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

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***

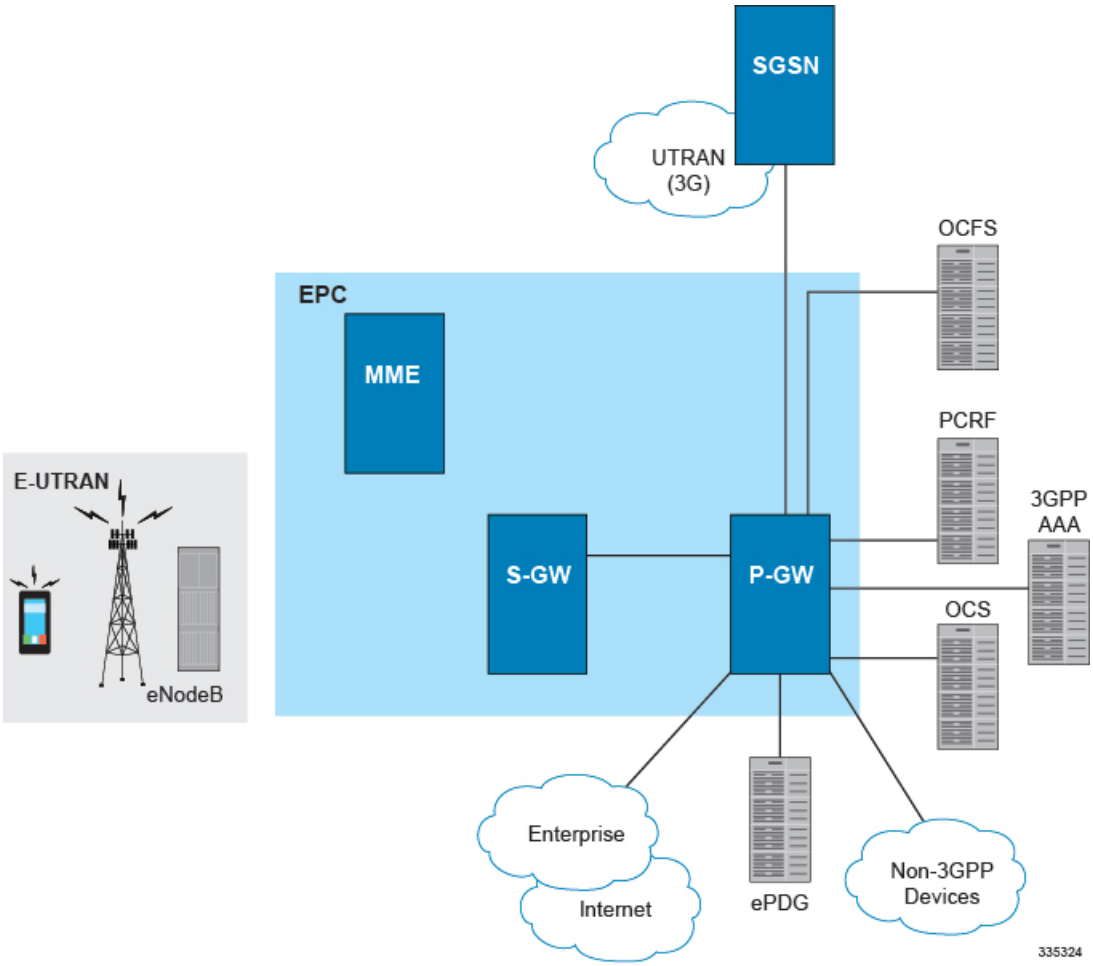
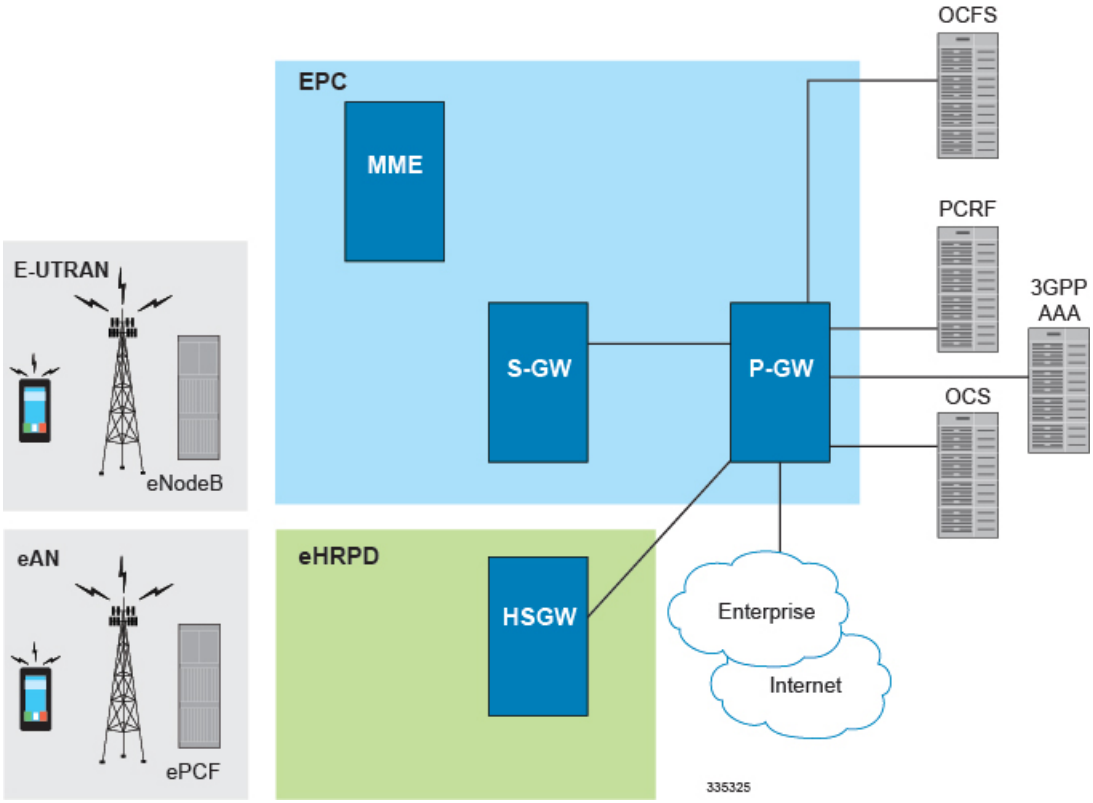


図 *2 :* 基本的な *E-UTRAN/EPC* および *eHRPD* ネットワークにおける *P-GW*



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。

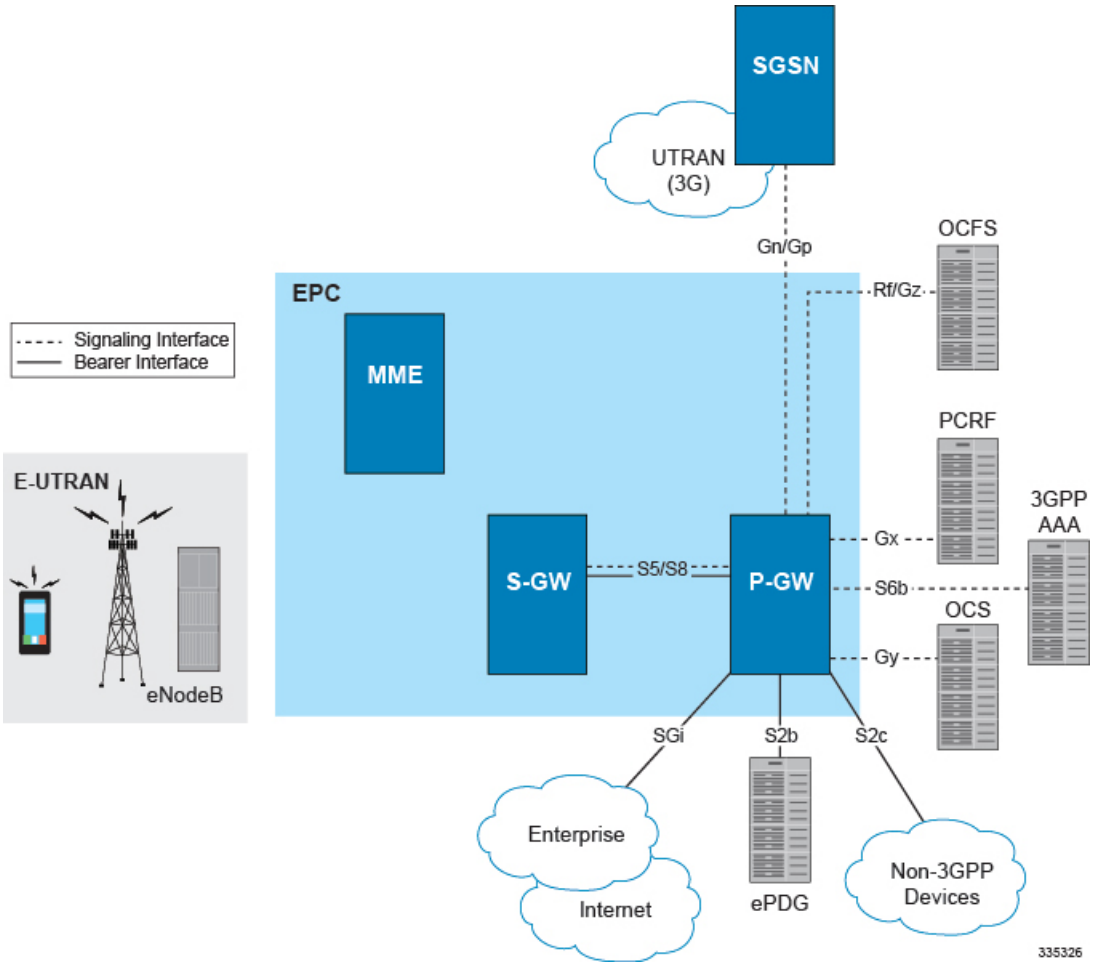
ネットワーク展開

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

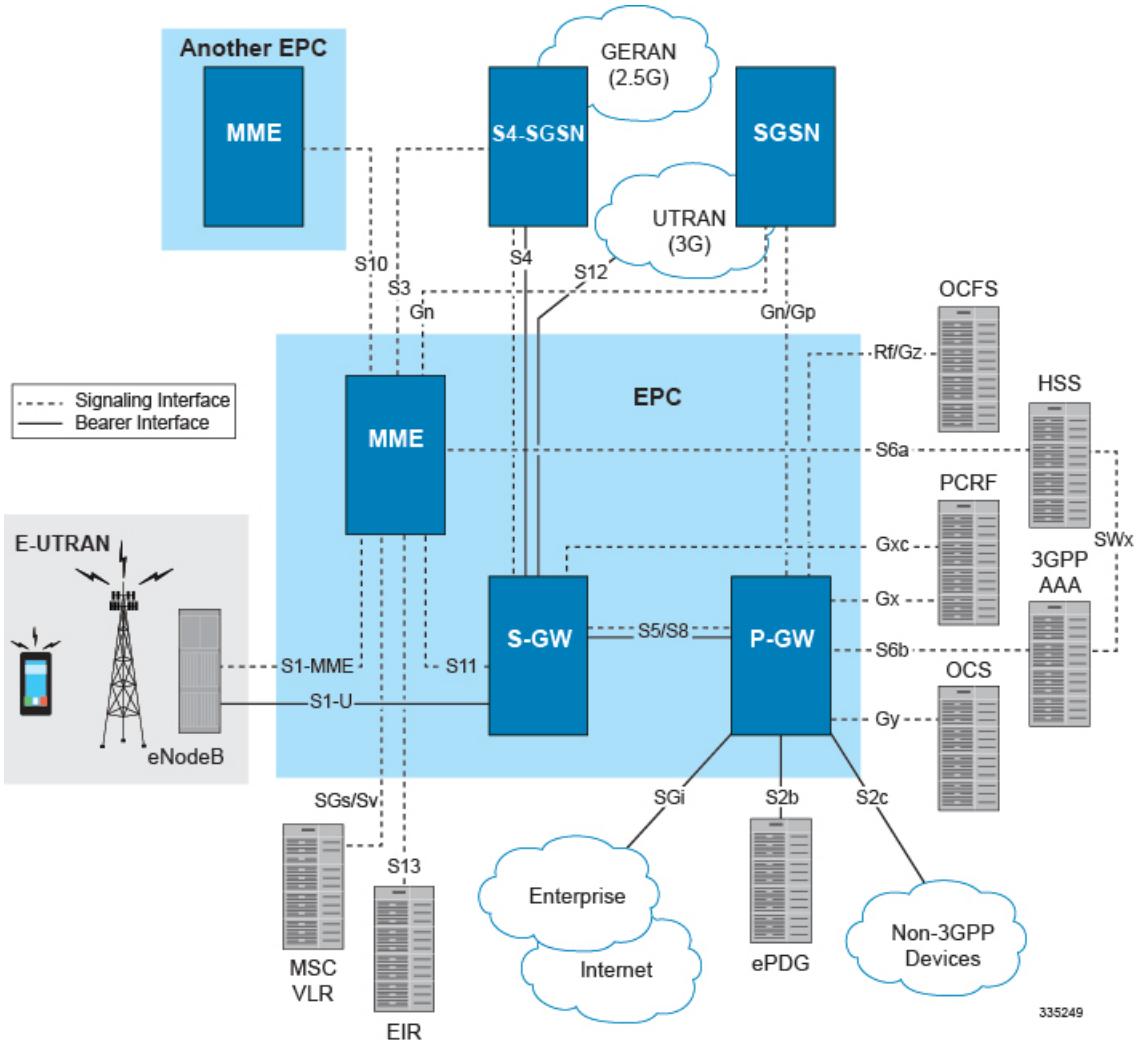
次の図は、P-GW でサポートされる特定のネットワークインターフェイスを示しています。各インターフェイスの詳細については、サポートされる論理ネットワークインターフェイス（参照ポイント）（14 ページ）を参照してください。

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。

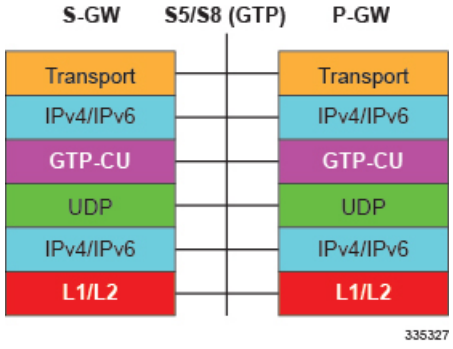
P-CSCFアドレス情報が欠落している場合、S4-SGSN から LTE（およびその逆）へのハンドオフ時にP-CSCF検出が開始されます。P-CSCFアドレス情報がすでに利用可能な場合は、S4-SGSN から LTE（およびその逆）へのハンドオフ時に、P-CSCF 検出を改めて明示的にトリガーする必要はありません。

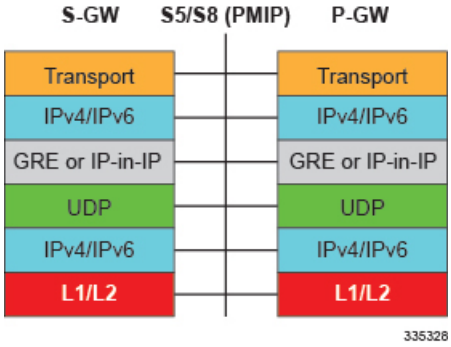
S5/S8 インターフェイス

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。

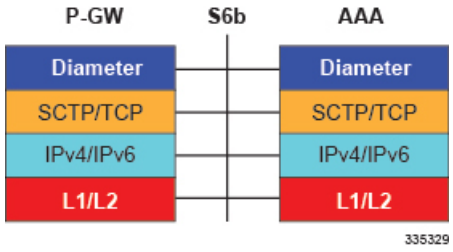
StarOS リリース 17 以降では、P-GW は、AAA サーバーから S6b インターフェイスを介して AVP「Restoration-Priority-Indicator」の受信をサポートしており、VoLTE が有効な IMS PDN 接

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

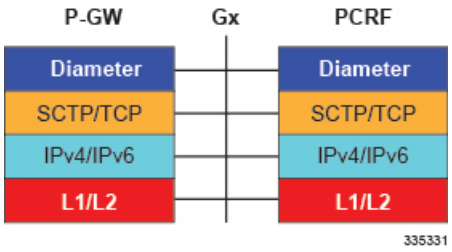
- トランスポート層：TCP、UDP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット

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



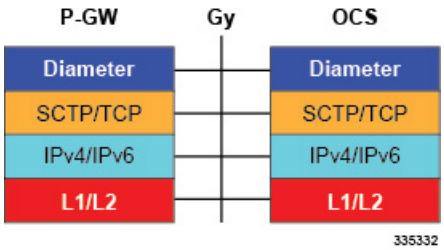
Gx インターフェイスの設定の詳細については、「ダイナミックポリシー課金制御（Gx 参照インターフェイス） （34 ページ）」を参照してください。

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



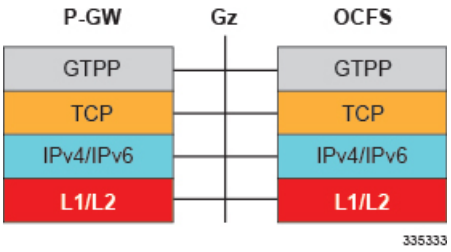
Gy インターフェイスおよびオンラインアカウンティングの詳細については、「Gy インターフェイスのサポート （41 ページ）」を参照してください。

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

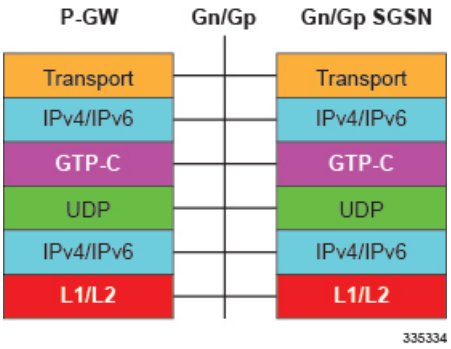


Gn/Gp インターフェイス

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

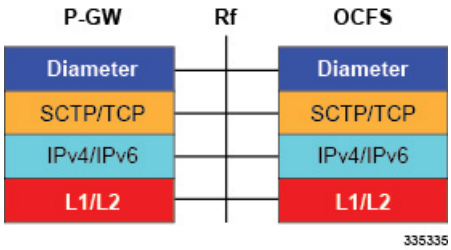


Rf インターフェイス

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

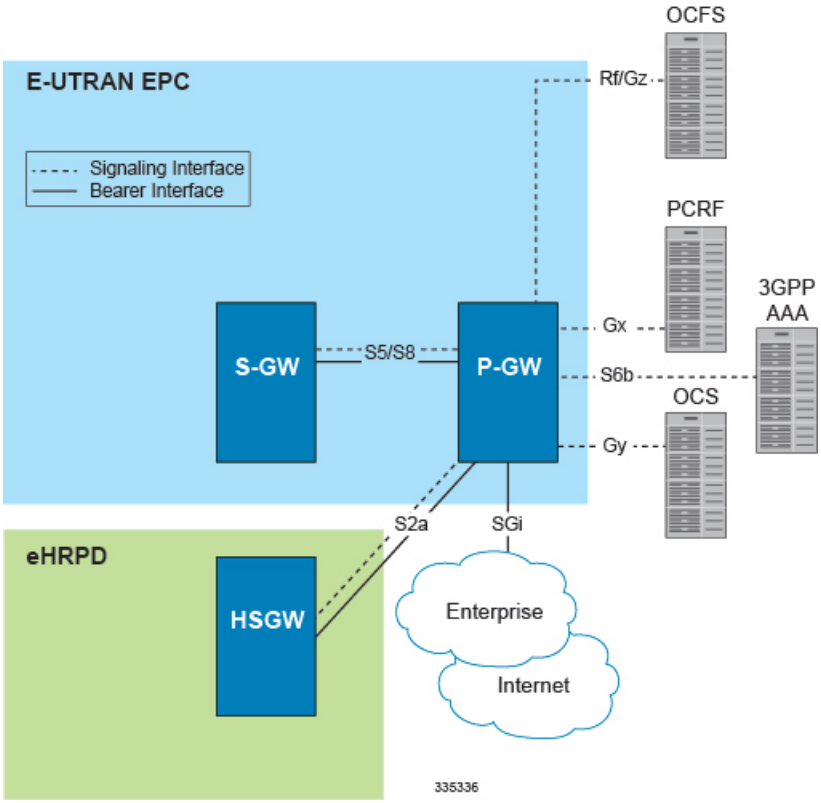
- トランスポート層：TCP、SCTP
- ネットワーク層：IPv4、IPv6
- データ リンク層：ARP
- 物理層：イーサネット



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

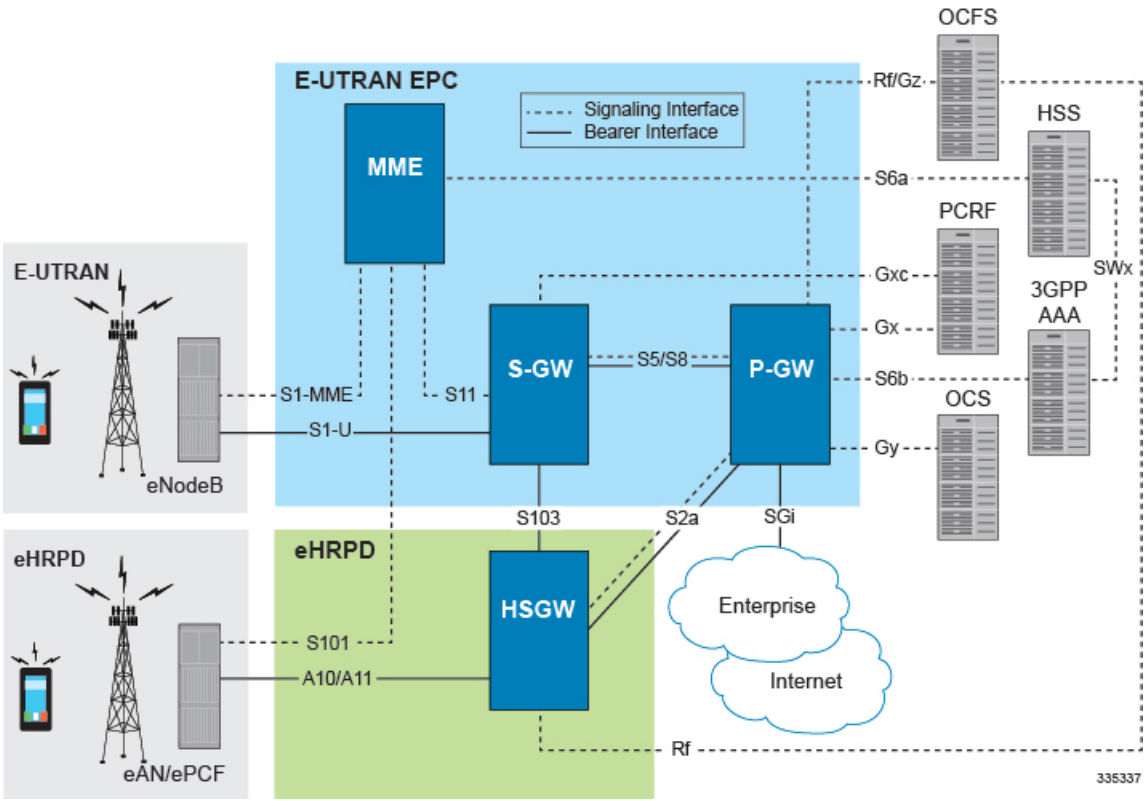
次の図は、eHRPD ネットワーク内の P-GW でサポートされる特定のネットワーク インターフェイスを示しています。各インターフェイスの詳細については、サポートされる論理ネットワーク インターフェイス（参照ポイント） （6 ページ）を参照してください。

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。

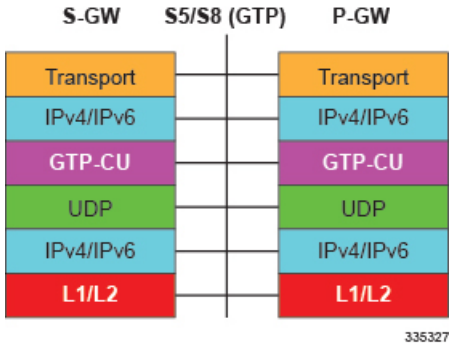
S5/S8 インターフェイス

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

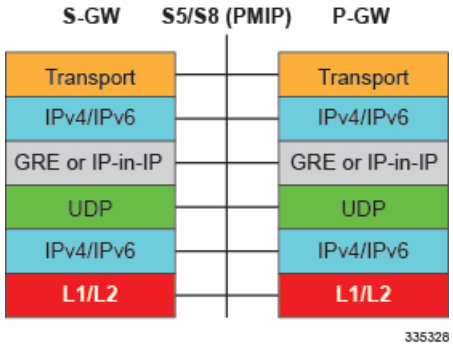


S2a インターフェイス

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。

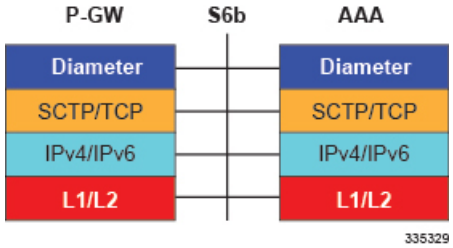
リリース 12.3 以降では、S6b インターフェイスへの承認認証要求（AAR）を介した IPv6 アドレスレポートがデフォルト機能ではなくなりました。これは、CLI を使用して設定できるようになりました。

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

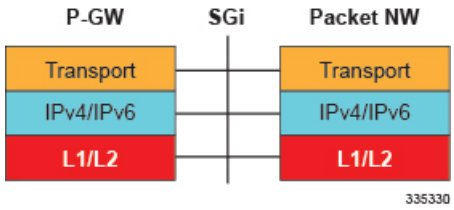


SGi インターフェイス

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

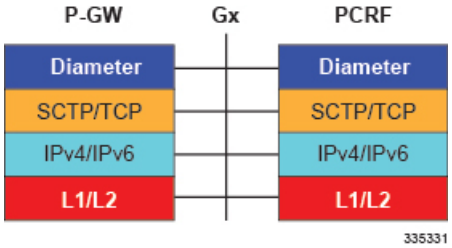


Gx インターフェイス

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



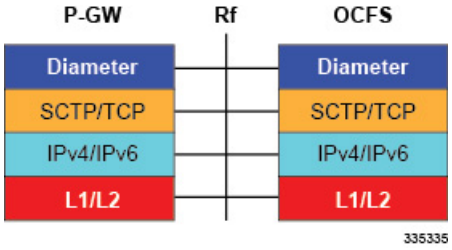
Gx インターフェイスの設定の詳細については、「ダイナミックポリシー課金制御（Gx 参照インターフェイス） （34 ページ）」を参照してください。

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



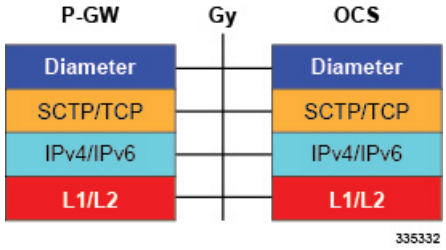
CCO アカウントの作成の詳細については、基本ソフトウェアの特長と機能 （19 ページ）を参照してください。

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

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。

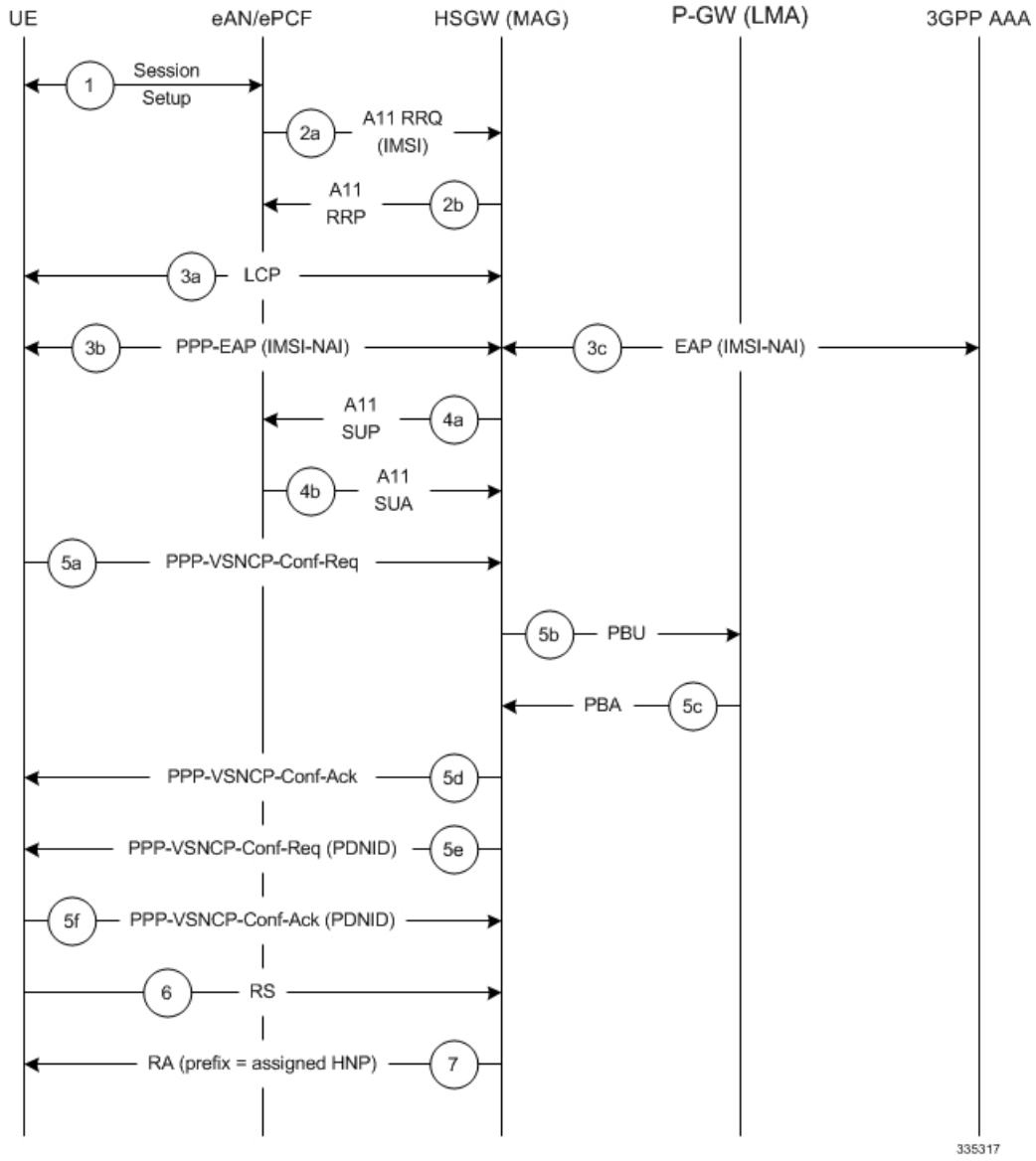


表 *7: IPv6/IPv4* アクセスコールフローによる初期アタッチの説明

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。

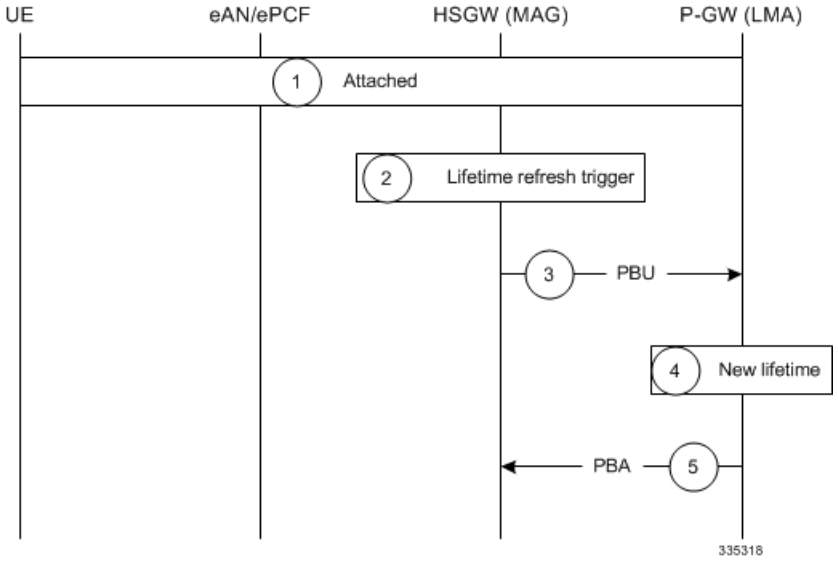


表 *8 : PMIPv6* ライフタイム延長（ハンドオーバーなし）コールフローの説明

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。

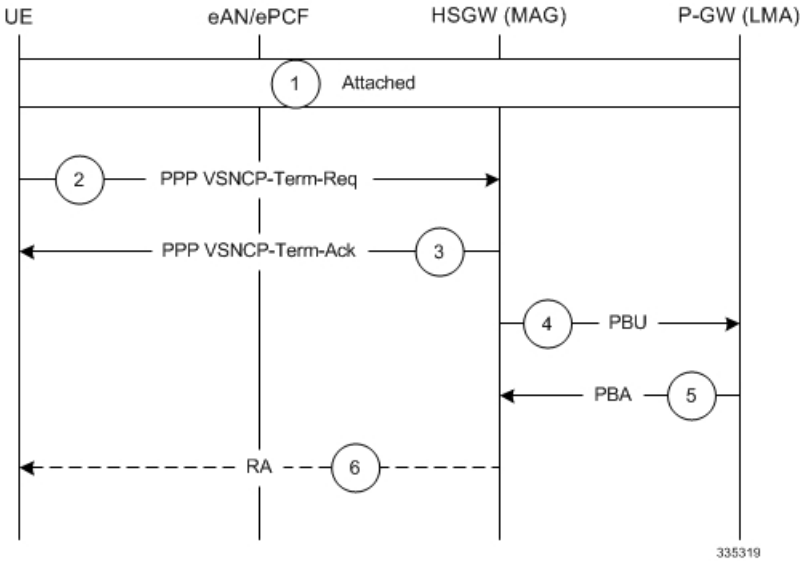


表 *9 : UE* コールフローによる *PDN* 接続解除の説明

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。

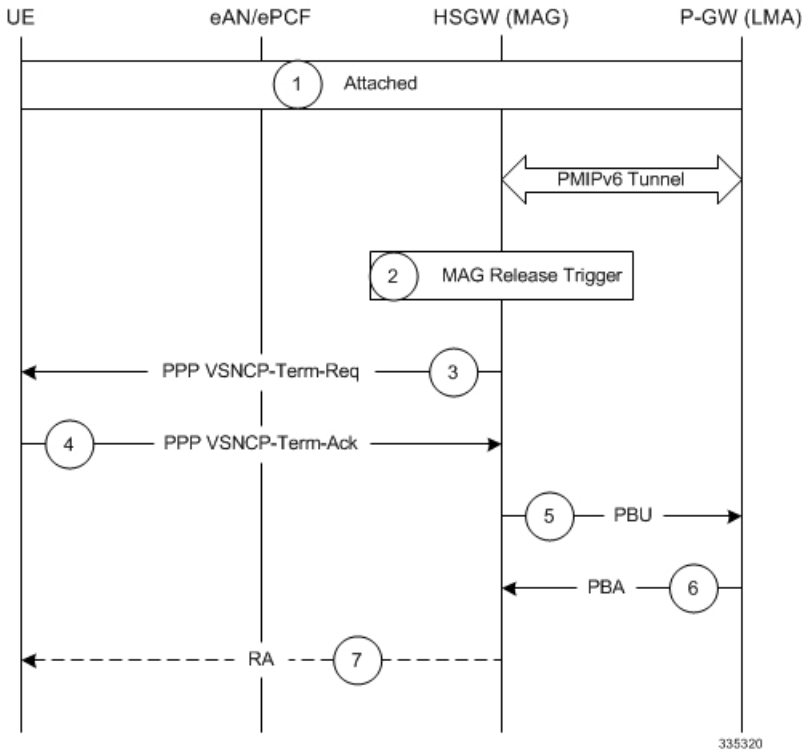


表 *10 : HSGW* コールフローによる *PDN* 接続解除の説明

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。

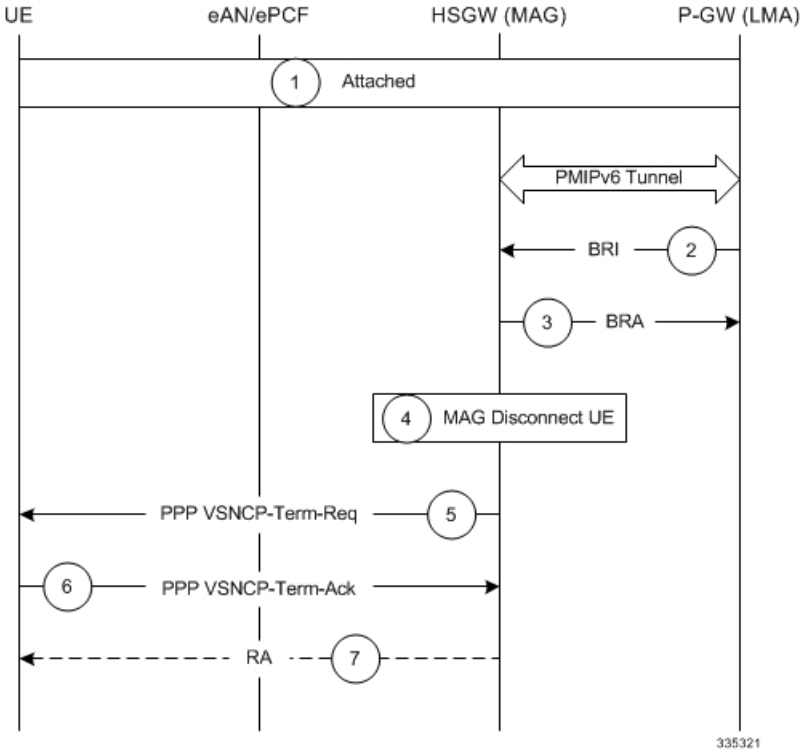


表 *11 : P-GW* コールフローによる *PDN* 接続解除の説明

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）

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。

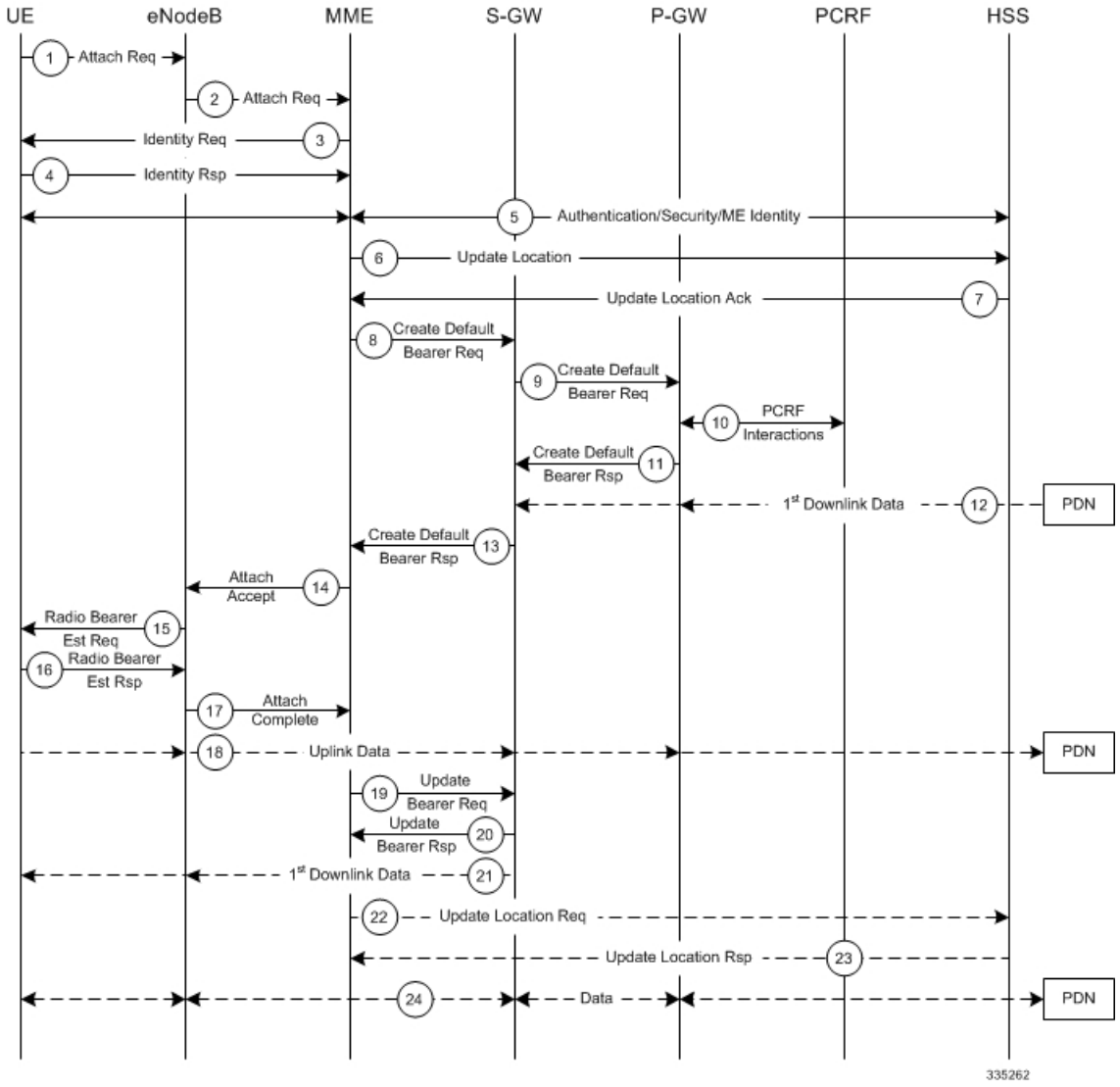


表 *12*：サブスクライバ開始アタッチ（初回）コールフローの説明

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。

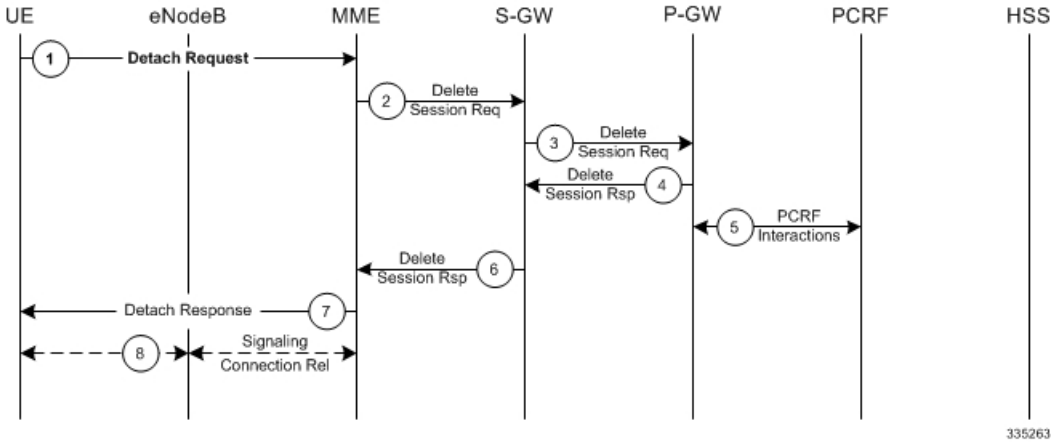


表 *13 :* サブスクライバ開始デタッチコールフローの説明

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

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

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。