されます。ターゲットの Time-Zone/ULI/3GPP2-BSID/QoS-Information/PLMN Change などに関する情報は、後続の Rf メッセージに含まれます。

表 *131 : LTE/e-HRPD/GGSN* の *ACR-Stop* および *ACR-Interim* の *Change-Condition* に対する *P-GW/GGSN* および *CCF* の動作

ACR メッセージ	Change-Condition の値	Change-Condition の値への CCF 応答			CC レベルの入力		注
		コンテナの追加	部分 FDR	最終 FDR	PS-Information レベル	SDC レベル	
ストップ	Normal Release	対応	非対応	非対応	Normal Release	Normal Release	PDN/IP セッションが閉じられると、両方レベルの C-C で通常リースが行われます
なし（この変更条件は課金条件の最大変更回数のカウンタであるため）。	Normal Release	対応	非対応	非対応	該当なし	Normal Release	フローが閉じられ、SDC CC が入力され閉じたコンテナがレコードに追加されます。この変更条件のンテナは P-GW/GGS によってキャッシュれ、コンテナは、部レコード（中間）、終レコード（停止）または AII トリガー（中間）トリガーのめに送信される AC Interim/Stop に含まれす。
ストップ	Abnormal Release	対応	非対応	非対応	Abnormal Release	Abnormal Release	PDN/IP セッションが閉じられると、両方レベルの C-C で異常リースが行われます

ACR メッセージ	Change-Condition の値	Change-Condition の値への CCF 応答			CC レベルの入力		注
		コンテナの追加	部分 FDR	最終 FDR	PS-Information レベル	SDC レベル	
なし（この変更条件は課金条件の最大変更回数のカウンタであるため）。	Abnormal Release	対応	非対応	非対応	該当なし	Abnormal Release	フローが閉じらあ SDC CC が入力さ 閉じたコンテナが コードに追加さあ す。この変更条件 ンテナは P-GW/(によってキャッシ れ、コンテナは、 レコード（中間） 終レコード（停止 または AII トリガ （中間）トリガー めに送信される Interim/Stop に含ま す。
なし（この変更条件は課金条件の最大変更回数のカウンタであるため）。	QoS-Change	対応	非対応	非対応	該当なし	QoS-Change	この変更条件のコ ナは P-GW/GGSN よってキャッシ れ、コンテナは、 レコード（中間） 終レコード（停止 または AII トリガ （中間）トリガー めに送信される Interim/Stop に含ま す。

ACR メッセージ	Change-Condition の値	Change-Condition の値への CCF 応答			CC レベルの入力		注
		コンテナの追加	部分 FDR	最終 FDR	PS-Information レベル	SDC レベル	
Interim	Volume Limit	対応	対応	非対応	Volume Limit	Volume Limit	PDN/IP セッションの場合は、Volume Lim です。Volume Limit 課金プロファイルの部として設定され、Charging-Characterist AVP がこの課金プロファイルを伝送しま す。このプロファイは、さまざまなインターフェイスを介し HSS/AAA から P-GW/GGSN に渡さ ます。課金プロファルは、HSS でプロビジョニングされます
Interim	Time Limit	対応	対応	非対応	Time Limit	Time Limit	PDN/IP セッションの場合は、Time Limit す。Time Limit は課プロファイルの一部して設定され、Charging-Characterist AVP がこの課金プロファイルを伝送しま す。このプロファイは、さまざまなインターフェイスを介し HSS/AAA から P-GW/GGSN に渡さ ます。課金プロファルは、HSS でプロビジョニングされます

ACR メッセージ	Change-Condition の値	Change-Condition の値への CCF 応答			CC レベルの入力		注
		コンテナの追加	部分 FDR	最終 FDR	PS-Information レベル	SDC レベル	
なし（この変更条件は課金条件の最大変更回数のカウンタであるため）。	Serving Node Change	対応	非対応	非対応	該当なし	Serving Node Change	この変更条件のナは P-GW/GGSよってキャッシれ、コンテナは、レコード（中間）終レコード（停止または AII トリガ（中間）トリガーめに送信される Interim/Stop に含す。
Interim	Serving Node PLMN Change	対応	対応	非対応	Serving Node PLMN Change	Serving Node PLMN Change	
なし（この変更条件は課金条件の最大変更回数のカウンタであるため）。	User Location Change	対応	非対応	非対応	該当なし	User Location Change	これは、eHRPD ける BSID の変す。この変更条ンテナは P-GW/によってキャッシれ、コンテナは、レコード（中間）終レコード（停止または AII トリガ（中間）トリガーめに送信される Interim/Stop に含す。
Interim	RAT の変更	対応	対応	非対応	RAT の変更	RAT の変更	
Interim	UE Timezone Change	対応	対応	非対応	UE Timezone change	UE Timezone change	これは eHRPD に用されません。
なし（この変更条件は課金条件の最大変更回数のカウンタであるため）。	Tariff Time Change	対応	非対応	非対応	該当なし	Tariff Time Change	タリフ時間が変るとトリガーさす。タリフ時間にには、オンライン側変更が必要での変更条件の実オンライン課金実装に依存しま

ACR メッセージ	Change-Condition の値	Change-Condition の値への CCF 応答			CC レベルの入力		注
		コンテナの追加	部分 FDR	最終 FDR	PS-Information レベル	SDC レベル	
なし（この変更条件は課金条件の最大変更回数のカウンタであるため）。	Service Idled Out	対応	非対応	非対応	該当なし	Service Idled Out	フローがアイドルアトしました。この変条件のコンテナは P-GW/GGSN によっキャッシュされ、コテナは、部分レコー（中間）、最終レコド（停止）、またにAII トリガー（中間トリガーのために送される ACR Interim/Stop に含まれす。
なし（この変更条件は課金条件の最大変更回数のカウンタであるため）。	Service Data Volume Limit	対応	非対応	非対応	該当なし	Service Data Volume Limit	特定のフローのボリューム制限に達しした。この変更条件コンテナは P-GW/GGSN によっキャッシュされ、コテナは、部分レコー（中間）、最終レコド（停止）、またにAII トリガー（中間トリガーのために送される ACR Interim/Stop に含まれす。

ACR メッセージ	Change-Condition の値	Change-Condition の値への CCF 応答			CC レベルの入力		注
		コンテナの追加	部分 FDR	最終 FDR	PS-Information レベル	SDC レベル	
なし（この変更条件は課金条件の最大変更回数のカウンタであるため）。	Service Data Time Limit	対応	非対応	非対応	該当なし	Service Data Time Limit	特定のフローの時限に達しました。変更条件のコンテ P-GW/GGSN によ キャッシュされ、テナは、部分レコ（中間）、最終レ ド（停止）、また AII トリガー（中 トリガーのために される ACR Interim/Stop に含ま す。

ACR メッセージ	Change-Condition の値	Change-Condition の値への CCF 応答			CC レベルの入力		注
		コンテナの追加	部分 FDR	最終 FDR	PS-Information レベル	SDC レベル	
Interim	Max Number of Changes in Charging Conditions	対応	対応	非対応	非対応	対応。発生した CC（Normal Release of Flow、Abnormal Release of Flow、QoS-Change、Serving Node Change、User Location Change、Tariff Time Change、Service Idled Out、Service Data Volunme Limt、Service Data Time Limit）に対応する SDC が含まれます。	

ACR メッセージ	Change-Condition の値	Change-Condition の値への CCF 応答			CC レベルの入力		注
		コンテナの追加	部分 FDR	最終 FDR	PS-Information レベル	SDC レベル	
							この ACR（Inter は、課金条件の変 最大回数に達した でトリガーされま 最大変更条件は、 QoS-Change、 Service-Idled Out change、Flow No Release、Flow Abnormal Release Service Data Volu Limit、Service D Time Limit、AII ACR Interim、お Service Node Char にのみ適用されま 課金条件の変更の 回数は 10 に設定 ます。PDNセッシ での 1 フローを想 た例：[1] P-GW/G で設定された課金 の最大の変更回数 です。[2] Change Condition 1 が発生 す。ACR Interim 信されません。 P-GW/GGSN が S 保存します。[3] Change Condition 生します。ACR I が送信されます。 時点で、課金条件 更の最大回数が PS-Information に され、2 つの Service-Data-Con （変更条件ごとに つ）が ACR Inter 入力されます。[4

ACR メッセージ	Change-Condition の値	Change-Condition の値への CCF 応答			CC レベルの入力		注
		コンテナの追加	部分 FDR	最終 FDR	PS-Information レベル	SDC レベル	
							が部分レコードを作します。
ストップ	Management Intervention	対応	非対応	非対応	対応	対応	管理介入により、P-GW/GGSN からのPDNセッションが閉られます。
Interim	-	対応	非対応	非対応	該当なし	該当なし	これがここに含まれのは、AII タイマーよる ACR[Interim] につまたはすべてのフローについて入力さた 1 つ以上の SDC が含まれるが、Change-Condition AV は入力され「ない」とを示すためです。

P-CSCF/S-CSCF Rf インターフェイスサポートの設定

P-CSCF/S-CSCF Rf インターフェイスサポートを設定するには、次の設定コマンドを使用します。

```
configure
   context vpn
      aaa group default
         diameter authentication dictionary aaa-custom8
         diameter accounting dictionary aaa-custom2
         diameter accounting endpoint <endpoint_name>
         diameter accounting server <server_name> priority <priority>
         exit
      diameter endpoint <endpoint_name>
         origin realm <realm_name>
         use-proxy
         origin host <host_name> address <ip_address>
         peer <peer_name> address <ip_address>
         exit
      end
```

注：

- Rf サポートの基本設定で使用されるコマンドについては、『*Command Line Interface Reference*』を参照してください。

統計情報の収集

ここでは、Rf および関連する統計と設定情報を収集する方法について説明します。

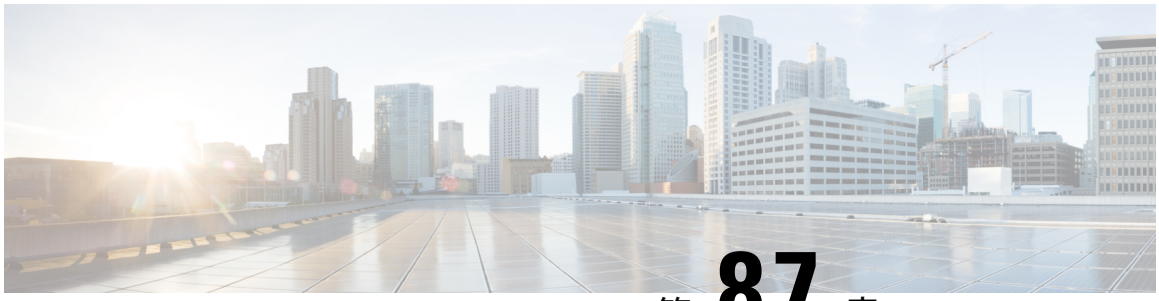
次の表では、最初の列に、収集する統計が示されており、2 つ目の列に、実行するアクションが示されています。

統計/情報	実行するアクション
Diameter Rf アカウンティングセッションの完全な統計	**show diameter aaa-statistics**

次に、**show diameter aaa-statistics** コマンドの出力例を示します。

```
Authentication  Servers Summary
 ------------------------------
Message Stats :
  Total MA Requests:            0       Total MA Answers:             0
  MAR - Retries:                0       MAA Timeouts:                 0
  MAA - Dropped:                0
  Total SA Requests:            0       Total SA Answers:             0
  SAR - Retries:                0       SAA Timeouts:                 0
  SAA - Dropped:                0
  Total UA Requests:            0       Total UA Answers:             0
  UAR - Retries:                0       UAA Timeouts:                 0
  UAA - Dropped:                0
  Total LI Requests:            0       Total LI Answers:             0
  LIR - Retries:                0       LIA Timeouts:                 0
  LIA - Dropped:                0
  Total RT Requests:            0       Total RT Answers:             0
  RTR - Rejected:               0
  Total PP Requests:            0       Total PP Answers:             0
  PPR - Rejected:               0
  Total DE Requests:            0       Total DE Answers:             0
  DEA - Accept:                 0       DEA - Reject:                 0
  DER - Retries:                0       DEA Timeouts:                 0
  DEA - Dropped:                0
  Total AA Requests:            0       Total AA Answers:             0
  AAR - Retries:                0       AAA Timeouts:                 0
  AAA - Dropped:                0
  ASR:                          0       ASA:                          0
  RAR:                          0       RAA:                          0
  STR:                          0       STA:                          0
  STR - Retries:                0
Message Error Stats:
  Diameter Protocol Errs:       0       Bad Answers:                  0
  Unknown Session Reqs:         0       Bad Requests:                 0
  Request Timeouts:             0       Parse Errors:                 0
  Request Retries:              0
Session Stats:
  Total Sessions:               0       Freed Sessions:               0
  Session Timeouts:             0       Active Sessions:              0
STR Termination Cause Stats:
  Diameter Logout:              0       Service Not Provided:         0
  Bad Answer:                   0       Administrative:               0
  Link Broken:                  0       Auth Expired:                 0
  User Moved:                   0       Session Timeout:              0
  User Request:                 0       Lost Carrier                  0
  Lost Service:                 0       Idle Timeout                  0
  NAS Session Timeout:          0       Admin Reset                   0
  Admin Reboot:                 0       Port Error:                   0
```

```
  NAS Error:                    0       NAS Request:                  0
  NAS Reboot:                   0       Port Unneeded:                0
  Port Preempted:               0       Port Suspended:               0
  Service Unavailable:          0       Callback:                     0
  User Error:                   0       Host Request:                 0
 Accounting Servers Summary
 --------------------------
Message Stats :
  Total AC Requests:            0        Total AC Answers:            0
  ACR-Start:                    0        ACA-Start:                   0
  ACR-Start  Retries :          0        ACA-Start  Timeouts:         0
  ACR-Interim:                  0        ACA-Interim:                 0
  ACR-Interim  Retries :        0        ACA-Interim  Timeouts:       0
  ACR-Event:                    0        ACA-Event:                   0
  ACR-Stop :                    0        ACA-Stop:                    0
  ACR-Stop  Retries :           0        ACA-Stop  Timeouts:          0
  ACA-Dropped :                 0
AC Message Error Stats:
  Diameter Protocol Errs:       0        Bad Answers:                 0
  Unknown Session Reqs:         0        Bad Requests:                0
  Request Timeouts:             0        Parse Errors:                0
  Request Retries:              0
```



第 87 章

APN上のモバイルステーション背後のルーティング

モバイルステーション（MS）の背後のルーティング機能により、PDNセッション（MS）に属していないが、その背後にある IPv4 アドレスへの、パケットのルーティングが可能になります。宛先のネットワークアドレスは、モバイルステーションのアドレスとは異なるアドレスにすることができます。

この章では、次の事項について説明します。

- 機能説明 （1347 ページ）
- 機能の仕組み （1348 ページ）
- モバイルステーション背後のルーティングの設定 （1348 ページ）
- モバイルステーション背後のルーティングのモニタリングと障害対応 （1353 ページ）

機能説明

Framed-Route 属性は、このネットワーク アクセス サーバー（NAS）上のユーザーに対して設定するルーティング情報を提供します。Framed-Route 情報は、Access-Accept メッセージで RADIUS サーバーに返されます。Framed-Route は、コンテキストレベルまたは VRF レベルで機能します。VRF は企業ごとに存在でき、それぞれが独自の一連の Framed-Route を持つことができます。このような構成では、Framed-Routeは、それぞれの企業専用のVRFにインストールされます。Framed-Route と VRF の関連付けは、サブスクライバ IP プールに基づいて行われます。

モバイルルータは、GGSN が RADIUS サーバーを使用して許可する PDN セッションをルータが作成できるようにします。RADIUS サーバーはこのルータを認証し、access-accept応答パケットにFramed-Route属性を含めます。また、Framed-Route属性は「モバイルルータ」用にGGSNにインストールされるサブネットルーティング情報も指定します。GGSNは、宛先アドレスがFramed-Route と一致するパケットを受信すると、関連付けられた PDN セッションを介してモバイルルータに転送されます。

機能の仕組み

APN 上のモバイルステーション背後のルーティング

次のルールが適用されます。

- GGSN/P-GW の AAA インターフェイスでは、RADIUS サーバーからの RADIUS Access-Accept メッセージで「Framed Route AVP」を受信できます。
- GGSN/P-GW の AAA インターフェイスは、Radius Access-Accept メッセージで最大 16 の「Framed Route AVP」に対応します。
- GGSN/P-GW は、宛先アドレスが 0.0.0.0 やネットマスクが 0.0.0.0 のフレーム化ルートを受け入れません。
- GGSN/P-GW は、ルート内のゲートウェイアドレスがモバイルステーションに割り当てられるアドレスと一致しない場合、フレーム化ルートを受け入れません。
- GGSN/P-GW は重複するフレーム化ルートを無視します。
- GGSN/P-GW では、APN 設定の CLI を介してこの機能の有効化/無効化を制御できます。
- GGSN/P-GW は、この機能によってインストールされるフレーム化ルートの数を制御できます。
- GGSN/P-GW では、ルートごとにモバイルステーションの背後でサポートするホスト（アドレス）の数を制御できます。
- MS の背後のルーティングは、IPv4 PDP コンテキストでのみサポートされます。
- MS の背後でルーティングされたパケットは、MS の同じ 3GPP QoS 設定を共有します。

モバイルステーション背後のルーティングの設定

MS の背後のルーティング機能により、PDN セッション（MS）に属していないが、その背後にある IPv4 アドレスへのパケットのルーティングが可能になります。宛先のネットワークアドレスは、MS のアドレスとは異なるアドレスにすることができます。

MS 背後のルーティングを有効にする前に、次の要件を満たす必要があります。

- MS では認証と承認に RADIUS を使用する必要があります。
- MS背後のルーティング機能を使用するには、インターネット技術特別調査委員会（IETF）標準の RFC 2865 で定義されている Framed-Route（属性 22）をユーザーのプロファイルに設定し、使用する MS ごとに 1 ～16 個のルートを追加する必要があります。

  設定すると、PDNセッション作成のRADIUS認証および承認フェーズ中に、Framed-Route属性がGGSNに自動的にダウンロードされます。アクセスポイントコンフィギュレーションモードでnetwork-behind-mobileコマンドを使用してMS背後のルーティング機能が有効になっていない場合、GGSN は Framed-Route 属性を無視します。

  MS セッションがアクティブでなくなると、このルートは削除されます。

- スタティックルートは設定されません。モバイルステーション背後のルーティング機能（Framed Route、属性 22）とスタティックルートを同時に設定することはできません。

コンフィギュレーションの概要

モバイルステーションの背後でルーティングを有効にするには、次の手順を実行します。

手順

ステップ 1 APN プロファイルを作成します。APN プロファイルの作成 （1349 ページ） を参照してください。

ステップ 2 APN に対してモバイルステーションの背後にあるネットワークを有効または無効にします。「モバイルステーション背後のルーティングの有効化 （1349 ページ）」を参照してください。

APN プロファイルの作成

次の例を使用して、P-GW/SAEGW/S-GW で APN プロファイルを作成します。

```
config
   context context_name
      apn apn_name
      end
```

注：

- APN 名は、1 ～ 64 文字の英数字文字列である必要があります。
- APN プロファイルを作成したら、アクセス ポイント プロファイル コンフィギュレーション モードが開始されます。

モバイルステーション背後のルーティングの有効化

MS の背後のルーティングを有効にするには、アクセスポイントコンフィギュレーションモードで次の手順コマンドを使用します。

```
config
   network-behind-mobile { max-addresses-behind-mobile max_addrs |
max-subnets max_subnets }
   { default | no } network-behind-mobile
 end
```

注：

- **default**

  この機能のデフォルト設定を有効にします。max-subnets を 10、max-addresses-behind-mobile をデフォルト値 16,777,214 として NBMS を有効にします。

- **no**

APN のモバイルステーション機能の背後にあるネットワークを無効にします。

- **max-addresses-behind-mobile** *max_addrs*

  MS の背後にある単一のネットワーク/サブネットで許可されるアドレスの最大数を設定します。

- **max-subnets** *max_subnets*

  APN でのコールで有効にできるサブネットの最大数を指定します。

  max_subnets は、1 ～ 16 の整数である必要があります。

  デフォルト：10

モバイルステーション背後のルーティングの確認

モバイルステーション設定の背後にあるルーティングを確認するには、次の show コマンドを使用します。

1.
```
Router show ip route vrf vpn_am2
"*" indicates the Best or Used route.  S indicates Stale.
Destination         Nexthop          Protocol   Prec Cost Interface
*17.18.19.20/32      10.7.104.2       bgp        20   0    bgp_neighbour
(nhlfe-ix:3)
*17.18.19.21/32      0.0.0.0          connected  0    0    vpn_am2lb1
*40.40.41.0/24       0.0.0.0          connected  0    0
*41.40.41.0/24       0.0.0.0          connected  0    0
*42.40.41.0/24       0.0.0.0          connected  0    0
*43.40.41.0/24       0.0.0.0          connected  0    0
*44.40.41.0/24       0.0.0.0          connected  0    0
*45.40.41.0/24       0.0.0.0          connected  0    0
*46.40.41.0/24       0.0.0.0          connected  0    0
*47.40.41.0/24       0.0.0.0          connected  0    0
*48.40.41.0/24       0.0.0.0          connected  0    0
*49.40.41.0/24       0.0.0.0          connected  0    0
*106.106.0.0/16      0.0.0.0          connected  0    0    pool pool_test_3
Total route count : 13
Unique route count: 13
Connected: 12 BGP: 1
```

2.
```
show subscribers pgw-only full all
Username: starent
  Subscriber Type : Visitor
  Status          : Online/Active
  State           : Connected
  Connect Time    : Mon Oct 12 12:23:52 2015
  Auto Delete     : No
  Idle time       : 00h00m50s
  MS TimeZone     : n/a                  Daylight Saving Time: n/a
  Access Type: gtp-pdn-type-ipv4         Network Type: IP
  Access Tech: eUTRAN                    pgw-service-name: PGW21
  Callid: 0db5d3a3                       IMSI: 123456789012345
  Protocol Username: starent             MSISDN: 9326737733
  Interface Type: S5S8GTP                Low Access Priority: N/A
  Emergency Bearer Type: N/A
  IMS-media Bearer: No
  S6b Auth Status: N/A
  Access Peer Profile: default
  Acct-session-id (C1): 141414650F55554B
```

```
  ThreeGPP2-correlation-id (C2): 17767C4D / 6SKDhW-2
  Card/Cpu: 12/0                          Sessmgr Instance: 47
  Bearer Type: Default                    Bearer-Id: 5
  Bearer State: Active
  IP allocation type: local pool
  IPv6 allocation type: N/A
  IP address: 209.165.200.225
  Framed Routes:                                  Framed Routes Source: RADIUS
    40.40.41.0      255.255.255.0   106.106.0.5
    41.40.41.0      255.255.255.0   106.106.0.5
    43.40.41.0      255.255.255.0   106.106.0.5
    44.40.41.0      255.255.255.0   106.106.0.5
    45.40.41.0      255.255.255.0   106.106.0.5
    46.40.41.0      255.255.255.0   106.106.0.5
    47.40.41.0      255.255.255.0   106.106.0.5
    48.40.41.0      255.255.255.0   106.106.0.5
    49.40.41.0      255.255.255.0   106.106.0.5
    42.40.41.0      255.255.255.0   106.106.0.5
  ULI:
   TAI-ID:
    MCC: 214  MNC: 365
    TAC: 0x6789
   ECGI-ID:
  MCC: 214 MNC: 365
    ECI: 0x1234567
  Accounting mode: None                   APN Selection Mode: Sent by MS
  MEI: 1122334455667788                   Serving Nw: MCC=123, MNC=765
  charging id: 257250635                     charging chars: normal
  Source context: EPC2                    Destination context: ISP1
 S5/S8/S2b/S2a-APN: cisco.com
  SGi-APN:   cisco.com
  APN-OI:    n/a
  Restoration priority level: n/a
  traffic flow template: none
 IMS Auth Service : IMSGx
  active input ipv4 acl: IPV4ACL         active output ipv4 acl: IPV4ACL
active input ipv6 acl:                  active output ipv6 acl:
ECS Rulebase: cisco
Bearer QoS:
QCI: 5
ARP: 0x04
PCI: 0 (Enabled)
PL : 1
PVI: 0 (Enabled)
MBR Uplink(bps): 0                     MBR Downlink(bps): 0
GBR Uplink(bps): 0                     GBR Downlink(bps): 0
PCRF Authorized Bearer QoS:
QCI: n/a
ARP: n/a
PCI: n/a
PL: n/a
PVI: n/a
MBR uplink (bps): n/a                      MBR downlink (bps): n/a
GBR uplink (bps): n/a                      GBR downlink (bps): n/a
Downlink APN AMBR: n/a                  Uplink APN AMBR: n/a
P-CSCF Address Information:
Primary IPv6  :   n/a
  Secondary IPv6:   n/a
Tertiary IPv6 :   n/a
 Primary IPv4  :   n/a
  Secondary IPv4:   n/a
   Tertiary IPv4 :   n/a
Access Point MAC Address:  N/A
  pgw c-teid: [0x8000002f] 2147483695    pgw u-teid: [0x8000002f] 2147483695
```

```
  sgw c-teid: [0x50010001] 1342242817    sgw u-teid: [0x60010001] 1610678273
  ePDG c-teid: N/A                       ePDG u-teid: N/A
  cgw c-teid: N/A                        cgw u-teid: N/A
  pgw c-addr: 2002::2:101                pgw u-addr: 209.165.200.232    2002::2:101
  sgw c-addr: 2002::2:61                 sgw u-addr: 2002::2:61
  ePDG c-addr: N/A                       ePDG u-addr: N/A
  cgw c-addr: N/A                        cgw u-addr: N/A
  Downlink APN AMBR:   16534000 bps    Uplink APN AMBR:   16534000 bps
Mediation context: None                Mediation no early PDUs: Disabled
  Mediation No Interims: Disabled        Mediation Delay PBA: Disabled
  input pkts: 0                                  output pkts: 0
  input bytes: 0                                 output bytes: 0
  input bytes dropped: 0                         output bytes dropped: 0
  input pkts dropped: 0                          output pkts dropped: 0
  input pkts dropped due to lorc    : 0          output pkts dropped due to lorc
  : 0
  input bytes dropped due to lorc   : 0
  in packet dropped suspended state: 0          out packet dropped suspended state:
 0
 in bytes dropped suspended state: 0            out bytes dropped suspended state:
 0
  in packet dropped overcharge protection: 0     out packet dropped overcharge
protection: 0
  in bytes dropped overcharge protection: 0      out bytes dropped overcharge
protection: 0
  in packet dropped sgw restoration state: 0     out packet dropped sgw restoration
 state: 0
  in bytes dropped sgw restoration state: 0      out bytes dropped sgw restoration
 state: 0
 pk rate from user(bps): 0                     pk rate to user(bps): 0
  ave rate from user(bps): 0                    ave rate to user(bps): 0
  sust rate from user(bps): 0                   sust rate to user(bps): 0
  pk rate from user(pps): 0                     pk rate to user(pps): 0
  ave rate from user(pps): 0                    ave rate to user(pps): 0
  sust rate from user(pps): 0                   sust rate to user(pps): 0
  link online/active percent: 65
  ipv4 bad hdr: 0                               ipv4 ttl exceeded: 0
  ipv4 fragments sent: 0                        ipv4 could not fragment: 0
  ipv4 input acl drop: 0                        ipv4 output acl drop: 0
  ipv4 bad length trim: 0
 ipv4 input mcast drop: 0                      ipv4 input bcast drop: 0
  ipv6 input acl drop: 0                        ipv6 output acl drop: 0
  ipv4 input css down drop: 0                   ipv4 output css down drop: 0
  ipv4 input css down drop: 0                   ipv4 output css down drop: 0
  ipv4 output xoff pkts drop: 0                 ipv4 output xoff bytes drop: 0
  ipv6 output xoff pkts drop: 0                 ipv6 output xoff bytes drop: 0
  ipv6 input ehrpd-access drop: 0               ipv6 output ehrpd-access drop: 0
input pkts dropped (0 mbr): 0                 output pkts dropped (0 mbr): 0
  ip source violations: 0                       ipv4 output no-flow drop: 0
  ipv6 egress filtered: 0
  ipv4 proxy-dns redirect: 0                    ipv4 proxy-dns pass-thru: 0
  ipv4 proxy-dns drop: 0
  ipv4 proxy-dns redirect tcp connection: 0
  ipv6 bad hdr: 0                               ipv6 bad length trim: 0
  ip source violations no acct: 0
  ip source violations ignored: 0
  dormancy total: 0                             handoff total: 0
  ipv4 icmp packets dropped: 0
  APN AMBR Input Pkts Drop: 0                   APN AMBR Output Pkts Drop: 0
  APN AMBR Input Bytes Drop: 0                  APN AMBR Output Bytes Drop: 0
```

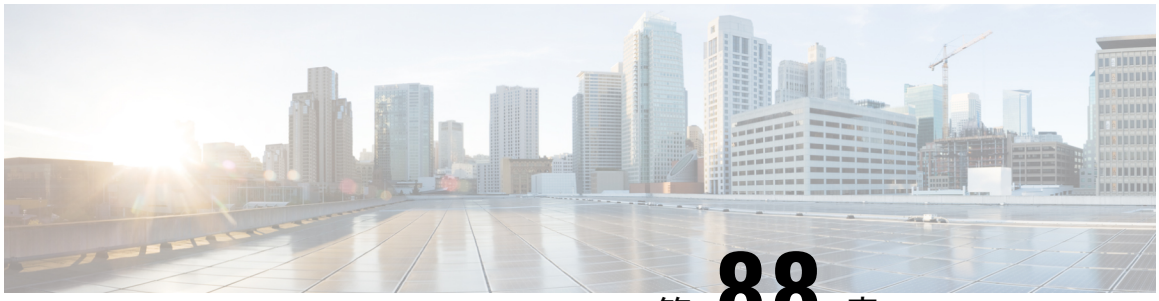
モバイルステーション背後のルーティングのモニタリングと障害対応

モバイルステーション背後のルーティング show コマンドおよび/または出力

show apn name<apn_name>

```
...
proxy-mip: Disabled
proxy-mipv6: Disabled
proxy-mip null-username static home address: Disabled
Network Behind Mobile Station: Enabled
Maximum subnets behind Mobile station: 10
Maximum Addresses Behind Mobile Station:  16777214
Tunnel peer load-balancing : random
L3-to-L2 tunnel address-policy no-alloc-validate
tunnel address-policy alloc-validate
NPU QoS Traffic Priority: Derive from packet DSCP
```

show apn name<apn_name>



第 88 章

レルム名 S6B ベースのルーティング

- 要約データ （1355 ページ）
- レルム P-GW に基づくルーティングの概要 （1356 ページ）
- 機能の仕組み （1356 ページ）
- S6b インターフェイスのレルムの有効化 （1356 ページ）

要約データ

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide*

表 *132* : マニュアルの変更履歴

改訂の詳細	リリース
初版	21.19

レルム P-GW に基づくルーティングの概要

現在、すべての Diameter アプリケーションに、P-GW から送信される初期 Diameter メッセージに設定可能な「Destination-Realm」名を持つオプションがあるわけではありません。その結果、P-GW が DRA を介して Diameter アプリケーションサーバーに接続されるたびに、DRA はそれらのメッセージ内を調査し、正しいアプリケーションサーバーにルーティングするようにルーティングを決定し、クライアントノードから受信した destination-realm を上書きしてから、メッセージをアプリケーション サーバー ノードに送信する必要があります。ただし、これにより、DRA の処理と負荷がある程度増加します。

この機能により、設定可能な値から「Destination-realm」の値を入力するファシリティが提供され、DRA は「トランスペアレント」モードで動作できるようになり、負荷が軽減されます。また、このファシリティにより、DRA は「Destination-realm」に基づいた、より高度なロードバランシング メカニズムを使用できるようになります。

この機能の一部は、MME（S6a および S13 インターフェイス）用に開発されました。P-GW の場合、このファシリティは Gx および Gy インターフェイスの「host-select」および「peer-select」コマンドで実現されていますが、S6b インターフェイスにはそのようなファシリティがありません。この機能は、そのギャップを埋めます。

機能の仕組み

この機能では、DRA への AAR メッセージの「Destination-Realm」AVP に、次のセクションで説明するように「realm」で設定された値が含まれます。これにより、DRA はトランスペアレントモードで動作できます。「Destination-Realm」AVP も、そのセッションの以降のメッセージで設定された値（STR など）に設定されます。

S6b インターフェイスのレルムの有効化

Diameter 認証サーバーをレルム名に関連付けるには、次の設定を使用します。

```
configure
   context context_name
    aaa group group_name
    diameter authentication server  diameter_host_name priority priority_value
 realm realm_name
    end
```

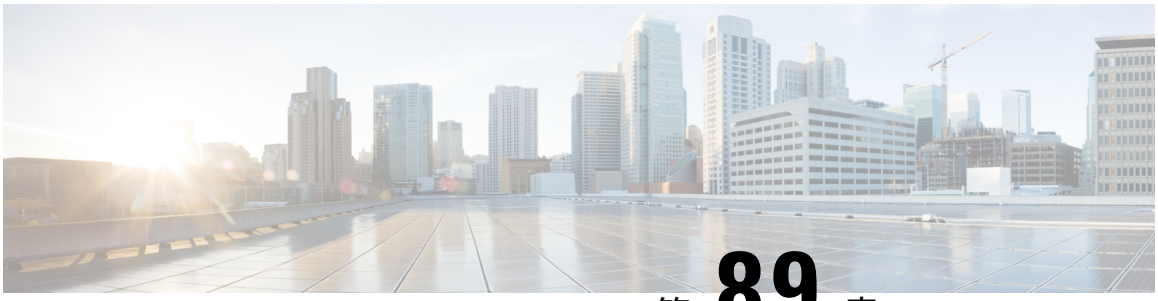
（注） 「realm」属性が設定されている場合、同じ「realm_name」を持つ「route-entry」が必要です。その点について、次に示す例で説明します。

例

```
aaa group s6b
 diameter authentication endpoint s6b
 diameter authentication server dra1.dra.mnc123.mcc456.3gppnetwork.org priority 10 realm
 xyz.org

...

diameter endpoint s6b
      origin realm abc.com
      use-proxy
      origin host SPRC01.s6b address 10.239.144.69
      watchdog-timeout 6
      device-watchdog-request max-retries 3
      response-timeout 5
      cea-timeout 3
      reconnect-timeout 30
      connection retry-timeout 10
     peer dra1.dra.mnc123.mcc456.3gppnetwork.org realm dra.mnc123.mcc456.3gppnetwork.org
 address 10.1.1.1
     peer dra2.dra.mnc123.mcc456.3gppnetwork.org realm dra.mnc123.mcc456.3gppnetwork.org
 address 10.1.1.2
      route-entry realm xyz.org peer dra1.dra.mnc123.mcc456.3gppnetwork.org
```



第 89 章

S6b インターフェイスの機能拡張

- 機能の概要と変更履歴 （1359 ページ）
- 機能説明 （1360 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：ライセンスが必要
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、S6b インターフェイスが拡張され、AVP を介したスタティックおよびダイナミック IP アドレスの割り当てにより、3GPP AAA に対応するようになりました。	21.22

機能説明

StarOS 21.22 以降のリリースでは、S6b インターフェイスが拡張され、次の AVP を介したスタティックおよびダイナミック IP アドレスの割り当てにより、3GPP AAA に対応するようになりました。

- **Class AVP**
- **User-Name AVP**
- **Origination-Time-Stamp AVP**

Class AVP：次の機能拡張がサポートされています。

最初の PDN 接続要求時に、PGW/GGSN は 3GPP AAA からの AA 応答メッセージで CLASS AVP（存在する場合）を受信します。その後、P-GW/GGSN は 3GPP AAA に応答を送信します。AA_request メッセージを 3GPP AA に送信しているときに、P-GW/GGSN が CLASS AVP をドロップします。PGW/GGSN には再承認を開始するオプションがあります。ただし、P-GW/GGSN が以前に 3GPP AAA から CLASS AVP を受信している場合、後続のセッション終了要求には Class AVP が含まれますが、再承認要求は含まれません。この結果、AA 応答メッセージとセッション終了メッセージ（STR メッセージと STA メッセージ）を除くすべてのメッセージから Class AVP が削除されます。

Auth-Session-State が STATE_MAINTAINED としてネゴシエートされた場合、セッションの終了時に、P-GW は Session-Termination-Request（Session-Id, Origin-Host, Origin-Realm, Destination-Realm, Auth-Application-Id=(16777999)、Destination-Host、Termination-Cause、User-Name）を 3GPP AAA に設定します。

（注） `aaa-custom15` ディクショナリが使用されていれば、インスタンスから Class AVP を削除できます。

User-Name AVP：次の機能拡張がサポートされています。

P-GW/GGSN が後続のセッション終了要求（STR）を 3GPP AAA に送信するときに、必須パラメータである **User-Name AVP** が含まれます。

（注） 後方互換性がある限り、3GPP AAA は **User-Name AVP**なしの STR を受け入れます。

User-Name にプレフィックスが含まれていないことを確認してください。

例：

```
<IMSI>@nai.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org.
```

Origination-Time-Stamp AVP：次の機能拡張がサポートされています。

Origination-TimeStamp AVP は、3GPP 標準の Origination-Time-Stamp AVP に置き換えられます。

Maximum-Wait-Time AVP：次の機能拡張がサポートされています。

Max-Wait-Time AVP は、3GPP 標準の Maximum-Wait-Time AVP **Maximum-Wait-Time AVP**に置き換えられます。



第 90 章

セッションマネージャにおける不均等リソース分配通知の処理

- 機能の概要と変更履歴 （1363 ページ）
- 機能説明 （1364 ページ）
- しきい値レベルと SNMP トラップの設定 （1364 ページ）
- モニタリングおよびトラブルシューティング （1366 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • GGSN • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.25

機能説明

SNMP トラップおよびアラームでは、システム全体でのセッションマネージャリソースの不均一な分配がサポートされます。アクティブなセッションマネージャのタスクにより、リソース使用量のしきい値が計算されます。サポートされている SNMP トラップとアラームにより、セッションマネージャ間でのコール数の差のモニタリングしきい値が設定されます。

この機能は、次の機能をサポートしています。

1. アラームとトラップの生成

   アラームは、最も負荷の大きいセッションマネージャと最も負荷が小さいセッションマネージャの負荷の差が、設定されているしきい値よりも大きい場合に生成されます。セッションマネージャの負荷は、セッション数によって計算されます。

2. アラームとトラップのクリア

   アラームは、最も負荷の大きいセッションマネージャと最も負荷が小さいセッションマネージャの負荷の差が、設定されているしきい値よりも小さい場合にクリアされます。セッションマネージャの負荷は、セッション数によって計算されます。

（注） しきい値の計算では、スタンバイ状態のセッション マネージャ インスタンスは考慮されません。

しきい値レベルと SNMP トラップの設定

しきい値レベルの設定

セッションマネージャのしきい値レベルを設定するには、次に示すように設定コマンドを使用します。

```
configure
   [ no ] threshold sess-uneven-dist threshold_percentage [ clear
clear_threshold_percentage [ sess-min-sessmgr-cnt number_of_sessmgr_with_least_calls
 [ sess-active number_of_min_active_session_system_wide  ]]]
   [ no ] threshold monitoring sess-uneven-dist
   threshold poll sess-uneven-dist interval interval_range
```

```
default threshold sess-uneven-dist
end
```

注：

- **threshold**：特定のしきい値ベースのアラームを設定します。
- **sess-uneven-dist** *threshold_percentage*：しきい値の数値は、最も負荷の高いセッションマネージャと最も負荷が低いセッションマネージャの間で確立されたセッションのパーセンテージの差を示します。しきい値のデフォルト値は 50% です。
- **clear** *clear_threshold_percentage*：設定されたアラームしきい値をクリアします。しきい値のデフォルト値は 50% です。
- **sess-min-sessmgr-cnt** *number_of_sessmgr_with_least_calls*：不均等なセッション分散を計算するためにモニター対象にする、最小コール回数が設定されたセッションマネージャ数を設定します。
- **sess-active** *number_of_min_active_session_system_wide*：不均等なコール分配しきい値のモニター対象にするアクティブセッション数を設定します。。デフォルト値は 10000 です。
- **monitoring sess-uneven-dist**：しきい値グループのしきい値アラートを有効または無効にします。しきい値の数値は、最も負荷の高いセッションマネージャと最も負荷が低いセッションマネージャの間で確立されたセッションのパーセンテージの差を示します。
- **poll sess-uneven-dist interval** *interval range*：しきい値のポーリング間隔を設定します。この値は、最も近い 30 秒の倍数に切り上げられます。デフォルト値は 900 です。
- **default**：指定したパラメータに割り当てられているデフォルト値を設定または復元します。

SNMP トラップの設定

セッションマネージャおよび不均等なリソース分配に関する SNMP トラップを設定するには、次の設定を使用します。

```
configure
   snmp trap [ enable | suppress ] { sessionUnevenDistribution |
sessionUnevenDistributionclear }
   end
```

注：

- **sessionUnevenDistribution**：セッションマネージャでの均等なコール分配の検出のしきい値を設定します。
- **sessionUnevenDistributionclear**：セッションマネージャでの均等なコール分散のしきい値検出をクリアします。

モニタリングおよびトラブルシューティング

ここでは、showコマンドとバルク統計を使用した、この機能のモニタリングとトラブルシューティングの方法について説明します。

コマンドと出力の表示

この項では、この機能のサポートにおけるshowコマンドまたはその出力について説明します。

show threshold コマンドを実行します。

このコマンドの出力には、次のフィールドが表示されます。

```
show threshold

Threshold operation model: ALARM

Configured thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
        Clear Threshold:  10%


Active thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
        Clear Threshold:  10%
        Poll Interval:    120Seconds
        Next Poll Time:   2021-Aug-10+17:32:00


Enabled threshold groups: (name, scope)
        sess-uneven-dist               SYSTEM

Non-default poll intervals:
        place-holder                             0Sec
        sess-uneven-dist                       120Sec

No outstanding alarm
```

show threshold all

このコマンドの出力には、次のフィールドが表示されます。

```
show threshold all

Threshold operation model: ALARM

Configured thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
```

```
        Clear Threshold:  10%


Active thresholds:

        Name:             sess-uneven-dist
        Config Scope:     SYSTEM
        Threshold:        20%
        Clear Threshold:  10%
        Poll Interval:    120Seconds
        Next Poll Time:   2021-Aug-10+17:34:00


Enabled threshold groups: (name, scope)
        sess-uneven-dist               SYSTEM

Non-default poll intervals:
        place-holder                             0Sec
        sess-uneven-dist                       120Sec

No outstanding alarm
```

show threshold default

このコマンドの出力には、次のフィールドが表示されます。

```
show threshold default
Default Thresholds:

sess-uneven-dist                      15Min     Notify Above     50%
```

show snmp trap statistics

このコマンドの出力には、次のフィールドが表示されます。

```
show snmp trap statistics
SNMP Notification Statistics:
  Total number of notifications   : 118
  Last notification sent          : Tuesday August 10 17:31:56 IST 2021
  Notification sending is         : enabled
  Notifications have never been disabled
  Notifications have never been cleared
  Notifications in current period : 2
  Notifications in previous period: 0
  Notification monitor period     : 300 seconds

Trap Name                           #Gen #Disc  Disable Last Generated
---------------------------------- ----- -----  ------- --------------------

SessionUnevenDistribution              1     0       0  2021:08:10:13:36:00
SessionUnevenDistributionClear         1     0       0  2021:08:10:15:12:00

Total number of notifications Disabled  : 92
```



第 91 章

CDR レコードのセカンダリ RAT 使用状況レポート

- 機能の概要と変更履歴 （1369 ページ）
- 機能説明 （1370 ページ）
- GTPP を介したセカンダリ RAT 使用状況レポートの設定 （1374 ページ）
- モニタリングおよびトラブルシューティング （1379 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW • S-GW
該当プラットフォーム	• ASR 5500 • VPC-DI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *GTPP Interface Administration and Reference* • *P-GW Administration Guide* • *SAEGW Administration Guide* • *S-GW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
P-GW と S-GW は、GTPP グループ設定 CLI を使用したセカンダリ RAT 使用状況レポートと CDR 処理をサポートします。	• 21.26 • 21.23.14
P-GW と S-GW は、GTPP グループ設定 CLI を使用したセカンダリ RAT 使用状況レポートと CDR 処理をサポートします。	21.20.31
最初の導入。	21.22.n7

機能説明

5G **RANSecondaryRATUsageReport** に関連するレポートの問題は、以下の不足によって発生します。

- **RANSecondaryRATUsageReport** を CDR で処理する必要があるかどうかの識別に関する制御。この制御により、S-GW、P-GW、および SAEGW は、当該レポートを SGW-CDR や PGW-CDR に含めたり、単に無視したりできます。
- 制御がアクティブな場合に、CDR 内で使用可能なレポートの数。
- ゼロボリュームレポートを CDR 内で作成する必要があるかどうかの識別に関する制御。

この結果、課金情報データが失われます。これらのレポートの問題を解決するには、GTPP グループ構成を使用して CLI 制御をトリガーし、次の手順を実行します。

- S-GW、P-GW、および SAEGW が、SGW-CDR や PGW-CDR に RANSecondary RAT 使用状況レポートを含めたり、単に無視したりできるようにします。
- SGW-CDR や PGW-CDR 内で使用可能なセカンダリ RAT 使用状況レポートの数を特定します。

（注） この制限は、システム機能に準拠する必要があるため、CDR のファイル形式を考慮する必要があります。設定された制限を超えると、適切な変更条件を使用して SGW-CDR または PGW-CDR が閉じられます。たとえば、**max-change-condition** CDR は、以降のレポートに再利用されます。

- CDR 内のゼロボリュームレポートを追加または無視します。
- CLI **gtpp limit-secondary-rat-usage** またはハードコードされた制限は削除され、CLI **gtpp limit-secondary-rat-usage** は 1 ～ 100 の範囲内のレコード数を制御するために再利用されます。

- CDR サイズが最大サイズに達したときにロギングを提供します。CDR がサイズ制限を超えた回数は、PGW-CDR カウンタでモニターできます。

動作マトリックス

次の表では、この機能の P-GW と S-GW の新しい動作について説明します。

CLI	P-GW の新しい動作	S-GW の新しい動作
gtpp attribute secondary-rat-usage デフォルトでは、このCLIコマンドはGTPPグループで有効になっています。	P-GW は、ゼロボリュームレコードを含むセカンダリ RAT 使用状況レコードをCDRで送信します。	S-GW は、ゼロボリュームレコードを含むセカンダリ RAT 使用状況レコードをCDRで送信します。
[no] gtpp attribute secondary-rat-usage	P-GW は、CDR でセカンダリ RAT 使用状況レコードを送信しません。	S-GW は、CDR でセカンダリ RAT 使用状況レコードを送信しません。
gtpp suppress-secondary-rat-usage zero-volume デフォルトでは、このCLIコマンドはGTPPグループで無効になっています。	P-GW は、CDR にゼロボリュームセカンダリ RAT レコードを含めず、送信しません。P-GW は、ゼロ以外のボリュームを含むセカンダリ RAT レコードのみを送信します。	S-GW は、CDR にゼロボリュームセカンダリ RAT レコードを含めず、送信しません。S-GW は、ゼロ以外のボリュームを含むセカンダリ RAT レコードのみを送信します。
[no] gtpp suppress-secondary-rat-usage zero-volume	P-GW は、ゼロボリュームレコードを含むセカンダリ RAT 使用状況レコードをCDRで送信します。	S-GW は、ゼロボリュームレコードを含むセカンダリ RAT 使用状況レコードをCDRで送信します。

CLI	P-GW の新しい動作	S-GW の新しい動作
gtpp limit-secondary-rat-usage *range_1–100*。設定されていない場合、デフォルト値は 32 です。デフォルトでは、この CLI コマンドは GTPP グループで有効になっています。 **例**：**gtpp limit-secondary-rat-usage 32** （注） この CLI は、1 ～ 100 の範囲を指定して既存の CLI コマンド **gtpp limit-secondary-rat-usage** を変更したものです。	P-GW は、受信したセカンダリ RAT レコードの総数が 32 を超え、報告された原因値が *maximum change condition* の場合、ただちに CDR を生成します。 受信したセカンダリ RAT レコードの合計が 32 の倍数の場合、P-GW は複数の CDR を生成します。 **例**：P-GW が 2 回のトリガーの間に 100 の RAT レコードを受信した場合、P-GW は 3 つの CDR を生成し、残りの 4 つの RAT レコードを次の CDR トリガー用に保持します。	S-GW は、受信したセカンダリ RAT レコードの総数が 32 を超え、報告された原因値が *maximum change condition* の場合、ただちに CDR を生成します。 受信したセカンダリ RAT レコードの合計が 32 の倍数の場合、S-GW は複数の CDR を生成します。 **例**：S-GW が 2 回のトリガーの間に 100 の RAT レコードを受信した場合、S-GW は 3 つの CDR を生成し、残りの 4 つの RAT レコードを次の CDR トリガー用に保持します。
例：**gtpp limit-secondary-rat-usage 40**	P-GW は、受信したセカンダリ RAT レコードの合計が 40 を超え、原因値が *maximum change condition* の場合、ただちに CDR を生成します。 受信したセカンダリ RAT レコードの合計が 40 の倍数の場合、P-GW は複数の CDR を生成します。 **例**：2 回のトリガーの間に 100 の RAT レコードを受信した場合、P-GW は 2 つの CDR を生成し、残りの 20 の RAT レコードを次の CDR トリガー用に保持します。	設定された値が 32 より大きく、すべての CDR で 32 のセカンダリ RAT レコードを送信する場合、**gtpp limit-secondary-rat-usage 40** CLI コマンドを無視します。

CLI	P-GW の新しい動作	S-GW の新しい動作
例：**gtpp limit-secondary-rat-usage 20**	P-GW は、受信したセカンダリ RAT レコードの合計が 20 を超え、原因値が *maximum change condition* の場合、ただちに CDR を生成します。 受信したセカンダリ RAT レコードの合計が 20 の倍数の場合、P-GW は複数の CDR を生成します。 **例**：P-GW が 2 回のトリガーの間に 100 の RAT レコードを受信した場合、P-GW は 2 つの CDR を生成し、残りの 20 の RAT レコードを次の CDR トリガー用に保存します。	S-GW は、受信したセカンダリ RAT レコードの合計が 20 を超え、原因値が *maximum change condition* の場合、ただちに CDR を生成します。 受信したセカンダリ RAT レコードの合計が 20 の倍数の場合、S-GW は複数の CDR を生成します。 **例**：S-GW が 2 回のトリガーの間に 100 の RAT レコードを受信した場合、5 つの CDR が生成されます。
[no] gtpp limit-secondary-rat-usage	受信したセカンダリ RAT レコードの合計が 255 を超え、原因値が *maximum change condition* の場合、ただちに CDR を生成します。 受信したセカンダリ RAT レコードの合計が 255 の倍数の場合、複数の CDR を生成します。 **例**：2 回のトリガーの間に 1,000 の RAT レコードを受信した場合、3 つの CDR が生成されます。残りの 235 の RAT レコードは、次の CDR トリガー用に保存されます。	**[no] gtpp limit-secondary-rat-usage** CLI を無視し、すべての CDR で 32 のセカンダリ RAT レコードを送信します。 この動作は **gtpp limit-secondary-rat-usage** *32* CLI の実装に似ています。 カウンタログとデバッグログは、CDR サイズの 64k を超えることはないため、必要ありません。
	サービス固有のユニット制限が **serviceConditionChange** ファイルで送信されます。	レコードクロージャ

他の機能との関係性

- 『*P-GW Administration Guide*』の「Sessmgr Restart While Processing Secondary RAT Usage CDR Records」[英語] を参照してください。

- GnGp ハンドオーバー時の Secondary RAT Usage IE、S-GW、および Gz CDR でのセカンダリ RAT データ使用状況レポートの P-GW サポートについては、『 *P-GW Administration Guide*』の「*5G Non-Standalone*」の章 [英語] を参照してください。
- Rf CDR でのセカンダリ RAT データ使用状況レポートの P-GW サポートについては、『 *P-GW Administration Guide*』の「*5G Non-Standalone*」の章 [英語] を参照してください。

制限事項

この機能には、次の制限事項があります。

- S-GW では、セッションリカバリ時およびチェックポインティング時に、ベアラーごとに最大 16 のセカンダリ RAT レコードを設定できます。
- P-GW では、セッションリカバリ時およびチェックポインティング時に、すべてのベアラーに渡り最大 142 のセカンダリ RAT レコードを設定できます。
- 最大数を超えた場合、セッションリカバリ中にレコードが失われます。

GTPP を介したセカンダリ RAT 使用状況レポートの設定

バッファサイズを超える前にセカンダリ RAT 使用状況の CDR レコードを閉じるには、次の GTPP 設定を使用します。

セカンダリ RAT 使用状況レポートの有効化または無効化

セカンダリ RAT 使用状況レポートを有効または無効にするには、次の設定を使用します。

```
configure
  context context_name
    gtpp group group_name
      gtpp attribute secondary-rat-usage
      default gtpp attribute secondary-rat-usage
      no gtpp attribute secondary-rat-usage
      end
```

注：

- **gtpp attribute secondary-rat-usage**：オプション属性のセカンダリ RAT 使用状況レコードを送信します。
- **default gtpp attribute secondary-rat-usage**：デフォルトで、オプション属性のセカンダリ RAT 使用状況レコードを送信します。
- **no gtpp attribute secondary-rat-usage**：オプション属性のセカンダリ RAT 使用状況レコードを送信しません。

エントリの最大数の制御

セカンダリ RAT の使用状況レコードが CDR 内で設定されている最大値に達すると、CDR 終了原因が発生し、**maxChangeCond** を使用します。**gtpp limit-secondary-RAT-usage** CLI コマンドは、P-GW および S-GW CDR のセカンダリ RAT 使用状況レコードエントリの最大数を制御します。32 を超える制限値が設定されている場合、S-GW CDR で部分的な CDR が最大 32 個生成されます。

（注） S-GW の既存の動作には、32 のセカンダリ RAT 使用状況レコードの制限があります。

次の表では、セカンダリ RAT レコードと CDR の動作、および上限数について説明します。

シリアル番号	CDR タイプ	設定された limit-secondary-rat-usage	有効な上限数	UE によって送られるセカンダリ RAT レコード数	セカンダリ RAT レコードと CDR の動作
1	P-GW	32 未満 例：20	20	35	部分的な CDR が 20 個のセカンダリ RAT レコードで生成されます。
					残りの 15 個のセカンダリ RAT レコードは次のトリガーで送信されます。
	S-GW	32 未満 例：20	20	35	部分的な CDR が 20 個のセカンダリ RAT レコードで生成されます。
					残りの 15 個のセカンダリ RAT レコードは次のトリガーで送信されます。

シリアル番号	CDR タイプ	設定された limit-secondary-rat-usage	有効な上限数	UE によって送られるセカンダリ RAT レコード数	セカンダリ RAT レコードと CDR の動作
2	P-GW	32	32	35	部分的な CDR が 32 個のセカンダリ RAT レコードで生成されます。
					残りの 3 個のセカンダリ RAT レコードは次のトリガーで送信されます。
	S-GW	32	32	35	部分的な CDR が 32 個のセカンダリ RAT レコードで生成されます。
					残りの 3 個のセカンダリ RAT レコードは次のトリガーで送信されます。

シリアル番号	CDR タイプ	設定された limit-secondary-rat-usage	有効な上限数	UE によって送られるセカンダリ RAT レコード数	セカンダリ RAT レコードと CDR の動作
3	P-GW	32 超 例：100	100	100	部分的な CDR が 100 個のセカンダリ RAT レコードで生成されます。
	S-GW	32 超 例：100	32	100	それぞれ 32 個のセカンダリ RAT レコードを含む 3 つの部分的な CDR が生成されます。
					残りの 4 個のセカンダリ RAT レコードは次のトリガーで送信されます。

シリアル番号	CDR タイプ	設定された limit-secondary-rat-usage	有効な上限数	UE によって送られるセカンダリ RAT レコード数	セカンダリ RAT レコードと CDR の動作
4	P-GW	設定なし	255	1000	それぞれ 255 個のセカンダリ RAT レコードを含む 3 つの部分的な CDR が生成されます。
					報告された残りのセカンダリ RAT レコードは、次のトリガーで CDR の一部になります。
	S-GW	設定なし	32	1000	部分的な CDR は生成されません。
					32 個のセカンダリ RAT レコードは、次のトリガーで CDR の一部になります。

エントリの上限数を制御するには、次の設定を使用します。

```
configure
   context context_name
      gtpp group group_name
         gtpp limit-secondary-rat-usage usage_limit
         default gtpp limit-secondary-rat-usage
         no gtpp limit-secondary-rat-usage
         end
```

注：

- **gtpp limit-secondary-rat-usage** *usage_limit*：セカンダリ RAT レポートの最大数を入力します。 *usage_limit* は、1 ～ 100 の範囲の整数にする必要があります。S-GW CDR の推奨値は 32 です。

たとえば、上限が 10 に設定されている場合、設定された値に達すると CDR が生成されます。

- **default gtpp limit-secondary-rat-usage**：32 のデフォルト値を指定します。
- **no gtpp limit-secondary-rat-usage**：限られた数のセカンダリ RAT 使用状況情報の CDR 生成を無効にします。

ゼロボリュームのセカンダリ RAT 使用状況レポートの抑制

ゼロボリュームのセカンダリ RAT 使用状況レポートを抑制するには、次の設定を使用します。

```
configure
  context context_name
    gtpp group group_name
      gtpp suppress-secondary-rat-usage zero-volume
      default gtpp suppress-secondary-rat-usage zero-volume
      no gtpp suppress-secondary-rat-usage zero-volume
      end
```

注：

- **gtpp suppress-secondary-rat-usage zero-volume**：セカンダリ RAT レコードまたはゼロボリュームのセカンダリ RAT レコードを抑制します。
- **default gtpp suppress-secondary-rat-usage zero-volume**：ゼロボリュームのセカンダリ RAT 使用状況レコードを抑制しません。
- **no gtpp suppress-secondary-rat-usage zero-volume**：ゼロボリュームのセカンダリ RAT 使用状況レコードを抑制しません。

モニタリングおよびトラブルシューティング

ここでは、この機能をサポートする show コマンドを使ったモニタリングと障害対応の方法について説明します。

コマンドと出力の表示

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show config

この CLI コマンドの出力には、次のパラメータが表示されます。

フィールド	説明
gtpp attribute secondary-rat-usage	CDR に [Secondary RAT reports] フィールドを含めるには、このオプションを指定します。

フィールド	説明
gtpp suppress-secondary-rat-usage zero-volume	ボリュームが 0 のセカンダリ RAT レポートの CDR からの除外を有効にします。
gtpp limit-secondary-rat-usage	設定された値による、CDR のセカンダリ RAT 使用状況レポート数の制限を有効にします。

show config verbose

この CLI コマンドの出力には、次のパラメータが表示されます。

フィールド	説明
gtpp attribute secondary-rat-usage	セカンダリ RAT 使用状況レコードが表示されます。
gtpp suppress-secondary-rat-usage zero-volume	P-GW および S-GW からのゼロ以外のボリュームを含むセカンダリ RAT レコードのみ表示されます。
gtpp limit-secondary-rat-usage	受信したセカンダリ RAT レコードの合計が 10 の倍数である場合、P-GW および S-GW によって生成された複数の CDR が表示されます。報告された原因値は、maximum change condition になります。
no gtpp limit-secondary-rat-usage	未設定の原因に関するセカンダリ RAT レコードが表示されます。

show gtpp group

この CLI コマンドの出力には、次のパラメータが表示されます。

フィールド	説明
Secondary RAT records present	セカンダリ RAT レコードが存在するかどうかを指定します。次のオプションを使用できます。 • なし • あり
Limit-secondary-rat-usage	セカンダリ RAT 使用状況レポートの制限を指定します。

show gtpp statistics group

この CLI コマンドの出力には、次のパラメータが表示されます。

フィールド	説明
Total PGW-CDR exceed size limit	P-GW のサイズ制限を超えた CDR の総数を表示します。



第 92 章

2G、3G、4G バルク統計の分離

ここでは、次の内容について説明します。

- 機能の概要と変更履歴 （1383 ページ）
- 機能説明 （1384 ページ）
- 統計プロファイルでの RAT タイプの設定 （1384 ページ）
- モニタリングおよびトラブルシューティング （1385 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• GGSN • P-GW • SAEGW
該当プラットフォーム	すべて（All）
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.5

機能説明

重要　このリリースでは、この機能は完全には機能しておらず、テスト目的でのみ使用できます。詳細については、シスコのアカウント担当者にお問い合わせください。

この機能は、バルク統計を RAT タイプ（2G、3G、および 4G）で分割します。これは、RAT タイプごとの KPI のモニタリングとレポートに役立ちます。APN タイプ、RAT タイプごとの統計は、既存の stats-profile の実装と統合されています。stats-profile に RAT-types を設定するために、新しい CLI コマンド **rat-type** が **stats- profile** コンフィギュレーション モードに追加されました。

統計プロファイルでの RAT タイプの設定

新しい CLI コマンド **rat-type** が **統計プロファイル** コンフィギュレーション モードに追加されました。この CLI コマンドにより、APN ごとの RAT タイプごとの統計が既存の統計プロファイルの実装と統合されます。RAT レベルの統計を収集するには、RAT レベルの統計が必要な統計プロファイルで RAT タイプを設定する必要があります。それが完了したら、RAT レベルごとの統計が必要な APN の統計プロファイルを関連付けます。この関連付けの後にのみ、統計が収集されます。統計プロファイルの関連付けが APN から削除されたり、RAT タイプオプションが統計プロファイルから削除されると、APN ごとの RAT レベルごとの統計が失われます。

APN ごとの RAT タイプごとの統計収集を有効にするには、次のコマンドを実行します。

```
configure
    stats-profile <stats_profile_name>
      [no] rat-type { [geran | utran | eutran]* }
      end
```

注：

- **no**：RAT タイプに基づいた統計収集を無効にします。
- **stats-profile**：パケットドロップカウンタや ARP レベルの統計を収集するように統計プロファイルを設定します。
- **rate-type**：RAT レベルの統計の収集を設定します。

- **geran**：RAT タイプ GERAN の統計の収集を設定します。
- **utran**：RAT タイプ UTRAN の統計の収集を設定します。
- **eutran**：RAT タイプ EUTRAN の統計の収集を設定します。

設定例

RAT タイプに基づいた統計収集を有効にする設定例：

```
config
   stats-profile stats-info
      rat-type eutran utran
      rat-type utran geran
      end
```

RAT タイプに基づいて統計情報収集を無効にする設定例：

```
config
   stats-profile stats-info
      no rat-type eutran utran
      end
```

モニタリングおよびトラブルシューティング

このセクションでは、2G/3G/4G バルク統計の分離をサポートするために使用できる show コマンドについて説明します。

コマンドと出力の表示

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show apn statistics all

上記のコマンドの出力が変更され、CLI コマンドが有効か無効かに応じて、次の新しいフィールドが表示されるようになりました。

- データ統計：
  - アップリンクとダウンリンクバイトの RAT タイプ統計：
    - GERAN
      - Uplnk DataBytes
      - Dnlnk DataBytes
    - UTRAN
      - Uplnk DataBytes

- Dnlnk DataBytes

- EUTRAN
  - Uplnk DataBytes
  - Dnlnk DataBytes

- IP アドレス割り当ての統計
  - PDN タイプ IPv4、IPv6、IPv4v6 の動的アドレス割り当てに関する RAT タイプ統計：
    - 割り当てられた GERAN ダイナミックアドレス：
      - IPv4
      - IPv6
      - IPv4v6
    - 割り当てられた UTRAN ダイナミックアドレス：
      - IPv4
      - IPv6
      - IPv4v6

show gtpc statistics

上記のコマンドの出力が変更され、次の新しいフィールドが表示されるようになりました。これらのフィールドは、stats-profile の設定に依存しません。gtpc stats は、次の RAT タイプで設定された stats profile に関係なく増加します。

- Total CPC Req GERAN
- Total CPC Req UTRAN

show stats profile all

上記のコマンドの出力が変更され、CLI が有効か無効かに応じて、次の新しいフィールドが表示されるようになりました。

- rat-type geran utran eutran

バルク統計

次のバルク統計が APN スキーマに追加され、2G、3G、4G バルク統計の分離機能をサポートするようになりました。

バルク統計	説明
att-pdp-ctxt-geran	RAT タイプが GERAN のコールで、APN ごとに受信した CPC 要求の総数を示します。
att-pdp-ctxt-utran	RAT タイプが UTRAN のコールで、APN ごとに受信した CPC 要求の総数を示します。
dyn-ipv4-success-geran	GERAN RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv4 コンテキストの合計数を示します。
dyn-ipv4-success-utran	UTRAN RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv4 コンテキストの合計数を示します。
dyn-ipv6-success-geran	GERAN RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv6 コンテキストの合計数を示します。
dyn-ipv6-success-utran	UTRAN RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv6 コンテキストの合計数を示します。
dyn-ipv4v6-success-geran	GERAN RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv4v6 コンテキストの合計数を示します。
dyn-ipv4v6-success-utran	UTRAN RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv4v6 コンテキストの合計数を示します。
uplnk-bytes-geran	GERAN RAT タイプの APN から Gi インターフェイス上のインターネット/PDN に送信された合計バイト数を示します。
dnlnk-bytes-geran	APN の Gi インターフェイスで受信した GERAN RAT タイプの合計バイト数を示します。
uplnk-bytes-utran	UTRAN RAT タイプの APN から Gi インターフェイス上のインターネット/PDN に送信された合計バイト数を示します。
dnlnk-bytes-utran	APN の Gi インターフェイスで受信した UTRAN RAT タイプの合計バイト数を示します。

バルク統計	説明
uplnk-bytes-eutran	EUTRAN RAT タイプの APN から Gi インターフェイス上のインターネット/PDN に送信された合計バイト数を示します。
dnlnk-bytes-eutran	APN の Gi インターフェイスで受信した EUTRAN RAT タイプの合計バイト数を示します。



第 93 章

テザリング検出バイパスインターフェイス ID

- 機能の概要と変更履歴 （1389 ページ）
- 機能説明 （1390 ページ）
- tethering-detection bypass interface-id の設定 （1390 ページ）
- モニタリングおよびトラブルシューティング （1391 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*Command Line Interface Reference*

マニュアルの変更履歴

改訂の詳細	リリース
テザリング検出バイパスメカニズムは、複数のインターフェイスをサポートするよう拡張されています。	21.24.2

機能説明

P-GW では、テザリング検出機能により CLI を介して最大 10 のインターフェイス ID がサポートされ、サブスクライバをテザリングルールからバイパスできます。テザリングされたデータフローが設定済みの IPv6 インターフェイス ID とともに着信する場合、P-GW はテザリングからそのデータをバイパスします。P-GW では、テザリング検出バイパスリストからすべてまたは複数のインターフェイス ID を削除することもできます。

tethering-detection bypass interface-id の設定

複数のインターフェイス ID を追加、除外、または削除するには、次の設定を使用します。

```
configure
  active-charging-service service_name
    [ no ] tethering-detection {  bypass interface-id ipv6 ifid | tac-db
 bypass interface-id ipv6 ifid  }
    default tethering-detection
    exit
  exit
```

注：

- **tethering-detection { bypass interface-id** *ipv6 ifid* **}**：複数のインターフェイス ID を設定します。最大 10 のインターフェイス ID を設定できます。

  複数のインターフェイス ID の例：`tethering-detection bypass interface-id 00-00-00-05-47-00-37-44 00-00-00-05-47-00-37-45 00-00-00-05-47-00-37-46 00-00-00-05-47-00-37-4700-00-00-05-47-00-37-48 00-00-00-05-47-00-37-49 00-00-00-05-47-00-37-50 00-00-00-05-47-00-37-51 00-00-00-05-47-00-37-52 00-00-00-05-47-00-37-53`

- **default tethering-detection**：インターフェイス設定をすべて削除します。
- **no tethering-detection bypass interface-id** *if-id1 if-idn*：指定された *if-id1* および *if-idn* インターフェイスが設定されている場合は、削除します。

  インターフェイス ID が存在しない場合は、設定されたすべてのインターフェイス ID が削除されます。

- **tac-db bypass interface-id** *ipv6 ifid*：指定されたインターフェイス ID の TAC-db ルックアップを有効にします。

設定の確認

テザリング検出バイパスインターフェイス ID の設定を確認するには、次のコマンドを使用します。

- **show configuration**
- **show configuration verbose**

設定を確認するためのコマンド例を以下に示します。

```
configure
  active-charging-service service_name
    tethering-detection { bypass interface-id  ipv6 ifid  }
    exit
  exit
```

モニタリングおよびトラブルシューティング

ここでは、テザリング検出機能に使用できるshowコマンドに関する情報について説明します。

show コマンドと出力

この項では、テザリング検出属性の現在の設定を表示する show コマンドと出力について説明します。

show active-charging-tethering-detection statistics

このコマンドの出力には、次のフィールドが含まれています。

- **Total flows bypassed for scanning**：設定されたインターフェイス ID でフローがバイパスされると、Total flow bypassed for scanning カウンタの値が増えます。



第 94 章

2G 3G 4G WLAN バルク統計の分離

- 機能の概要と変更履歴 （1393 ページ）
- 機能説明 （1394 ページ）
- **統計プロファイルでの RAT タイプの設定** （1394 ページ）
- モニタリングおよびトラブルシューティング （1395 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• GGSN • P-GW • SAEGW
該当プラットフォーム	すべて（All）
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、2G 3G 4G WLAN バルク統計の分離が導入されました。	21.23
最初の導入。	21.5

機能説明

一部の契約上の重要業績評価指標（KPI）は、無線アクセス技術（RAT）タイプ（2G、3G、4G）ごとのレポートを必要とする操作によってモニターされます。現在導入されているいくつかのバルク統計カウンタは、RAT タイプを分離していません。APN RAT タイプごとの統計を有効または無効にするために、新しく導入された RAT タイプは「gtpv2-s2a」と「gtpv2-s2b」です。これらのタイプによって RAT の分離（2G、3G、4G、WLAN）が実現します。

この分離により、運用チームは RAT タイプごとの使用状況を個別に報告できるようになり、ネットワーク問題の検出に使用されるトラブルシューティング ツールを強化できます。

統計プロファイルでの RAT タイプの設定

設定コマンド gtpv2-s2a および gtpv2-s2b が統計プロファイル コンフィギュレーション モードに追加されました。この機能は、APN ごとに、RAT タイプごと（2G、3G、4G、gtpv2-s2a、gtpv2-s2b）の統計を既存の統計プロファイルの実装と統合します。

APN ごとの RAT タイプごとの統計収集を有効にするには、次のコマンドを実行します。

```
configure
  stats-profile stats_profile_name
    [ no ]  rat-type { gtpv2-s2a | gtpv2-s2b }
  end
```

stats-profile を APN に関連付けると、統計が収集されます。これには、RAT レベルごとの APN の統計が必要です。

stats-profile の関連付けが APN から削除され、RAT タイプオプションが stats-profile から削除されると、APN ごとの RAT レベルごとの統計が失われます。

stats-profile を APN に関連付けるには、次のコマンドを実行します。

```
configure
  context context_name
    apn apn_name
      stats-profile stats_profile_name
  end
```

注：

- **stats-profile** ：パケットドロップカウンタや ARP レベルの統計を収集するように統計プロファイルを設定します。
- **rat-type** RAT レベルの統計の収集を設定します。
- **gtpv2-s2a** RAT タイプ WLAN S2A の統計の収集を設定します。
- **gtpv2-s2b** RAT タイプ WLAN S2B の統計の収集を設定します。

モニタリングおよびトラブルシューティング

ここでは、2G、3G、4G、WLAN バルク統計の分離をサポートするために使用できる show コマンドとバルク統計について説明します。

show コマンドと出力

show stats-profile all

このコマンドの出力には、次のように RAT タイプ gtpv2-S2A および gtpv2-S2B について収集された統計情報が表示されます。

- 統計プロファイル名
- RAT タイプ
- gtpv2-s2a
- gtpv2-s2b

show apn statistics all

このコマンドの出力には、動的アドレス割り当て、gtpv2-s2a および gtpv2-s2b のアップリンクとダウンリンクの統計情報が次のように表示されます。

- データ統計
  - gtpv2-s2a
    - Uplnk Bytes
    - Dnlnk Bytes
  - gtpv2-s2b
    - Uplnk Bytes
    - Dnlnk Bytes
- RAT タイプの統計

- gtpv2-s2a
  - Ipv4
  - Ipv6
  - Ipv4v6
- gtpv2-s2b
  - Ipv4
  - Ipv6
  - Ipv4v6

show gtpc statistics

このコマンドの出力には、GERAN および UTRAN の更新された PDP コンテキストの送受信の統計情報が表示されます。

- トンネル管理メッセージ
  - Total GERAN Accepted
  - Total UTRAN Accepted
  - GERAN UPC RX
  - Accepted



（注） 上記の Accepted カウンタは、GERAN UPC RX 用です。

  - UTRAN UPC RX
  - Accepted



（注） 上記の Accepted カウンタは、UTRAN UPC RX 用です。

  - GERAN UPC TX
  - Accepted



（注） 上記の Accepted カウンタは、GERAN UPC TX 用です。

  - UTRAN UPC TX
  - Accepted

（注） 上記の Accepted カウンタは、UTRAN UPC TX 用です。

show gtpc statistics apn <apn_name> verbose

このコマンドの出力には、GERAN および UTRAN の pdp コンテキスト統計作成 RAT タイプの統計が表示されます。

- トンネル管理メッセージ
  - Total GERAN Accepted
  - Total UTRAN Accepted
  - GERAN UPC RX
  - Accepted

（注） 上記の Accepted カウンタは、GERAN UPC RX 用です。

  - UTRAN UPC RX
  - Accepted

（注） 上記の Accepted カウンタは、UTRAN UPC RX 用です。

  - GERAN UPC TX
  - Accepted

（注） 上記の Accepted カウンタは、GERAN UPC TX 用です。

  - UTRAN UPC TX
  - Accepted

（注） 上記の Accepted カウンタは、UTRAN UPC TX 用です。

  - GERAN PDP Context Denied
    - No Resources
    - メモリ

- All Dyn Addr Occupied
- User Auth Failed
- Unknown Missing/APN
- システム障害
- Service Not Supported
- No APN Subscription

- UTRAN PDP Context Denied
  - No Resources
  - メモリ
  - All Dyn Addr Occupied
  - User Auth Failed
  - Unknown Missing/APN
  - システム障害
  - Service Not Supported
  - No APN Subscription

show gtpc statistics apn <apn_name> verbose

このコマンドの出力には、GERAN および UTRAN の更新された PDP コンテキストの送受信の統計情報が表示されます。

- トンネル管理メッセージ
  - Total GERAN Accepted
  - Total UTRAN Accepted
  - GERAN UPC RX
  - Accepted



（注） 上記の Accepted カウンタは、GERAN UPC RX 用です。

  - UTRAN UPC RX
  - Accepted



（注） 上記の Accepted カウンタは、UTRAN UPC RX 用です。

- GERAN UPC TX
- Accepted

（注） 上記の Accepted カウンタは、GERAN UPC TX 用です。

- UTRAN UPC TX
- Accepted

（注） 上記の Accepted カウンタは、UTRAN UPC TX 用です。

バルク統計

APN スキーマ

次のバルク統計が APN スキーマに追加され、2G、3G、4G、WLAN バルク統計の分離機能をサポートするようになりました。

バルク統計	説明
uplnk-bytes-gtpv2-s2a	GTPV2 ベース S2A RAT タイプの APN から Gi インターフェイス上のインターネット/PDN に送信された合計バイト数を示します。
dnlnk-bytes-gtpv2-s2a	APN の Gi インターフェイスで受信した GTPV2 ベース S2A RAT タイプの合計バイト数を示します。
uplnk-bytes-gtpv2-s2b	GTPV2 ベース S2B RAT タイプの APN から Gi インターフェイス上のインターネット/PDN に送信された合計バイト数を示します。
dnlnk-bytes-gtpv2-s2b	APN の Gi インターフェイスで受信した GTPV2 ベース S2B RAT タイプの合計バイト数を示します。
dyn-ipv4-success-eutran	EUTRAN RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv4 コンテキストの合計数を示します。

dyn-ipv4-success-gtpv2-s2a	GTPV2 ベース S2A RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv4 コンテキストの合計数を示します。
dyn-ipv4-success-gtpv2-s2b	GTPV2 ベース S2B RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv4 コンテキストの合計数を示します。
dyn-ipv6-success-eutran	EUTRAN RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv6 コンテキストの合計数を示します。
dyn-ipv6-success-gtpv2-s2a	GTPV2 ベース S2A RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv6 コンテキストの合計数を示します。
dyn-ipv6-success-gtpv2-s2b	GTPV2 ベース S2B RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv6 コンテキストの合計数を示します。
dyn-ipv4v6-success-eutran	EUTRAN RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv4v6 コンテキストの合計数を示します。
dyn-ipv4v6-success-gtpv2-s2a	GTPV2 ベース S2A RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv4v6 コンテキストの合計数を示します。
dyn-ipv4v6-success-gtpv2-s2b	GTPV2 ベース S2B RAT タイプに正常に設定され、動的に割り当てられた IP アドレスを要求する IPv4v6 コンテキストの合計数を示します。
upc-rx-geran	APN ごとの、GERAN RAT タイプで SGSN から受信した PDP コンテキスト更新要求メッセージの合計数を示します。
upc-tx-geran	APN ごとの、GERAN RAT タイプで SGSN に送信された PDP コンテキスト更新要求メッセージの合計数を示します。

upc-rx-accept-geran	APN ごとの、GERAN RAT タイプで SGSN から受信した、原因値128（80H、要求が承認された）を含む PDP コンテキスト更新要求メッセージの合計数を示します。
upc-tx-accept-geran	APN ごとの、GERAN RAT タイプで SGSN に送信された、原因値128（80H、要求が承認された）を含む PDP コンテキスト更新要求メッセージの合計数を示します。
upc-rx-utran	APN ごとの、UTRAN RAT タイプで SGSN から受信した PDP コンテキスト更新要求メッセージの合計数を示します。
upc-tx-utran	APN ごとの、UTRAN RAT タイプで SGSN に送信された PDP コンテキスト更新要求メッセージの合計数を示します。
upc-rx-accept-utran	APN ごとの、UTRAN RAT タイプで SGSN から受信した、原因値128（80H、要求が承認された）を含む PDP コンテキスト更新要求メッセージの合計数を示します。
upc-tx-accept-utran	APN ごとの、UTRAN RAT タイプで SGSN に送信された、原因値128（80H、要求が承認された）を含む PDP コンテキスト更新要求メッセージの合計数を示します。
cpc-accept-geran	APN ごとの、GERAN RAT タイプで送信された、原因値128（80H、要求が承認された）を含む PDP コンテキスト作成要求メッセージの合計数を示します。
cpc-accept-utran	APN ごとの、UTRAN RAT タイプで送信された、原因値128（80H、要求が承認された）を含む PDP コンテキスト作成要求メッセージの合計数を示します。
cpc-nomem-geran	APN ごとの、GERAN RAT タイプで SGSN に送信された、原因コード212（D4H、使用可能なメモリなし）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-nomem-utran	APN ごとの、UTRAN RAT タイプで SGSN に送信された、原因コード212（D4H、使用可能なメモリなし）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。

cpc-noresource-geran	APN ごとの、GERAN RAT タイプで SGSN に送信された、原因コード199（C7H、使用可能なリソースなし）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-noresource-utran	APN ごとの、UTRAN RAT タイプで SGSN に送信された、原因コード199（C7H、使用可能なリソースなし）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-srv-not-supp-geran	APN ごとの、GERAN RAT タイプで SGSN に送信された、原因コード200（C8H、サービスがサポートされていない）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-srv-not-supp-utran	APN ごとの、UTRAN RAT タイプで SGSN に送信された、原因コード200（C8H、サービスがサポートされていない）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-sys-fail-geran	APN ごとの、GERAN RAT タイプで SGSN に送信された、原因コード 204（CCH、システム障害）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-sys-fail-utran	APN ごとの、UTRAN RAT タイプで SGSN に送信された、原因コード 204（CCH、システム障害）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-auth-fail-geran	APN ごとの、GERAN RAT タイプで SGSN に送信された、原因コード 209 を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-auth-fail-utran	APN ごとの、UTRAN RAT タイプで SGSN に送信された、原因コード 209 を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-no-apn-subscription-geran	APN サブスクリプションがなかったことを原因とする、APN ごとの、GERAN RAT タイプで SGSN に送信された PDP コンテキスト作成拒否応答メッセージの合計数を示します。

cpc-no-apn-subscription-utran	APN サブスクリプションがなかったことを原因とする、APN ごとの、UTRAN RAT タイプで SGSN に送信された PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-missing-apn-geran	APN ごとの、GERAN RAT タイプで SGSN に送信された、原因コード 219（DBH、APN の欠落または不明な APN）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-missing-apn-utran	APN ごとの、UTRAN RAT タイプで SGSN に送信された、原因コード 219（DBH、APN の欠落または不明な APN）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-addr-occupied-geran	APN ごとの、GERAN RAT タイプで SGSN に送信された、原因コード 211（D3H、すべての動的 PDP アドレスが使用中）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。
cpc-addr-occupied-utran	APN ごとの、UTRAN RAT タイプで SGSN に送信された、原因コード 211（D3H、すべての動的 PDP アドレスが使用中）を含む PDP コンテキスト作成拒否応答メッセージの合計数を示します。



第 95 章

セッションのトレース

この章では、サブスクライバ セッション トレース機能について説明します。この機能を使用すると、ネットワーク内のさまざまなポイントでのサブスクライバのアクティビティを、通信事業者がさまざまな詳細レベルで追跡できます。サブスクライバ セッション トレースは、次の UMTS/EPC GW ネットワーク要素でサポートされています。

- GGSN
- P-GW
- SAEGW
- S-GW

重要 MME でのセッショントレースの詳細については、『*MME Administration Guide*』を参照してください。

製品アドミニストレーションガイドには、システム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、それぞれの製品のアドミニストレーションガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

この章では、機能の説明、設定手順、モニタリングコマンド、およびセッショントレースファイルの例を提供します。

- セッショントレースの概要 （1405 ページ）
- セッショントレース機能の設定 （1410 ページ）
- セッショントレース機能のモニタリング （1422 ページ）
- サポートされている SAEGW セッショントレースの設定 （1423 ページ）
- セッショントレースファイルの例 （1427 ページ）

セッショントレースの概要

セッショントレース機能を使用すると、ネットワーク内のさまざまなポイントでのサブスクライバのアクティビティを、通信事業者がさまざまな詳細レベルで追跡できます。トレースは、サブスクライバが開始する（つまり、シグナリングベース）か、管理者がCLI（コマンドライ

ン インターフェイス）から開始することができ、UMTS/EPC ネットワーク要素で使用可能なさまざまなシグナリング インターフェイスを介してアクセスクラウド全体に伝達できます。

基本的に、セッショントレース機能は、モニター対象インターフェイスでのモニター対象サブスクライバの制御アクティビティをすべて記録および転送します。これは、通常、ユーザー機器（UE）がアクセスネットワークに接続するときに送信されるすべてのシグナリングおよび認証/サブスクライバ サービス メッセージです。

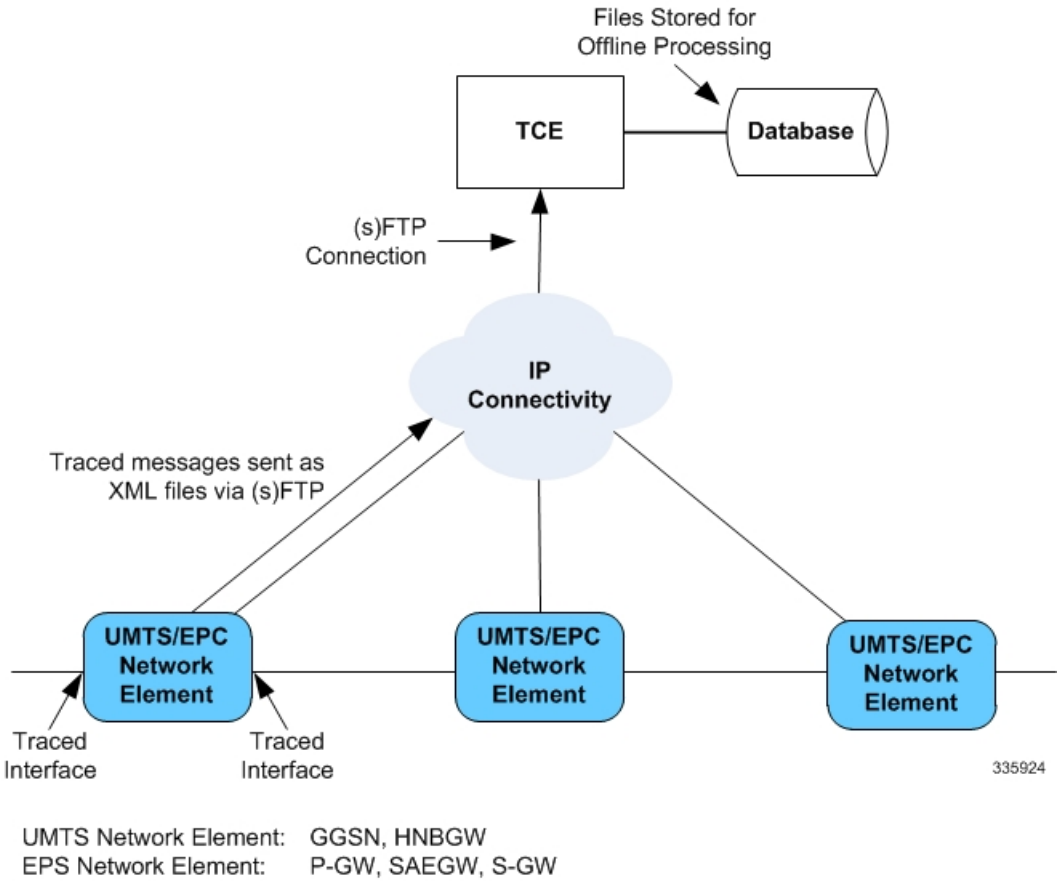
モニター対象のすべてのアクティビティは、File Transfer Protocol（FTP）またはセキュア FTP（sFTP）接続を介して、標準ベースの XML 形式でオフラインのトレース収集エンティティ（TCE）に送信されます。

重要 セッショントレースは、CPU 使用率の点でリソースを大量に消費するアプリケーションであり、使用時にはコールレートおよびデータスループットに影響します。既存のサービスへの影響を最小限に抑えるために、実稼働ネットワークでのこの機能の使用を制限する必要があります。

重要 セッショントレース機能では、SFTP オプションのみがサポートされます。FTP は、セッショントレース機能ではサポートされていません。

次の図に示すように、示されている 3 つのネットワーク要素（NE）のうち、1 つの NE が 1 つまたは複数のインターフェイス上のデータをアクティブにトレースしています。収集されたすべてのデータは、XML 形式のファイルとして保存され、（S）FTP または FTP を使用して収集エンティティに転送されます。ファイルを転送するには、NE と TCE の間に IPv4 または IPv6 接続が必要であることに注意してください。

図 *114* : セッショントレースのアーキテクチャ



セッショントレースのタイプ

3 種類のセッショントレース機能を使用できます。

- **管理トレース**：通信事業者は、CLI を介して、トレースを開始する UMTS/EPC ネットワーク要素にアクティブ化要求を直接送信します。ネットワーク要素が、トレースセッションを確立し、設定されたトリガーイベントによってアクティブトレースが開始されるのを待ちます。管理者によって開始されるトレースアクティブ化がネットワーク要素で実行された場合、コールの実際の録音に関与しているかどうかにかかわらず、それらが他の NE に伝達されることはありません。
- **ランダムトレース**：UMTS/EPC ネットワーク要素のランダムトレースに基づいて、サブスクライバセッションのトレース機能を有効または無効にします。トレース制御および設定パラメータは、**random trace** CLI コマンドを使用して、指定されたネットワーク要素で直接設定されます。ランダムベースのトレースのアクティブ化では、トレースパラメータは伝達されません。この NE は、コールの実際の録音に関与しているかどうかにかかわらず、受信したデータを他の NE に伝達しません。有効にすると、指定された UMTS/EPC ネットワーク要素にあるセッションのすべてのインスタンスについて、サブスクライバ選択がランダムロジックに基づいて実行されます。

- **シグナリングトレース**：シグナリングベースのアクティブ化により、トレースセッションは、トレース呼び出しメッセージを介してシグナリング インターフェイスを介して UMTS/EPC ネットワーク要素に示されます。このメッセージは、既存のベアラー セットアップ メッセージを使用（すべての制御メッセージをトレースする場合）するか、別のトレース呼び出しメッセージを送信（ユーザーがすでにアクティブである場合）することにより、ピギーバックできます。シグナリングベースのアクティブ化は、現在の NE がトレースに参加しない場合でも（設定によって有効になっていないか、設定されたトレースパラメータに存在しない場合）、常に隣接 NE に伝達されます。



重要 一意の International Mobile Subscriber Identification（IMSI）番号または International Mobile Equipment Identification（IMEI）番号の最大数は 32 を超えることができないことに注意してください。ただし、各 NE は 32 の一意の IMSI/IMEI をすべてトレースできます。



注意 セッショントレースは、CPU 使用率の点でリソースを大量に消費するアプリケーションであり、使用時にはコールレートおよびデータスループットに影響します。既存のサービスへの影響を最小限に抑えるために、実稼働ネットワークでのこの機能の使用を制限する必要があります。

セッショントレースのアクティブ化

トレースのアクティブ化は、管理インターフェイスとシグナリングインターフェイスのいずれを使用しても同様です。どちらの場合も、トレースセッションのすべての設定と状態情報を格納するトレース セッション状態ブロックが割り当てられます。さらに、トレース コレクション エンティティ（TCE）への(S)FTP接続がまだ存在しない場合は確立されます。NEは、(S)FTP接続を確立して TCE との間でファイルをプッシュまたはプルできるように、ローカルディスクに最大 2 MB の XML データを保存します。

トレース対象セッションがすでにアクティブである場合、トレースがすぐに開始されます。それ以外の場合は、開始トリガーが発生するまでトレースアクティビティは待機します（通常は、トレース対象のサブスクライバまたは UE が接続を開始した時点）。トレースのアクティブ化が（最大数を超えたか、その他の失敗理由のため）失敗した場合、失敗を示す通知がTCEに送信されます。

セッショントレースの非アクティブ化

セッションのトレースの非アクティブ化は、管理によってアクティブ化された場合もシグナリングによってアクティブ化された場合も同様です。いずれの場合も、有効なトレース参照を含む非アクティブ化要求を NE が受信すると、トレースセッション状態ブロックの割り当てが解除され、保留中のトレースデータがフラッシュされます。さらに、これが特定の TCE への最後のトレースセッションである場合、最後のトレースファイルが TCE に正常に転送された後に、TCE への（S）FTP 接続がリリースされます。

Data Collection

データ収集は、各 NE によってインラインで行われます。制御パケット単位でのオーバーヘッド低減のために、パケット全体のコピーが作成され、パケットの内部データベース（DB）に格納されます。

トレースデータベースのローカル内部パスは **/hd-raid/trace** です。

この格納は、トレースの深さに関係なく行われます。xx バイト（または xx 個のメッセージ）が格納された後、または設定可能な秒数が経過した後、キャッシュされたすべてのデータは標準の XML 形式にエンコードされ、TCE に転送するファイルまたは TCE からプルするファイルに書き出されます。アクティブな TCE がない場合、UMTS/EPC ネットワーク要素は、使用可能なスペースがある限りデータをキャッシュし続け、トレースファイルを作成します。スペースがなくなると、トレース記録セッションが停止します。TCE への接続がアクティブになると、キャッシュされたすべてのデータがただちに TCE に送信されます。

データ転送

セッションがアクティブ化される場合、セッションアクティブ化要求で TCE の IP アドレスが提供されます。アクティブ化の際に、プッシュモードが使用されている場合、TCE への（S）FTP 接続がすでに存在するかどうかが確認されます。存在する場合は、それがこのトレースセッションに関連付けられているすべてのトラフィックに使用されます。存在しない場合は、指定された IP アドレスを使用して TCE への（S）FTP 接続が確立されます。データはローカルにバッファリングされ、接続が確立されるまでトレースファイルが生成されます。接続が確立すると、以前に作成されたすべてのトレースファイルが TCE に送信されます。トレース記録セッションがトリガーされたかどうかに関係なく、セッションのアクティブ化時に TCE への（S）FTP接続が確立されることに注意してください。（S）FTP接続は、トレースセッションが非アクティブ化されるまで維持されます。

次の点に注意してください。

- トレース機能の設定時にデフォルトの TCE IP アドレスが指定されている場合は、リモート TCE へのデフォルトの（S）FTP 接続が確立されます。
- TCE は、IPv4 または IPv6 アドレッシングを介して到達可能にすることができます。提供された TCE アドレスがバージョンを示します。
- プッシュモードを使用しない場合、ファイルはローカルハードドライブ（**/hd-raid/trace**）に保存され、FTP または SFTP を使用して TCE によってプルされる必要があります。

サポートされる標準

セッショントレース機能には、次の標準規格および Requests for Comments（RFC）のサポートが追加されました。

- 3GPP TS 32.421 V8.5.0 (2009-06)：3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace concepts and requirements (Release 8)

- 3GPP TS 32.422 V8.6.0 (2009-09)：3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace; Trace control and configuration management (Release 8)
- 3GPP TS 32.423 V8.2.0 (2009-09)：3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace data definition and management (Release 8)

セッショントレース機能の設定

UMTS および EPC ネットワーク要素でのセッショントレースの設定は、次の手順で構成されます。

1. セッショントレースの有効化 （1410 ページ）
2. 管理トレース機能のセッション トレース テンプレートの設定 （1412 ページ）
3. 管理セッショントレースの設定 （1416 ページ）
4. シグナリング セッション トレースの設定 （1417 ページ）
5. ランダムトレースの設定 （1418 ページ）

トレースファイルは、ローカルに保存することも、さまざまなtraceコマンドで指定したトレース コレクション エンティティ（TCE）にプッシュすることもできます。



重要 SAEGW では、セッショントレース設定タイプのすべての組み合わせが使用できるわけではありません。サポートされているセッショントレース設定タイプの詳細については、このドキュメントの サポートされている SAEGW セッショントレースの設定 （1423 ページ） を参照してください。

セッショントレースの有効化

特定の管理、ランダム、またはシグナリング セッション トレースを設定する前に、セッショントレース機能を有効にする必要があります。

以下のコマンドは、指定されたサブスクライバデバイスまたは ID に基づいて、指定された UMTS/EPC ネットワーク要素におけるセッションの 1 つまたはすべてのインスタンスでサブスクライバ セッション トレース機能を有効または無効にします。

UMTS/EPC ネットワーク要素でセッショントレースを有効にするには、次の例を使用します。

```
config
   session trace network-element { all | ggsn | hnbgw | mme | pgw |
saegw | sgw } [  file-type <a-type  |  b-type>  ]  tce-mode none | push
 transport  ftp | sftp  username  username encrypted password password  path
  directory_path  collection timer  ctimer_value
   end
```

注：

- **session trace network-element**：指定したネットワーク要素でセッショントレース機能を有効にします。サポートされているすべてのネットワーク要素のセッショントレースを有効にするには、**all** を入力します。
- **file-type { a-type | b-type }**：セッショントレースによって生成される XML ファイルの種類を指定します。オプションには、A-type のファイルと B-type のファイルがあります。B-type の XML ファイルが使用される場合、複数のトレース記録セッション要素が 1 つの XML ファイルにエンコードされます。アクティベーション時に指定された TCE IP アドレスに従って、異なるトレース記録セッションが異なる TCE に関連付けられる場合があることに注意してください。期待されたとおり、Type-B XML ファイルにはそれぞれ、同じターゲット TCE にのみ関連する traceRecSession 要素が含まれます。異なる XML Type-B ファイルが異なる TCE 用に作成され、ターゲット TCE へ送信するために異なる tce_x ディレクトリに配置されます。デフォルトは **a-type** です。
- **tce-mode**：トレースファイルがローカルに保存され、TCE（**none**）がプルする必要があること、またはトレースファイルが TCE（**push**）にプッシュされることを指定します。デフォルトは **none** です。
- **transport**：トレースファイルを TCE にプッシュする方法を指定します（**ftp** または **sftp**）。デフォルトは **sftp** です。
- **username**：**tce-mode** が **push** の場合に指定する必要があります。
- **password**：**tce-mode** が **push** の場合に指定する必要があります。
- **encrypted**：ファイルを TCE サーバーにプッシュするために使用されるパスワードを暗号化することを指定します。
- **password**：ファイルを TCE サーバーにプッシュするために使用するパスワードを指定します。ユーザー名は 1 ～ 31 文字の英数字を使用できます。
- **collection-timer**：最初のアクティブ化またはデータ収集から TCE にデータが報告されるまで待機する時間（秒）を指定します。デフォルトは 10 秒です。
- **retry-timer**：前の転送が失敗した場合に、ファイル転送を再試行するまで待機する時間（秒）を指定します。デフォルトは 60 秒です。

例：

```
session trace network-element saegw tce-mode push transport sftp path /SessionTrace
username root encrypted password 5c4a38dc2ff61f72 collection-timer 5
```

セッショントレースが有効であることの確認

UMTS または EPC ネットワーク要素でセッショントレース機能が有効になっていることを確認するには、次の例を使用します。

show session trace statistics

出力には、どの NE のセッショントレースが有効になっているかが示され、また設定されているトレースタイプも示されます（該当する場合）。次に例を示します。

```
Network element status:
      MME:      Enabled      Cell-Trace: Disabled
      S-GW:    Enabled
SAEGW Enabled
            PGW:                    Trace-Type: None
            SGW:                    Trace-Type: None
```

セッショントレース機能の無効化

セッショントレース機能を無効にするには、次の例を使用します。

```
config
      no session trace network-element { all | ggsn | hnbgw | mme | pgw
 | saegw | sgw }
      end
```

管理トレース機能のセッション トレース テンプレートの設定

オペレータは、グローバル コンフィギュレーション モードで管理トレースのテンプレートを作成する必要があります。EXECモードで実行される管理トレースでは、テンプレートが使用されます。作成したテンプレートをさまざまなサブスクライバに関連付けて、テンプレートで設定されているインターフェイスをトレースできます。

特定の IMSI/IMEI のサブスクライバ セッション トレースをアクティブ化するため、オペレータは、事前設定済みのテンプレートと IMSI/IMEI、トレース参照、およびTCEアドレスを指定する EXEC モード **session trace subscriber** コマンドを使用することに注意してください。

session trace subscriber コマンドで使用するテンプレートを設定するには、次の例を使用します。

```
config
   template-session-trace network-element { ggsn | hnbgw | mme | pgw |
 saegw | sgw } template-name template_name
```

このコマンドを入力すると、ユーザーがセッション トレース テンプレート設定モードになります。このモードで、オペレータは、選択されたネットワーク要素をトレースするインターフェイスを選択します。



重要 セッション トレース テンプレート設定モードで使用できるオプションは、先行するコマンドで選択したネットワーク要素によって異なります。

GGSN、**MME**、**P-GW**、および **S-GW** の場合は、セッション トレース テンプレート設定モードで次のコマンドを入力します。

```
interface interface_name
end
```

SAEGWの場合、セッション トレース テンプレート設定モードで次のコマンドを入力します。

```
{ func-pgw | func-sgw } interface interface_name
end
```

- 注：使用可能な UMTS/EPC ネットワーク要素により、セッション トレース テンプレート用のさまざまなインターフェイスオプションが提供されます。

GGSN

使用可能な **ggsn** インターフェイスには以下が含まれます。

- **all**：使用可能なすべての GGSN インターフェイスをトレース対象に指定します。
- **gi**：トレースが実行されるインターフェイスとして、GGSN と RADIUS サーバー間の Gi インターフェイスを指定します。
- **gmb**：トレースが実行されるインターフェイスとして、GGSN と BM-SC 間の Gmb インターフェイスを指定します。
- **gn**：トレースが実行されるインターフェイスとして、GGSN と SGSN 間の Gn インターフェイスを指定します。
- **gx**：トレースが実行されるインターフェイスとして、GGSN と PCRF 間の Gx インターフェイスを指定します。
- **gy**：トレースが実行されるインターフェイスとして、GGSN と PCRF 間の Gx インターフェイスを指定します。

HNBGW

使用可能な **hnbgw** インターフェイスは次のとおりです。

- **all**：すべての **hnbgw** インターフェイスをトレース対象に指定します。
- **iucs**：トレースが実行されるインターフェイスとして、3G UMTS フェムトセル アクセス ネットワーク内の HNB-GW とモバイル スイッチング センター（3G MSC）間の iucs インターフェイスを指定します。
- **iups**：トレースが実行されるインターフェイスとして、HNB-GW と SGSN 間の ipps インターフェイスを指定します。

MME

使用可能な **mme** インターフェイスには以下が含まれます。

- **all**：すべての MME インターフェイスをトレース対象に指定します。
- **s10**：トレースが実行されるインターフェイスとして、MME と別の MME 間の S10 インターフェイスを指定します。
- **s11**：トレースが実行されるインターフェイスとして、MME と S-GW 間の S11 インターフェイスを指定します。
- **s13**：トレースが実行されるインターフェイスとして、MME と EIR 間の S13 インターフェイスを指定します。
- **s1mme**：トレースが実行されるインターフェイスとして、MME と eNodeB 間の S1-MME インターフェイスを指定します。
- **s3**：トレースが実行されるインターフェイスとして、MME と SGSN 間の S3 インターフェイスを指定します。
- **s6a**：トレースが実行されるインターフェイスとして、MME と HSS 間の S6a インターフェイスを指定します。

P-GW

使用可能な **pgw** インターフェイスは次のとおりです。

- **all**：使用可能なすべての P-GW インターフェイスをトレース対象に指定します。
- **gx**：トレースが実行されるインターフェイスとして、P-GW と PCRF 間の Gx インターフェイスを指定します。

- **gy**：トレースが実行されるインターフェイスとして、P-GW と OCS 間の Gy インターフェイスを指定します。
- **s2a**：トレースが実行されるインターフェイスとして、P-GW と HSGW 間の S2a インターフェイスを指定します。
- **s2b**：トレースが実行されるインターフェイスとして、P-GW と ePDG 間の S2b インターフェイスを指定します。
- **s2c**：トレースが実行されるインターフェイスとして、P-GW と非 3GPP アクセスデバイス間の S2c インターフェイスを指定します。
- **s5**：トレースが実行されるインターフェイスとして、同じ管理ドメイン内（非ローミング）にある S-GW と P-GW 間の S5 インターフェイスを指定します。
- **s6b**：トレースが実行されるインターフェイスとして、P-GW と 3GPP AAA サーバー間の S6b インターフェイスを指定します。
- **s8**：トレースが実行されるインターフェイスとして、S-GW とローミングシナリオで使用される P-GW 間の S8 インターフェイス（PLMN 間参照ポイント）を指定します。
- **sgi**：トレースが実行されるインターフェイスとして、P-GW と PDN 間の SGi インターフェイスを指定します。

SAEGW

SAEGW でトレースできるインターフェイスは、SAEGW（**func-pgw**）で設定された P-GW で使用可能なインターフェイスと、SAEGW（**func-sgw**）で設定された S-GW で使用可能なインターフェイスごとに分類されます。

- 使用可能な **func-pgw interface** オプションは次のとおりです。
  - **all**：使用可能なすべての **func-pgw** インターフェイスをトレース対象に指定します。
  - **gx**：トレースが実行されるインターフェイスとして、P-GW と PCRF 間の Gx インターフェイスを指定します。
  - **gy**：トレースが実行されるインターフェイスとして、P-GW とオンライン課金システム間の GTPP ベースのオンライン課金インターフェイスを指定します。
  - **s2a**：トレースが実行されるインターフェイスとして、P-GW と HSGW 間の S2a インターフェイスを指定します。
  - **s2b**：トレースが実行されるインターフェイスとして、P-GW と ePDG 間の S2b インターフェイスを指定します。
  - **s2c**：トレースが実行されるインターフェイスとして、P-GW と非 3GPP アクセスデバイス間の S2c インターフェイスを指定します。
  - **s5**：トレースが実行されるインターフェイスとして、P-GW と S-GW 間の S5 インターフェイスを指定します。
  - **s6b**：トレースが実行されるインターフェイスとして、P-GW と 3GPP AAA サーバー間の S6b インターフェイスを指定します。
  - **s8**：トレースが実行されるインターフェイスとして、P-GW と S-GW 間の S8b インターフェイスを指定します。
  - **sgi**：トレースが実行されるインターフェイスとして、P-GW と PDN 間の SGi インターフェイスを指定します。
- 使用可能な **func-sgw interface** オプションは次のとおりです。

- **all**：使用可能なすべての **func-sgw** インターフェイスをトレース対象に指定します。
- **gxc**：トレースが実行されるインターフェイスとして、P-GW と PCRF 間の Gx インターフェイスを指定します。
- **s11**：トレースが実行されるインターフェイスとして、MME と S-GW 間の S11 インターフェイスを指定します。
- **s4**：トレースが実行されるインターフェイスとして、S-GW と SGSN 間の S4 インターフェイスを指定します。
- **s5**：トレースが実行されるインターフェイスとして、S-GW と P-GW 間の S5 インターフェイスを指定します。
- **s8**：トレースが実行されるインターフェイスとして、S-GW と P-GW 間の S8b インターフェイスを指定します。

S-GW

使用可能な **sgw** インターフェイスは次のとおりです。

- **all**：使用可能なすべての S-GW インターフェイスをトレース対象に指定します。
- **gxc**：トレースが実行されるインターフェイスとして、S-GW と PCRF 間の Gxc インターフェイスを指定します。
- **s11**：トレースが実行されるインターフェイスとして、S-GW と MME 間の S11 インターフェイスを指定します。
- **s4**：トレースが実行されるインターフェイスとして、S-GW と SGSN 間の S4 インターフェイスを指定します。
- **s5**：トレースが実行されるインターフェイスとして、S-GW と P-GW 間の S5 インターフェイスを指定します。
- **s8**：トレースが実行されるインターフェイスとして、S-GW と P-GW 間の S8 インターフェイスを指定します。

セッション トレース テンプレート設定の確認

セッション トレース テンプレート設定を確認するには、Exec モードで次のコマンドを入力します。

```
show session trace template network-element { ggsn | hnbgw | mme | pgw
 | saegw | sgw } all
```

出力には、テンプレート名、NE タイプ、およびトレース対象として設定されたすべてのインターフェイスが表示されます。

セッション トレース テンプレート設定の無効化

セッション トレース テンプレート設定を無効にするには、次の例に示すようにコマンドを使用します。

```
no template-session-trace network-element { ggsn | hnbgw | mme | pgw |
 saegw | sgw }
```

ネットワーク要素およびサブスクライバ単位でのセッション トレース テンプレート設定の無効化

ネットワーク要素およびサブスクライバ単位でセッション トレース テンプレートを無効にするには、次を実行します。

no session trace subscriber network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name *template_name* **{ imsi** *id* **| imei** *id* **} trace-ref** *trace_ref_value* **collection-entity** *ip_address*

管理セッショントレースの設定

管理トレースを設定する前に、セッショントレース機能を有効にする必要があります。手順については、セッショントレースの有効化 （1410 ページ） を参照してください。

EXEC モードから UMTS または EPC ネットワーク要素で管理セッショントレースを設定するには、次を実行します。

session trace subscriber network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name *template_name* **{ imei** *id* **| imsi** *id* **} { all |** *interface* **} } trace-ref** *id* **collection-entity** *ip_address*

注：

- **template-name**：このセッショントレースに使用するセッション トレース テンプレートの名前を指定します。セッション トレース テンプレートは グローバル コンフィギュレーション モード で **template-session-trace** コマンドを使用して設定します。EXEC モードで実行される管理トレースでは、指定されたこのテンプレートが使用されます。
- **imsi** *id*：サブスクライバの International Mobile Subscriber Identity 番号を指定します。
- **imei** *id*：サブスクライバの International Mobile Equipment Identity 番号を指定します。
- **trace-ref**：このサブスクライバ管理トレースのトレース参照を指定します。モバイル国コード（MCC）＋モバイルネットワークコード（MNC）＋3 バイトオクテット文字列トレース ID で構成する必要があります。例：31001212349。
- **collection-entity**：生成されたトレースファイルの送信先であるトレース収集エンティティ（TCE）の IP アドレスを指定します。IP アドレスは IPv4 形式で指定します。

例：

以下に、すべての S-GW および P-GW インターフェイスへのサブスクライバ管理トレースの設定を示す完全な例を示します。これは、SAEGW でのセッショントレースの有効化、すべての S-GW および P-GW インターフェイスに対するセッション トレース テンプレートの作成、およびテンプレートを使用した特定 IMSI へのサブスクライバ管理トレースの実行により構成されます。

```
config
  session trace network-element saegw
  end
config
  template-session-trace network-element saegw template-name saegw_all
    func-pgw interface all
```

```
    func-sgw interface all
    end
session trace subscriber network-element saegw template-name saegw_all imsi
 123456789012345 trace-ref 123456789012 collection-entity 209.165.200.225
```

管理トレース設定の確認

サブスクライバの管理トレース設定が有効になっていることを確認するには、Exec モードで **show session trace statistics** コマンドを入力します。正しい NE がネットワーク要素のステータスを **Enabled** と表示していることを確認します。次に例を示します。

```
SAEGW Enabled
            PGW:                    Trace-Type: M
            SGW:                    Trace-Type: M
```

サブスクライバ管理トレースに対して特定のパラメータがアクティブになっていることを確認するには、次の例を使用します。

show session trace subscriber network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } trace-ref *trace_ref_value*

出力のフィールドには、各ネットワーク要素に設定された NE タイプとトレースタイプが表示されます。次に、SAEGW 管理トレース設定の出力例を示します。

```
NE Type: SAEGW
            PGW:                    Trace-Type:                 M
            SGW:                    Trace-Type:                 M
......
Traced Interfaces:
PGW:
      <P-GW interfaces configured for the trace.>
SGW:
      <S-GW interfaces configured for the trace.>
```

管理トレース設定の無効化

EXEC モードで管理トレース設定を無効にするには、次の手順を実行します。

no session trace subscriber network element { ggsn | hnbgw | mme | pgw | saegw | sgw } trace ref *trace_ref_value*

シグナリング セッション トレースの設定

シグナリング セッション トレースを設定する前に、セッショントレース機能を有効にする必要があります。手順については、セッショントレースの有効化（1410ページ） を参照してください。

シグナリング セッション トレースを設定するには、次のコマンドを実行します。

session trace signaling network-element { ggsn | hnbgw | mme | pgw | saegw [func-pgw | func-sgw] | sgw }

注：

- **func-pgw**：SAEGW において P-GW シグナリングのトレースを有効にします。
- **func-sgw**：SAEGW において S-GW シグナリングのトレースを有効にします。

- **func-sgw** または **func-pgw** のいずれも指定されていない場合、シグナリングトレースは、SAEGW のすべての P-GW および S-GW インターフェイスを対象に実行されます。
- **collection-entity**：トレースファイルの送信先であるトレース収集エンティティ（TCE）の IPv4 アドレスまたは IPv6 アドレスを指定します。

例：

この例では、SAEGW におけるすべての S-GW および P-GW インターフェイスのシグナリング セッション トレースが設定されます。

session trace signaling network-element *saegw*

シグナリング セッション トレース設定の確認

シグナリング セッション トレースの設定を確認するには、次の手順を実行します。

show session trace statistics

次のフィールドを探して、シグナリングトレースの設定を確認します。次に例を示します。

```
Network element status:
......
SAEGW Enabled
          PGW:                    Trace-Type: S
          SGW:                    Trace-Type: S
```

シグナリング セッション トレースの無効化

SAEGW でシグナリングトレースを非アクティブ化する手順は次のとおりです。

no session trace signaling network-element { ggsn | hnbgw | mme | pgw | saegw [func-pgw | func-sgw] | sgw }

ランダムトレースの設定

ランダムトレースを設定する前に、まず UMTS/EPC ネットワーク要素でセッショントレース機能を有効にする必要があります。手順については、この章のセッショントレースの有効化（1410 ページ）を参照してください。

次のコマンドは UMTS/EPC ネットワーク要素のランダムトレースに基づいて、サブスクライバセッションのトレース機能を有効または無効にします。有効にすると、指定されたネットワーク要素にあるセッションのすべてのインスタンスについて、サブスクライバ選択がランダムロジックに基づいて実行されます。

ランダムセッショントレースを設定するには、次のコマンドを実行します。

session trace random *range* **network-element { ggsn | hnbgw | pgw | saegw | sgw [func-pgw | func-sgw] } interface [all | *interface* } collection-entity** *ipv4_address*

注：

- **session trace random range**：指定した数のサブスクライバのランダムトレースを有効にします。有効なエントリは 1 ～ 1000 のサブスクライバです。

- **{ ggsn | hnbgw | pgw | saegw | sgw [func-pgw | func-sgw] }**：選択したネットワーク要素のランダムトレースを有効にすることを指定します。
- **func-pgw**：SAEGW で P-GW インターフェイスのランダムトレースを有効にします。
- **func-sgw**：SAEGW で S-GW インターフェイスのランダムトレースを有効にします。
- **func-pgw**、**func-sgw** のいずれも指定されていない場合、ランダムトレースは P-GW と S-GW の両方で実行されます。
- **interface**：ランダムトレースの対象にするネットワークインターフェイスを指定します。使用可能なインターフェイスは、選択したネットワーク要素のタイプによって異なります。

GGSN

使用可能な **ggsn** インターフェイスは次のとおりです。

- **all**：使用可能なすべての GGSN インターフェイスをトレース対象に指定します。
- **gi**：トレースが実行されるインターフェイスとして、GGSN と RADIUS サーバー間の Gi インターフェイスを指定します。
- **gmb**：トレースが実行されるインターフェイスとして、GGSN と BM-SC 間の Gmb インターフェイスを指定します。
- **gn**：トレースが実行されるインターフェイスとして、GGSN と SGSN 間の Gn インターフェイスを指定します。
- **gx**：トレースが実行されるインターフェイスとして、GGSN と PCRF 間の Gx インターフェイスを指定します。
- **gy**：トレースが実行されるインターフェイスとして、GGSN と PCRF 間の Gx インターフェイスを指定します。

HNBGW

使用可能な **hnbgw** インターフェイスは次のとおりです。

- **all**：すべての **hnbgw** インターフェイスをトレース対象に指定します。
- **iucs**：トレースが実行されるインターフェイスとして、3G UMTS フェムトセル アクセス ネットワーク内の HNB-GW とモバイル スイッチング センター（3G MSC）間の **iucs** インターフェイスを指定します。
- **iups**：トレースが実行されるインターフェイスとして、HNB-GW と SGSN 間の **iups** インターフェイスを指定します。

P-GW

使用可能な P-GW インターフェイスは次のとおりです。

- **all**：すべてのインターフェイスをトレース対象に指定します。
- **gx**：トレースが実行されるインターフェイスとして、P-GW と PCRF 間の Gx インターフェイスを指定します。
- **gy**：トレースが実行されるインターフェイスとして、P-GW と OCS 間の Gy インターフェイスを指定します。
- **s2a**：トレースが実行されるインターフェイスとして、P-GW と HSGW 間の S2a インターフェイスを指定します。

- **s2b**：トレースが実行されるインターフェイスとして、P-GW と ePDG 間の S2b インターフェイスを指定します。
- **s2c**：トレースが実行されるインターフェイスとして、P-GW と非 3GPP アクセスデバイス間の S2c インターフェイスを指定します。
- **s5**：トレースが実行されるインターフェイスとして、同じ管理ドメイン内（非ローミング）にある S-GW と P-GW 間の S5 インターフェイスを指定します。
- **s6b**：トレースが実行されるインターフェイスとして、P-GW と 3GPP AAA サーバー間の S6b インターフェイスを指定します。
- **s8**：トレースが実行されるインターフェイスとして、S-GW とローミングシナリオで使用される P-GW 間の S8 インターフェイス（PLMN 間参照ポイント）を指定します。
- **sgi**：トレースが実行されるインターフェイスとして、P-GW と PDN 間の SGi インターフェイスを指定します。

SAEGW

SAEGW でトレースできるインターフェイスは、SAEGW（**func-pgw**）で設定された P-GW で使用可能なインターフェイスと、SAEGW（**func-sgw**）で設定された S-GW で使用可能なインターフェイスごとに分類されます。

使用可能な SAEGW **func-pgw interface** オプションは次のとおりです。

- **all**：SAEGW で設定されたすべての **func-pgw** インターフェイスをトレース対象に指定します。
- **gx**：トレースが実行されるインターフェイスとして、P-GW と PCRF 間の Gx インターフェイスを指定します。
- **s2a**：トレースが実行されるインターフェイスとして、P-GW と HSGW 間の S2a インターフェイスを指定します。
- **s2b**：トレースが実行されるインターフェイスとして、P-GW と ePDG 間の S2b インターフェイスを指定します。
- **s2c**：トレースが実行されるインターフェイスとして、P-GW と非 3GPP アクセスデバイス間の S2c インターフェイスを指定します。
- **s5**：トレースが実行されるインターフェイスとして、P-GW と S-GW 間の S5 インターフェイスを指定します。
- **s6b**：トレースが実行されるインターフェイスとして、P-GW と 3GPP AAA サーバー間の S6b インターフェイスを指定します。
- **s8**：トレースが実行されるインターフェイスとして、P-GW と S-GW 間の S8b インターフェイスを指定します。
- **sgi**：トレースが実行されるインターフェイスとして、P-GW と PDN 間の SGi インターフェイスを指定します。
- **gy**：トレースが実行されるインターフェイスとして、P-GW とオンライン課金システム間の GTPP ベースのオンライン課金インターフェイスを指定します。

使用可能な SAEGW **func-sgw** インターフェイスは次のとおりです。

- **all**：SAEGW にある使用可能なすべての **func-sgw** インターフェイスをトレース対象に指定します。

- **gxc**：トレースが実行されるインターフェイスとして、P-GW と PCRF 間の Gx インターフェイスを指定します。
- **s11**：トレースが実行されるインターフェイスとして、MME と S-GW 間の S11 インターフェイスを指定します。
- **s4**：トレースが実行されるインターフェイスとして、S-GW と SGSN 間の S4 インターフェイスを指定します。
- **s5**：トレースが実行されるインターフェイスとして、S-GW と P-GW 間の S5 インターフェイスを指定します。
- **s8**：トレースが実行されるインターフェイスとして、S-GW と P-GW 間の S8b インターフェイスを指定します。

S-GW：使用可能な **sgw** インターフェイスは次のとおりです。

- **all**：すべてのインターフェイスをトレース対象に指定します。
- **gxc**：トレースが実行されるインターフェイスとして、S-GW と PCRF 間の Gxc インターフェイスを指定します。
- **s11**：トレースが実行されるインターフェイスとして、S-GW と MME 間の S11 インターフェイスを指定します。
- **s4**：トレースが実行されるインターフェイスとして、S-GW と SGSN 間の S4 インターフェイスを指定します。
- **s5**：トレースが実行されるインターフェイスとして、S-GW と P-GW 間の S5 インターフェイスを指定します。
- **s8**：トレースが実行されるインターフェイスとして、S-GW と P-GW 間の S8 インターフェイスを指定します。

- **collection-entity** トレース収集エンティティ（TCE）の IPv4 アドレスを指定します。

例：

SAEGW 内のすべての S-GW インターフェイスと P-GW の s5 インターフェイスで 40 人の SAEGW サブスクライバの範囲でランダムトレースを有効にするには、次のコマンド例を入力します。

session trace random *40* **network-element** *saegw* **func-pgw interface** *s5* **func-sgw interface** *all* **collection-entity** *209.165.200.225*

ランダムトレース設定の確認

ランダムセッショントレース設定を確認するには、次の手順を実行します。

show session trace statistics

ネットワーク要素に対してランダムセッショントレースが有効になっていることを確認するフィールドを探します。次に例を示します。

```
Network element status:
...
SAEGW Enabled
          PGW:                    Trace-Type: R
          SGW:                    Trace-Type: R Configured-Random: 40
```

特定のネットワーク要素に対するランダムトレースの無効化

特定のネットワーク要素に対するランダムセッショントレースを無効にするには、次のコマンドを実行します。

```
no session trace random network-element { ggsn | hnbgw | pgw | saegw |
 sgw [ func-pgw | func-sgw ] }
```

セッショントレース機能のモニタリング

ここでは、セッショントレース機能をモニターするために使用できるコマンドに関する情報を提供します。

show session trace statistics

このコマンドは、セッショントレース機能の現在の使用状況に関する高度な統計情報を提供します。これには次の情報が含まれます。

- 現在のトレースセッションの数
- トレースセッションの合計数
- アクティブ化されたセッションの合計数
- アクティベーションエラーの数
- トリガーされたセッションの数
- メッセージの合計数
- 現在の TCE 接続の数
- 接続の TCE 接続の合計数
- すべての TCE にアップロードされたファイルの合計数

show session trace subscriber network-element trace-ref

このコマンドは、セッションの trace-ref 値およびネットワーク要素のタイプに基づいて、特定のトレースに関する詳細情報を表示します。これには、アクティベーション時間、IMSI、開始時刻、トレースメッセージ数、および作成されたファイルの総数が含まれます。また、このセッショントレースの対象として設定されているインターフェイスの一覧も表示されます。

show session trace trace-summary

このコマンドは、すべてのセッショントレースの trace-ref 値をマイネットワーク要素のタイプごとに分類して表示します。

show session trace tce-summary

このコマンドは、設定されているすべての TCE の IP アドレスとインデックス情報を表示します。

show session trace tce-address

このコマンドは、IP アドレス、開始時刻、アップロードされたファイルの総数など、特定の TCE に関する詳細情報を表示します。

サポートされている SAEGW セッショントレースの設定

SAEGW では、さまざまなトレース設定がサポートされています。セッショントレースタイプのさまざまな組み合わせは、コールタイプおよびトレースタイプと、通信事業者が Func-SGW トレースと Func PGW トレースのいずれかまたは両方を設定するかどうかによって異なります。

次の点に注意してください。

- M = 管理
- R = ランダム
- S = シグナリング

表 *133 : SAEGW* でサポートされるセッショントレースの設定

Func-S-GW トレース設定	Func-P-GW トレース設定	コール タイプ	S-GW トレースか	P-GW トレースか	出力	注
M	M	Collapsed	対応	対応	1 つの SAEGW トレースファイルが生成される	M トレース Func-SGW、Func-PGW、コールタイ Collapsed に効になって合、S-GW セージ（gt P-GW 制御ジの両方が SAEGW トファイルで されます。
R	R	Collapsed	対応	対応	1 つの SAEGW トレースファイルが生成される	
S	S	Collapsed	対応	対応	1 つの SAEGW トレースファイルが生成される	

Func-S-GW トレース設定	Func-P-GW トレース設定	コール タイプ	S-GW トレースか	P-GW トレースか	出力	注
M+S	M+S	Collapsed	対応	対応	2 つの SAEGW トレースファイルが生成される	M+S トレース Func-S-GW、 Func-P-GW、お コールタイプ Collapsed に対 効になってい 合、S-GW 制御 セージ（gtpv2 P-GW 制御メッ ジの両方が 2 つ SAEGW トレー ファイルでト されます。1 つ レースファイル 理によるもの り、もう 1 つは ナリングによ です。両方の ルの内容は同 す。
M+R	M+R	Collapsed	対応	対応	1 つの SAEGW トレースファイルが生成される	
S	R	Collapsed	非対応	非対応	なし	有効なトレース ではありませ
R	S	Collapsed	非対応	非対応	なし	有効なトレース ではありませ
M	R	Collapsed	対応	非対応	1 つの SAEGW トレースファイルが生成される	
R	M	Collapsed	非対応	対応	1 つの SAEGW トレースファイルが生成される	
M	S	Collapsed	非対応	対応	1 つの SAEGW トレースファイルが生成される	

Func-S-GW トレース設定	Func-P-GW トレース設定	コール タイプ	S-GW トレースか	P-GW トレースか	出力	注
S	M	Collapsed	対応	非対応	1 つの SAEGW トレースファイルが生成される	
M+S	M	Collapsed	対応	非対応	2 つの SAEGW トレースファイルが生成される	P-GW トレ成されませ
M	M+S	Collapsed	非対応	対応	2 つの SAEGW トレースファイルが生成されるが、S-GW トレースは生成されない	S-GW トレ成されませ
M+S	S	Collapsed	対応	対応	2 つの SAEGW トレースファイルが生成される	
S	M+S	Collapsed	対応	対応	2 つの SAEGW トレースファイルが生成される	
M+R	M	Collapsed	対応	対応	1 つの SAEGW トレースファイルが生成される	
M	M+R	Collapsed	対応	対応	1 つの SAEGW トレースファイルが生成される	
M+R	R	Collapsed	対応	非対応	1 つの SAEGW トレースファイルが生成される	
R	M+R	Collapsed	非対応	対応	1 つの SAEGW トレースファイルが生成される	
M	n/a	Pure S	対応	非対応	1 つの SAEGW トレースファイルが生成される	Func-P-GW Pure S コー用されませ

Func-S-GW トレース設定	Func-P-GW トレース設定	コール タイプ	S-GW トレースか	P-GW トレースか	出力	注
S	n/a	Pure S	対応	非対応	1 つの SAEGW トレースファイルが生成される	
R	n/a	Pure S	対応	非対応	1 つの SAEGW トレースファイルが生成される	
M+S	n/a	Pure S	対応	非対応	2 つの SAEGW トレースファイルが生成される	
M+R	n/a	Pure S	対応	非対応	1 つの SAEGW トレースファイルが生成される	
R+S	n/a	Pure S	非対応	非対応	なし	有効なトレース ではありません
n/a	M	Pure P	非対応	対応	1 つの SAEGW トレースファイルが生成される	
適用対象外	S	Pure P	非対応	対応	1 つの SAEGW トレースファイルが生成される	
n/a	R	Pure P	非対応	対応	1 つの SAEGW トレースファイルが生成される	
n/a	M+S	Pure P	非対応	対応	2 つの SAEGW トレースファイルが生成される	
n/a	M+R	Pure P	非対応	対応	1 つの SAEGW トレースファイルが生成される	
n/a	R+S	Pure P	非対応	対応	なし	有効なトレース ではありません

セッショントレースファイルの例

このセクションでは、シグナリング トレース ファイルの例を示します。

図 *115 :* シグナリング トレース ファイルの例（*1/3*）

```
<<<<OUTBOUND  10:04:53:997 Eventid:141005(3)
[MME-S11]GTPv2C Tx PDU, from 1.20.20.13:30016 to 1.20.20.3:2123 (62)
TEID: 0x000004D3, Message type: EGTP_TRACE_SESSION_ACTIVATION (0x47)
Sequence Number: 0x000401 (1025)
GTP HEADER
        Version number: 2
        TEID flag: Present
        Piggybacking flag: Not present
        Message Length: 0x003A (58)

INFORMATION ELEMENTS
        IMSI:
            Type: 1  Length: 8  Inst: 0
            Value: 123456789012345
            Hex: 0100 0800 2143 6587 0921 43F5

        Trace Info:
            Type: 96  Length: 34  Inst: 0
            Value:
                MCC: 123
                MNC: 456
                Trace Id: 03039

                Triggering Event: 1/0: Event shall be traced / not traced.
                    MSC Server:
                        SS: 0
                        HANDOVERS: 0
                        LU/IMSI ATT/DET: 0
                        MO & MT SMS: 0
                        MO & MT CALLS: 0

                    MGW:
                        CONTEXT: 0

                    SGSN:
                        MBMS CONTEXT: 0
                        RAU/GPRS ATT/DET: 0
                        MO & MT SMS: 0
                        PDP CONTEXT: 0

                    GGSN:
                        MBMS CONTEXT: 0
                        PDP CONTEXT: 0

                    MME:
                        HANDOVERS: 1
                        BEARER ACT/MOD/DEL: 1
                        UE INIT PDN DISC: 1
                        INIT ATT/TAU/DET: 1
                        SERVICE REQUEST: 1
                        UE INIT PDN CON REQ: 1
```

335925

図 *116 :* シグナリング トレース ファイルの例（*2/3*）

```
PGW:
                            BEARER ACT/MOD/DEL: 1
                            PDN CONN TERMINATE: 1
                            PDN CONN CREATE: 1

                        SGW:
                            BEARER ACT/MOD/DEL: 0
                            PDN CONN TERMINATE: 0
                            PDN CONN CREATE: 0

                    List of NE Types: 1/0: Trace Session activated/ not activated.
                        SGW: 0
                        MME: 1
                        BMSC: 0
                        RNC: 0
                        GGSN: 0
                        SGSN: 0
                        MGW: 0
                        MSC-S: 0
                        ENODEB: 1
                        PDN-GW: 1

                    Trace Depth:
                        Value: 5 (MAXIMUM w/o Vendor Specific Extension)

                    List of Interfaces: 1/0: Interface will be traced/ not traced.
                        MSC Server:
                            CAP: 0
                            MAP-F: 0
                            MAP-E: 0
                            MAP-B: 0
                            MAP-G: 0
                            MC: 0
                            IU: 0
                            A: 0
                            MAP-C: 0
                            MAP-D: 0

                        MGW:
                            IU-UP: 0
                            Nb-UP: 0
                            MC: 0

                        SGSN:
                            GE: 0
                            GS: 0
                            MAP-GF: 0
                            MAP-GD: 0
                            MAP-GR: 0
                            GN: 0
                            IU: 0
                            GB: 0

                        GGSN:
                            GMB: 0
                            GI: 0
                            GN: 0
                                                                        335926
```

図 *117* : シグナリング トレース ファイルの例（*3/3*）

```
                RNC:
                    UU: 0
                    IUB: 0
                    IUR: 0
                    IU: 0

                BMSC:
                    GMB: 0

                MME:
                    S11: 1
                    S10: 1
                    S6A: 1
                    S3: 1
                    S1-MME: 1

                SGW:
                    GXC: 0
                    S11: 0
                    S8B: 0
                    S5: 0
                    S4: 0

                PDN-GW:
                    SGi: 0
                    S8B: 1
                    GX: 1
                    S6B: 0
                    S5: 1
                    S2C: 0
                    S2B: 0
                    S2A: 0

                ENODEB:
                    UU: 0
                    X2: 1
                    S1-MME: 1

            TCE IP Addr:
                IPV4 Addr: 1.1.1.1


        Hex: 6000 2200 2163 5400 3039 0000 0000 0000
             003F 7040 0305 0000 0000 0000 0000 1F00
             6803 0101 0101                          335927
```



第 96 章

S-GW 復元サポート

この章では、S-GW 復元サポート機能について説明します。

- 機能説明 （1431 ページ）
- 機能の仕組み （1432 ページ）
- S-GW 復元サポートの設定 （1434 ページ）
- S-GW 復元サポートのモニタリングと障害対応 （1435 ページ）

機能説明

S-GW 復元機能は、EPC ネットワークで発生した S-GW 障害に対応するのに役立ちます。影響を受けた PDN にサービスを提供する別の S-GW を選択することで、S-GW が原因の障害で影響を受けた PDN を復元できます。これにより、PDN のクリーンアップのためにシグナリングの不要なフラッディングが発生するのを回避できます。

GTP-C シグナリングのリカバリ IE 中にパス障害が検出された場合や S-GW の再起動が検出された場合、P-GW はセッションを維持します。P-GW はこのシナリオでドロップされたパケットが課金されないようにします。また、P-GW は S-GW 障害検出後に維持された PDN 接続で受信したベアラーの追加要求や変更要求を拒否します。これは、PDN が復元されるまで行われます。

MME によってセッションが復元され、P-GW が再起動された S-GW または別の S-GW からベアラー変更要求を受信すると、P-GW は受信したダウンリンクデータの転送を続行し、課金を開始します。

サブスクライバが S-GW 復元フェーズにある場合、すべての RAR（セッション終了を予測）は PCEF を拒否します。P-GW は、PCRF に対して CCR-U をトリガーできる内部更新をすべて拒否します。S-GW が復元時に変更された場合、P-GW は復元された PDN の AN-GW の変更を含む CCR-U をトリガーします。

MME/S4-SGSN は、同じ PLMN の P-GW が S-GW 復元機能をサポートしていることを認識するようにローカルで設定されます。この機能が P-GW で有効になっている場合、すべての S-GW/MME でサポートされます。

重要 MME/S4-SGSN によってトリガーされた S-GW 復元手順のみがサポートされます。

GTP-U パスの障害に基づく S-GW 復元の検出は、このリリースでは考慮されません。この機能を有効にするには、GTP-C パス障害検出を有効にする必要があります。

GTP-U パスの障害に基づく S-GW 復元の検出は、このリリースでは考慮されません。この機能を有効にするには、GTP-C パス障害検出を有効にする必要があります。

P-GW 再起動通知は、ピア P-GW に障害が発生し、再起動していないことを通知するために使用することもできます。この場合、P-GW 再起動通知には「P-GW not responding」という理由値が含まれます。PRN の送信中、S-GW はエコー応答に応じて、この新しい理由値を追加します。

他の機能との関係

この機能を有効にするには、GTP-C パス障害検出を有効にする必要があります。

機能の仕組み

P-GW での変更

デマルチプレクサでパス障害が検出されると、パス障害通知が P-GW のすべてのセッションマネージャに送信されます。次に、セッションマネージャは進行中のトランザクションをクリーンアップします。すべてのトランザクションが削除されると、sessmgr-egtpc はトンネルをペーシングキューに追加してトンネルを削除します。

P-GW は、S-GW 復元を実行して、パス障害を検出した直後にセッションを削除することはありません。P-GW は、維持されている PDN 接続の受信ダウンリンクパケットを破棄し、復元されていない S-GW の障害後に、維持されている PDN 接続の課金を停止します。

MME/S4-SGSN は、コアネットワークノードの過負荷を回避するために、S-GW の再配置のペースを制御します。MME/S4-SGSN は、RAU/TAU プロシージャのサービス要求に関与している UE の S-GW 再配置を、どのモビリティ製品のプロシージャにも関与しておらず MME/S4-SGSN へのシグナリング接続がない UE よりも優先します。

セッションが S-GW 復元対象としてマークされ、新しい要求によってコンテキスト置換が発生する場合、既存のセッションが中止され、新しい要求通知イベントが続きます。

E-GTPC での変更

デマルチプレクサが eGTP-C にパス障害について通知したら、すべてのアクティブな手順を中止します。中止手順では、S-GW 復元がセッションに対して有効になっているかどうかを P-GW に示します。すべてのセッションをキューに追加し、S-GW のセッションホールドタイマーを

開始します。MME は、セッションを新しい S-GW または同じ S-GW に再配置することで、これらのセッションを復元します。P-GW で MBReq が受信され、セッションに S-GW 復元がマークされている場合、S-GW フラグがリセットされます。この時点で、セッションホールドタイマーが期限切れになり、S-GW 復元は削除されます。

MME および SGSN での変更

MME と SGSN が S-GW へのパスの障害を検出し、MME が S-GW の復元をサポートしている場合、MME は障害が発生した S-GW から別の S-GW にセッションを再配置します。

S-GW の復元は、リリース 21.3 以降の MME でサポートされます。ただし、SGSN では S-GW の復元はサポートされません。

デマルチプレクサ障害検出

EGTPIN マネージャはパス障害を検出し、その障害についてすべてのセッションマネージャに通知します。次に、セッションマネージャはパス障害通知を受け取り、S-GW 復元が有効であるため、進行中のすべてのトランザクションを停止します。Sessmgr-egtpc は、パス障害について P-GW-drv に通知します。P-GW がセッションを削除します。

次に、eGTP-C はセッションホールドタイマーを開始します。セッションホールドタイマーの期限前に MME が S-GW サービスの復元をトリガーすると、古い S-GW からのセッションが新しい S-GW に移動します。これにより、セッションがハンドオーバーされたり、削除されたりしないことが保証されます。

セッションホールドタイマーが期限切れになると、そのピアとのすべてのセッションがクリーンアップされます。この時点では、新しいセッションは新しい S-GW に移動しません。



重要 S-GW がダウンしてから非常に短い間隔で復旧する場合、P-GW はパスの障害を検出しません。この場合、S-GW の復元は行われません。ホールドタイマーが期限切れになる前に古い S-GW が再び稼働した場合は、一部のセッションだけが新しい S-GW に移動する可能性があります。この場合、eGTP-C はそのピアとの残りのセッションを削除する必要はありません。eGTP-C はタイマーを停止します。

セッションマネージャがパス障害を検出すると、デマルチプレクサマネージャに通知します。上記のシナリオは、この場合でも発生します。

パス障害の検出後、デマルチプレクサは S-GW に ECHO メッセージを送信しません。新しいセッションの追加が発生した場合、または新しいセッションがノードから復元された場合、デマルチプレクサはピアに ECHO メッセージを送信します。

標準準拠

S-GW 復元機能は、次の標準規格に準拠しています。

- 3GPP TS 23.007：Restoration procedures

• 3GPP TS 29.212：Policy and Charging Control over Gx reference point

S-GW 復元サポートの設定

セッションホールドタイマーは設定可能なパラメータです。通信事業者は、**egtpc sgw-restoration session-hold timeout seconds** CLI コマンドを使用してこのパラメータを設定できます。

sgw-restoration キーワードは、S-GW の復元機能を有効にし、P-GW サービスにおけるセッション ホールド タイムアウトを設定します。

ピア S-GW がダウンしていることを P-GW が検出すると（検出は再起動カウンタの変化、またはエコー応答障害によるパス障害に基づく）、P-GW はピア S-GW に関連付けられているすべての PDN セッションを SGW-RESTORATION-STATE に移行します。また、P-GW は、session-hold timeout に指定された値でピア S-GW ごとにタイマーを開始します。タイマーの期限が切れると、P-GW は SGW-RESTORATION-STATE のすべてのセッションをクリーンアップします。



重要 デフォルトでは、S-GW 復元のサポートは有効になりません。

設定例

S-GW 復元のサポートを有効にするには、次の例を使用します。

```
configure
  context context_name
    pgw-service service_name
      egtpc sgw-restoration session-hold timeout seconds
      { default | no } egtpc sgw-restoration session-hold
      end
```

注：

- **session-hold timeout** は、S-GW 復元のセッション保留タイマーを設定します。
- *seconds* は、1 ～ 3600 の整数にする必要があります。デフォルト：0（無効）。
- S-GW 障害が通知されると、P-GW は、S-GW 復元機能が有効かどうかを確認します。有効にすると、P-GW は、セッション保留タイムアウトの間、影響を受けるすべてのセッションを維持します。セッション保留タイムアウト後、P-GW は、まだ回復していないすべてのセッションをクリアします。

S-GW 設定の確認

S-GW 復元の設定を確認するには、次のコマンドを使用します。

show pgw-service all

S-GW 復元の設定情報を表示するために、以下のフィールドが追加されました。

- EGTP SGW 復元の処理
- セッション保留タイマー
- タイムアウト（Timeout）

S-GW 復元サポートのモニタリングと障害対応

このセクションでは、S-GW 復元のサポートにおける show コマンドについて説明します。

S-GW show コマンド

このセクションでは、S-GW 復元をサポートするための show コマンドとその出力について説明します。

show ims-authorization policy-control statistics

次のフィールドは、S-GW 復元サポートで導入された統計を表示するために追加されました。

- SGW Restoration
- RAR Reject
- Internal Updates Dropped
- Revalidation Timeout
- Pending Updates

show pgw-service statistics all

S-GW 復元サポートを表示するために、次のカウンタが追加されています。

- SGW 復元の統計情報
- PDN の総数
- 復元状態
- 回復
- リリース日
- SGW 復元状態でのドロップ数
- パケット
- Bytes

show subscribers pgw-only full all

S-GW 復元サポートを表示するために、次のフィールドとカウンタが追加されています。

- Bearer State
- in packet dropped sgw restoration state
- in bytes dropped sgw restoration state

- out packet dropped sgw restoration state
- out bytes dropped sgw restoration state



第 97 章

Override-Control AVP での Execution-Time AVP のサポート

- 機能の概要と変更履歴 （1437 ページ）
- 機能説明 （1438 ページ）
- 機能の仕組み （1438 ページ）
- モニタリングおよびトラブルシューティング （1442 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• ECS • P-GW
該当プラットフォーム	ASR 5500
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*ECS Administration Guide*

マニュアルの変更履歴



重要 リリース 21.2 および N5.5 よりも前に導入された機能の改訂履歴の詳細は示していません。

改訂の詳細	リリース
このリリースでは、Override-Control AVP における Execution-Time AVP のサポートが追加され、オーバーライドされたパラメータを、1つまたはすべての課金アクション（ワイルドカードを使用）のルール（静的または事前定義済み）に対して指定でき、特定のルールを除外できるようになりました。	21.3
最初の導入。	21.2 よりも前

機能説明

以前のリリースで導入されたオーバーライド制御（OC）機能では、Gx インターフェイスを介して PCRF から送信されたパラメータを使用して、静的ルールまたは事前定義済みルールのパラメータを動的に変更できました。RAR/CCA メッセージで受信した OC パラメータは、PCEF によってすぐに適用されました。将来の指定された時間に OC のインストールを強制する方法はありませんでした。

この機能の実装により、オーバーライドされたパラメータを、1つまたはすべての課金アクション（ワイルドカードを使用）のルール（静的または事前定義済み）に対して指定でき、特定のルールを除外できるようになりました。これらのオーバーライドは、CCA または RAR メッセージの AVP 構造を使用して PCRF によって送信されます。

この機能の一部として、P-GW は、独自の Override-Control グループ AVP に含まれる次の 2 つの新しい AVP をサポートしています。

- Execution-Time（AVP コード 132025）：この AVP のタイプは時間です。指定された Override-Control インスタンスが有効になる UNIX エポックを示します。
- Override-Control-Pending-Queue-Action（AVP コード 132078）：この AVP のタイプは ENUM であり、許容される値は FLUSH（0）と RETAIN（1）です。ゲートウェイが Pending-OC-Queue に対して実行するアクションを示します。

どちらの AVP も Override-Charging-Action-Parameters グループ AVP に含まれます。

機能の仕組み

Execution-Time AVP は、PCRF によって RAR/CCA メッセージで送信される Override-Control グループ AVP に含まれるオプションの AVP です。ルールレベル、課金アクションレベル、およびワイルドカードレベルの OC で有効です。

Override-Control AVP が PCRF から RAR/CCA メッセージで送信されるたびに、次のようになります。

1. Execution-Time AVP が含まれていない場合は、下位互換性のために既存の OC アプリケーション手順が採用されます。つまり、OC パラメータが PCEF によってすぐに適用されます。
2. 「過去」のものである Execution-Time AVP が含まれている場合は、Execution-Time AVP が送信されていないかのように扱われ、OC パラメータが PCEF によってすぐに適用されます。
3. 「将来」のものである Execution-Time AVP が含まれている場合、PCEF は、その OC を「Pending」としてマークし、実行時間に達すると OC をインストールします。

セッションリカバリと ICSR

保留中の OC は、シャーシ内/シャーシ間のセッションリカバリで回復します。PCEF は、他の OC パラメータのチェックポインティングに使用される既存のフレームワークを使用して Execution-Time のチェックポインティングを行います。セッションマネージャが再起動するか、ICSR のスイッチオーバーが発生すると、Execution-Time AVP を含む回復された各 OC のタイマーが開始されます。この新しいタイマーの値は、OC がアクティブ化されるまでの残り時間、または OC がコールに適用されるまでの残り時間と等しくなります。

回復中にタイマーが期限切れになると、OC は回復直後に適用されます。

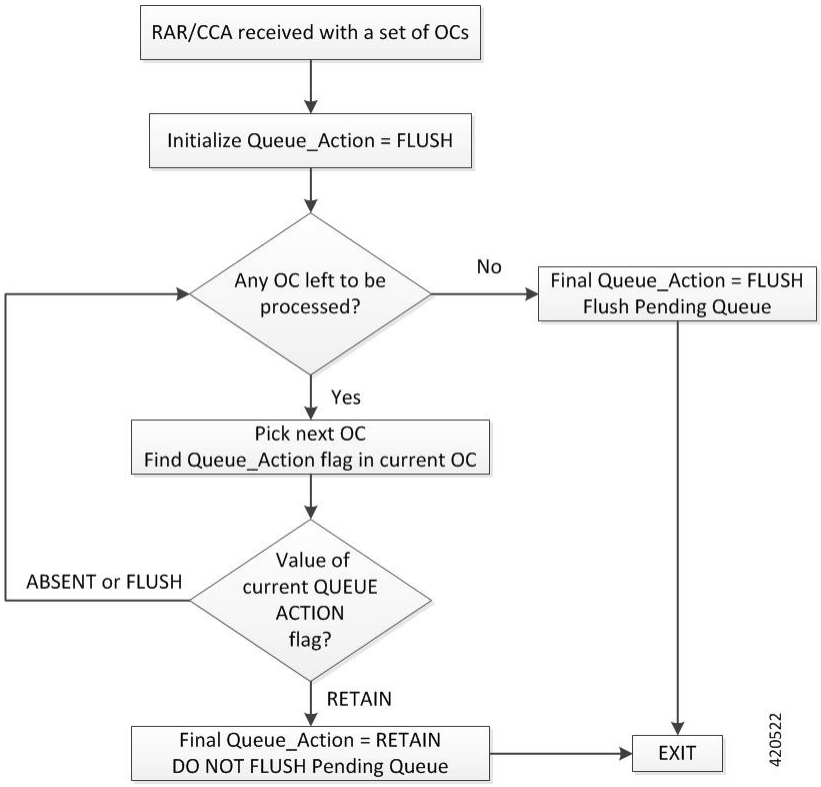
N から N-1 ビルドへのダウングレード中、現在アクティブな N シャーシ上の保留中の OC は、スタンバイ N-1 シャーシにチェックポインティングされません。

保留中の OC のフラッシュ

PCEF は、オーバーライド制御保留キューアクションの有無に基づいて、サブスクライバのすでに保留中の OC をフラッシュするか保持するかを決定します。

新しい RAR/CCA メッセージで新しい OC（Execution-Time AVP の有無にかかわらず）を受信すると、PCEF はそのサブスクライバの以前の保留中の OC をすべてフラッシュします。PCEF は、Execution-Time AVP の有無に基づいて、新しく受信した OC をバッファリングまたは適用します。この動作はデフォルトの動作です。

保留中の OC をフラッシュしないことが要件の場合、次の図で示されているように、新しい AVP である Override-Control-Pending-Queue-Action が、RAR/CCA メッセージの少なくとも 1 つの Override-Control AVP 内で送信されます。

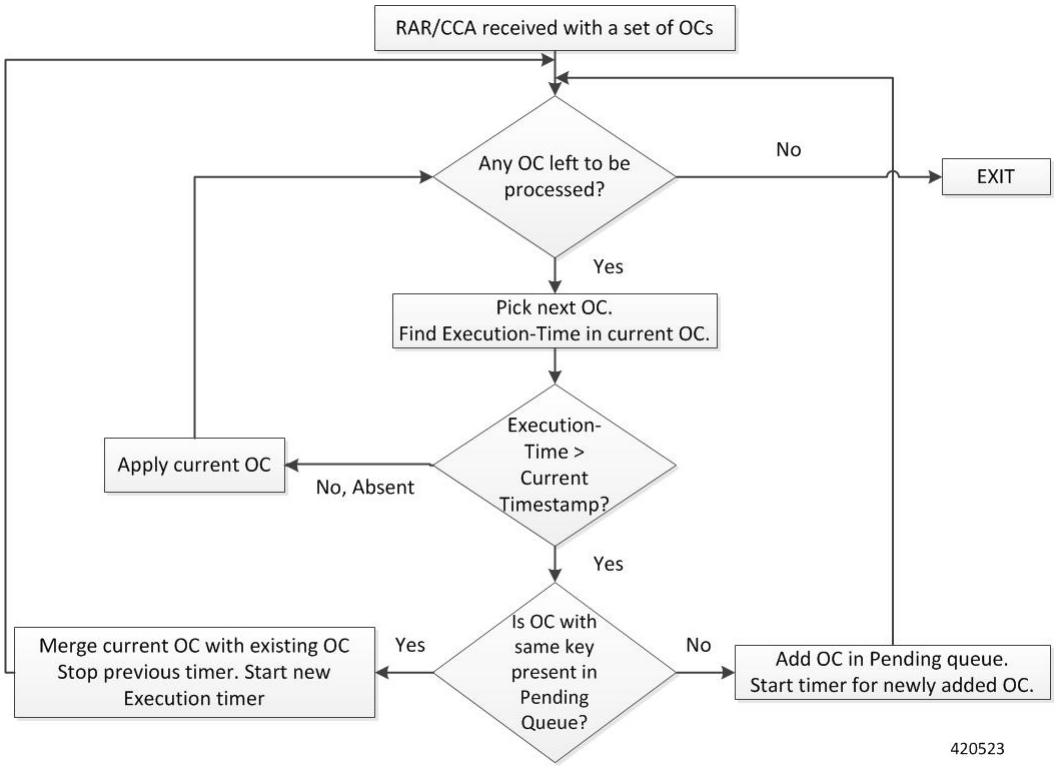


保留中のキューへの OC の追加

PCEF は、RAR/CCA メッセージで PCRF から受信した Override-Control グループ AVP のすべてのインスタンスを処理します。Override-Control AVP に「将来」のタイムスタンプを持つ Execution-Time AVP がある場合、PCEF は、それをそのサブスクライバに関して「Pending」とマークします。OC を Execution-Time AVP とともに受信し、同じ OC 識別子を持つ保留中の OC がすでに存在する場合、新たに受信した OC は保留中の OC とマージされます。マージされた OC の実行時間は、新しく受信した OC の実行時間になります。

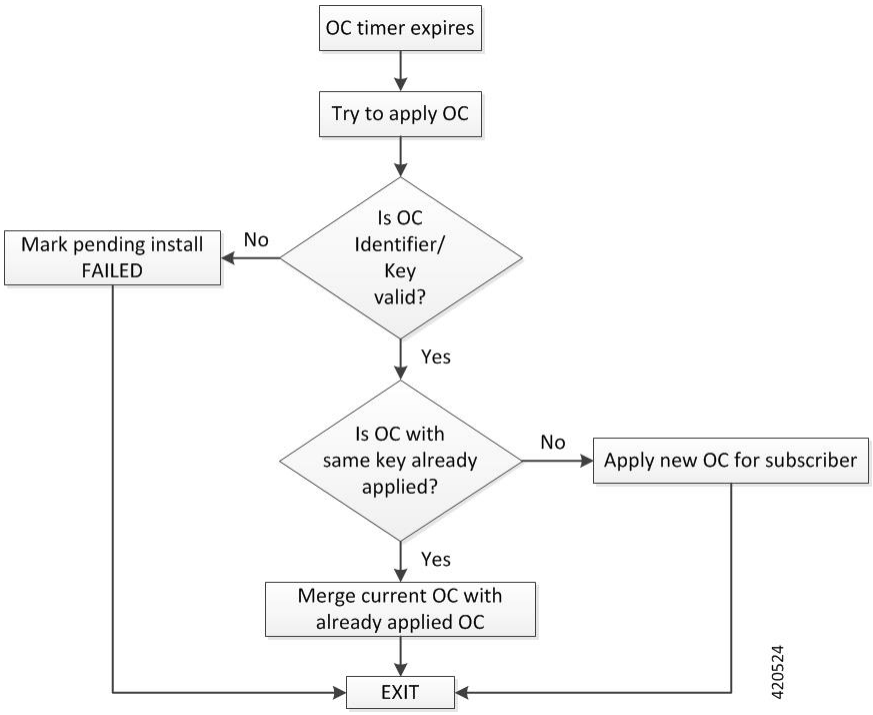
Execution-Time AVP なしで受信した、または実行時間がすでに「過去」のものである Override-Control グループ AVP は、リストに追加されません。つまり、すぐに適用されます。

次の図では、保留中のキューへの OC の追加について説明しています。



保留中 OC のインストール

PCEF は、そのようなすべての保留中 OC の実行時間も保存するため、OC の実行時間に達すると、次の図で説明されているように、OC がサブスクライバに適用されます。



制限事項

この機能の既知の制限事項と制約事項は次のとおりです。

- Execution-Time AVP は、名前のない OC でのみサポートされます。
- OC をバッファリングできる最大期間は 44 日です。
- サブスクライバに対してバッファリングできる OC の数に厳格な制限はありません。ただし、OC をバッファリングするかどうかの決定は、使用できるシステムリソースに依存します。
- 識別子が同じで将来の実行時間が異なる OC は、PCEF での処理順にマージされるため、RAR および CCA での発生順序と同じにならないことがあります。結果として、OC には、最後に処理される OC の実行時間が含まれます。

モニタリングおよびトラブルシューティング

ここでは、機能のモニタリングとトラブルシューティングに使用できるコマンドについて説明します。

show コマンドと出力

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show active-charging subscribers callid <call_id> override-control pending

この新しい show コマンドは、サブスクライバレベルで保留中の OC をチェックするために導入されました。次に、出力例を示します。

```
show active-charging subscribers callid 00004e21 override-control pending
CALLID: 00004e21
Override Control :
  Rule Name :
                    qci2
  Charging Parameters:
    Rating Group     : 100
    Offline Enabled  : TRUE
  Execution-Time     : <Day Month DD HH:MM:SS GMT YYYY>
Override Control :
  Rule Name :
                    qci1
  Charging Parameters:
    Rating Group     : 100
    Offline Enabled  : TRUE
  Policy Parameters:
    QCI              : 4
    ARP Byte         : 81
    MBR UL           : 25000
    MBR DL           : 13000
    TOS UL           : af23 (22)
    TOS DL           : af23 (22)
    NEXTHOP ADDR     : 10.20.10.10
    CF State       : 0
  Execution-Time     : <Day Month DD HH:MM:SS GMT YYYY>
```

show active-charging sessions full all

この CLI コマンドの出力は、サブスクライバレベルで保留中の OC に関連する情報が表示されるように変更されました。出力例の一部を以下に示します。

```
show active-charging sessions full all
.
.
.
Override Control:
    Installs Received:              2
    Installs Succeeded:             1  Installs Failed:             0
    Install Pending:
      Total  :                      2
      Merged :                      0
      Flushed:                      0
      Failed :                      0
    Disables Received:              0
    Disables Succeeded:             0  Disables Failed:             0

No Charging ruledef(s) match the specified criteria
No Firewall ruledef(s) match the specified criteria

  Post-processing Rulestats : No Post-processing ruledef(s) match the specified criteria
Dynamic Charging Rule Name Statistics: n/a
Total Dynamic Rules:             0
Total L7 Dynamic Rules:          0
Total Predefined Rules:          0
Total ADC Rules:                 0
Total Firewall Predefined Rules: 0
Total Override Control:          0
Total Override Control Pending:  3
```

show active-charging rulebase statistics name <rulebase_name>

このCLIコマンドの出力は、ルールベースレベルで保留中のOCに関連する情報が表示されるように変更されました。出力例の一部を以下に示します。

```
show active-charging rulebase statistics name cisco

    Override Control Statistics:
       Total number of Installs Received:                6
       Total number of Installs Succeeded:               1
       Total number of Installs Failed:                  1
       Install Pending:
         Total:                                          4
         Merged:                                         1
         Flushed:                                        1
         Failed:                                         1
       Total number of Disables Received:                0
       Total number of Disables Succeeded:               0
       Total number of Disables Failed:                  0
       Total number of Subscribers:                      1
```



第 98 章

100 万の S1-U ピアツーピア接続のサポート

この章では、100 万の S1-U ピアツーピア接続機能に対する StarOS のサポートについて説明します。

- 機能説明 （1445 ページ）
- 機能の仕組み （1445 ページ）
- 機能の設定 （1447 ページ）
- show コマンドの出力 （1447 ページ）

機能説明

実稼働予測により、StarOS のサポートが強化され、1 つの S-GW で 100 万の S1-U 接続に対応できるようになりました。

S1-U インターフェイスは、端末から受信したユーザーデータを eNodeB と S-GW の間で伝送するユーザー プレーン インターフェイスです。StarOS では、VPN コンテキストごとに S1-U ピアの数を 100 万まで拡張できるようになりました。

CLI コマンドを使用して、オペレータは統計を収集する S1-U ピアの数を設定できます。StarOS のメモリ制限により、100 万ピア（128k）未満で設定する必要があります。

機能の仕組み

gtpumgr は次のガイドラインに従って、ピアを割り当てます。

- セッションインストールがセッションマネージャから実行されると、ピアが作成されます。統計情報がセッションマネージャで維持管理されている場合、gtpumgr は統計情報を含むピアレコードも作成します。
- ピアレコードはサービス単位で保持されます。
- ピアの数は、gtpumgr インスタンスレベルで維持されます。S1-U ピアの数の上限は gtpumgr インスタンスごとに 100 万です。

- 上限の 100 万ピアを超えると、ピアの作成に失敗します。これにより、gtpumgr ではコールのインストールに失敗し、監査がトリガーされると監査に失敗します。

機能の変更は、gtpu-service including GGSN/S4-SGSN/S-GW/P-GW/SAEGW/ePDG/SaMOG/HNB-GW/HeNB-GW を使用する次のインターフェイス/サービスのすべてに影響します。

- General Packet Radio Service（GPRS）の Gn および Gp インターフェイス
- UMTS システムの Iu、Gn、および Gp インターフェイス
- Evolved Packet System（EPS）の S1-U、S2a、S2b、S4、S5、S8、および S12 インターフェイス。

リカバリ/ICSR の考慮事項

- セッションマネージャ/gtpumgr のリカバリ後、または ICSR スイッチオーバー後に、統計情報の収集用に設定された一連のピアが回復されます。
  - セッション数が 0 で統計情報がないピアは回復されません。
  - セッション数が 0 で統計情報があるピアは回復されます。
  - 拡張ヘッダーのサポートが無効になっているピアは回復されます。
- 以前のリリースからアップグレードする場合は、新しいリリースのシャーシ **gtpu peer statistics threshold** が以前のリリース以上であることを確認してください。このようにして、GTPU ピアの統計情報がアップグレード時に保持されます。たとえば、StarOS リリース 19.0 から 20.2 にアップグレードする場合、StarOS 19.0 システムに 17,000 の GTPU セッションがある場合は、StarOS 20.2 システムのしきい値も 17,000 に設定します。

設定と制約事項

- StarOS に接続される GTP-U エンティティの数が多いため、GTP-U パス管理機能を無効にすることを推奨します。
- 分散型のシステムであるため、統計情報の割り当てに関して設定するしきい値に厳しい上限はありません。統計情報を含む GTP-U ピアの合計数が、設定されたしきい値を若干超える可能性があります。
- 100 万個のピアすべてがポイントツーポイントでノードに接続されているわけではないことを前提としています。ピアはルータを介して接続されます。
- StarOS がこの機能をサポートするために ARP のテーブルサイズが変更されることはありません。

機能の設定

この項では、100 万の S1-U ピア接続機能のサポートを設定する方法について説明します。

gtpu peer statistics threshold

この新しいコマンドが コンテキスト コンフィギュレーション モードに追加され、StarOS が統計を維持する S1-U ピアの数を指定できるようになりました。

この機能を設定するには、次の例を使用します。

```
configure
  context context_name
    gtpu peer statistics threshold value
    end
```

注記：

- *value* は、統計が維持される S1-U ピアの数を示します。有効なエントリは 16000 ～ 128000 です。デフォルト設定は 16000 です。
- しきい値を現在の値よりも低い値に設定することはできません。

show コマンドの出力

この項では、100 万の S1-U ピア機能をサポートするために行われた show コマンド出力の変更ついて説明します。

clear gtpu statistics peer-address

all キーワードがこのコマンドに追加され、通信事業者は統計情報が保持されているすべての S1-U ピアで統計情報をクリアできるようになりました。

```
clear gtpu statistics peer-address all
```

show gtpu statistics

このコマンドの出力が強化され、GTPU ピアの合計数と、統計収集用に設定された GTPU ピアの合計数が表示されるようになりました。

- 合計 GTPU ピア
- 統計を使用した合計 GTPU ピア

show session subsystem facility sessmgr

このコマンドの出力が強化され、統計収集用に設定された S1-U（GTP-U）ピアの合計数が表示されるようになりました。

- 統計を使用した合計 GTPU ピア



第 99 章

有効性タイマーによるCCR-Uクォータの抑制

- 機能の概要と変更履歴 （1449 ページ）
- 機能説明 （1450 ページ）
- 有効性タイマーが実行されている状態での CCR-U クォータの抑制 （1450 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• GGSN • P-GW • SAEGW
該当プラットフォーム	すべて（All）
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
初版	21.20.16

機能説明

Validity-Time 属性値ペア（AVP）は、主に次の条件で使用されます。

1. Granted-Service-Unit（GSU）
2. Final-Unit-Indication（FUI）

この機能は、Granted-Service-Unit（GSU）のみを処理します。Validity-Time AVP には、GSU が有効である時間が含まれます。Validity-Time の期限が切れた後、新しい GSU を取得するために、更新要求がサーバーに送信されます。

GSUがゼロである場合は、既存の動作で有効性タイマーがまだ実行中であるにもかかわらず、P-GW は、受信するすべてのパケットの更新要求をクレジット制御サーバーに送信します。

この既存の動作が強化され、GSUがゼロであり、有効性タイマーが実行中である場合でも、クレジット制御サーバーに更新要求が送信されません。新しい動作は、Final-Unit-Indication AVP が着信していない場合にのみ有効です。

これは、**suppress-ccru zero-gsu-with-validity-timer** コンフィギュレーション コマンドを使用してアクティビティを制御することで実行されます。

有効性タイマーが実行されている状態での CCR-U クォータの抑制

有効性タイマーが実行されている状態での CCR-U クォータを抑制するには、次の設定コマンドを使用します。

```
configure
   active-charging-service service_name
      credit-control
       diameter suppress-ccru zero-gsu-with-validity-timer
       [ no ] diameter suppress-ccru
          end
```

注：

- **suppress-ccru**：P-GW がクォータの CCR-U メッセージの送信を抑制するように指定します。
- **zero-gsu-with-validity-timer**：有効性タイマーが実行されているときに P-GW が No GSU のクォータの CCR-U の送信を抑止するように指定します。

- **[no]**：以前に設定されている場合に、CCR-U 抑制 **zero-gsu-with-validity-timer** 設定が無効になることを指定します。

有効性タイマーが実行されている状態での CCR-U クォータの抑制



第 100 章

ULI 変更との TEID コリジョン

- 機能の概要と変更履歴 （1453 ページ）
- 機能説明 （1454 ページ）
- 機能の仕組み （1454 ページ）
- ULI 変更との TEID コリジョンの設定 （1458 ページ）
- モニタリングおよびトラブルシューティング （1459 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • GGSN
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
デフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

マニュアルの変更履歴

改訂の詳細	リリース
P-GW、SAEGW、および GGSN サービスでの TEID コリジョン中に MCC のみがチェックされることを確認するために、ULI 変更による TEID コリジョン機能が強化されました。	21.28.m4

改訂の詳細	リリース
このリリースで、ULI 変更によるトンネルエンドポイント識別子（TEID）コリジョン要求機能を拒否する P-GW および GGSN 設定がサポートされました。	21.6.13
最初の導入。	21.2 よりも前

機能説明

トンネルエンドポイント識別子（TEID）コリジョンが発生しているシナリオでは、P-GW または GGSN が、ホームサブスクライバに TEID を割り当てます。古いセッションの場合、S-GW または SGSN では、P-GW または GGSN によって割り当てられたものと同じ TEID がローミングサブスクライバに割り当てられます。次に、S-GW は、BRCmd、DBCmd、MBR メッセージを P-GW に送信します。SGSN は PDP コンテキスト更新メッセージを P-GW に送信します。ホームサブスクライバとローミングサブスクライバの両方に同じ TEID が割り当てられ、P-GW には重複する TEID 割り当てに関する情報がないため、P-GW は要求を受け入れます。同じ TEID を重複して使用すると、ローミングサブスクライバが使用するデータにホームサブスクライバへの課金が適用されます。

このシナリオを排除するために、ユーザーロケーション情報（ULI）変更による TEID コリジョン機能が導入されました。この機能を使用すると、TEID コリジョンが発生した場合に要求を拒否するように P-GW と GGSN を設定できます。

ULI 変更による TEID コリジョン機能により、mcc+mnc の比較ではなく、モバイル国コード（MCC）のみとの比較が可能になりました。この機能は、P-GW、SAEGW、GGSN での MOCN シナリオをサポートします。

機能の仕組み

次の項では、ULI 変更による TEID コリジョン機能の概要を説明します。

アーキテクチャ

4G コールの場合、P-GW で、pgw-service の CLI を使用して ULI 変更機能との TEID コリジョンを設定できます。3G コールの場合、GGSN で、ggsn-service の CLI を使用してこの機能を設定できます。この機能は、P-GW と GGSN に対して次のように動作します。

- P-GW のホームユーザー機器（UE）では、ULI のモバイル国コードとモバイルネットワークコード（mcc_mnc）の情報が P-GW 上の UE のセッションで使用可能な ULI の情報と異なる場合、要求は拒否されます。この要求は、次のいずれかのメッセージに対するものです。
  - ベアラーリソースコマンド

- ベアラー変更要求
- ベアラー削除コマンド

- GGSN のホーム UE では、ULI のモバイル国コードとモバイルネットワークコードの情報が GGSN 上の UE のセッションで使用可能な ULI の情報と異なる場合、要求は拒否されます。この要求は、次のメッセージに対するものです。
  - PDP コンテキスト更新

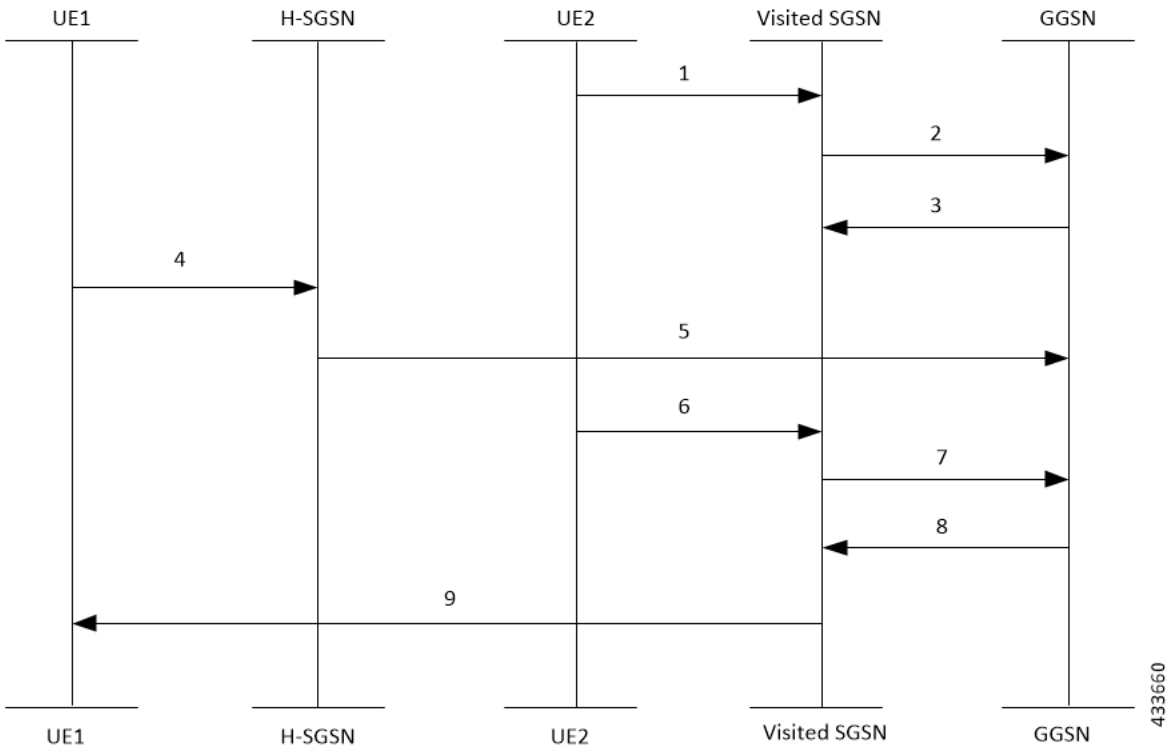
コール フロー

次のコールフローは、P-GW および GGSN の両方における ULI 変更による TEID コリジョンの処理を示しています。

GGSN 設定における ULI 変更による TEID コリジョン

次のコールフローは、GGSN における ULI 変更による TEID コリジョンの処理を示しています。

図 *118 : ULI* 変更に基づく *GTPC* ベースの *TEID* コリジョン検出



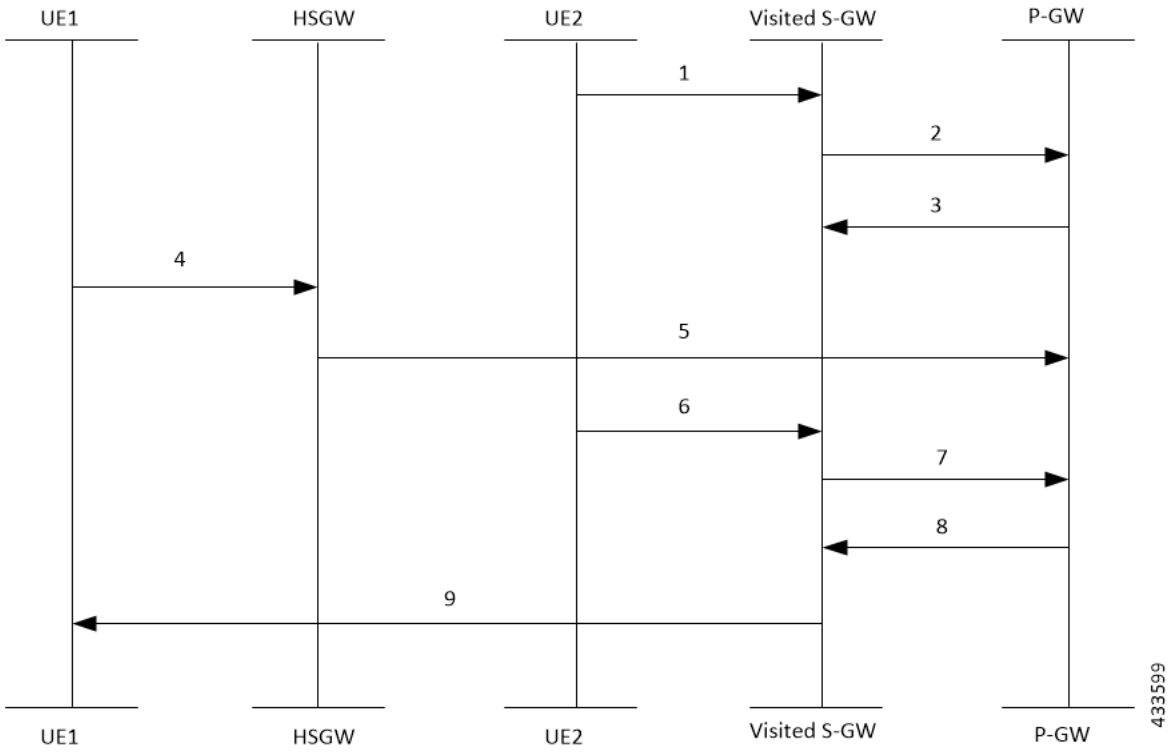
コールフローのステップは次のとおりです。

1. ローミングサブスクライバからコールを受信すると、UE2 がアクセス先の SGSN を介して GGSN への接続を試みます。
2. GGSN によってローミング UE に TEID-x が割り当てられます。
3. UE2 がネットワークから切断されると、GGSN でセッションが終了します。ただし、このセッションは引き続きアクセス先の SGSN で続行されます。
4. ホーム SGSN を介して GGSN でホーム UE 接続が行われます。
5. GGSN が、以前に GGSN で割り当てられたものと同じ TEID-x を割り当てます。
6. ローミング UE が GGSN に戻ります。アクセス先の SGSN のセッションはまだ存在するため、アクセス先の SGSN から同じ TEID-x が使用されます。
7. ULI 変更との TEID コリジョン機能が GGSN で有効になっており、（ステップ 4 のように）UE1 がホーム PLMN 内にある場合、ULI 変更に基づいた TEID ベースのコリジョンをチェックするためにすべての制御要求（GTPv1-C）が GGSN で処理されます。
8. GGSN が、GGSN サービスの PLMN リストに照らして ULI の MCC のみをチェックします。一致するものがない場合、GGSM は要求を拒否します。たとえば、GGSN のホーム UE の場合、ULI 情報の MCC がメッセージの PLMN リストと異なると要求は拒否されます。
9. 一致するものがある場合、要求はさらなる処理のために送信されます。

P-GW 設定での ULI 変更による TEID コリジョン

次のコールフローは、P-GW における ULI 変更による TEID コリジョンの処理を示しています。

図 *119 : ULI* 変更に基づく *EGTPC* ベースの *TEID* コリジョン検出



コールフローのステップは次のとおりです。

1. ローミングサブスクライバからコールを受信すると、UE2 がアクセス先の S-GW を介して P-GW への接続を試みます。
2. P-GW によってローミング UE に TEID-x が割り当てられます。
3. UE2 がネットワークから切断されると、P-GW でセッションが終了します。ただし、このセッションは引き続きアクセス先の S-GW で続行されます。
4. ホーム S-GW を介して P-GW でホーム UE アタッチが発生します。
5. P-GW が、以前に P-GW で割り当てられたものと同じ TEID-x を割り当てます。
6. ローミング UE が P-GW に戻ります。アクセス先の S-GW のセッションはまだ存在するため、アクセス先の S-GW から同じ TEID-x が使用されます。
7. ULI 変更との TEID コリジョン機能が P-GW で有効になっており、（ステップ 4 のように）UE1 がホーム PLMN 内にある場合、ULI 変更に基づいた TEID ベースのコリジョンをチェックするためにすべての制御要求（GTPv2-C）が P-GW で処理されます。
8. P-GW が、PGW サービスの PLMN リストに照らして ULI の MCC のみをチェックします。一致するものがない場合、P-GW は要求を拒否します。
9. 一致するものがある場合、要求はさらなる処理のために送信されます。

ULI 変更との TEID コリジョンの設定

このセクションでは、P-GW と GGSN での TEID コリジョンのシナリオで要求を拒否する CLI コマンドの設定について説明します。

GGSN における ULI 変更との TEID コリジョンの設定

TEID コリジョンが発生したときに要求を拒否するように P-GW を設定するには、次の設定コマンドを使用します。

```
configure
  context  context_name
    ggsn-service service_name
      [ default | no ] gtpc update-pdp-resp reject uli-mismatch
mcc-only
        end
```

注：

- **default**：コマンドをデフォルト設定の [Disabled] にリセットします。
- **no**：GTPC パラメータを無効にします。
- **update-pdp-resp reject**：PDP 応答拒否オプションを更新します。
- **uli-mismatch**：ULI がホーム PLMN セッションの一部ではない場合、PDP 更新要求メッセージを拒否します。
- **mcc-only**：PDP 更新要求で受信した MCC がホーム PLMN と一致しない場合、NON_EXISTENT（CC 192）原因コードを含む PDP 更新応答を送信します。

P-GW における ULI 変更との TEID コリジョンの設定

TEID コリジョンが発生したときに要求を拒否するように P-GW を設定するには、次の設定コマンドを使用します。

```
configure
  context  context_name
    pgw-service service_name
      [ default | no ] egtp bearer-req reject uli-mismatch mcc-only
      end
```

注：

- **default**：コマンドをデフォルト設定の [Disabled] にリセットします。
- **no**：GTPC パラメータを無効にします。
- **bearer-req**：ベアラー要求の処理に関連する設定を実行します。

- **reject**：ベアラー要求拒否オプションを表示します。
- **uli-mismatch**：ベアラー要求で受信した ULI が既存のセッションの ULI と一致しない場合、CONTEXT_NOT_FOUND（CC 64）原因コードを含むベアラー応答を送信します。
- **mcc-only**：ベアラー要求で受信した MCC を含む ULI が既存のセッションの MCC と一致しない場合、CONTEXT_NOT_FOUND（CC 64）原因コードを含むベアラー応答を送信します。

モニタリングおよびトラブルシューティング

コマンドや出力の表示

ここでは、ULI 変更との TEID コリジョンをサポートするために導入された show コマンドとフィールドについて説明します。

show egtpc statistics

この表示コマンドの出力が変更され、ULI 変更による TEID コリジョンに関する次のフィールドが表示されるようになりました。

- ベアラー変更要求
  - Total TX
  - Initial TX
  - Retrans TX
  - Total RX
  - Initial RX
  - Retrans RX
  - 破棄（Discarded）
  - No Rsp RX
- ベアラー変更応答
  - Total TX
  - Initial TX
  - Accepted
  - 拒否
  - Retrans TX
  - Total RX

- Initial RX
- Accepted
- 拒否
- 破棄（Discarded）

- ベアラーリソースコマンド
  - Total TX
  - Initial TX
  - Retrans TX
  - Total RX
  - Initial RX
  - Retrans RX
  - 破棄（Discarded）
  - No Rsp RX
- ベアラーリソース障害表示
  - Total TX
  - Initial TX
  - Retrans TX
  - Total RX
  - Initial RX
  - 破棄（Discarded）
- ベアラー削除コマンド
  - Total TX
  - Initial TX
  - Retrans TX
  - Total RX
  - Initial RX
  - 破棄（Discarded）
- MME S11u TEID を使用しないベアラー変更要求：
  - Local teid Mismatch：
    - Remote teid Mismatch

- GnGp Call MBReq rejected FTEID absent
- Tun Remote TEID Updated
- Teid Collision with uli mismatch for BRcmd
- Teid Collision with uli mismatch for DBCmd

show gtpc statistics

この表示コマンドの出力が変更され、ULI 変更による TEID コリジョンに関する次のフィールドが表示されるようになりました。

- Update PDP Context RX
- Update PDP Context TX

show pgw-service name

この show コマンドの出力が変更され、MCC 不一致での TEID コリジョン ULI 変更に関する次のフィールドが表示されるようになりました。

```
EGTP Bearer Request with Context Not Found cause if MCC mismatch : Enabled
EGTP Bearer Request with Context Not Found cause if MCC mismatch : Disabled
```

show ggsn-service name ggsn-service | more

この show コマンドの出力が変更され、MCC 不一致での TEID コリジョン ULI 変更に関する次のフィールドが表示されるようになりました。

```
GTPC Update PDP Response with Non Existent cause if IMSI mismatch : Enabled
  GTPC Update PDP Response with Non Existent cause if ULI mismatch : Enabled
  GTPC Update PDP Response with Non Existent cause if MCC mismatch : Enabled
```



第 101 章

時間ベースのルールのアクティブ化と非アクティブ化

- 機能の概要と変更履歴 （1463 ページ）
- 機能説明 （1464 ページ）
- 機能の仕組み （1464 ページ）
- 時間ベースルールのアクティブ化と非アクティブ化の設定 （1467 ページ）
- モニタリングおよびトラブルシューティング （1467 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	ASR 5500
デフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、時間ベースのルールのアクティブ化および非アクティブ化機能がサポートされています。	21.10
最初の導入。	21.2 よりも前

機能説明

3GPP 仕様 29.212 では、ポリシーおよび課金ルール機能（PCRF）が、Network Time Protocol（NTP）時間とともに、ポリシーおよび課金制御（PCC）ルールを送信できます。この時間になると、ルールが Rule-Activation-Time AVP を介してアクティブ化されます。以前のリリースでは、StarOS は Rule-Activation-Time が指定された PCC ルールを受け取ったときに、PCC ルールをインストールしていました。StarOS は、必要に応じてネットワークリソースを予約するための専用ベアラーも作成していました。このアプローチでは、ネットワークリソースの無駄が発生し、次のようないくつかのシナリオに対応できませんでした。

- ポリシーおよび課金ルール機能（PCRF）が PCC ルールを送信した場合。
- PCC ルールに Rule-Deactivation-Time AVP が設定されている場合、ルールの非アクティブ化時間が完了した後でも、そのルールがインストールされたままになります。

ネットワークリソースの無駄を排除し、必要に応じて利用するために、時間ベースのルールのアクティブ化および非アクティブ化機能が開発されました。この機能の目的は次のとおりです。

- Rule-Activation-Time の後に時間ベースの PCC ルールをインストールできます。
- Rule-Activation-Time の後に時間ベースの PCC ルールを削除できます。
- 事前定義されたルールとダイナミックルールでは、既存の動作が維持されます。
- セッションリカバリと ICSR がサポートされています。

機能の仕組み

次の項では、時間ベースの PCC ルールのアクティブ化および非アクティブ化機能の概要を示します。

アーキテクチャ

時間ベースの PCC ルールのアクティブ化と非アクティブ化を設定するため、StarOS によって、ルールがアクティブ化されるまでこれらのルールが個別に保存されます。ルールがアクティブ化されると、それらは PCC ルールとして処理されてインストールされます。必要に応じて、専用のベアラーが作成されます。非アクティブ化された PCC ルールは削除され、ベアラーを更新または削除する要求が生成されます。

（注） この機能は、後方互換性を維持するために CLI によって制御されます。

ルール変更シナリオ

PCC ルールがルールアクティブ化時間で使用可能な場合、StarOS はこの機能が有効か無効かを確認します。この機能が有効になっている場合、StarOS は PCC ルールをすぐにインストールしません。ルールアクティブ化時間がタイムアウトすると、PCC ルールがインストールされます。

次に、ルール変更のシナリオとそのシナリオにおける StarOS の動作の一部を示します。

- タイマーが実行中のルールが PCRF によって変更されると、StarOS は、既存のタイマーを停止し、ルールアクティブ化時間を使用して新しいタイマーを開始します。
- ルール変更に Rule-Activation-Time AVP が含まれていない場合、StarOS はルールをすぐにインストールします。このシナリオでは、Rule-Activation-Time は引き継がれません。
- 時間ベースルールのルール変更中は、ルールのパラメータはマージされません。これは、最新の定義で受信されたパラメータのみが適用されることを意味します。

  たとえば、料金設定グループが 500、課金 ID が 10、ルールアクティベーション化時間が T1 と定義された時間ベースルールが受信されたとします。しばらくすると（T1 よりも前）、料金設定グループが 400、ルールアクティブ化時間が T2 という新しい定義でルールが変更され、T2 の後、料金設定グループが 400 であるパラメータでルールがインストールされます。ここでは T2 の課金 ID は受信されず、料金設定グループのパラメータには課金 ID がありません。

デフォルトベアラー QoS の変更

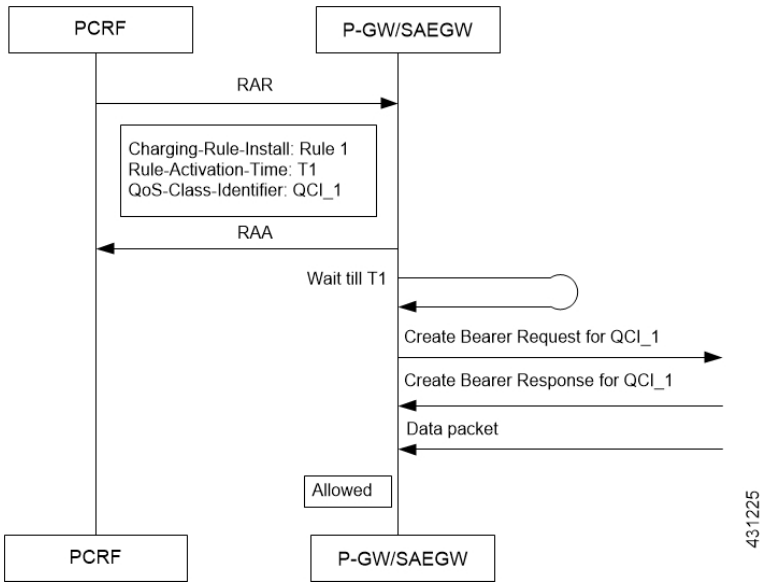
サブスクライバには、デフォルトベアラーの QoS が QCI_8 として設定されています。PCRF は QCI_5 と Rule-Activation-Time を T1 にして Rule1 ルールを送信します。T1 が期限切れになる前に、デフォルトのベアラー QoS が QCI_5 に変更されます。T1 の期限が切れると、Rule1 ルールをインストールするために、ベアラー更新要求がデフォルトのベアラーに送信されます。

コール フロー

次のコールフローは、Rule-Activation-Time と Rule-Deactivation-Time の処理を示しています。

ルールアクティブ化時間の設定

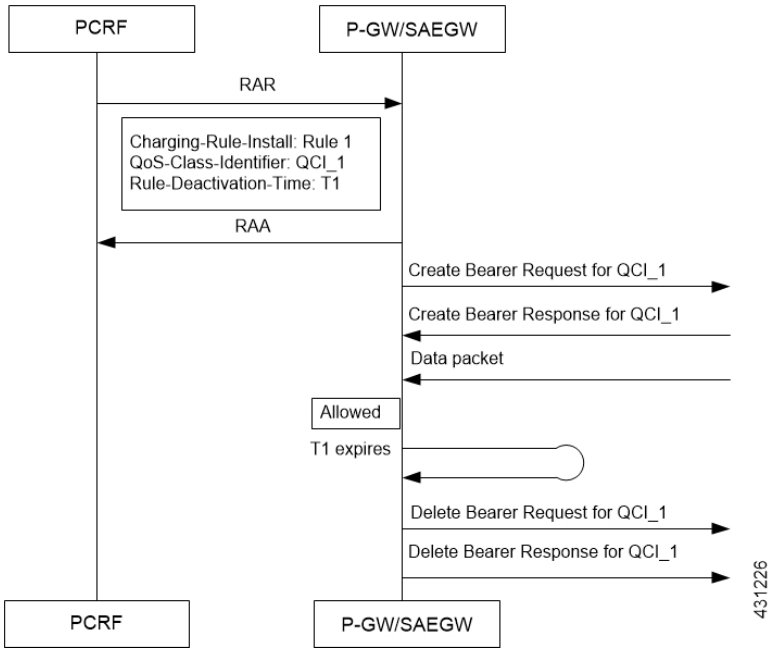
次のコールフローは、ルールアクティブ化時間の処理を示しています。



このコールフローでは、QCI_1 QoS クラス ID を持つベアラーは使用できません。QCI_1 を持つベアラーが使用できる場合、T1 タイマーが期限切れになった後に、ベアラー更新要求が想定されます。

ルールの非アクティブ化時間の設定

次のコールフローは、ルールの非アクティブ化時間の処理を示しています。



このコールフローでは、QCI_1 QoS-Class-Identifier を持つベアラーに、ルール 1 だけがあります。ベアラーに複数のルールがある場合、T1 タイマーが期限切れになった後に、ベアラー更新要求が想定されます。

時間ベースルールのアクティブ化と非アクティブ化の設定

ここでは、時間ベースの PCC ルールをアクティブ化および非アクティブ化する CLI コマンドの設定について説明します。

時間ベースの PCC ルールの設定

時間ベースの PCC ルールを設定するには、次のコンフィギュレーション コマンドを使用します。

```
configure
   require active-charging
   [ default | no ] policy-control time-based-pcc-rule
install-on-activation-time remove-on-deactivation-time
     end
```

注：

- **default**：コマンドをデフォルト設定の [Disabled] にリセットします。
- **no**：PCC ルールの時間ベースのアクティブ化または非アクティブ化を無効にします。
- **policy-control**：ACS ポリシー制御を設定します。
- **time-based-pcc-rule**：アクティブ化または非アクティブ化時間を使用して PCC ルールを設定します。
- **install-on-activation-time**：アクティブ化時間にのみ PCC ルールをインストールします。
- **remove-on-deactivation-time**：非アクティブ化時間に PCC ルールを削除します。

モニタリングおよびトラブルシューティング

コマンドや出力の表示

ここでは、時間ベースの PCC ルールアクティブ化/非アクティブ化をサポートするために導入された show コマンドとフィールドについて説明します。

show active-charging sessions full callid *callid*

この show コマンドの出力が変更され、時間ベースの PCC ルールの次のフィールドが表示されるようになりました。

- Installs Deferred

- 時間ベースの保留中の PCC ルールの合計

show active-charging service statistics

この show コマンドの出力は、次のフィールドを表示するように変更されました。

- 時間ベースの PCC ルール統計
  - ダイナミック ルール
    - Activation-Time Received
    - Deactivation-Time Received
    - Removed received before Activation
    - Removed due to Deactivation
  - 定義済みルール
    - Activation-Time Received
    - Deactivation-Time Received
    - Removed received before Activation
    - Removed due to Deactivation

show active-charging subscribers callid *callid* pending-pcc-rules

この show コマンドの出力は、次のフィールドを表示するように変更されました。

- CALLID
- Dynamic Charging Rule Definition(s) Configured
  - 名前
  - Prior
  - Content-Id
  - Chrg-Type
  - Rule Parameters
- ステータス
- Service Identifier
- QoS クラス識別子
- ARP Priority Level
- Reporting Level
- Metering Method

- アップリンク MBR
- ダウンリンク MBR
- アップリンク GBR
- ダウンリンク GBR
- Rule Activation Time
- Rule De-activation Time
- Filter 1
- 方向
- プロトコル
- Dst Addr
- Filter 2
- 方向
- プロトコル
- Src Addr
- Predefined Rules Enabled List



第 102 章

タイムスタンプの精度の向上

- 機能の概要と変更履歴 （1471 ページ）
- 機能説明 （1472 ページ）
- モニタリングおよびトラブルシューティング （1472 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *P-GW Administration Guide* • *Statistics and Counters Reference*

マニュアルの変更履歴

改訂の詳細	リリース
show active-charging flows full debug-info all コマンドが拡張され、VPP とセッションマネージャ間のタイムスタンプの精度が表示されるようになりました。詳細については、『*P-GW Administration Guide*』の「*VPP* メトリックの機能拡張」の章を参照してください。	21.27

機能説明

データパケットがオフロードされると、最後に到着したパケットから計算されたティックは、セッションマネージャの Starent Network Transmission（SNX）グローバルティックタイムよりも遅れが生じます。これにより、VPP とセッションマネージャの間で時刻が同期されなくなります。フロータイムアウトが誤って推定されるため、フローがセッションから削除されます。

show active-charging flows full debug-info all コマンドが拡張され、正しいフローアイドルタイムアウトが表示されるようになりました。

モニタリングおよびトラブルシューティング

ここでは、この機能をサポートする show コマンドを使ったモニタリングと障害対応の方法について説明します。

コマンドと出力の表示

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show active-charging flows full debug-info all

表 *134 : show active-charging flows full debug-info all* コマンド出力の説明

フィールド	説明
Last Active Tick Time	データパケットの最後のアクティブなティック時間を示します。
Current Tick Time	現在のシステムティック時刻を示します。



第 103 章

トラフィックのポリシングとシェーピング

この章では、シスコのシャーシでのサブスクライバ単位のトラフィックポリシングおよびシェーピング機能のサポートについて説明し、この機能の実装に使用される コマンドと RADIUS 属性について説明します。製品アドミニストレーション ガイドには、システム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、それぞれの製品のアドミニストレーション ガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

重要 トラフィックポリシングとシェーピングは、シスコのライセンス供与された機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

この項では次のトピックについて説明します。

- 機能説明 （1473 ページ）
- トラフィック ポリシング （1474 ページ）
- トラフィック シェーピング （1474 ページ）
- トラフィックポリシングの設定 （1475 ページ）
- トラフィックシェーピングの設定 （1478 ページ）
- トラフィック シェーピングの設定 （1481 ページ）
- RADIUS 属性 （1483 ページ）

機能説明

ここでは、個々のサブスクライバのトラフィックポリシングとトラフィックシェーピングについて説明します。

トラフィック ポリシング

トラフィックポリシングにより、3GPP/3GPP2 サービスの特定のトラフィッククラスの個々のサブスクライバや APN の帯域幅制限が可能になります。

帯域幅の適用は、ダウンリンクとアップリンクの方向で個別に設定および適用されます。

トラフィックポリシング機能は、RFC2698 で規定されているトークン バケット アルゴリズム（trTCM の修正版）を使用します。このアルゴリズムは、次の基準を測定してパケットを判断します。

- **認定データレート（CDR）**：サンプリング間隔中の、サブスクライバに対してパケットを送信/受信できる保証レート（ビット/秒）。
- **ピークデータレート（PDR）**：サンプリング間隔中の、サブスクライバに対してサブスクライバパケットを送信/受信できる最大レート（ビット/秒）。
- **バーストサイズ**：認定（CBS）およびピーク（PBS）レート条件の両方について、サンプリング間隔中にサブスクライバに対して送受信できる最大バイト数。これは、サブスクライバの「バケット」に格納できるトークンの最大数を表します。認定バーストサイズ（CBS）は、各サブスクライバのピークバーストサイズ（PBS）と等しくなります。

システムは、超過または違反と判断されたパケットに対して、次のいずれかのアクションを実行するように設定できます。

- **ドロップ**：問題のあるパケットは破棄されます。
- **送信**：問題のあるパケットは渡されます。
- **IP プレシデンスを引き下げる**：パケットの ToS ビットは「0」に設定されるため、パケットが渡される前にベストエフォートにダウングレードされます。パケットの ToS ビットはすでに「0」に設定されています。このアクションは「送信」と同等です。

トラフィック シェーピング

トラフィックシェーピングは、設定された制限を超えるパケットにバッファ機能を提供するレート制限方式です。データレートを超過したパケットは、バッファ内でキューに入れられて、後で配信されます。

帯域幅の適用は、ダウンリンクとアップリンクの方向で個別に実行できます。サブスクライバデータに使用できるバッファスペースがなくなった場合は、パケットをドロップするか、または次にスケジュールされているトラフィックセッションで送信するかをシステムを設定できます。

トラフィックポリシングの設定

トラフィックポリシングは、サブスクライバ単位で設定されます。サブスクライバは、システムにローカルに設定されたサブスクライバを使用することも、リモートのRADIUSサーバーに設定されたサブスクライバプロファイルを使用することもできます。

3GPPサービスでは、サブスクライバに対するトラフィックポリシングは、APN設定を使用して設定することもできます。

重要 3GPPでは、RADIUSサーバーから受信したサービス属性が、APNの設定よりも優先されます。

重要 この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンドや、キーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

トラフィックポリシングのサブスクライバの設定

重要 このドキュメントでは、RADIUSベースのサブスクライバプロファイルの設定手順は説明していません。詳細については、ご使用のサーバーに関するドキュメントを参照してください。

手順

ステップ1 トラフィックポリシングをサポートするように、システムでローカルサブスクライバのプロファイルを設定するには、次の設定例を適用します。

a) 指定した制限とアクションをダウンリンク（サブスクライバへのデータ）に適用するには、次を使用します。

```
configure
    context context_name
        subscriber name <user_name>
            qos traffic-police direction downlink
            end
```

b) 指定された制限とアクションをアップリンク（サブスクライバからのデータ）に適用するには、次を使用します。

```
configure
    context context_name
        subscriber name <user_name>
            qos traffic-police direction uplink
            end
```

注：

- **qos traffic-police direction { downlink | uplink }** コマンドには、多数のキーワードオプションが関連付けられています。
- 設定対象となる追加のサブスクライバごとに繰り返します。

（注）
超過/違反アクションが「low-ip-precedence」に設定されている場合、外部パケットの TOS 値は、サブスクライバ コンフィギュレーション モードでどの **ip user-datagram-tos-copy** コマンドが設定されているかに関わらず、トラフィック制限を超過/違反するパケットの「ベストエフォート」になります。さらに、「lower-ip-precedence」オプションは、**ip qos-dscp** コマンドの設定をオーバーライドする場合があります（サブスクライバ コンフィギュレーション モードでも同様）。そのため、上記のオプションを指定するときはこのコマンドを使用しないことを推奨します。

ステップ 2 次の設定例を適用して、サブスクライバプロファイルの設定を確認します。

```
context <context_name>
    show subscriber configuration username <user_name>
```

ステップ 3 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

3GPP ネットワークでのトラフィックポリシング用の APN の設定

ここでは、トラフィックポリシングをサポートする APN テンプレートの QoS プロファイルを設定するための情報と手順について説明します。

プロファイル情報は、GTP の PDP コンテキスト作成/更新要求メッセージへの応答で SGSN に送信されます。SGSN から要求された QoS プロファイルが、設定されている QoS プロファイルよりも小さい場合は、SGSN から要求されたプロファイルが使用されます。SGSN によって要求された QoS プロファイルの方が高い場合は、設定されたレートが使用されます。

認定データレートおよびピークデータレートのパラメータの値は、GGSN と SGSN の間の GTP メッセージで交換されます。そのため、使用される値は設定値よりも小さい場合があります。SGSN とでレートをネゴシエートする際、システムはこのレートを GTP で許可されている値に変換します。以下の表を参照してください。

表 *135 : GTP* メッセージの認定データレートとピークデータレートの許容値

値（bps）	増分粒度（bps）
1000 ～ 63,000	1,000（たとえば、1000、2000、3000、... 63000）

値（bps）	増分粒度（bps）
64,000 ー 568,000	8,000（たとえば、64000、72000、80000、...
576,000 ～ 8,640,000	64,000（たとえば、576000、640000、704000 86400000）
8,700,000 ～ 16,000,000	100,000 bps（たとえば、8700000、8800000、8 16000000）

手順

ステップ 1 次の設定例を適用して、パラメータを設定します。

a) 指定した制限とアクションをダウンリンク（Gn 方向）に適用するには、次を使用します。

```
configure
    context <context_name>
        apn <apn_name>
            qos rate-limit downlink
            end
```

b) 指定した制限とアクションをアップリンク（Gi 方向）に適用するには、次を使用します。

```
configure
    context <context_name>
        apn <apn_name>
            qos rate-limit uplink
            end
```

注：

- **qos rate-limit { downlink | uplink }** コマンドには、多数のキーワードオプションが関連付けられています。
- 必要に応じて、設定で次のコマンドを入力して、APN によって支援できる PDP コンテキストの最大数を設定し、APN の帯域幅消費を制限します。

  max-contents primary *<number>* **total** *<total_number>*

- 必要に応じてこの手順を繰り返して、追加の QoS トラフィック ポリシング プロファイルを設定します。

重要
「サブスクライブ済み」トラフィッククラスを受信した場合、システムはクラスをバックグラウンドに変更し、以下を設定します。アップリンクとダウンリンクの保証データレートを 0 に設定します。受信のアップリンクまたはダウンリンクデータレートが 0 で、トラフィックポリシングが無効の場合、デフォルトの 64 kbps が使用されます。有効にすると、APN の設定値が使用されます。ダウンリンクの最大データレートの設定値が R4 QoS プロファイルに収まらない場合は、デフォルトの 64 kbps が使用されます。受信したアップリンクまたはダウンリンクのいずれかの最大データレートがゼロ以外の

場合、トラフィックポリシングは、バックグラウンドクラスに対して有効になっていれば適用されます。トラフィックポリシングが無効の場合は、受信した値が応答に使用されます。

ステップ 2 次のコマンドを入力して、APN が正しく設定されていることを確認します。

show apn { all | name *apn_name* }

出力には、設定済みの APN パラメータの設定が簡潔にリストされています。

ステップ 3 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイスや、ネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

トラフィックシェーピングの設定

トラフィックシェーピングは、サブスクライバ単位で設定されます。サブスクライバは、システムにローカルに設定されたサブスクライバを使用することも、リモートのRADIUSサーバーに設定されたサブスクライバプロファイルを使用することもできます。

3GPPサービスでは、サブスクライバに対してAPN設定を使用してトラフィックポリシーを設定することもできます。

重要 3GPP では、RADIUS サーバーから受信したサービス属性が、APN の設定よりも優先されます。

重要 この項の設定例で使用されているコマンドは、最もよく使用されているコマンドまたはその可能性の高いコマンドや、キーワードオプションが提示される範囲で、基本機能を提供します。多くの場合は、他のオプションのコマンドやキーワードオプションを使用できます。すべてのコマンドの詳細については、『*Command Line Interface Reference*』を参照してください。

トラフィックシェーピングのサブスクライバの設定

このセクションでは、トラフィックシェーピングをサポートするように、システムでローカルサブスクライバ プロファイルを設定するための情報と手順について説明します。

重要 このドキュメントでは、RADIUSベースのサブスクライバプロファイルの設定手順は説明していません。詳細については、ご使用のサーバーに関するドキュメントを参照してください。

手順

ステップ 1 次の設定例を適用して、パラメータを設定します。

a) 指定した制限とアクションをダウンリンク（サブスクライバへのデータ）に適用するには、次を使用します。

```
configure
    context <context_name>
        subscriber name <user_name>
            qos traffic-shape direction downlink
            end
```

b) 指定した制限とアクションをアップリンク（サブスクライバへのデータ）に適用するには、次を使用します。

```
configure
    context <context_name>
        subscriber name <user_name>
            qos traffic-shape direction uplink
            end
```

注：

- **qos traffic-shape direction { downlink | uplink }** コマンドには、多数のキーワードオプションが関連付けられています。
- 設定対象となる追加のサブスクライバごとに繰り返します。

重要
超過/違反アクションが「low-ip-precedence」に設定されている場合、外部パケットの TOS 値は、サブスクライバ コンフィギュレーション モードでどの **ip user-datagram-tos-copy** コマンドが設定されているかに関わらず、トラフィック制限を超過/違反するパケットの「ベストエフォート」になります。さらに、「lower-ip-precedence」オプションは、**ip qos-dscp** コマンドの設定をオーバーライドする場合があります（サブスクライバコンフィギュレーションモードでも同様）。そのため、上記のオプションを指定するときはこのコマンドを使用しないことを推奨します。

ステップ 2 次の設定例を適用して、サブスクライバプロファイルの設定を確認します。

```
context <context_name>
    show subscriber configuration username <user_name>
```

ステップ 3 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイスや、ネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

3GPP ネットワークでのトラフィックシェーピング用の APN の設定

ここでは、トラフィックシェーピングをサポートする APN テンプレートの QoS プロファイルを設定するための情報と手順について説明します。

プロファイル情報は、GTP の PDP コンテキスト作成/更新要求メッセージへの応答で SGSN に送信されます。SGSN から要求された QoS プロファイルが、設定されている QoS プロファイルよりも小さい場合は、SGSN から要求されたプロファイルが使用されます。SGSN によって要求された QoS プロファイルの方が高い場合は、設定されたレートが使用されます。

認定データレートおよびピークデータレートのパラメータの値は、GGSN と SGSN の間の GTP メッセージで交換されます。そのため、使用される値は設定値よりも小さい場合があります。SGSN とレートをネゴシエートする際、システムはこのレートを GTP で許可されている値に変換します。以下の表を参照してください。

表 *136 : GTP* メッセージの認定データレートとピークデータレートの許容値

値（bps）	増分粒度（bps）
1000 ～ 63,000	1,000（たとえば、1000、2000、3000、... 63000）
64,000 ～ 568,000	8,000（たとえば、64000、72000、80000、... 568000）
576,000 ～ 8,640,000	64,000（たとえば、576000、640000、704000、... 8640
8,700,000 ～ 16,000,000	100,000 bps（たとえば、8700000、8800000、8900000 16000000）

手順

ステップ 1 次の設定例を適用して、パラメータを設定します。

a) 指定した制限とアクションをダウンリンク（サブスクライバへのデータ）に適用するには、次を使用します。

```
configure
    context context_name
        subscriber name user_name
            qos rate-limit downlink
            end
```

b) 指定した制限とアクションをアップリンク（サブスクライバへのデータ）に適用するには、次を使用します。

```
configure
    context context_name
        apn apn_name
            qos rate-limit uplink
            end
```

ステップ 2 次のコマンドを入力して、APN が正しく設定されていることを確認します。

```
show apn { all | name apn_name}
```

出力には、設定済みの APN パラメータの設定が簡潔にリストされています。

ステップ 3 Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

トラフィック シェーピングの設定

トラフィックシェーピングのサブスクライバの設定

このセクションでは、トラフィックシェーピングをサポートするように、システムでローカルサブスクライバ プロファイルを設定するための情報と手順について説明します。

重要 このドキュメントでは、RADIUS ベースのサブスクライバプロファイルの設定手順は説明していません。詳細については、ご使用のサーバーに関するドキュメントを参照してください。

手順

ステップ 1 次の設定例を適用して、パラメータを設定します。

a) 指定した制限とアクションをダウンリンク（サブスクライバへのデータ）に適用するには、次を使用します。

```
configure
    context <context_name>
        subscriber name <user_name>
            qos traffic-shape direction downlink
            end
```

b) 指定した制限とアクションをアップリンク（サブスクライバへのデータ）に適用するには、次を使用します。

```
configure
    context <context_name>
        subscriber name <user_name>
            qos traffic-shape direction uplink
            end
```

注：

- **qos traffic-shape direction { downlink | uplink }** コマンドには、多数のキーワードオプションが関連付けられています。
- 設定対象となる追加のサブスクライバごとに繰り返します。

重要
超過/違反アクションが「low-ip-precedence」に設定されている場合、外部パケットの TOS 値は、サブスクライバ コンフィギュレーション モードでどの **ip user-datagram-tos-copy** コマンドが設定されているかに関わらず、トラフィック制限を超過/違反するパケットの「ベストエフォート」になります。さらに、「lower-ip-precedence」オプションは、**ip qos-dscp** コマンドの設定をオーバーライドする場合があります（サブスクライバコンフィギュレーションモードでも同様）。そのため、上記のオプションを指定するときはこのコマンドを使用しないことを推奨します。

ステップ 2 次の設定例を適用して、サブスクライバプロファイルの設定を確認します。

```
context <context_name>
    show subscriber configuration username <user_name>
```

ステップ 3 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイスや、ネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

3GPP ネットワークでのトラフィックシェーピング用の APN の設定

ここでは、トラフィックシェーピングをサポートする APN テンプレートの QoS プロファイルを設定するための情報と手順について説明します。

プロファイル情報は、GTP の PDP コンテキスト作成/更新要求メッセージへの応答で SGSN に送信されます。SGSN から要求された QoS プロファイルが、設定されている QoS プロファイルよりも小さい場合は、SGSN から要求されたプロファイルが使用されます。SGSN によって要求された QoS プロファイルの方が高い場合は、設定されたレートが使用されます。

認定データレートおよびピークデータレートのパラメータの値は、GGSN と SGSN の間の GTP メッセージで交換されます。そのため、使用される値は設定値よりも小さい場合があります。SGSN とレートをネゴシエートする際、システムはこのレートを GTP で許可されている値に変換します。以下の表を参照してください。

表 *137 : GTP* メッセージの認定データレートとピークデータレートの許容値

値（**bps**）	増分粒度（**bps**）
1000 ～ 63,000	1,000（たとえば、1000、2000、3000、... 63000）
64,000 ～ 568,000	8,000（たとえば、64000、72000、80000、... 568000）
576,000 ～ 8,640,000	64,000（たとえば、576000、640000、704000、... 8640
8,700,000 ～ 16,000,000	100,000 bps（たとえば、8700000、8800000、8900000 16000000）

手順

ステップ 1 次の設定例を適用して、パラメータを設定します。

a) 指定した制限とアクションをダウンリンク（サブスクライバへのデータ）に適用するには、次を使用します。

```
configure
    context context_name
        subscriber name user_name
            qos rate-limit downlink
            end
```

b) 指定した制限とアクションをアップリンク（サブスクライバへのデータ）に適用するには、次を使用します。

```
configure
    context context_name
        apn apn_name
            qos rate-limit uplink
            end
```

ステップ 2 次のコマンドを入力して、APN が正しく設定されていることを確認します。

```
show apn { all | name apn_name}
```

出力には、設定済みの APN パラメータの設定が簡潔にリストされています。

ステップ 3 Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

RADIUS 属性

CDMA サブスクライバのトラフィックポリシング

次の表に記載されている RADIUS 属性は、リモート RADIUS サーバーに設定されている CDMA サブスクライバ（PDSN および HA）のトラフィックポリシングの設定に使用されます。これらの属性の詳細については、『*AAA Interface Administration and Reference*』を参照してください。

表 *138 : CDMA* サブスクライバのトラフィックポリシングのサポートに必要な *RADIUS* 属性

属性	説明
SN-QoS-Tp-Dnlk （または SN1-QoS-Tp-Dnlk）	ダウンリンク方向のトラフィックポリシングを有効ま 効にします。
SN-Tp-Dnlk-Committed-Data-Rate （または SN1-Tp-Dnlk-Committed-Data-Rate）	ダウンリンクの認定データ レートを bps 単位で指定し
SN-Tp-Dnlk-Peak-Data-Rate （または SN1-Tp-Dnlk-Committed-Data-Rate）	ダウンリンクのピークデータレートを bps 単位で指定し
SN-Tp-Dnlk-Burst-Size （または SN1-Tp-Dnlk-Burst-Size）	通常のバーストサイズをバイト単位で指定します。 **注**：このパラメータには、次の 2 つのうち大きい方の 定する必要があります。1）サブスクライバ接続のパ MTU の 3 倍。2）設定されたピークデータレートの「 ト」内での 3 秒のトークン蓄積 。
SN-Tp-Dnlk-Exceed-Action （または SN1-Tp-Dnlk-Exceed-Action）	実行するダウンリンク超過アクションを指定します。
SN-Tp-Dnlk-Violate-Action （または SN1-Tp-Dnlk-Violate-Action）	実行するダウンリンク違反アクションを指定します。
SN-QoS-Tp-Uplk （または SN1-QoS-Tp-Uplk）	ダウンリンク方向のトラフィックポリシングを有効ま 効にします。
SN-Tp-Uplk-Committed-Data-Rate （または SN1-Tp-Uplk-Committed-Data-Rate）	アップリンクの認定データレートを bps 単位で指定し
SN-Tp-Uplk-Peak-Data-Rate （または SN1-Tp-Uplk-Committed-Data-Rate）	アップリンクのピークデータレートを bps 単位で指定し
SN-Tp-Uplk-Burst-Size （または SN1-Tp-Uplk-Burst-Size）	アップリンクのバーストサイズをバイト単位で指定し （注） このパラメータには、次の 2 つのうち大きい方の値に る必要があります。1）サブスクライバ接続のパケッ の 3 倍。2）設定されたピークデータレートの「バケ 内での 3 秒のトークン蓄積。
SN-Tp-Uplk-Exceed-Action （または SN1-Tp-Uplk-Exceed-Action）	実行するアップリンク超過アクションを指定します。

属性	説明
SN-Tp-Uplk-Violate-Action （または SN1-Tp-Uplk-Violate-Action）	実行するアップリンク違反アクションを指定しま

UMTS サブスクライバのトラフィックポリシング

次の表に記載されている RADIUS 属性は、リモート RADIUS サーバーに設定されている UMTS サブスクライバのトラフィックポリシングの設定に使用されます。これらの属性の詳細については、『*AAA Interface Administration and Reference*』を参照してください。

表 *139 : UMTS* サブスクライバのトラフィックポリシングのサポートに必要な *RADIUS* 属性

属性	説明
SN QoS カンバセーションクラス （または SN1 QoS カンバセーションクラス）	QoS カンバセーション トラフィック クラスを指定
SN QoS ストリーミングクラス （または SN1 QoS ストリーミングクラス）	QoS ストリーミング トラフィック クラスを指定し
SN QoS 対話型 1 クラス （または SN1 QoS 対話型 1 クラス）	QoS 対話型トラフィッククラスを指定します。
SN QoS 対話型 2 クラス （または SN1 QoS 対話型 2 クラス）	QoS 対話型 2 トラフィッククラスを指定します。
SN QoS 対話型 3 クラス （または SN1 QoS 対話型 3 クラス）	QoS 対話型 3 トラフィッククラスを指定します。
SN QoS バックグラウンドクラス （または SN1 QoS バックグラウンドクラス）	QoS バックグラウンド トラフィック クラスを指定
SN QoS トラフィックポリシー （または SN1 QoS トラフィックポリシー）	この複合属性により、RADIUS サーバーからのトラ クラス（上記の属性）、方向、バーストサイズ、許 レート、ピークデータレート、超過アクション、お アクションの QoS 値の送信が簡素化されます。 この属性は、さまざまなトラフィッククラスで複数 きます。クラスを 0 に設定すると、すべてのトラフ ラスに適用されます。



第 104 章

事前に定義されたルールのサービスタイプ/トラフィッククラス設定

- 機能の概要と変更履歴 （1487 ページ）
- 機能説明 （1488 ページ）
- 機能の仕組み （1488 ページ）
- 事前設定されたルールに対応する TOS/トラフィッククラスの設定 （1490 ページ）
- モニタリングおよびトラブルシューティング （1490 ページ）

機能の概要と変更履歴

要約データ

該当製品および機能エリア	• GGSN • P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC - DI • VPC - SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *GGSN Administration Guide* • *P-GW Administration Guide* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入	21.3

機能説明

トラフィック フローテンプレート（TFT）は、パケットデータプロトコル（PDP）コンテキストのパラメータと操作を指定する情報要素です。この情報要素は、追加のパラメータをネットワークに転送するために使用される場合があります（認証トークンなど。3GPP TS 24.229 [95] を参照）。TFTには、ダウンリンク方向、アップリンク方向、または両方向のパケットフィルタが含まれる場合があります。

これらのパケットフィルタにより、PDPコンテキストへのトラフィックマッピングが決定されます。理想的には、ネットワークではダウンリンク パケット フィルタが使用され、モバイルステーションではアップリンク パケット フィルタが使用されます。この動作は、両方向に適用されるパケットフィルタでも観察されます。

TFTは、最小長が3オクテットのタイプ4情報要素です。IEの最大長は257オクテットです。

現在、オペレータは、「タイプオブサービス(TOS)/トラフィッククラス」情報に基づいて、データトラフィックを識別しフィルタリングする必要があります。この情報は、事前定義ルールまたはダイナミックルール（あるいはその両方）の一環として設定する必要があります。また、オペレータは、ベアラー作成要求（CBR）およびベアラー更新要求（UBR）メッセージで、TFTの一部として「サービスタイプ（TOS）/トラフィッククラス」情報を送信します。この動作はローカルポリシーまたはPCRFを介してトリガーできます。

ダイナミックルールの場合、P-GWは、特定のデータトラフィックの識別に使用される「タイプオブサービス（TOS）/トラフィッククラス」情報をすでにサポートしています。ただし、定義済みルールの場合、パケットフィルタ設定の一環として「タイプオブサービス（TOS）/トラフィッククラス」情報を設定するオプションはありません。

この機能では、**ip tos-traffic-class** CLIが導入され、オペレータの要件に対応するために、課金アクションで設定されたパケットフィルタに対してタイプオブサービス（TOS）/トラフィッククラス情報を設定します。

機能の仕組み

新しいCLIでは、「タイプオブサービス（TOS）/トラフィッククラス」設定を使用して、事前定義ルールに関連付けられるパケットフィルタを設定します。該当する事前定義ルールは、ローカルポリシーを介して、またはPCRF通信の一部としてトリガーできます。

事前定義ルールで「タイプオブサービス（TOS）/トラフィッククラス」情報を設定するCLIシンタックスは、PCRFから動的ルールの一部として受信される「Type of Service (TOS)/Traffic Class」AVP情報に対応しています。

3GPPP 24.008 - セクション 10.5.6.12 によると、「タイプオブサービス/トラフィッククラスタイプ」の場合、パケット フィルタ コンポーネント値フィールドは、1 オクテットのタイプオブサービス/トラフィック クラス フィールドと、1 オクテットのタイプオブサービス/トラフィック クラス マスク フィールドのシーケンスとしてエンコードされます。タイプオブサービス/トラフィック クラス フィールドが最初に送信されます。

次に例を示します。

```
toS/traffic class: 0x20 0xff
```

また、P-GW は、TFT IE に、ベアラー作成要求（CBR）およびベアラー更新要求（UBR）メッセージの一部として、両方の「タイプオブサービス（TOS）/トラフィッククラス」情報を含めるようになりました（3GPP 29.212 セクション 5.3.14 に準拠）。



重要

- この CLI は、TOS/トラフィッククラス情報を設定するために、「パケットフィルタ」設定モードで追加されます。
- ピアに対するベアラー作成要求またはベアラー更新要求をトリガーする際に、そのベアラーに関連付けられている事前定義ルールが「タイプオブサービス (TOS)」で設定されている場合、P-GW は、TFT IE に「タイプオブサービス（TOS）/トラフィッククラス」情報を入力します。
- セッションマネージャ リカバリまたは ICSR は、既存のベアラーパケットフィルタ情報に影響しません。

制限事項

この機能には次の制限があります。

- 通信事業者は TOS とともにマスクを設定する必要があり、TOS 値とマスクにはデフォルト値はありません。
- パケットフィルタでの「Type of Service（TOS）/トラフィッククラス」設定の変更については、動作は他のパケットフィルタパラメータ設定の変更の場合と同様です。
- 現在の PGW/GGSN/SAEGW の動作は、以下のとおりです。異なるベアラーにインストールされた事前定義ルールで、あるベアラーのアップリンクトラフィックと別のベアラーのダウンリンクトラフィックに ToS/トラフィッククラスが設定されている場合、同じフローのアップリンクとダウンリンクのパケットはそれぞれ異なるベアラーを通過します。ただし、ToS/トラフィッククラスが設定されたこれらの事前定義ルールがその場で削除されても、同じフローのアップリンクとダウンリンクパケットは引き続き異なるベアラーを通過します。
- 事前定義されたルールを含んでインストールされた 2 つの専用ベアラーが存在するシナリオを考えます。特定の ToS/トラフィッククラス（t1 とします）を持つアップリンクトラフィックが最初の専用ベアラーに一致し、別の ToS/トラフィッククラス（t2 とします）を持つダウンリンクトラフィックがダウンリンクトラフィックに一致するというものです。

IP ToS/トラフィッククラス CLI が対応する事前定義ルールで無効になった後に SESSMGR が再起動した場合、ToS/トラフィッククラスが t2 のダウンリンクパケットは、このダウンリンクパケットの前に受信した同じフロー（送信元 IP、送信元ポート、宛先 IP、宛先ポート）のアップリンクパケットがある場合、2 番目ではなく最初の専用ベアラーを通過します。

事前設定されたルールに対応するTOS/トラフィッククラスの設定

次のセクションでは、この機能を有効または無効にするための設定コマンドについて説明します。

ip tos-traffic-class コマンドの有効化または無効化

変更されたコマンド **ip tos-traffic-class** は、パケットフィルタモードの課金アクションで ToS/トラフィッククラスを設定するために使用されます。

デフォルトでは、この CLI は無効になっています。

この機能を有効または無効にするには、以下のコマンドを入力します。

```
configure
  active-charging service service_name
    packet-filter packet_filter
      [ no ] ip tos-traffic-class { type_of_service | traffic class }
mask { mask_value }
      end
```

注：

- **no** ：以前に設定されている場合、課金アクションでの ToS/トラフィッククラスを削除します。
- **tos-traffic-class** = { *type_of_service* | *traffic class* }：トラフィックのフィルタリングに使用されるタイプオブサービス（TOS）/トラフィッククラス（Traffic Class）の値を指定します。0 ～ 255 の整数を入力します。
- **mask** [*mask_value*]：スイッチオーバー後の自動回復用のダイナミックルールを検証します。0 ～ 255 の整数を入力します。

モニタリングおよびトラブルシューティング

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

コマンドの表示

ここでは、この機能をモニターするために使用できるすべての show コマンドについて説明します。

show configuration

このコマンドは、以下の出力を表示するように変更されました。

```
show configuration
configure
   active-charging service acs
    packet-filter PF226
      ip protocol = 6
      ip remote-port = 226
      ip  tos-traffic-class = 32 mask = 255
      exit
```

show active-charging packet-filter

このコマンドは、以下の出力を表示するように変更されました。

ToS/トラフィッククラスが有効/設定されている場合：

```
show active-charging packet-filter { all | name }
Service Name: acs

   Packet Filter Name: abcd
      IP Proto: 6
     Local Port: Not configured
     Remote Port: 226
     Remote IP Address: Not configured
     Direction: Bi-Directional
     Priority: None
    Tos-traffic-class: 32
    Tos-traffic-class-mask: 255
```

ToS/トラフィッククラスが無効/未設定の場合：

```
show active-charging packet-filter { all | name }

Service Name: acs

   Packet Filter Name: abcd
      IP Proto: 6
     Local Port: Not configured
     Remote Port: 226
     Remote IP Address: Not configured
     Direction: Bi-Directional
     Priority: None
    Tos-traffic-class: Not configured
    Tos-traffic-class-mask: Not configured
```

ユーザーが[supportrecord]セクションを指定していない場合は、showconfigurationverbose

このコマンドは、以下の出力を表示するように変更されました。

ToS/トラフィッククラスが有効/設定されている場合：

```
show configuration verbose
configure
   active-charging service acs
    packet-filter PF226
      ip protocol = 6
      ip remote-port = 226
      ip  tos-traffic-class = 32 mask = 255
      ---
      exit
```

ToS/トラフィッククラスが無効/未設定の場合：

```
show configuration verbose
configure
   active-charging service acs
    packet-filter PF226
      ip protocol = 6
      ip remote-port = 226
      no ip   tos-traffic-class
      ---
     exit
```



第 105 章

UE 過負荷防止

- 機能の概要と変更履歴 （1493 ページ）
- 機能説明 （1494 ページ）
- 機能の仕組み （1495 ページ）
- 制限事項 （1496 ページ）
- ue-overload-control-profile の設定 （1496 ページ）
- ue-overload 基準の設定 （1497 ページ）
- モニタリングおよびトラブルシューティング （1498 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	ASR 5500
デフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.22

機能説明

UE 過負荷保護機能は、システム帯域幅、チャネルドロップレート、SM CPU、SM メモリ、および VPP CPU のリソース使用状況をモニターするためのメカニズムを提供します。リソースが設定されたしきい値を超えると、識別された特定の UE が影響を受けます。たとえば、グローバルなシステム帯域幅リソースが設定されたしきい値を超えると、この機能が有効になっているシステム全体の UE が影響を受けます。残りのリソースは、CPU コンプレックスに対してローカルであると見なされます。

現在、P-GW は、トラフィックの管理またはスロットリングをサポートしており、UE 過負荷保護機能の一部として次の機能を備えています。

- P-GW に対するサブスクライバの影響の識別
- P-GW に対するサブスクライバの影響に関するしきい値または条件の設定
- しきい値を超過した 1 つまたは複数のサブスクライバをスロットリングすることによって、これらのしきい値に応答を送信する

UE 過負荷保護機能は、DPC2 カードを搭載した VPP 対応 ASR 5500 およびその他のプラットフォームでのみ動作します。しきい値処理は、Demux カードではない DPC2 カード（最大 6 枚の DPC2 カード）にのみ適用されます。CLI を使用して、この機能をグローバルに設定できるようになりました。次の機能がサポートされています。

- UE 過負荷制御プロファイルの設定。
- PCRF で管理：セッション確立中に受信した AVP に基づいて、各サブスクライバの *UE* 過負荷保護機能を有効または無効にします。
- しきい値に達した場合の設定アクションを指定できます。過負荷条件が持続するようになるまで、APN-AMBR-DL と APN-AMBR-UL を一時的に調整できます。セッションマネージャの再起動、カードの移行、および ICSR が発生した場合、UE に適用されている UE 過負荷 APN AMBR UL/DL の値は元の値に戻ります。

（注） UE セッションがスロットリング中の場合、新しい APN_AMBR 値が現在適用されている値よりも小さいと、APN-AMBR 値はすぐに変更されます。そうでなければ、値は高速パスでプログラムされず、しきい値が緩和されると適用されます。

- リソースマネージャから定期的に負荷条件（VPP 負荷を含む）を受信し、セッションマネージャで過負荷条件を設定するようにプロビジョニングできます。
- **show status**：システムの負荷を最適化するために、**show status** コマンドは、システム全体の基準とともに、最大 18 レコードの最新のステータスを表示するように構成されています。システムの基準が低優先順位基準として満たされている場合でも、コンプレックス全

体の高優先順位は、コンプレックスレベルのしきい値超過に基づいて、すべてのコンプレックスレベルをオーバーライドできます。**show status** で次の結果を表示できます。

- すべての「満たされた」パラメータ（1つのしきい値パラメータが原因でCPUコンプレックスがスロットル状態になっている場合、および他のしきい値パラメータがその同じ CPU コンプレックスで満たされている場合）。

  すべてのしきい値パラメータ（特定の設定済み基準内で複数のしきい値パラメータが満たされている場合）。

  システム帯域幅のしきい値が満たされている場合、そのしきい値は **show status** に別個の行（最後の行）として表示されます。システム帯域幅の**アクティブ化時間**は、CPU コンプレックスのアクティブ化時間のいずれかにすることができます。

機能の仕組み

StarOS では、すべてのセッションが複数のセッションマネージャに分散されます。デマルチプレクサマネージャは、CPUコンプレックスレベルでのリソース使用率収集の中心的な要素として機能します。5G の導入とともにネットワークトラフィック速度が増加すると、P-GW によりサブスクライバは、Demux マネージャを利用して、高速ダウンロード、ユーザー機器（UE）過負荷の検出または回復シナリオなど、ネットワークのパフォーマンスを管理できます。

UE 過負荷防止機能は、DPC2 カードベースアーキテクチャを対象として、これで動作するように設計された検出アルゴリズムで動作します。ただし、このアルゴリズムは各種ラインカードで機能します。次の表に、過負荷検出アルゴリズムの手順を示します。

表 *140 :* ワークフロー

ステップ	説明
1	CPU コンプレックスレベルでリソース情報を収集します。
2	CLI で、リソース使用率のしきい値を定義します。
3	プログラム可能なタイマー（時間は CLI を通じて提供される）が、その期限切れ時に検出アルゴリズムを実行し、上限しきい値に対して、その上限を超えたリソース使用率があるかどうかをチェックします。 • 超えた場合は、VPP スレッドまたはセッションマネージャのインスタンスの問題のあるユーザー部分をスキャンで特定し、一時的な **APN-AMBR-DL** および **APN-AMBR-UL** しきい値を適用します。 • それ以外の場合は、次のサイクルを待ちます。

ステップ	説明
4	リカバリアルゴリズムのループをチェックします。また、リソース使用率が CLI で設定された下限しきい値を下回っているかどうかを確認します。 条件を下回っている場合、**APN-AMBR-DL** および **APN-AMBR-UL** インスタンスをスキャンで特定し、元の **APN-AMBR-DL** および **APN-AMBR-UL** の値に置き換えます。
5	カウンタにインシデントを記録して統計を更新します。
6	条件が満たされたらタイムスタンプを適用し、ダンプニング期限をチェックするために使用されます。

制限事項

制限事項は次のとおりです。

- VPP 対応 ASR 5500 でのみ動作し、負荷モニタリングは DPC2 カードで実行されます。
- この機能の目的は、AMBR パラメータを介してユーザートラフィックをスロットリングすることによってシステムの負荷を軽減することであるため、通信事業者はセッションがスロットリングされるように対処する必要があります。
- 通信事業者は、リストに APN 名を入力する際に、APN の実際の名前を入力する必要があります。これは、システムで使用されている APN 名に関してこのリストでは検証がないためです。システムに存在しない APN 名を入力した場合、設定時にエラーが表示されません。エラーは **show config errors** コマンドで表示できます。

ue-overload-control-profile の設定

UE 過負荷機能は、UE 過負荷の設定後に発生する新しい UE セッションにのみ適用されます。有効な仮想 APN またはベース APN に対して UE 過負荷設定を有効にすると、既存の UE セッションを変更してこの機能を適用することはできなくなります。

ASR5500 で UE 過負荷制御プロファイル設定を構成するには、次のコマンドを使用します。

```
configure
    context context_name
     ue-overload-control-profile name
        end
```

注：

- **ue-overload-control-profile**：確認のプロンプトなしで新しい UE 過負荷制御プロファイルを作成します。

（注） UE 過負荷プロファイル、または適用された/アクティブな基準、または適用された/アクティブなアクションプロファイル、またはパラメータを削除すると、カード/CPU コンプレックスに適用されているしきい値がすぐに緩和されます。

設定の変更は、次回の *check-interval*でのみ有効になります。

ue-overload 基準の設定

ue-overload 基準を設定するには、次のコマンドを使用します。

```
configure
   context context_name
     ue-overload-control-profile overload-criteria  value
prioritypriority_value
        system
           bandwidth-thresholdvalue
           drop-rate-thresholdvalue
       exit
        sessmgr
           cpu-thresholdvalue
           memory-thresholdvalue
        exit
        vpp
           cpu-thresholdvalue
        exit
        overload action name
        exit
        apn name
           overload-actionname
           downlink-ambrvalue
           uplink-ambrvalue
        check-intervalseconds
        dampen-intervalseconds
       exit
```

注：

- **overload-criteria**：system、sessmgr、vpp パラメータの過負荷基準のしきい値と、基準の優先順位を設定します。

  overload-action：この過負荷基準に関連付けられた過負荷アクションを設定します。

- **sessmgr** ：さまざまな過負荷基準パラメータのセッションマネージャしきい値を設定します。

- **system** ：さまざまな過負荷基準パラメータのシステムしきい値を設定します。

- **vpp**：さまざまな過負荷基準パラメータの VPP しきい値を設定します。
- **apn**：この UE 過負荷制御プロファイルに適用する APN 名が含まれます。APN は、次の 2 つの方法で UE 過負荷設定に追加されます。
  - enable-by-default：**UEOVERLOAD** フィールドが Service-Feature AVP で有効になっている場合や、**UEOVERLOAD** フィールドまたは Service-Feature AVP が完全に欠落している場合は、UE 過負荷機能を UE セッションに適用できます。
  - enable-by-gx：**UEOVERLOAD** フィールドが Service-Feature AVP で有効になっている場合にのみ、UE 過負荷機能を UE セッションに適用できます。

check-interval：UE過負荷パラメータのモニタリング間隔（秒単位）を設定します。デフォルト値は 30 秒です。

- **dampen-interval** ：過負荷状態または通常状態になるようにシステムに対して定義される最小時間を設定します（秒単位）。デフォルト値は 300 秒です。
- **default** ：次のオプションに割り当てられているデフォルト値を復元します。
  - **do** ：管理者に情報を表示する EXEC モードコマンドを生成します。
  - **end**：コンフィギュレーション モードを終了し、EXEC モードに戻ります。
  - **exit**：現在のコンフィギュレーション モードを終了し、以前のモードに戻ります。
  - **no**：次のオプションを有効または無効にします。
    - **overload-criteria**：システム、セッションマネージャ、および VPP パラメータの過負荷基準のしきい値と、基準の優先順位を設定します。

モニタリングおよびトラブルシューティング

コマンドと出力の表示

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show ue-overload-control-profile

このコマンドの出力には、次のフィールドが含まれています。

フィールド	説明
すべて	すべての UE 過負荷制御プロファイルを表示します。
すべての	UE 過負荷制御プロファイルの詳細を表示します。
name：UE 過負荷制御プロファイル名を表示します。	

フィールド	説明
ステータス	UE 過負荷制御プロファイルの現在のステータスを表示します。
APN List	UE過負荷制御プロファイルで設定されているAPNリストを表示します。

show ue-overload-action

このコマンドの出力には、次のフィールドが含まれています。

フィールド	説明
ue-overload-action	すべてのUE過負荷アクション情報または基準とその統計を表示します。
統計	そのアクティブ化以降にUEに適用された基準に関する収集された情報の合計を表示します。

show ue-overload-control-profile name

このコマンドの出力には、次のフィールドが含まれています。

フィールド	説明
UE 過負荷制御プロファイル	
Profile Name	UE 過負荷制御プロファイルの名前を表示します。
ステータス	UE 過負荷制御プロファイルの現在のステータスを表示します。

show ue-overload-profile full all

このコマンドの出力には、次のフィールドが含まれています。

フィールド	説明
UE 過負荷制御プロファイル	
UE 過負荷制御プロファイル名	UE 過負荷制御プロファイルの名前を表示します。
過負荷基準	
名前	過負荷基準の名前を表示します。
優先順位	UE 過負荷プロファイルの優先順位を表示します。

フィールド	説明
システム	さまざまな過負荷基準パラメータのシステムしきい値を表示します。
Sessmgr	さまざまな過負荷基準パラメータのセッションマネージャしきい値を表示します。パーセンテージは0～100の整数である必要があります。
vpp	VPPのCPU使用率しきい値をパーセンテージで表示します。
帯域幅のしきい値	システム帯域幅のしきい値をパーセンテージで表示します。
ドロップ率のしきい値	システムのドロップ率を pps 単位で表示します。
cpu threshold	セッションマネージャ CPU のしきい値をパーセンテージで表示します。
メモリのしきい値	セッションマネージャメモリのしきい値をパーセンテージで表示します。
過負荷アクション	関連するUE過負荷アクションプロファイルを表示します。
APN	
デフォルトで有効	デフォルトで有効になっているすべてのAPNを表示します。
Gx で有効	Gxインターフェイスで有効になっているすべてのAPNを表示します。
Check-interval：チェック間隔を秒単位で表示します。**check-interval** は 15 ～ 300 秒の整数である必要があります。	
dumpen-interval：ダンプ間隔を秒単位で表示します。**dampen-interval** は 30 ～ 3000 秒の整数である必要があります。	

show ue-overload-action statistics full

システム負荷を最適化するために、統計エントリは7レコードに制限されています（複合レベル用に6つ、システム全体用に1つ）。システム全体の統計エントリは、常に最後の行として表示されます。

このコマンドの出力には、次のフィールドが含まれています。

フィールド	説明
Profile-name：UE 過負荷プロファイルの名前を表示します。 （注） UE 過負荷プロファイルが削除された場合、またはSAEGW サービスから関連付けが削除された場合、収集された統計はすべて消去されます。	

フィールド	説明
Criteria Name (Priority)	過負荷基準の名前と優先順位を表示します。 （注） 特定の基準で、複数のしきい値がシステム帯域幅とともに満たされる場合は、しきい値を緩和した後に、統計がシステム帯域幅エントリの一部として収集されます。
Activation Time	過負荷基準のアクティブ化時間。 （注） EGTPMGR リカバリ後に収集された統計の場合、**Activation Time** は空白として表示されます。
Activation Duration	過負荷基準がアクティブであった期間。 （注） EGTPMGR リカバリ後に収集された統計の場合、**Activation Duration** は空白として表示されます。
No.of Impacted UEs	一時的な UL-AMBR 値が適用されている UE の数を表示します。
Total UEs	カード/CPU 複合体上の UE の合計数を表示します。 （注） **Total UEs** エントリが **No.of Impacted UEs** よりも少ない場合、しきい値を超えると、カード/CPU 複合体で統計が収集されるため、一部の UE セッションがダウンする可能性があります。
Card/CPU	特定の基準がアクティブであったカード/CPU 複合体。システム全体の過負荷アクション基準がある場合は、**SYSTEM** と表示されます。 カード/CPU 複合体で UE セッションがスロットリングされていない場合は、カード/CPU 複合体が、設定されているしきい値パラメータのいずれかを超えていても、UE セッションのエントリは統計に表示されません。

show configuration bulkstats

次の例は、バルク統計サーバーの設定を示しています。

```
config
  bulkstats collection
  bulkstats historical collection
  bulkstats mode
    sample-interval 1
    transfer-interval 2
    file 1
      remotefile format data/bulkstats/%host%-%date%-%time%.csv
```

```
      receiver 10.105.84.124 primary mechanism ftp login root encrypted password
+B3qmvomy0b fenh0p6bitcxn3lfs19 febnhcv66ry0uocxu3s2zrze0zompd le3gc7d2bjdm
199d61ny1360gwn1 zr8332rg vnjsjvanb4
    #exit
    file 2
      header format UE-AMBR-drop-stats
      remotefile format data/bulkstats/%host%-%date%-%time%.csv
      receiver 10.105.84.124 primary mechanism ftp login root encrypted password +B0nu
axjhro0b lg2lspsbf12eupo2cxv6ljisgtxb01ap 2239iddb925p69epd in6cc05jm1v96b59uz0moxiz1gsk9qx
 3ijqpsossxi89
    #exit
    file 3
      header format UE-Overload-drop-stats
      remotefile format data/bulkstats/%host%-%date%-%time%.csv
      receiver 10.105.84.124 primary mechanism ftp lo gin root encrypted password
+B3iw43muh3b2j62d9ib6t2jo50232r3dt9ih97iq1ga70qh7r0cbq2a0z j68wpxki22fn9b2t
9i69td06rq782uc83vs2xlfi96h64bi3
      saegw schema ueoverload-stats format
Server1,pgw-apnambrratelimit-ulpktdrop:%pgw-apnambrratelimit-ulpktdrop%,pgw-apnambrratelimit-dlpktdrop:
 %pgw-apnambrratelimit-dlpktdrop%, pgw-apnambrratelimit-ulbytedrop:%pgw-apnambr
ratelimit-ulbytedrop%,
       pgw-apn ambrratelimit-dlbytedrop:%pgw-apn ambrratelimit-
dlbytedrop%,pgw-ueoverload-apnambrratelimit-ulpktdrop:%pgw-ueoverload-apnambrratelimit-ulpktdrop%,
 pgw-ueoverload-apnambrratelimit-dlpktdrop: %pgw-ueoverload-apnambr ratelimit-dlpktdrop%,

       pgw-ueov erload-apnamb rratelimit-ulbytedrop:% pgw-ueoverload-
apnambrratelimit-ulbytedrop%,pgw- ueoverload-apnambrratelimit-dlbytedrop:
%pgw-ueoverload-apnambrratelimit-dlbytedrop%
    #exit
  #exit
end
```

サーバーでのバルク統計出力

```
UE-Overload-drop-stats
Server1,pgw-apnambr ratelimit-ulpktdrop:11060, pgw-apnambrr
atelimit-dlpktdrop:14231,pgw-apnambrra telimit-ulbytedrop:888455,
pgw-apnambrratelimit-dlbytedrop:14965964,
pgw-ueoverload-apnamb rratelimit-ulpktdrop:11060,pgw-ueov erload-apnam br
ratelimit-dlpktdrop:14231,pgw-ueover load-apnambrratelimit-ulbytedrop:888455,
pgw-ueoverload-apnambrratelimit-dl bytedrop:14965964
```

show saegw-service all

次の例は、SAEGW サービスの UE 過負荷制御プロファイルの結果を示しています。

```
Service name                    : SAEGW21
  Service-Id                    : 12
  Context                       : EPC2
  Status                        : STARTED
  sgw-service                   : SGW21
  pgw-service                   : PGW21
  sx-service                    : Not defined
  User Plane Tunnel GTPU Service : Not defined
  Ue Overload Control Profile   : prof-1
  Newcall policy                : n/a
  downlink-dscp-per-call-type   : n/a
  CUPS Enabled                  : No
```



第 106 章

課金ギャップを解消するためのベアラー変更要求の強化

- 機能の概要と変更履歴 （1503 ページ）
- 機能説明 （1504 ページ）
- 機能の仕組み （1504 ページ）
- default-bearer-rule-removal の保留の有効化 （1505 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	P-GW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、P-GW は課金の不一致を回避するためのルール削除遅延ポリシーをサポートしています。	21.22

機能説明

デフォルトベアラーの Quality of Service クラスインデックス（QCI）の変更を含む **charging-rule-install** および **charging-rule-remove** 属性値ペア（AVP）を持つ再承認要求（RAR）を P-GW で受信すると、P-GW は古いダイナミック課金ルールを削除し、ベアラー更新要求をトリガーします。ベアラー更新要求を受信した場合にのみ、新しいルールが適用されます。これにより、デフォルトのベアラーに関連付けられているポリシーがない期間の課金に矛盾が生じます。

StarOS 21.22 以降のリリースでは、課金の矛盾を回避するために、上記のケースでは、ベアラー更新要求が受信されるまで、ルールの削除が延期されます。この新しいルール削除遅延ポリシーは、QOS パラメータ（QCI、GBR、MBR、または ARP）が変更され、**charging-rule-install** および **charging-rule-remove** の上記の条件が満たされたデフォルトベアラーにのみ適用されます。

機能の仕組み

課金ルール削除ポリシーは、RAR を受信した直後ではなく、ベアラー更新応答の受信後に適用されます。この変更は CLI 設定によってサポートされており、次の機能が発生します。

1. RAR またはクレジット制御応答更新は、Rule1 のルール削除、デフォルトのベアラー QCI 更新、および Rule2 のルールインストールとともに P-GW によって受信されます。
2. ACS マネージャは、次のことを確認します。
   - 遅延ルール削除ポリシーをチェックします。
   - デフォルトベアラーの QoS 変更とデフォルトベアラーのルール削除があるかどうかをチェックします。
   - ベアラー更新要求応答を受信した後、保存されているポリシーを削除します。
3. ベアラー更新要求に対して正しい QCI、MBR、および GBR 値が送信されているかどうかを確認します。また、正しいデフォルトベアラー QoS がベアラーに反映されているかどうかも確認します。
4. ベアラー更新応答が受信されない場合は、次の操作を実行します。
   - 遅延ルールの削除をキャンセルする場合は、タイムアウト処理を実行します。
   - 復元された正しいベアラー QoS を検証します。

default-bearer-rule-removal の保留の有効化

デフォルトのベアラールール削除ポリシーを有効または無効にするには、次の設定コマンドを使用します。

```
configure
   active-charging service service_name
     [no] policy-controldefer default-bearer-rule-removal
    end
```

注：

- **active-charging service**：課金アクションは、ルール定義が一致したときに実行するアクションを定義します。
- **no**：動的ルール削除の保留を無効にします。
- **defer default-bearer-rule-removal**：ベアラー更新応答またはタイムアウトまで、デフォルトのベアラーからのルールの削除を延期します。



第 107 章

VPP メトリックの拡張

- 機能の概要と変更履歴 （1507 ページ）
- 機能説明 （1508 ページ）
- 機能の仕組み （1509 ページ）
- ロギングの有効化または無効化 （1510 ページ）
- メトリック収集の設定 （1511 ページ）
- モニタリングおよびトラブルシューティング （1511 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	• P-GW • SAEGW
該当プラットフォーム	• ASR 5500 • VPC-DI • VPC-SI
機能のデフォルト	• 無効：設定が必要 • 有効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	• *Command Line Interface Reference* • *P-GW Administration Guide* • *Statistics and Counters Reference* • *SAEGW Administration Guide*

マニュアルの変更履歴

改訂の詳細	リリース
show active-charging flows full debug-info all コマンドが拡張され、VPP とセッションマネージャ間のタイムスタンプの精度が表示されるようになりました。	21.27
show active-charging flows full all コマンドと **show active-charging flows summary** コマンドが拡張され、VPP から統計を取得できるようになりました。	21.26
P-GW が拡張され、ログメッセージを収集して、VPP とセッションマネージャ間のフロートランザクションのオフロードおよびオンロードを監視するようになりました。	21.26
次の拡張機能が導入されました。 • アナライザレベルの統計（TCP、UDP、P2P、HTTP、HTTPS） • CLI 設定を使用した VPP 統計の収集	21.25
最初の導入。	21.24

機能説明

ベクトルパケット処理（VPP）メトリックは、VPP オフロードトラフィックの分析とデバッグに役立ちます。この機能は、VPP をサポートするプラットフォームにのみ適用されます。

トラフィックフローは、P-GW がそれを認識する方法に基づいて、さまざまな方法で処理されます。たとえば、一部のフローは VPP で管理されますが、一部は管理されません。障害対応を強化するために、VPP フローのルールベース、サブスクライバ、およびアナライザプロトコルの各レベルで統計情報が追加されています。サポートされているアナライザプロトコルには、Transmission Control Protocol（TCP）、User Datagram Protocol（UDP）、ピアツーピア（P2P）アナライザ、Hypertext Transfer Protocol（HTTP）、および Hypertext Transfer Protocol Secure（HTTPS）が含まれています。システムレベルのバルク統計が、障害対応のためにサポートされています。

この機能は、active-charging サービスの設定によって部分的に制御されます。VPP オフロードに関連するサブスクライバ固有の統計情報のみが CLI を使用して制御されます。

VPP フロー統計

show active-charging flows full コマンドが拡張され、VPP からフローごとの情報を受信できるようになりました。このコマンドは、VPP ストリームからフローへのマッピング情報を表示します。

show active-charging flows full および **show active-charging flows summary** コマンドは、次のフィルタをサポートしています。

- imsi
- ip-address
- msisdn
- username
- callerid
- flow-id
- session-id
- インスタンス



（注） アイドルフロータイマーが期限切れになると、アイドルフローカウンタがインクリメントされます。フローがクリアされると、カウンタがクリアされ、アイドル状態にある特定のフローがあるかどうか短期間観察されます。

VPP フロートランザクションのオフロードとオンロードのモニタリング

P-GW が拡張され、ログメッセージを収集して、VPP とセッションマネージャ間のフロートランザクションのオフロードおよびオンロードを監視するようになりました。ログは、トラフィックの状態がオフロードからオンロードに、またはその逆に変化したときに収集されます。ログはファイルに保存されます。サポートされている CLI を使用して、モニタリングを有効または無効にすることができます。

タイムスタンプの精度の向上

データパケットがオフロードされると、最後に到着したパケットから計算されたティックは、セッションマネージャの Starent Network Transmission（SNX）グローバルティックタイムよりも遅れが生じます。これにより、VPP とセッションマネージャの間で時刻が同期されなくなります。フロータイムアウトが誤って推定されるため、フローがセッションから削除されます。

show active-charging flows full debug-info all コマンドが拡張され、正しいフローアイドルタイムアウトが表示されるようになりました。

機能の仕組み

P-GW は、トラフィックの VPP へのオフロード、sessmgr へのオンロードを監視するユーザー制御メカニズムをサポートし、監視対象期間のトラフィック統計情報を収集します。この機能を有効にすると、ログは */tmp/fpflowchangelog_2021-11-24_02h35m44sEST_1.csv* に保存されます。ロギングを無効にすると、ログファイルは */hd-raid/fpflowchangelog/fpflowchangelog_2021-12-16_04h06m55sEST_1.csv* に移動します。ログ数

が 32K を超えると、ログファイルは閉じて */hd-raid/fpflowchangelog/fpflowchangelog_2021-12-16_04h06m55sEST_2.csv* に移動します。次に、新しいファイルがインデックスローテーション形式で作成されます。たとえば、*_2.csv* のような番号が増分され、現在のスタンプで */tmp/fpflowchangelog_2021-11-24_02h35m44sEST* に保存されます。ただし、ロギングは通常どおり行われ、ログは新しいファイルに書き込まれます。

ロギングの有効化または無効化

ログは次の形式でファイルに保存されます。

```
Timestamp,IMSI, Session-ID, Stream-Idx, Client-IP, Client-Port, Server-IP, Server-Port,
 Protocol, Trigger-Type, Trigger-Reason
```

オフロードとオンロードのロギングを有効または無効にするには、Exec モードで次の CLI コマンドを使用します。モニタリングは、デフォルトでは無効に設定されています。

logging session fp-flow-state-change facility sessmgr instance *instance_number* **number-of-events** *events_value*

logging session fp-flow-state-change facility sessmgr instance *instance_number* **duration** *duration_value*

このコマンドを有効にすると、次に示すような警告メッセージが表示されます。

警告 フロー状態変更のロギングファシリティが有効になりました。ログは /hd-raid/fpflowchangelog/fpflowchangelog_2021-12-16_04h06m55sEST_1.csv に書き込む必要があります。警告：フロー状態変更のロギングは、パフォーマンスに影響を与える可能性があるため、慎重に使用してください。

このコマンドを実行したときにロギングがすでに有効になっている場合は、次のメッセージが表示されます。

```
[local]laas-setup# logging session fp-flow-state-change facility sessmgr instance 8
duration 10
Flow state change event logging is already enabled. Disable before enabling.
```

```
[local]laas-setup# logging session fp-flow-state-change facility sessmgr instance 12
duration 10
Error in flow stream state change logging enable. Invalid parameter.
```

（注） **number-of-events** の設定値に達するか、秒単位の期間が経過すると、この機能は自動的に無効になります。

イベントロギングは、他の機能またはモジュールのログとは独立して有効にする必要があります。

メトリック収集の設定

VPPからのサブスクライバやルールベースのメトリック収集を有効または無効にするには、次の設定例に示すコマンドを使用します。

```
configure
  active-charging service service_name
    [ no ] statistics-collection { all | vpp }
    end
```

注：

- **all**：Ruledef と VPP の両方の統計収集を設定します。
- **vpp**：VPP の統計収集を設定します。
- **no**：シード時間の値をデフォルト値の 0 にリセットします。
- デフォルトでは、この CLI は無効になっています。

モニタリングおよびトラブルシューティング

ここでは、showコマンドとバルク統計を使用した、この機能のモニタリングとトラブルシューティングの方法について説明します。

コマンドと出力の表示

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show active-charging flows full

表 *141 : show active-charging flows full* コマンド出力の説明

フィールド	説明
FP-Stream-ID (Up)	アップリンクパケットの fastpath ストリーム ID を示します。
FP-Stream-State (Up)	アップリンクパケットの fastpath ストリーム状態を示します。
FP-Stream-ID (Down)	ダウンリンクパケットの fastpath ストリーム ID を示します。
FP-Stream-State (Down)	ダウンリンクパケットの fastpath ストリーム状態を示します。
FP-Client-ID	VPP fastpath クライアント ID を示します。
Offload-Stream-at-packet (up)	アップリンクトラフィックの開始時に、セッションマネージャから VPP にオフロードされるストリームのパケット番号を示します。

フィールド	説明
Offload-Stream-at-packet (Down)	ダウンリンクトラフィックの開始時に、セッションマネージャから VPP にオフロードされるストリームのパケット番号を示します。
VPP FP UL Packets	アップリンクパケットの VPP 数を示します。
VPP FP UL Bytes	アップリンクバイトの VPP 数を示します。
VPP FP DL Packets	ダウンリンクパケットの VPP 数を示します。
VPP FP DL Bytes	ダウンリンクバイトの VPP 数を示します。
VPP FP Packets	オフロードされた合計 fastpath パケット数を示します。
VPP FP Dropped Packets	VPP によってドロップされたパケット数を示します
VPP Onload Succeeded	VPP から（セッションマネージャに）オンロードされた合計パケット数を示します。
Flow-ID	フローの識別子です。
Session-ID	ACS セッションの識別子です。
Uplink Packets	アップリンクパケットの合計数です。
Uplink Bytes	アップリンクバイトの合計数です。
Downlink Packets	ダウンリンクパケットの合計数です。
Downlink Bytes	ダウンリンクバイトの合計数です。
FP Packets	このフローの fastpath で処理されるデータパケット数です。
MS IP	MS IP アドレスです。
MS NAT IP	MS NAT IP アドレスです。
サーバ IP（Server IP）	サーバーの IP アドレスです。
トランスポートプロトコル	トランスポートプロトコル（TCP、UDP、ICMP）です
アプリケーション プロトコル	アプリケーションプロトコルです。
Video Pacing	ビデオペーシングが有効か無効かを示します。
Video Encoded Bit Rate	ビデオペーシングに現在適用されているビットレートです。
Video Pacing Initial Burst Size	ビデオペーシング中に許可される初期バーストサイズ（バイト単位）です。
Video Pacing Normal Burst Size	ビデオペーシング中に許可される通常バーストサイズ（バイト単位）です。
Video Pacing Dropped Bytes	ビデオペーシング中にドロップされたデータバイト数です。

フィールド	説明
Video Payload Bytes Sent towards User	ビデオペーシング中に UE に送信されたデータバイト数です。
Video Pacing Duration	ビデオペーシングの合計秒数です。
TCP MS Port	TCP MS ポート番号です。
TCP MS NAT Port	TCP MS NAT ポート番号です。 このフィールドは、1 対 1 NAT の場合は表示されません。
TCP Server Port	TCP サーバーのポート番号です。
TCP State	TCP の状態を示します。
TCP Prev State	以前の TCP の状態を示します。
MS Window Size	モバイルでのウィンドウサイズです。
Server Window Size	サーバーでのウィンドウサイズです。
MS Retries	モバイルサブスクライバの合計試行回数です。
Server Retries	サーバーの合計試行回数です。
ITC Action Applied	ITC アクションが適用されていることを示します。
Throttle-Suppress Countdown	フローがスロットル抑制されているときに設定されているタイムアウト（経過時間）を表示します。
Throttle-Suppress	スロットル抑制が非アクティブの場合、「n/a」と表示されます。
Socket Migration Details:	TCP プロキシソケットの移行に関連する情報です。
都道府県	フローのソケット移行状態を示します。 たとえば、SOCK_MIG_DONE と表示されます。
Highest ACK Frm Server	サーバーからの最大確認応答番号です。
Highest Seq Frm Server	サーバーからの最大シーケンス番号です。
Highest ACK Frm MS	MS からの最大確認応答番号です。
Highest Seq Frm MS	MS からの最大シーケンス番号です。
Seq Frm MS at Mig	移行時の MS からのシーケンス番号です。
ACK Frm MS at Mig	移行時の MS からの確認応答番号です。
Seq Frm Server at Mig	移行時のサーバーからのシーケンス番号です。

フィールド	説明
ACK Frm Server at Mig	移行時のサーバーからの確認応答番号です。
Data To Be Delivered To MS	MS に配信されるデータです。
Data To Be Delivered To Server	サーバーに配信されるデータです。
Highest Seq Frm MS	MS からの最大シーケンス番号です。
Timestamps Enabled	タイムスタンプオプションが有効になっているかどうかを示します。
SACK Enabled	選択的確認応答が有効になっているかどうかを示します。
Wscale From MS	MS からのウィンドウスケール値です。
Wscale From Server	サーバーからのウィンドウスケール値です。
Buffering Statistics:	
Buffered Uplink Packets	バッファリングされたアップリンクパケットの合計数です。
Buffered Uplink Bytes	バッファリングされたアップリンクバイトの合計数です。
Buffered Downlink Packets	バッファリングされたダウンリンクパケットの合計数です。
Buffered Downlink Bytes	バッファリングされたダウンリンクバイトの合計数です。
Uplink Packets in Buffer	バッファ内のアップリンクパケットの合計数です。
Uplink Bytes in Buffer	バッファ内のアップリンクバイトの合計数です。
Downlink Packets in Buffer	バッファ内のダウンリンクパケットの合計数です。
Downlink Bytes in Buffer	バッファ内のダウンリンクバイトの合計数です。
Buff Over-limit Uplink Pkts	バッファ内の制限を超えるアップリンクパケットの合計数です。
Buff Over-limit Uplink Bytes	バッファ内の制限を超えるアップリンクバイトの合計数です。
Buff Over-limit Downlink Pkts	バッファ内の制限を超えるダウンリンクパケットの合計数です。
Buff Over-limit Downlink Bytes	バッファ内の制限を超えるダウンリンクバイトの合計数です。
CAE-Readdressing:	
Requests CAE-Readdressed	再アドレス指定が行われた要求の合計数です。
Responses CAE-Readdressed	再アドレス指定が行われた応答の合計数です。
Requests having xheader inserted	x ヘッダーが挿入された HTTP 要求の合計数です。
Total connect failed to CAE	失敗した CAE への接続の合計数です。

フィールド	説明
Total CAE-Readdressed Uplink Bytes	再アドレス指定されたアップリンクバイトの合計数です。
Total CAE-Readdressed Uplink Packets	再アドレス指定されたアップリンクパケットの合計数です。
Total CAE-Readdressed Downlink Bytes	再アドレス指定されたダウンリンクバイトの合計数です。
Total CAE-Readdressed Downlink Packets	再アドレス指定されたダウンリンクパケットの合計数です。
Flows connected to CAE	CAE に接続されているフローの合計数です。
Proxy Disable Success	プロキシが無効になっているフローの合計数です。
Proxy Disable Failed	プロキシ無効化機能が失敗した合計回数です。
リンク モニタリング	
Average Throughput	モバイルデバイスへのダウンリンク TCP トラフィックの平均 TCP スループット（Kbps 単位）です。
Average RTT	モバイルデバイスへのダウンリンク TCP トラフィックの平均 TCP RTT（ラウンドトリップ時間、ミリ秒単位）です。
Tethering detection performed	テザリング検出が実行されたかどうかを示します。
Tethering detected	テザリングが検出されたかどうかを示します。
Total ACS flows matching specified criteria	指定された条件に一致する ACS フローの合計数です。

show active-charging flows full debug-info all

表 *142 : show active-charging flows full debug-info all* コマンド出力の説明

フィールド	説明
Last Active Tick Time	データパケットの最後のアクティブなティック時間を示します。
Current Tick Time	現在のシステムティック時刻を示します。

show active-charging flows summary

表 *143 : show active-charging flows summary* コマンド出力の説明

フィールド	説明
[現在（Current）] :	
アクティブ フロー（Active Flows）	システム上で現在アクティブなフローの合計数を示します。
TCP Active flows	TCP トラフィックのアクティブフローの合計数を指定します。
DNS Active flows	DNS トラフィックのアクティブフローの合計数を指定します。
ICMPV6 Active flows	ICMPv6 トラフィックのアクティブフローの合計数を指定します。
Idle Flows :	
TCP Idle flows	TCP トラフィックのアイドルフローの合計数を指定します。
UDP Idle flows	UDP トラフィックのアイドルフローの合計数を指定します。
ICMPv6 Idle flows	ICMPv6 トラフィックのアイドルフローの合計数を指定します。
DNS Idle flows	DNS トラフィックのアイドルフローの合計数を指定します。
Cumulative :	
Uplink Packets	アップリンクパケットの合計数を指定します。
Uplink Bytes	アップリンクバイトの合計数を指定します。
Downlink Packets	ダウンリンクパケットの合計数を指定します。
Downlink Bytes	ダウンリンクバイトの合計数を指定します。

show active-charging rulebase statistics name

このコマンドの出力には、次のフィールドが表示されます。

表 *144 : show active-charging rulebase statistics name* コマンド出力の説明

フィールド	説明
VPP オフロード統計 :	
フローの総数（Total Flows）	フローの合計数。
Current Active Flows	現在アクティブなフローの合計数。
IPv4 :	

フィールド	説明
Uplink Pkts	IPv4 アップリンクパケットの合計数。
Uplink Bytes	IPv4 アップリンクバイトの合計数。
Downlink Pkts	IPv4 ダウンリンクパケットの合計数。
Downlink Bytes	IPv4 ダウンリンクバイトの合計数。
Dropped Uplink Pkts	破棄された IPv4 アップリンクパケットの合計数。
ドロップされたアップリンクバイト数	破棄された IPv4 アップリンクバイトの合計数。
Dropped Downlink Pkts	破棄された IPv4 ダウンリンクパケットの合計数。
ドロップされたダウンリンクバイト数	破棄された IPv4 ダウンリンクバイトの合計数。
IPv6	
Uplink Pkts	IPv6 アップリンクパケットの合計数。
Uplink Bytes	IPv6 アップリンクバイトの合計数。
Downlink Pkts	IPv6 ダウンリンクパケットの合計数。
Downlink Bytes	IPv6 ダウンリンクバイトの合計数。
Dropped Uplink Pkts	破棄された IPv6 アップリンクパケットの合計数。
ドロップされたアップリンクバイト数	破棄された IPv6 アップリンクバイトの合計数。
Dropped Downlink Pkts	破棄された IPv6 ダウンリンクパケットの合計数。
ドロップされたダウンリンクバイト数	破棄された IPv6 ダウンリンクバイトの合計数。

show active-charging subscribers all

このコマンドの出力には、次のフィールドが表示されます。

表 *145 : show active-charging subscribers all* コマンド出力の説明

フィールド	説明
VPP-PKTS-UP	VPP を介してアップリンク方向で検出されたパケットの合計数。
VPP-PKTS-DOWN	VPP を介してダウンリンク方向で検出されたパケットの合計数。

show-active-charging subscribers full all

このコマンドの出力が強化され、以下のフィールドが表示されるようになりました。

表 *146 : show active-charging subscribers full all* コマンド出力の説明

フィールド	説明
VPP Offload Statistics：**Enabled/Disabled**	
フローの総数（Total Flows）	フローの合計数。
Current Active Flows	現在アクティブなフローの合計数。
IPv4：	
Uplink Pkts	IPv4 アップリンクパケットの合計数。
Uplink Bytes	IPv4 アップリンクバイトの合計数。
Downlink Pkts	IPv4 ダウンリンクパケットの合計数。
Downlink Bytes	IPv4 ダウンリンクバイトの合計数。
Dropped Uplink Pkts	破棄された IPv4 アップリンクパケットの合計数。
Dropped Uplink Bytes	破棄された IPv4 アップリンクバイトの合計数。
Dropped Downlink Pkts	破棄された IPv4 ダウンリンクパケットの合計数。
Dropped Downlink Bytes	破棄された IPv4 ダウンリンクバイトの合計数。
IPv6	
Uplink Pkts	IPv6 アップリンクパケットの合計数。
Uplink Bytes	IPv6 アップリンクバイトの合計数。
Downlink Pkts	IPv6 ダウンリンクパケットの合計数。
Downlink Bytes	IPv6 ダウンリンクバイトの合計数。
Dropped Uplink Pkts	破棄された IPv6 アップリンクパケットの合計数。
Dropped Uplink Bytes	破棄された IPv6 アップリンクバイトの合計数。
Dropped Downlink Pkts	破棄された IPv6 ダウンリンクパケットの合計数。
Dropped Downlink Bytes	破棄された IPv6 ダウンリンクバイトの合計数。

show active-charging analyzer statistics name

このコマンドの出力には、次のフィールドが表示されます。フィールドは http、secure-http、p2p、tcp、udp で共通です。

表 *147 : show active-charging analyzer statistics name* コマンド出力の説明

フィールド	説明
VPP FP パケット合計数	VPP を介した高速パスパケットの合計数。
VPP Fastpath 統計：	
フローの総数（Total Flows）	フローの合計数。
現在アクティブなフロー	現在アクティブなフローの合計数。
IPv4：	
Uplink Pkts	IPv4 アップリンクパケットの合計数。
Uplink Bytes	IPv4 アップリンクバイトの合計数。
Downlink Pkts	IPv4 ダウンリンクパケットの合計数。
Downlink Bytes	IPv4 ダウンリンクバイトの合計数。
IPv6	
Uplink Pkts	IPv6 アップリンクパケットの合計数。
Uplink Bytes	IPv6 アップリンクバイトの合計数。
Downlink Pkts	IPv6 ダウンリンクパケットの合計数。
Downlink Bytes	IPv6 ダウンリンクバイトの合計数。

show session fp-flow-state-change statistics

フィールド	説明
オンロードとオフロードイベントのロギング	ロギングのステータスが表示され、現在有効になっているか無効になっているかを示します。
開始時刻	最後のロギングの開始時刻を表示します。ロギングが開始されなかった場合、開始時刻は「NA」と表示されます。

フィールド	説明
終了時刻（End time）	ロギングが停止された時刻を表示します。ロギングが開始されなかった場合、終了時刻は NA と表示されます。ロギングが現在有効になっている場合は、「In progress」と表示されます。
記録されたイベントの合計数	生成されたログの合計数が表示されます。
イベントの数/ 期間に対して有効なロギング	イベントの数または期間（秒単位）。
セッションマネージャ インスタンス	ロギングが有効になっているセッションマネージャ インスタンス。

バルク統計

ECS スキーマには、次のバルク統計が含まれています。

ECS スキーマ

表 *148 : ECS* スキーマのバルク統計変数

変数	説明
vpp-tot-flows	VPP を介したフローの合計数を示します。
vpp-cur-flows	VPP を介したアクティブな現在のフローの総数を示します。
IPv4	
vpp-IPv4-uplk-pkts	VPP を介してアップリンク方向で検出された IPv4 パケットの総数を示します。
vpp-IPv4-dwnlk-pkts	VPP を介してダウンリンク方向で検出された IPv4 パケットの総数を示します。
vpp-IPv4-uplk-bytes	VPP を介してアップリンク方向で検出された IPv4 バイトの総数を示します。
vpp-IPv4-dwnlk-bytes	VPP を介してダウンリンク方向で検出された IPv4 バイトの総数を示します。
vpp-IPv4-uplk-drop-pkts	VPP を介してアップリンク方向で検出されたドロップされた IPv4 パケットの総数を示します。
vpp-IPv4-dwnlk-drop-pkts	VPP を介してダウンリンク方向で検出されたドロップされた IPv4 パケットの総数を示します。

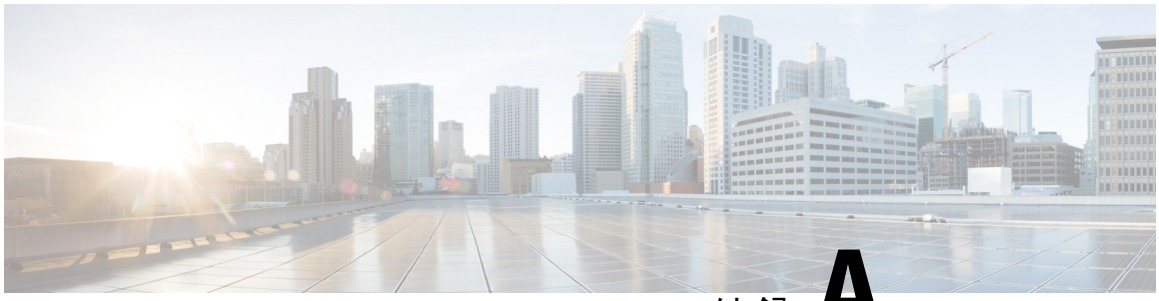
変数	説明
vpp-IPv4-uplk-drop-bytes	VPP を介してアップリンク方向で検出されたドロップされた IPv4 バイトの総数を示します。
vpp-IPv4-dwnlk-drop-bytes	VPP を介してダウンリンク方向で検出されたドロップされた IPv4 バイトの総数を示します。
IPv6	
vpp-IPv6-uplk-pkts	VPP を介してアップリンク方向で検出された IPv6 パケットの総数を示します。
vpp-IPv6-dwnlk-pkts	VPP を介してダウンリンク方向で検出された IPv6 パケットの総数を示します。
vpp-IPv6-uplk-bytes	VPP を介してアップリンク方向で検出された IPv6 バイトの総数を示します。
vpp-IPv6-dwnlk-bytes	VPP を介してダウンリンク方向で検出された IPv6 バイトの総数を示します。
vpp-IPv6-uplk-drop-pkts	VPP を介してアップリンク方向で検出されたドロップされた IPv6 パケットの総数を示します。
vpp-IPv6-dwnlk-drop-pkts	VPP を介してダウンリンク方向で検出されたドロップされた IPv6 パケットの総数を示します。
vpp-IPv6-uplk-drop-bytes	VPP を介してアップリンク方向で検出されたドロップされた IPv6 バイトの総数を示します。
vpp-IPv6-dwnlk-drop-bytes	VPP を介してダウンリンク方向で検出されたドロップされた IPv6 バイトの総数を示します。
TCP	
tcp-vpp-flows-cur	TCP アナライザ用 VPP を介した現在のフロー数を示します。
tcp-vpp-flows	TCP アナライザ用 VPP を介したフローの総数を示します。
tcp-vpp-pkts	TCP アナライザ用 VPP を介した IP パケットの総数。
tcp-ipv4-vpp-dwnlk-pkts	TCP アナライザ用 VPP を介して IPv4 トラフィックのダウンリンク方向で検出された IP パケットの総数を示します。

変数	説明
tcp-ipv4-vpp-uplk-pkts	TCP アナライザ用 VPP を介して IPv4 トラフィックのアップリンク方向で検出された IP パケットの総数を示します。
tcp-ipv4-vpp-dwnlk-bytes	TCP アナライザ用 VPP を介して IPv4 トラフィックでダウンリンク方向で検出された IP バイトの総数を示します。
tcp-ipv4-vpp-uplk-bytes	TCP アナライザ用 VPP を介して IPv4 トラフィックのアップリンク方向で検出された IP バイトの総数を示します。
tcp-ipv6-vpp-dwnlk-pkts	TCP アナライザ用 VPP を介して IPv6 トラフィックのダウンリンク方向で検出された IP パケットの総数を示します。
tcp-ipv6-vpp-uplk-pkts	TCP アナライザ用 VPP を介して IPv6 トラフィックのアップリンク方向で検出された IP パケットの総数を示します。
tcp-ipv6-vpp-dwnlk-bytes	TCP アナライザ用 VPP を介して IPv6 トラフィックでダウンリンク方向で検出された IP バイトの総数を示します。
tcp-ipv6-vpp-uplk-bytes	TCP アナライザ用 VPP を介して IPv6 トラフィックのアップリンク方向で検出された IP バイトの総数を示します。
UDP	
udp-vpp-flows-cur	UDP アナライザ用 VPP を介した現在のフロー数を示します。
udp-vpp-flows	UDP アナライザ用 VPP を介したフローの総数を示します。
udp-vpp-pkts	UDP アナライザ用 VPP を介した IP パケットの総数。
udp-ipv4-vpp-dwnlk-pkts	UDP アナライザ用 VPP を介してダウンリンク方向で検出された IPv4 パケットの総数を示します。
udp-ipv4-vpp-uplk-pkts	UDP アナライザ用 VPP を介してアップリンク方向で検出された IPv4 パケットの総数を示します。
udp-ipv4-vpp-dwnlk-bytes	UDP アナライザ用 VPP を介してダウンリンク方向で検出された IPv4 バイトの総数を示します。
udp-ipv4-vpp-uplk-bytes	UDP アナライザ用 VPP を介してアップリンク方向で検出された IPv4 バイトの総数を示します。

変数	説明
udp-ipv6-vpp-dwnlk-pkts	UDP アナライザ用 VPP を介してダウンリンク方向で検出された IPv6 パケットの総数を示します。
udp-ipv6-vpp-uplk-pkts	UDP アナライザ用 VPP を介してアップリンク方向で検出された IPv6 パケットの総数を示します。
udp-ipv6-vpp-dwnlk-bytes	UDP アナライザ用 VPP を介してダウンリンク方向で検出された IPv6 バイトの総数を示します。
udp-ipv6-vpp-uplk-bytes	UDP アナライザ用 VPP を介してアップリンク方向で検出された IPv6 バイトの総数を示します。
[HTTP]	
http-vpp-flows-cur	HTTP アナライザ用 VPP を介した現在のフロー数を示します。
http-vpp-flows	HTTP アナライザ用 VPP を介したフローの総数を示します。
http-vpp-pkts	HTTP アナライザ用 VPP を介した IP パケットの総数。
http-ipv4-vpp-dwnlk-pkts	HTTP アナライザ用 VPP を介してダウンリンク方向で検出された IPv4 パケットの総数を示します。
http-ipv4-vpp-uplk-pkts	HTTP アナライザ用 VPP を介してアップリンク方向で検出された IPv4 パケットの総数を示します。
http-ipv4-vpp-dwnlk-bytes	HTTP アナライザ用 VPP を介してダウンリンク方向で検出された IPv4 バイトの総数を示します。
http-ipv4-vpp-uplk-bytes	HTTP アナライザ用 VPP を介してアップリンク方向で検出された IPv4 バイトの総数を示します。
http-ipv6-vpp-dwnlk-pkts	HTTP アナライザ用 VPP を介してダウンリンク方向で検出された IPv6 パケットの総数を示します。
http-ipv6-vpp-uplk-pkts	HTTP アナライザ用 VPP を介してアップリンク方向で検出された IPv6 パケットの総数を示します。
http-ipv6-vpp-dwnlk-bytes	HTTP アナライザ用 VPP を介してダウンリンク方向で検出された IPv6 バイトの総数を示します。
http-ipv6-vpp-uplk-bytes	HTTP アナライザ用 VPP を介してアップリンク方向で検出された IPv6 バイトの総数を示します。
Secure-HTTP	
https-vpp-flows-cur	HTTPS アナライザ用 VPP を介した現在のフロー数を示します。

変数	説明
https-vpp-flows	HTTPS アナライザ用 VPP を介したフローの総数を示します。
https-vpp-pkts	HTTPS アナライザ用 VPP を介した IP パケットの総数。
https-ipv4-vpp-dwnlk-pkts	HTTPS アナライザ用 VPP を介してダウンリンク方向で検出された IPv4 パケットの総数を示します。
https-ipv4-vpp-uplk-pkts	HTTPS アナライザ用 VPP を介してアップリンク方向で検出された IPv4 パケットの総数を示します。
https-ipv4-vpp-dwnlk-bytes	HTTPS アナライザ用 VPP を介してダウンリンク方向で検出された IPv4 バイトの総数を示します。
https-ipv4-vpp-uplk-bytes	HTTPS アナライザ用 VPP を介してアップリンク方向で検出された IPv4 バイトの総数を示します。
https-ipv6-vpp-dwnlk-pkts	HTTPS アナライザ用 VPP を介してダウンリンク方向で検出された IPv6 パケットの総数を示します。
https-ipv6-vpp-uplk-pkts	HTTPS アナライザ用 VPP を介してアップリンク方向で検出された IPv6 パケットの総数を示します。
https-ipv6-vpp-dwnlk-bytes	HTTPS アナライザ用 VPP を介してダウンリンク方向で検出された IPv6 バイトの総数を示します。
https-ipv6-vpp-uplk-bytes	HTTPS アナライザ用 VPP を介してアップリンク方向で検出された IPv6 バイトの総数を示します。
P2P	
p2p-vpp-flows-cur	P2P アナライザ用 VPP を介した現在のフロー数を示します。
p2p-vpp-flows	P2P アナライザ用 VPP を介したフローの総数を示します。
p2p-vpp-pkts	P2P アナライザ用 VPP を介した IP パケットの総数。
p2p-ipv4-vpp-dwnlk-pkts	P2P アナライザ用 VPP を介してダウンリンク方向で検出された IPv4 パケットの総数を示します。
p2p-ipv4-vpp-uplk-pkts	P2P アナライザ用 VPP を介してアップリンク方向で検出された IPv4 パケットの総数を示します。

変数	説明
p2p-ipv4-vpp-dwnlk-bytes	P2P アナライザ用 VPP を介してダウンリンク方向で検出された IPv4 バイトの総数を示します。
p2p-ipv4-vpp-uplk-bytes	P2P アナライザ用 VPP を介してアップリンク方向で検出された IPv4 バイトの総数を示します。
p2p-ipv6-vpp-dwnlk-pkts	P2P アナライザ用 VPP を介してダウンリンク方向で検出された IPv6 パケットの総数を示します。
p2p-ipv6-vpp-uplk-pkts	P2P アナライザ用 VPP を介してアップリンク方向で検出された IPv6 パケットの総数を示します。
p2p-ipv6-vpp-dwnlk-bytes	P2P アナライザ用 VPP を介してダウンリンク方向で検出された IPv6 バイトの総数を示します。
p2p-ipv6-vpp-uplk-bytes	P2P アナライザ用 VPP を介してアップリンク方向で検出された IPv6 バイトの総数を示します。



付録 A

P-GW 導入ルール

この付録では、ネットワーク展開で ASR 5500 を設定する前に考慮する必要がある PDN ゲートウェイ固有の導入ルールまたはガイドラインについて説明します。一般的なルールおよびネットワーク固有のルールは、特定のネットワークタイプに対応する『 *Administration and Configuration Guide*』[英語] の付録を参照してください。

この項では次のトピックについて説明します。

- インターフェイスとポートのルール （1527 ページ）
- P-GW コンテキストとサービスルール （1528 ページ）
- P-GW サブスクライバルール （1529 ページ）

インターフェイスとポートのルール

ここで説明するルールは、アプリケーションに関係なく、イーサネット 10/100 ラインカード、イーサネット 1000 ラインカード、および 4 ポートクアッド Gig-E ラインカード、およびそれらが支援するインターフェイスのタイプに関連します。

S2a インターフェイスルール

この項では、HSGW に存在するモビリティ アクセス ゲートウェイ（MAG）サービスと P-GW に存在するローカルモビリティアンカー（LMA）サービス間の通信に関する S2a インターフェイスのエンジニアリングルールについて説明します。

LMA から MAG

LMA サービスから HSGW に存在する MAG サービスにつながる S2a インターフェイスには、次のエンジニアリングルールが適用されます。

- 論理インターフェイスの IP アドレスが LMA サービスにバインドされると、S2a インターフェイスが作成されます。
- S2a インターフェイスの作成を容易にするために使用される論理インターフェイスは、入力コンテキスト内で設定する必要があります。

- LMA サービスは、入力コンテキスト内で設定する必要があります。
- サブスクライバに提供されるサービスに応じて、サブスクライバごとの帯域幅を大きくするために、S2a インターフェイスによって促進されるセッションの数を制限できます。

S5/S8 インターフェイスルール（GTP）

P-GW から S-GW への S5/S8 インターフェイスには、次のエンジニアリングルールが適用されます。

- P-GW は、共通の P-GW が 2 つのサービス間のアンカーポイントとして使用されている場合、ユーザーが Wi-Fi と LTE の間を移動するときに、S2a インターフェイス（PMIPv6）と S5/S8 インターフェイス（GTP）間の IP アドレスを保持します。

P-GW コンテキストとサービスルール

システム内に設定されているサービスには、次のエンジニアリングルールが適用されます。

- システムごとに（タイプに関係なく）最大 256 のサービスを設定できます。

⚠

注意 多数のサービスによって管理の複雑度が大幅に増大し、システム全体のパフォーマンスに影響を与える可能性があります（システムハンドオフなどの結果として）。そのため、アプリケーションが絶対に必要とする場合にのみ、多数のサービスを設定することをお勧めします。詳細については、サービス担当者にお問い合わせください。

- システムは、P-GW ごとに無制限のピア HSGW/MAG アドレスをサポートしています。
  - システムは、P-GW サービスごとに最大 8192 のピア HSGW の統計を維持します。
  - 8192 を超える HSGW が接続されている場合、古い統計が特定され、上書きされます。
  - PMIPv6 は、ピアレベルの統計（MAG レベルの統計ごと）をサポートしていません。
- システムは、P-GW あたり 65,000 の S-GW アドレスをサポートしています。
  - システムは、P-GW サービスごとにすべてのピア S-GW の統計を維持します。
- システムは、HSGW または S-GW サービスごとに最大 64,000 のピア P-GW の統計を維持します。
- コンテキストごと、およびシャーシごとに最大 8 つの P-GW 割り当てテーブルがあります。
- テーブルあたりおよびシャーシあたりのエントリの合計数は、256 に制限されます。

P-GW サブスクライバルール

システム内に設定されているサブスクライバには、次のエンジニアリングルールが適用されます。

- デフォルトのサブスクライバテンプレートは、P-GW サービスごとに設定できます。

翻訳について
このドキュメントは、米国シスコ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。