Ultra Packet Core CUPS リリース 21.28 ユーザープレーン アドミニストレーション ガイド

最終更新：2024 年 10 月 11 日

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

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

このマニュアルについて

（注） コントロールプレーンとユーザープレーンの分離（CUPS）は、StarOS ベースの製品の 3G、4G、および 5G のネットワークでの展開方法におけるアーキテクチャ上の著しい変更を表します。このドキュメントでは、3G/4G ネットワークに展開されたこの 3G/4G CUPS 製品で特にサポートされている機能に関する情報を提供します。レガシー製品または CUPS 以外の製品で以前サポートされていた機能がこの製品でもサポートされていると想定しないでください。レガシー製品または CUPS 以外の製品または機能への言及は、情報提供のみを目的としています。さらに、このドキュメントで言及されている構成（コマンド、統計、属性、MIB オブジェクト、アラーム、ログ、サービスを含むがこれらに限定されない）が、レガシー製品または CUPS 以外の製品との機能的な同等性を示すと想定しないでください。この製品とレガシー製品または CUPS 以外の製品間のパリティについてのご質問は、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

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

このガイドでは、コントロールプレーンとユーザープレーンの分離（CUPS）におけるユーザープレーン（UP）機能について説明します。また、機能の説明、設定手順、モニタリング、障害対応に関する情報も記載します。

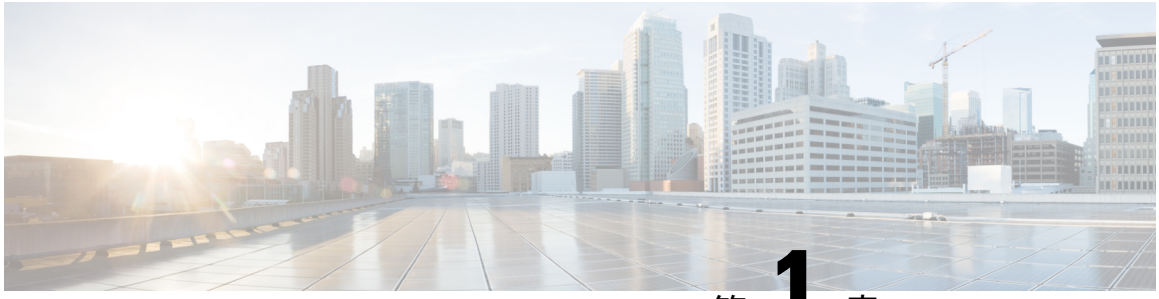
• 使用する表記法 （l ページ）

使用する表記法

次の表に、このマニュアル全体で使用される表記法を示します。

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

書体の表記法	説明
スクリーンディスプレイとして表されるテキスト	この書体は、端末画面に表示されるディスプレイを表します。次に例を示します。 ログイン：
commands として表されるテキスト	この書体は、入力したコマンドを表します。次に例を示します。 **show ip access-list** このマニュアルでは、コマンドの完全表記に常に小文字を使用しています。コマンドには、大文字と小文字の区別はありません。
command 変数として表されるテキスト	この書体は、コマンドの一部である変数を表します。次に例を示します。 **show card** *slot_number* *slot_number* は、目的のシャーシのスロット番号を表す変数です。
メニュー名またはサブメニュー名として表されるテキスト	この書体は、ソフトウェアアプリケーション内でアクセスするメニューとサブメニューを表します。次に例を示します。 [File] メニュー、[New] の順にクリックてください。



第 1 章

概要

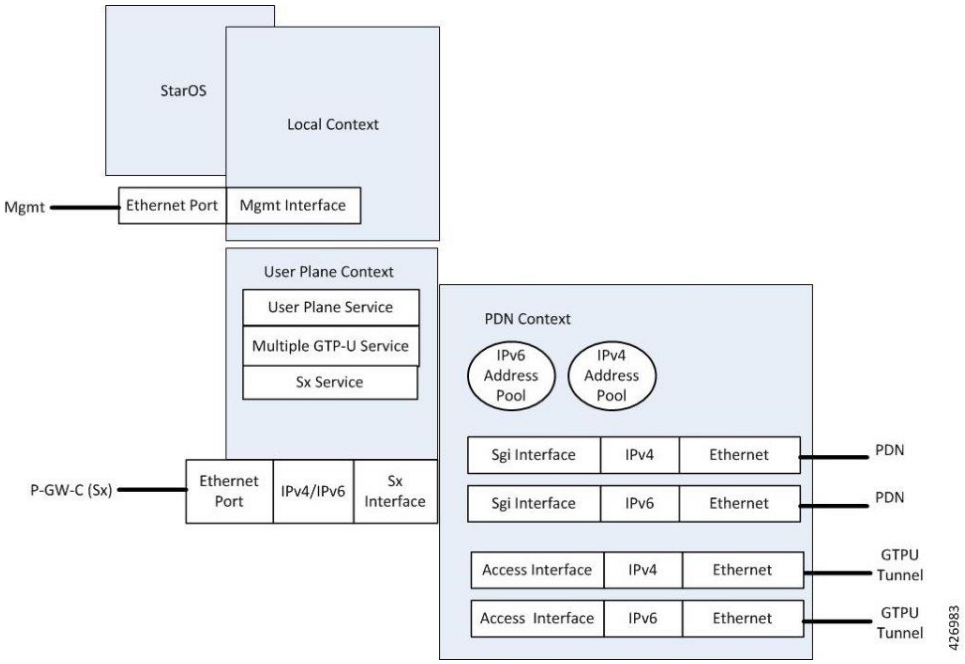
Evolved Packet Core（EPC）ネットワークは、ユーザープレーンとコントロールプレーンが P-GW、S-GW、および TDF 製品の個別のノードである、コントロール ユーザー プレーン分離（CUPS）ベースのアーキテクチャに向けて進化しています。ユーザープレーンとコントロールプレーンが統合することで、EPC ネットワーク内の他の要素に対してもノードの機能が提供されます。ただし、ネットワークの観点から見ると、ユーザープレーンとコントロールプレーンを分離しておくことには多くの利点があります。たとえば、コントロールプレーンとユーザープレーンでそれぞれ異なる拡張をサポートできること、ユーザープレーンでセッションあたりにより多くのキャパシティをサポートできることなどが挙げられます。

この章では、P-GW、S-GW、および SAEGW 製品のコントロールプレーン実装に関連する詳細、コールフロー、および設定について概要を説明します。

製品の説明

SAEGW-U 仮想化ネットワーク機能（VNF）は、COTS ハードウェアまたは ASR 5500/DPC2 シャーシ上の Cisco Ultra Services Platform（USP）でホストできます。SAEGW-U は、同じデータセンター内の SAEGW-C と同じ場所に配置したり、離れた場所にある別のデータセンターに配置したりできます。

次に、サービスとしてのユーザープレーンのアーキテクチャの概要を示します。



サービスとしてのユーザープレーンを説明する重要なポイント：

- ユーザープレーンはコントロールプレーンからプログラムできます。
- シングル ユーザー プレーン サービスは、SGW-U タイプと P-GW-U タイプの両方のセッションに対応できます。
- ノードタイプ（SGW-U および PGW-U）ごとに、2 つ以上の個別のユーザープレーンサービスを定義できます。
- SAEGW-U のグループは、APN に明示的に関連付けられます。グループが関連付けられていない場合は、SAEGW-C に登録されていて、設定されている SAEGW-U グループの一部ではないすべての登録済みユーザープレーンを含むデフォルトグループが使用されます。
- ユーザープレーンサービスは、コントロール プレーン インターフェイスの Sx サービスと、GTP-U パケットを受信する GTP-U サービスに関連付けられます。

重要 現在、各ユーザープレーンサービスは、コントロールプレーンとインターフェイスする単一の Sx サービスにのみ関連付けられています。

- ユーザープレーンサービスは、SaMOG、GGSN、および ePDG をサポートするように拡張できる 4 つの GTP-U サービスに関連付けられます。
- コントロール プレーン サービスの複数のピアでは、単一のユーザープレーンサービスが使用されます。
- IP プールとその設定を関連付けるには、APN 設定が必要です。

重要　現在、ユーザープレーンは APN とプール設定をサポートしています。IP アドレスはコントロールプレーンから割り当てられ、ユーザープレーンで検証されます。

サポートされる機能

3GPP ULI 拡張レポートのサポート

この機能拡張は、3GPP 標準に従って 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。P-GW が変更を検出し、変更要求が PCRF からイベントトリガーとして送信された場合、P-GW は PCRF に ULI を報告します。

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。GGSN が変更を検出し、変更要求が PCRF からイベントトリガーとして送信された場合、GGSN は PCRF に ULI を報告します。この機能は、GGSN で ULI フィールドの一部として受信した RAI の変更の検出もサポートします。

3GPP ULI レポートのサポート強化の詳細については、StarOS P-GW アドミニストレーションガイド [英語] の「3GPP ULI Reporting Support Enhanced」の項を参照してください。

AAA サーバーグループ

AAA サーバーグループ機能は、コンテキストまたはシステム内で Diameter/RADIUS サーバーグループを作成および管理するために使用されます。AAA サーバーグループにより、AAA 機能のサブスクライバ/APN/レルム単位で、サーバーグループ（リスト）を管理しやすくなります。

（注）　AAA サーバーグループは、非 CUPS アーキテクチャでサポートされている既存の機能です。このリリースでは、この機能が CUPS アーキテクチャで認定されました。

AAA サーバーグループに関連する CLI 設定の詳細については、『*Command Line Interface Reference*』[英語] の「*AAA Server Group Configuration Mode Commands*」の章を参照してください。

APN 設定のサポート

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

CLI コマンド **radius-group**、**cc-home behaviour 0x10 profile 2**、**mediation-device** が APN 設定をサポートすることが、CUPS アーキテクチャで認定および検証済みです。

radius-group

この機能検証に基づき、CUPS アーキテクチャは、RADIUS 認証およびアカウンティングサーバーが設定された各グループで 800 の RADIUS サーバーグループをサポートします。

cc-home { behavior *bits* | profile *index* }

SGSN からの課金特性（CC）が受け付けられない場合に GGSN が使用する Home サブスクライバの課金特性を設定します。CLI で設定された値は、CUPS SAEGW サービスによって優先され、GTPP CDR レコードに適切に入力されます。

注：

- **behavior** *bits*：Home サブスクライバの課金特性の動作ビットを指定します。ビットは、001H ～ FFFH（2 進数では 0001 ～ 1111 1111 1111）までの任意の一意のビットに設定できます。最下位ビットは B1 に相当し、最上位ビットは B12 に相当します。
- **profile** *index*：Home サブスクライバの課金特性のプロファイル指数を指定します。指数は、0 ～ 15 までの任意の整数値に設定できます。デフォルト：8
- 詳細については、『*Command Line Interface Reference A-B*』[英語] の「*APN Configuration Mode Commands* 」の章にある **cc-home** コマンドを参照してください。

mediation-device [context-name *context_name*] [delay-GTP-response] [no-early-PDUs] [no interims] +

このコマンドおよび関連するすべてのサブセクション CLI が CUPS でサポートされます。この CLI を使用すると、CUPS SAEGW サービスで**仲介デバイス**と、特定の APN に使用できるすべての関連設定を使用できます。

注：

- **context-name** *context_name*：この APN の仲介 VPN コンテキストを、大文字と小文字を区別する 1 ～ 79 文字の英数字で設定します。指定しない場合、仲介コンテキストはサブスクライバの接続先コンテキストと同じになります。デフォルト：サブスクライバの接続先コンテキスト。

- **delay-GTP-response**：有効にすると、仲介デバイスからアカウンティング開始応答を受信するまで CPC 応答を遅延させます。デフォルトで、ディセーブルになっています。
- **no-early-pdus**：仲介デバイスから GGSN アカウンティング開始要求に対する応答を受信するまで、システムが MS からの PDU を遅延させるように設定します。PDU はキューに追加され、破棄されません。デフォルトで、ディセーブルになっています。
- **no-interim**：仲介サーバーへの中間の送信を無効にします。デフォルトで、ディセーブルになっています。
- 詳細については、『*Command Line Interface Reference A-B*』[英語] の「*APN Configuration Mode Commands* 」の章にある **mediation-device** コマンドを参照してください。

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 CUPS に追加されました。

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 CUPS で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。

（注） egtpinmgr の非同期コア転送サポートは、非 CUPS アーキテクチャでサポートされている既存の機能です。このリリースでは、この機能が CUPS アーキテクチャで認定されました。

HDD に対する課金データレコード

課金データレコード（CDR）は、課金対象イベントに関する情報のフォーマットされたコレクションです。生成された GTPP アカウンティング CDR は、保管のために外部ノードに送信されます。CDR は、外部ノードでサポートされている形式でファイルに書き込まれ、ハードディスク（HDD）に保存されます。FTP または SFTP プロトコルを使用して、CDR ファイルを HDD にプッシュしたり、HDD からプルしたりできます。

（注） バックアップなどの展開の使用例では、*/hd-raid/records/* の下に StarOS によって作成されたシステムディレクトリを使用しないことを強く推奨します。そのようなディレクトリを使用すると、製品の正常な機能に影響を与える可能性があります。

CDR は、非 CUPS アーキテクチャでサポートされていて、CUPS アーキテクチャで認定されている既存の機能です。詳細については、GTPP インターフェイス管理およびリファレンスガイド [英語] の「HDD Storage」の章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

CUPS アーキテクチャでは、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。また、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、CUPS に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。

（注） GTP-C パス障害の機能拡張と改善されたデバッグツールは、非 CUPS アーキテクチャでサポートされている既存の機能です。このリリースでは、この機能は CUPS アーキテクチャで認定されています。詳細については、P-GW アドミニストレーション ガイド [英語] の「GTP-C Path Failure Enhancements and Enhanced Debugging Tools」の項を参照してください。

GTPP Suppress-CDR No Zero Volume

この機能により、バイト数カウントがゼロの CDR を抑制できるため、OCG ノードが CDR のフラッディングで過負荷になることはありません。CDR は次のように分類できます。

- Final-cdrs：これらの CDR は、コンテキストの最後に生成されます。
- Internal-trigger-cdrs：これらの CDR は、音量制限、時間制限、料金変更、または CLI コマンドを使用してユーザーが生成したインテリムなどの内部トリガーによって生成されます。
- External-trigger-cdrs：これらの CDR は、QoS 変更、RAT 変更などの外部トリガーによって生成されます。final-cdrs や internal-trigger-cdrs と見なされないすべてのトリガーは、external-trigger-cdrs と見なされます。

カスタマーは抑制する CDR を選択できます。

次に示す CLI コマンドは、CUPS でサポートされているさまざまな CDR トリガーで CDR を抑制するのに役立ちます。

- **[default | no] gtpp suppress-cdrs zero-volume { external-trigger-cdr | final-cdr | internal-trigger-cdr }**

ロケーションベースの DNS および PCSCF IP アドレスの選択

ロケーションベースの DNS および P-CSCF の選択により、ロケーション情報に従って DNS サーバーアドレスと P-CSCF IP アドレスを管理するオプションが使用可能となります。

P-GW は、トラッキングエリア識別子（TAI）によって DNS サーバーアドレスと P-CSCF IP アドレス情報を収集します。これは、TAC ベースの仮想 APN（VAPN）の選択によって実現されます。

セッション作成で UE が PCO 要求を送信すると、P-GW は受信したロケーション情報をもとに仮想 APN（VAPN）を選択します。PCO IE を含む選択済みの VAPN（DNS サーバーアドレスと P-CSCF IP アドレスが設定されている）がセッション作成応答で送信されます。

以下に、ロケーションベースの DNS および PCSCF IP アドレスの選択を有効にするための CLI コマンドを示します。

コマンド	説明
Tracking-area-code-range from <*start value*> **to** <*end value*>	トラッキングエリアコードの範囲（0 ～ 65536）を指定します。終了値は常に開始値より大きくなります。
P-cscf priority <*priority*> **ip/ipv6** <*IPv4/Ipv6 address*>	APN の P-CSCF アドレスの優先順位を指定します。Address_priority は 1 ～ 3 までの整数です。最も優先順位が高いのが「1」です。IPv4_address は、IPv4 ドット付き 10 進表記です。IPv6_address は、IPv6 コロン区切り 16 進表記です。
Show apn name <*APN Name*>	APN の PCSCF IP アドレスを表示します。

コマンド	説明
dns primary <*IPv4 address*> **Dns secondary** <*IPv4 address*> **ipv6 dns primary** <*IPv6 address*> **ipv6 dns secondary** <*IPv6 address*>	Primary：APN のプライマリ DNS サーバーを設定します。 Secondary：APN のセカンダリ DNS サーバーを設定します。設定できるセカンダリ DNS サーバーは 1 つのみです。 Address：IPv4 ドット付き 10 進表記で表記された DNS サーバーの IP アドレスです。デフォルト：primary = 0.0.0.0、secondary = 0.0.0.0 dns_address：削除する DNS サーバーの IP アドレスです。IPv4 ドット付き 10 進表記で表記します。
Show apn name <*APN Name*>	APN の DNS IP アドレスを表示します。

MPRA サポート

P-GW は、PCRF を使用する Gx インターフェイスを介した Feature-List-ID 2 の Multiple-Presence Reporting Area 機能のネゴシエーションをサポートします。CNO-ULI 機能は、P-GW や PCRF が Multiple-PRA をサポートしておらず、P-GW と PCRF の両方が CNO-ULI をサポートしている場合にのみ機能します。

IP-CAN セッションのライフタイム中に Multiple-PRA 機能をサポートするために、P-GW は、Presence-Reporting-Area-Information AVP を含む PRA-Install AVP の PCRF からのレポートエリア要求内にある UE プレゼンスの変更を処理します。各 AVP には、Presence-Reporting-Area-Identifier AVP 内の Presence Reporting Area 識別子が含まれています。

Presence Reporting Area（PRA）と Multiple-PRA の詳細については、StarOS P-GW のアドミニストレーション ガイド [英語] の「Presence Reporting Area」の章を参照してください。

No udp-checksum のサポート

この機能は、ダウンリンク サブスクライバ パケットの外部 GTPU ヘッダーで **udp-checksum** が無効になっている、GTPU サービスの CUPS の **no udp-checksum** CLI コマンドをサポートします。ダウンリンクパケットがインターネットから到着すると、GTPU ヘッダーがパケットの先頭に追加され、アクセス側に送信されます。このパケットの外部 UDP レイヤの「チェックサム」値はゼロなので、最適化が可能になり、パフォーマンススループットが向上します。

この機能を有効にするには、次の設定を使用します。

```
configure
  context context_name
    gtpu-service gtpu_service_name
    [ no ] udp-checksum
    end
```

show コマンドと出力

この項では、この機能をサポートするために使用可能な show CLI コマンドについて説明します。

次のコマンドを使用して、**GTPU UDP チェックサム**が有効か無効かを確認します。

- **show gtpu-service all**：すべての GTPU サービスを表示します。
- **show gtpu-service name** *service_name*：特定の GTPU サービス名の情報を表示します。

QUIC IETF の導入

現在のフレームワークでは、プラグイン到達時に、フロー内のすべてのパケットに対してディープ パケット インスペクション（DPI）が実行されます。DPI は、パケットを分析し、確定的なパターンを抽出することによって実行されます。DPI は順番に実行され、アプリケーションの検出とそのサブタイプの分類を行います。プラグインは、DPI 後のフローを除外します。フローは検出後にオフロードされます。QUIC IETF の一部として、初回の QUIC ハンドシェイク パケット（Client Hello/Server Hello）はネットワーク上で暗号化されます。したがって、アプリケーションの検出に使用できる確定的なパターンはありません。p2p プラグインによる、検出用 SNI（Server Name Indication）の復号と取得が新たにサポートされるようになりました。

QUIC IETF の設定

QUIC IETF 復号を有効または無効にするには、次の設定を使用します。

```
configure
  active-charging service acs_service_name
    p2p-detection debug-param protocol-param p2p_quic_ietf_decrypt 1
    end
```

（注） デフォルトでは、CLI は無効になっており、TLS 復号によるパフォーマンスへの影響は最小限です。

egtpinmgr リカバリの最適化

以前は、egtpinmgr タスクが再起動すると、回復にかなりの時間がかかったため、egtpinmgr の回復中に SAEGW が新しいコールを受け入れられず、障害時間が長くなっていました。

ソフトウェアが拡張され、egtpinmgr リカバリの内部アルゴリズムと必要なデータ構造を最適化することで、egtpinmgr タスクが再起動した場合のリカバリ障害期間が最適化されています。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。

（注） egtpinmgr リカバリの最適化は、非 CUPS アーキテクチャでサポートされている既存の機能です。このリリースでは、この機能は CUPS アーキテクチャで認定されています。

クォータホールド時間のサポート

Quota-Hold-Time（QHT）は非アクティブ期間であり、この期間が経過すると、ゲートウェイ（Diameter クライアント）は使用状況を含む課金バケットを返し、クリーンな状態となります。

QHT 値は、OCS によって Multiple-Services-Credit-Control（MSCC）のカテゴリごとに提供されます。また、ゲートウェイには QHT のデフォルト値を設定するオプションがあります。このオプションでは、OCS から QHT AVP が提供されていない MSCC のデフォルト QHT 値を有効にします。

QHT タイマーは、MSCC バケットごとに実行されます。実行時にパケットなしで QHT タイマーが切れると、3GPP 仕様に従って [Reporting-Reason: QHT] として使用状況が報告されます。

OCS から CP で受信した QHT 値は、CUPS 仕様 3GPP TS 29.244 で定義されている「Quota Holding Time」IE で送信されます。また、Quota-Holding-Time IE を UP にプロビジョニングするとともに、Quota-Holding-Time SET に対応するビットを含む Reporting-Trigger が送信されるため、QHT が終了するとレポートが実行されます。

QHT Reporting-Trigger が有効になっている Quota-Holding-Time IE を受信した UP は、非アクティブ期間をモニターするために URR ごとのタイマーを開始します。非アクティブ期間が QHT 時間を超えると、Quota-Holding-Time のトリガーによって UP からの使用状況レポートが開始されます。

CP は、UP から QHT イベントを受信すると、MSCC バケットの使用状況を更新した後、OCS への QHT レポートをトリガーします。

クォータホールド時間の設定

CUPS でクォータホールド時間を有効にするには、次の設定を使用します。

```
configure
  require active-charging
  active-charging service service_name
    credit-control group group_name
      quota-hold-time timer_value
      end
```

注：

- **quota-hold-time**：課金バケットが使用状況を報告し、クリーンな状態になるまでの非アクティブ期間を設定します。

制限事項

QHT（inactivity-timer）は、通常、flow-idle timer よりも大きな値となります。flow-idle timer が QHT よりも大きいと、QHT が経過した後もフローが存在し、[NoQuota Pending-Traffic-Treatment] 設定に従って VPP によって処理される可能性があります。

S-GW ページングの機能拡張

S-GW ページングには、次のシナリオが含まれます。

シナリオ 1：S-GW が MME/S4-SGSN ノードにダウンリンクデータ通知（DDN）メッセージを送信します。MME/S4-SGSN は、DDN Ack メッセージで S-GW に応答します。MME/S4-SGSN からの DDN Ack メッセージを待つ間に、S-GW が優先順位の高いダウンリンクデータを受信した場合、S-GW は MME/S4-SGSN に DDN を再送信しません。

シナリオ 2：DDN が MME/S4-SGSN に送信され、TAU/RAU MBR が別の MME/S4-SGSN から受信された場合、S-GW は DDN を送信しません。

シナリオ 3：DDN が MME/S4-SGSN に送信され、[Cause] が 110 の DDN Ack を受信します。原因が 110 の DDN Ack は DDN 障害として扱われ、標準の DDN 障害アクション手順が開始されます。

これらのシナリオに対処するため、CUPS アーキテクチャの DDN 機能に次の 2 つの拡張機能が追加されました。

- S-GW での高優先順位 DDN
- MBR-DDN コリジョン処理

これらの拡張機能は、次をサポートします。

- S-GW および SAEGW での高優先順位 DDN。これにより、MME/S4-SGSN によるページングの優先順位付けが可能になります。
- ページング KPI および VoLTE サービスの拡張。
- DDN が失われないようにするための DDN メッセージとモビリティ手順。
- MBR ガードタイマー。一時的な HO を含む DDN Ack を受信すると開始されます。CLI コマンド **ddn temp-ho-rejection mbr-guard-timer** が導入され、原因が 110（一時的なハンドオーバーが進行中）の DDN Ack を受信した後、ガードタイマーによって MBR を待機できるようになりました。
- 制御ノードの変更によってトリガーされた DDN による TAU/RAU。

さらに、3GPP 標準規格に準拠するため、ダウンリンクデータ通知メッセージおよびモビリティ手順のサポートも強化されます。これにより、DDN メッセージと DDN をトリガーするダウンリンクデータが失われることがなくなります。そのため、SIP Invite データが原因で DDN が開始されるシナリオにおいて、ページング KPI と VoLTE の成功率が向上します。

（注） DDN 遅延および DDN スロットリングをサポートするダウンリンクデータ通知（DDN）メッセージについては、このガイドの「*DDN* 遅延および *DDN* スロットリングを使用した *SAEGW* アイドルバッファリング」の章を参照してください。

S-GW ページング拡張機能の動作、設定、モニタリング、および障害対応の詳細については、StarOS の『*S-GW Administration Guide*』[英語] の「*S-GW Paging Enhancements*」の章を参照してください。

ユーザープレーンでのセッションリカバリ

クラッシュ発生時のセッション マネージャ プロセスのリカバリが、新たにサポートされるようになりました。回復したセッションマネージャには、直近にクラッシュしたセッション マネージャ プロセスの既存のサブスクライバセッションがすべて含まれます。

回復したすべてのサブスクライバセッションについて、アップリンクおよびダウンリンクのデータフローは、新たに回復したセッション マネージャ プロセスで処理されます。

SRVCC PS から CS へのハンドオーバー指示および QoS クラスインデックス IMS メディア設定のサポート

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原因を PCRF に通知します。この通知は、PCRF が適切に追加のアクションを実行するのに役立ちます。

この機能により、SRVCC のコンプライアンスが保証されます。この機能は、音声ベアラーの解放後の PS から CS へのハンドオーバー通知もサポートします。

LTE の SRVCC サービスを使用すると、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）で、LTE ネットワークから回線交換ドメインに切り替えることができます。1 つのアクセスネットワークだけで送受信に対応している間に、UE はネットワークを切り替えます。SRVCC サービスにより、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、送信元 MME は音声ベアラー（VB）を削除します。MME は、音声ベアラーを非アクティブ化することで VB を削除します。MME は、S-GW/P-GW に対する VB を禁止し、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 フラグを設定します。

IP-CAN ベアラーの終了は、PS から CS へのハンドオーバーが原因で発生します。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 ルールを報告します。

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）のサポートは、PS から CS への連続性のベアラーサポートを示します。

QCI IMS メディア設定のサポート

セッションリカバリおよびICSRスイッチオーバー時の優先処理対象のIMSメディアベアラーをマークするには、QoS Class Index（QCI）の値を指定します。

モード

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context <*context_name* > **apn** <*apn_name*>

上記のコマンドシーケンスを入力すると、次のプロンプトが表示されます。

[context_name]host_name(config-apn)#

構文

qci *value_bytes* **ims-media**

no qci *value_bytes* **ims-media**

（注）

- *no*：この IMS QCI 機能を無効にします。
- *ims_media*：セッションリカバリおよびICSRスイッチオーバー時の優先処理対象のIMSメディアとして分類されたベアラーにマークを付けます。
- *value_bytes*：QCI 値を 1 ～ 254 の整数で指定します。

使用上のガイドライン

このコマンドを使用すると、セッションリカバリおよびICSRスイッチオーバー時に優先的に処理するIMSメディアとして分類されたベアラーをマークするためのQCI値を指定できます。

この機能の導入には、次の前提条件が適用されます。

- 専用の APN を VoLTE トラフィック用に予約する必要があります。
- この APN に接続されたコールは、VoLTE に設定された QCI に一致する専用ベアラーがない限り、アクティブ VoLTE として分類されません。
- 優先処理は、アクティブな VoLTE であるコールにのみ適用されます。
- この APN に接続されたGGSNコールは、VoLTE に設定された QCIに一致するネットワーク開始ベアラーがない限り、アクティブ VoLTE として分類されません。
- VoLTE マーキングは、Gn-Gp ハンドオフで保持されます。

CLI コマンドを使用してこの機能を有効にすると、次のアクションが実行されます。

- ベアラーの作成時
  - 新しいベアラー QCI が APN 設定と照合されます。

- QCI が APN 設定と一致する場合、ベアラーは優先処理の対象としてマークが付けられます。
- Flow_entries はこの情報で変更されます（これが最初の VoLTE ベアラーの場合）。
- Egtpu_session は、rx_setup 要求中に VoLTE タグで更新されます。
- 通知メッセージは、VoLTE のタグ付けについて ECS に通知します。

- ベアラーの削除時
  - これが最後の VoLTE ベアラーである場合、Flow_entry は VoLTE 情報を使用して更新されます。
  - ECS には、指示メッセージを介して削除が通知されます。

次のコマンドは、QCI が 9 の IMS ベアラーの優先処理を有効にします。

qci 9 ims-media

ip hide-service-address CLI コマンドのサポート

ip hide-service-address CLI コマンドは CUPS でサポートされます。

この CLI を有効にすると、この APN を使用する GGSN の IP アドレスがモバイルステーション（MS）から到達不能になります。このコマンドは、APN ごとに設定します。

この機能を有効または無効にするには、次の設定を使用します。

```
configure
  context context_name
    apn apn_name
      [ default | no ] ip hide-service-address
      end
```

- **default**：モバイルステーションがこの APN を使用して GGSN IP アドレスに到達することを許可しません。
- **no**：モバイルステーションがこの APN を使用して GGSN IP アドレスに到達することを許可します。
- このコマンドを使用して、サブスクライバがトレースルートを使って、公的領域内にあり、サービスに設定されているネットワークアドレスを検出しないようにします。

regardless-of-other-triggers CLI コマンドのサポート

この機能は、CUPS の CLI で **regardless-of-other-triggers** オプションをサポートします。**regardless-of-other-triggers** オプションは、合間に発生する他の eG-CDR または P-GW-CDR トリガーに関係なく、一定の時間間隔での eG-CDR または P-GW-CDR の生成を有効にします。したがって、このオプションを有効にすると、他の CDR トリガーが発生しても、Time Limit

CDR は秒単位の [interval] ごとに動的にトリガーされます。つまり、[Time Threshold] は、前回のしきい値時間とこの間隔の合計をもとに計算されます。このオプションは、セッションリカバリと ICSR をサポートします。

この機能を有効にするには、次の設定を使用します。

```
configure
  active-charging service service_name
    rulebase rulebase_name
      egcdr threshold interval interval regardless-of-other-triggers
      end
```

新しいコールを受信すると、次の手順が実行されます。

- 有効にすると、**regardless-of-other-triggers** の間に他の使用状況レポートがトリガーされてもタイマーはリセットされず、設定された間隔ごとに時間しきい値に対応するセッション使用状況レポートが生成されます。

show コマンドと出力

ここでは、この機能をサポートするために使用可能な show CLI コマンドについて説明します。

- **show active-charging rulebase name** *name*
- **show active-charging rulebase all**

これらの CLI コマンドの出力には、この機能をサポートする次のフィールドが含まれます。

- Interval Threshold：<seconds> (secs) Regardless of Other Triggers

デフォルトベアラーの TFT 抑制

機能説明

デフォルトベアラーの TFT 抑制は、UPC CUPS アーキテクチャでサポートされています。この機能をサポートするために、次の CLI コマンドが追加されました。

- **policy-control update-default-bearer**
- **no tft-notify-ue-def-bearer**

上記の CLI コマンドを使用して、QoS および ARP を使用せずに、またはデフォルトのベアラーと同じ QoS および ARP を使用して PCRF から受信したすべての定義済みルールをデフォルトのベアラーにバインドします。

重要 この CLI は、シャーシ設定のすべてのルールベースに適用されます。その間またはその後にルールベースが変更された場合、この CLI は現在の新しいルールベースにも引き続き適用されます。

TFT 抑制の設定

デフォルトベアラーの事前定義ルールの TFT 抑制の設定

デフォルトベアラーの TFT 抑制を設定するには、次のコマンドを使用します。

```
configure
  require active-charging
  require active-charging service_name
    [ default | no ] policy-control update-default-bearer
    end
```

注意 **no policy-control update-default-bearer** CLI コマンドを実行する際、charging-action に TFT 情報が追加されていないと、システムクラッシュが発生する可能性が高くなります。

デフォルトベアラーの TFT 抑制の設定

デフォルトベアラーの TFT 抑制を設定するには、次のコマンドを使用します。

```
configure
  require active-charging
  require active-charging service_name
    rulebase rulebase_name
      [ default | no ] tft-notify-ue-def-bearer
    end
```

（注）

- **default**：このコマンドにデフォルト設定を設定します。

  デフォルトベアラーの QoS を持つルールのみデフォルトベアラーへのバインドを無効にし、他のルールを無視しないように指定します。ルールはそれぞれの QoS に応じて、適切なベアラーにアタッチされます。また、UE（アクセス側）への TFT 更新は抑制されません。

- **no**：デフォルトベアラーの QoS を持つルールのデフォルトベアラーへのバインドを有効にし、他のルールを無視するよう指定します。

  QoS が指定されていない場合、ルールはデフォルトベアラーにアタッチされます。また、デフォルトベアラーでは、UE（アクセス側）への TFT 更新が抑制されます。このため、作成される default-bearer は常に 1 つのみです。

ゼロバイト EDR 抑制

CLI 制御機能であるゼロバイト イベント データ レコード（EDR）抑制は、フローのデータがない場合の EDR の作成を有効または無効にします。通常、ゼロバイト EDR は、フローに対し

て2つの連続するEDRが生成される場合に可能です。CLIコマンドは、フローの2番目のEDRを抑制します。

ゼロバイトEDRの抑制を有効または無効にするには、次の設定を使用します。

```
configure
  active-charging service service_name
    rulebase rulebase_name
      [ default | no ] edr suppress-zero-byte-records
      end
```

注：

- **default**：デフォルト設定でこのコマンドを設定します。

  デフォルト：[Disabled]。**no edr suppress-zero-byte-records** と同じ。

- **no**：ゼロバイトEDRの抑制を無効にします。

- **edr suppress-zero-byte-records**：ゼロバイトEDRを抑制します。

- **show user-plane-service statistics rulebase name** *rulebase_name* CLIコマンドの出力の「Total zero-byte EDRs suppress」フィールドを使用して、ゼロバイトEDRが抑制されているか確認できます。

機能の仕組み

この項では、ユーザープレーンサービスのコールフローについて説明します。

コール フロー

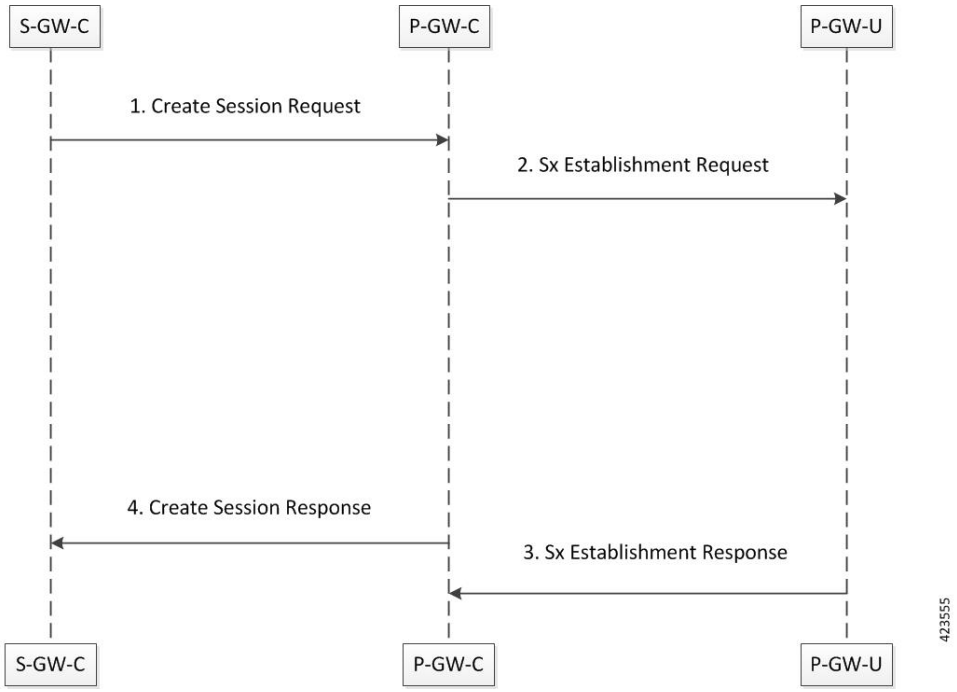
ここでは、CUPSアーキテクチャのユーザー プレーン コール フローについて説明します。

P-GW データセッション

ここでは、P-GWの初期接続手順について説明します。

初期接続手順（Pure P）

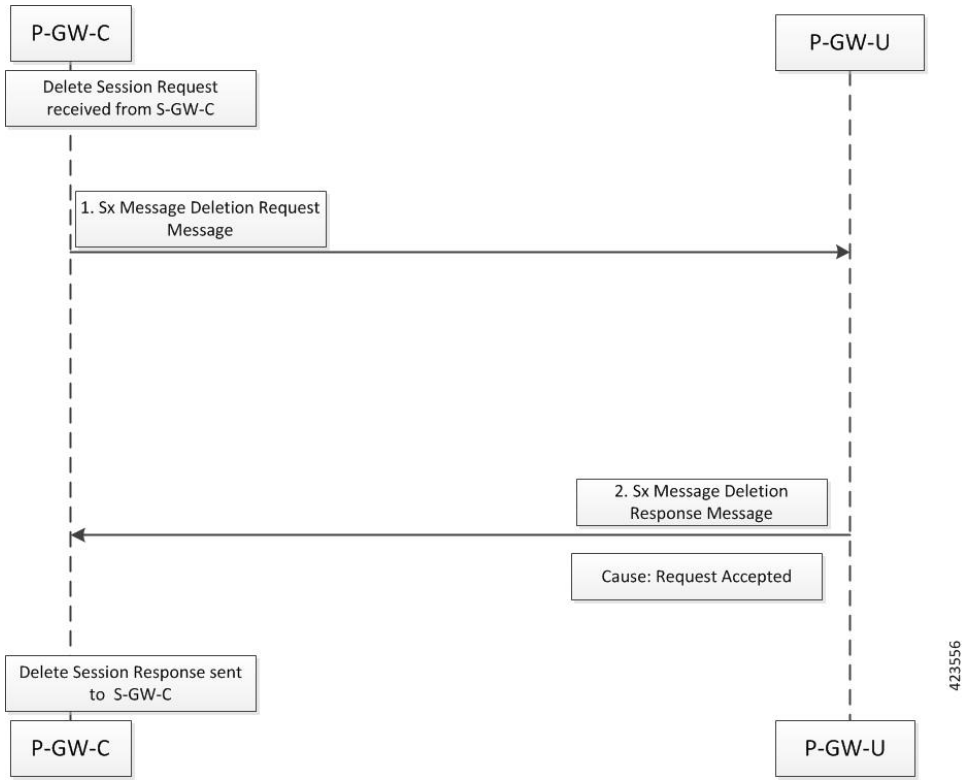
次のコールフローは、Pure-P PDNの初期接続手順の概要を示しています。



- P-GW は S5/S8 インターフェイスで APN を含むセッション作成要求メッセージを受信します。
- P-GW-C はデータパスを確立するために、PRD、FAR 情報を使用して、Sxb インターフェイスから選択された P-GW-U に向けて Sx 確立要求を開始します。PGW-C は TEID（トンネル識別子）の割り当てをサポートしていません。 トンネル識別子は PGW-U によって割り当てられます。
- リソースが割り当てられると（TEID など）、P-GW-U は P-GW-C に Sx 確立応答メッセージを送信します。
- P-GW は、割り当てられたアドレス、TEID、および追加情報を含む Create Session Response メッセージで S-GW に応答します。
- S5/S8 データプレーントンネルが確立され、PGW-U は PDN との間でパケットを送受信できます。

初期切断手順（Pure P）

次のコールフローは、Pure-P PDN の初期切断手順の概要を示しています。



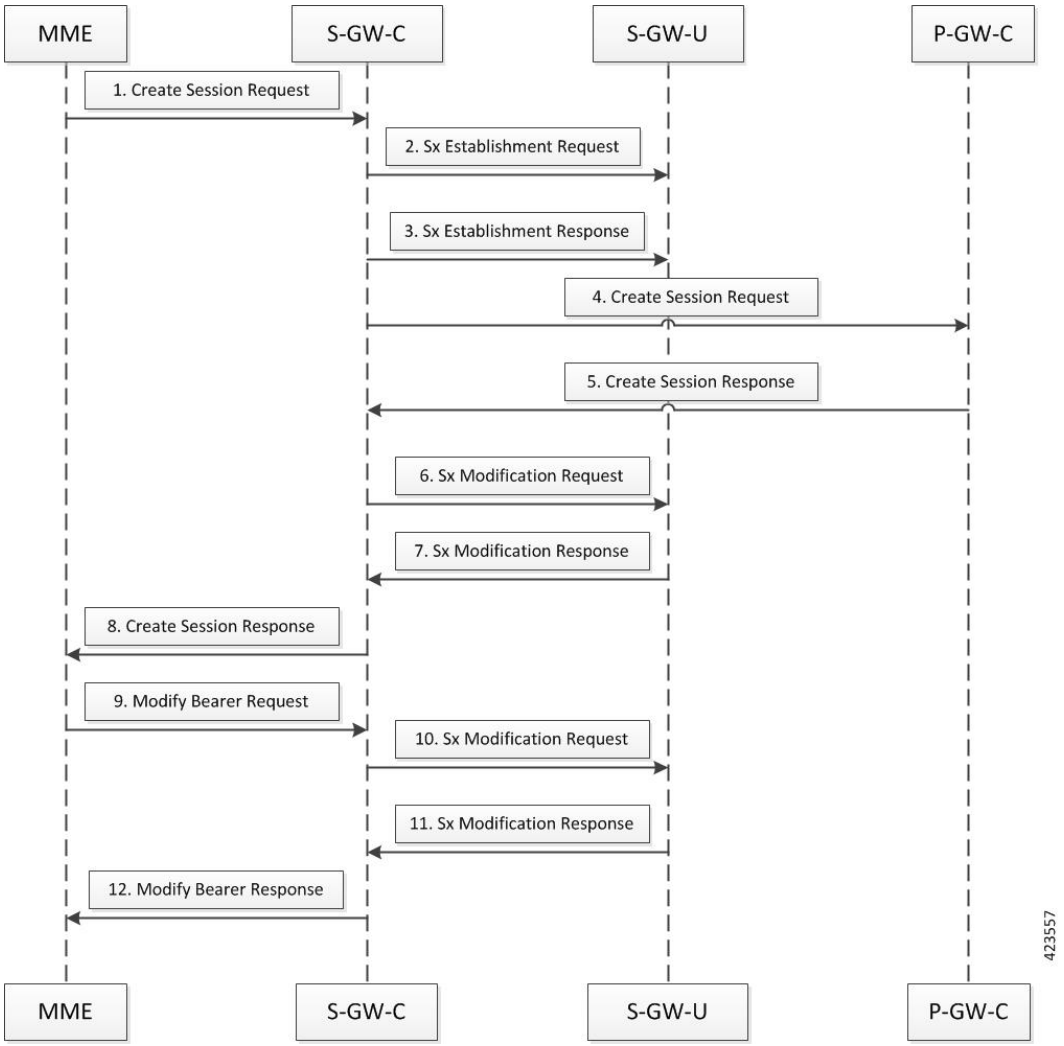
- P-GW は S5/S8 インターフェイスで APN を含むセッション作成要求メッセージを受信します。
- P-GW-C はデータパスを確立するために、PRD、FAR 情報を使用して、Sxb インターフェイスから選択された P-GW-U に向けて Sx 確立要求を開始します。PGW-C は TEID（トンネル識別子）の割り当てをサポートしていません。 トンネル識別子は PGW-U によって割り当てられます。
- リソースが割り当てられると（TEID など）、P-GW-U は P-GW-C に Sx 確立応答メッセージを送信します。
- P-GW は、割り当てられたアドレス、TEID、および追加情報を含む Create Session Response メッセージで S-GW に応答します。
- S5/S8 データプレーントンネルが確立され、PGW-U は PDN との間でパケットを送受信できます。

S-GW データセッション

ここでは、S-GW の初期接続手順について説明します。

初期接続手順（Pure S）

次のコールフローは、Pure-S PDN の初期接続手順の概要を示しています。

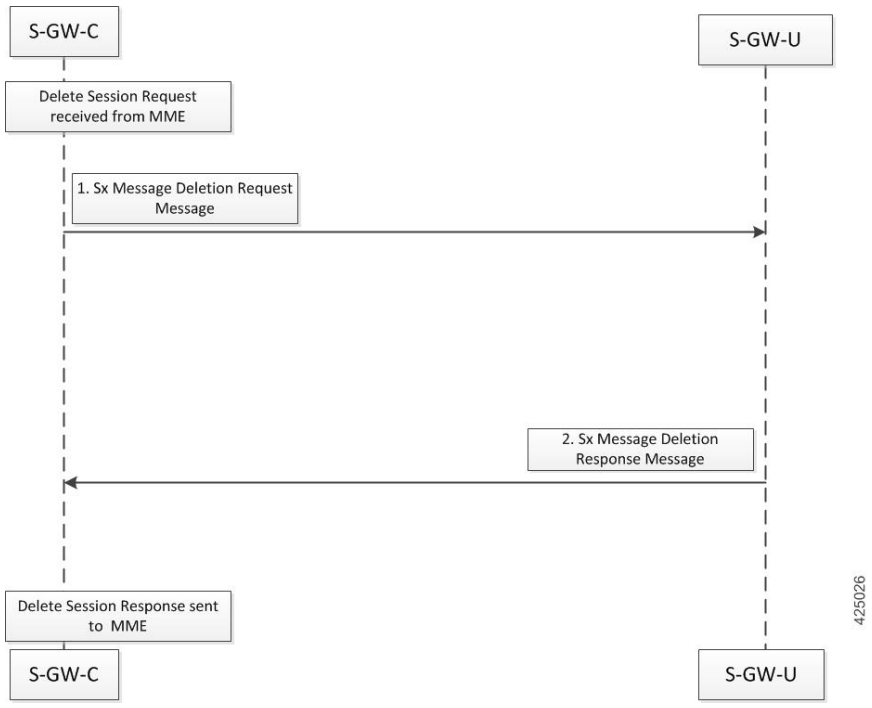


- S11 インターフェイスで、S-GW-C は MME から、アクセスポイント名（APN）を含むセッション作成要求メッセージを受信します。
- S-GW-C は、データパスを確立するため、選択した S-GW-U への Sxa インターフェイスで PDR、FAR 情報を含む Sx 確立要求を開始します。このとき、S-GW-C による TEID（トンネル識別子）の割り当てはサポートされません。割り当ては S-GW-U が行います。
- egree TEID などのリソース割り当て後、S-GW-U は S-GW-C に対して Sx 確立応答メッセージを送信します。
- S-GW-C は、選択した P-GW-C に対してセッション作成要求を開始します。
- P-GW-C は、IP アドレスとデフォルトベアラー関連情報を含むセッション作成応答で応答します。
- SGW-C は、既存のセッションの FAR（転送アクション）情報を更新するため、SGW-U に対して Sx 変更要求メッセージを開始します。

- SGW-U は、情報を更新した後、Sx 変更の成功応答を返します。
- SGW-Cは、デフォルトベアラーに必要なすべての情報を含むセッション作成応答をMMEに送信します。
- MME は、eNodeB の F-TEID 情報を受信すると、SGW-C に対するベアラー変更要求メッセージを開始します。
- SGW-C は、eNodeB の F-TEID の FAR 情報を更新するため、SGW-U に対して Sx 変更要求を開始します。
- 正常に更新されると、Sx 変更応答が SGW-C に送信されます。
- 今度は SGW-C が MME に変更応答メッセージを送信して、接続手順を完了します。
- SGW-U では、eNodeB への S1U 側のデータトンネルと PGW-U への S5/S8 側のデータトンネルが確立しました。これで SGW-U は、PGW および eNodeB との間でパケットを送受信できます。
- S5/S8 データプレーントンネルが確立され、PGW-U は PDN との間でパケットを送受信できます。

初期切断手順（Pure S）

次のコールフローは、Pure-S PDN の初期切断手順の概要を示しています。



- MME からセッション削除要求を受信すると、SGW は SGW-U への Sx 削除要求メッセージを開始します。

- SGW-Uは、割り当てられたすべてのユーザープレーンリソースをクリアし、Cause Successとともに SGW-C に応答します。
- SGW-C は、セッション削除応答メッセージで MME に応答します。

S-GW の専用ベアラーの追加、削除、および更新のサポート

機能説明

CUPS アーキテクチャでは、Pure-S コール向けの専用ベアラーの追加、削除、および更新がサポートされています。

この機能をサポートするため、次の機能が追加されています。

- SAEGW-CP は、Pure-S コール専用ベアラーのベアラー作成要求をサポートします。
- SAEGW-CPは、単一のベアラー作成要求で複数のベアラーコンテキストに対応できます。
- SAEGW-CP は、異なる PDN に対する複数のベアラー作成要求を並行してサポートします。これらの PDN は、Pure-S PDN または Collapsed と Pure-S の組み合わせです。
- SAEGW-UP は、ベアラーごとに Pure-S コールの VPP でアップリンク方向とダウンリンク方向のベアラーストリームを作成します。各方向ごとのストリーム数は、GTP-Uサービスの IP アドレスによって異なります。
- SAEGW-CP は、専用ベアラーを使用したアクセスベアラー解放（RAB）要求をサポートしているため、すべてのベアラーに対応するすべての FAR が変更されます。
- SAEGW-CP は、専用ベアラーを使用したベアラー変更要求（アイドルモード、接続モード）をサポートします。
- SAEGW-CP は、MME からのベアラー作成応答の障害処理をサポートします。
- SAEGW-CPおよびSAEGW-UPは、VPPを使用したデフォルトおよび専用ベアラーのDSCPマーキングをサポートします。
- SAEGW-CPおよびSAEGW-UPは、専用ベアラーのベアラー削除要求をサポートします。SAEGW-UP は、それらのベアラーに属するベアラーストリームと TEP エントリを削除します。
- SAEGW-CP は、コールがアイドル状態の場合に Pure-S 専用ベアラーの作成をサポートします。
- SAEGW-CP は、Pure-S 専用ベアラーの S-GW 再配置（X2 ベースと S1 ベースの両方）をサポートします。
- SAEGW-CP は、Pure-S 専用ベアラーの更新シナリオをサポートします。
- SAEGW-CP は、セッション作成応答とともに Pure-S コール専用ベアラーのベアラー作成要求のピギーバックをサポートします。
- SAEGW-CP は、ベアラー変更要求とともに Pure-S コール専用ベアラーのベアラー作成応答のピギーバックをサポートします。

- P-GW が CCA-I の一部としてベアラー作成を受信し、P-GW がピギーバック要求を送信しない場合、SAEGW-CP は Pure-S 専用ベアラ—の作成をサポートします。この結果、セッション作成応答の後にベアラー作成要求が続きます。
- SAEGW-CP は、Pure-S 専用ベアラーを使用したセッションリカバリと ICSR をサポートします。
- SAEGW-CP は、ベアラー作成要求とベアラー削除要求（デフォルトのベアラー）のコリジョンをサポートします。
- SAEGW-CP は、ベアラー作成要求とセッション削除要求のコリジョンをサポートします。
- SAEGW-CP は、ベアラー作成応答とベアラー削除要求（デフォルトのベアラー）のコリジョンをサポートします。
- SAEGW-CP は、ベアラー作成応答とセッション削除要求のコリジョンをサポートします。
- SAEGW-CP は、Pure-S のデフォルトおよび専用ベアラーを使用した終了マーカーをサポートします。
- SAEGW-UP は、Pure-S のデフォルトおよび専用ベアラーを使用したセッションリカバリをサポートします。
- SAEGW-UP は、アイドル状態からアクティブ状態に遷移中の IPv4 から IPv6 へ、または IPv6 から IPv4 への IP トランスポートの動作、および S1U インターフェイスでのハンドオーバー手順をサポートします。接続時に S1U で選択されたトランスポートがサポートされます。たとえば、IPv4 eNodeB から IPv6 eNodeB への eNode ハンドオーバーが該当します。
- SAEGW-CP は、原因が Partially Accepted および Context Not Found の CBRsp をサポートします。
- SAEGW-CP は Pure-S コールのダウンリンク方向のデータ通知をサポートしているため、UE が Pure-S コールでアイドル状態に遷移すると、FAR アクションはバッファに設定されます。
- SAEGW-CP は、原因が PARTIALLY_ACCEPTED でコンテキストが見つからない場合のベアラー更新応答をサポートします。
- SAEGW-CP は、ユーザープレーンノードを含む他のピアノードからのエラー処理と障害処理をサポートします。

制限事項

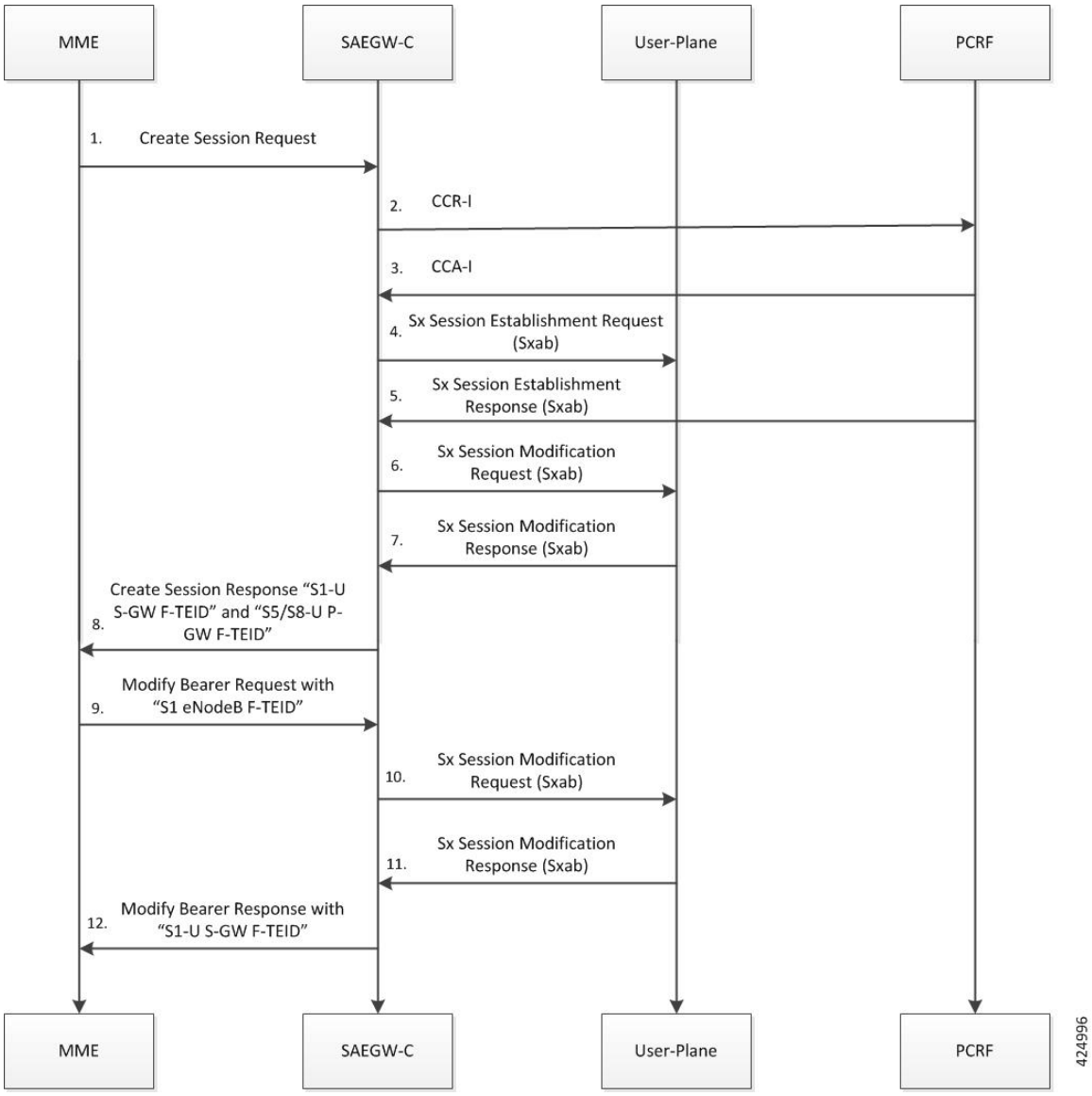
Pure-S コールの場合、アイドル セッション タイムアウトはサポートされていません。

Collapsed コールのサポート

次のコールフローは、UE が開始した Collapsed PDN の切断手順の概要を示しています。

初期接続手順（Collapsed PDN）

次のコールフローは、Collapsed PDN の初期接続手順の概要を示しています。



1. CUPS SAEGW Collapsed コールの場合、SAEGW-C で次の処理が実行されます。
   - Gx インタラクション後、Gx 通信（CCR-I および CCA-I）を実行します。
   - IP プール（IP プールに関連付けられた APN）を使用して設定された **user-plane-profile** に基づいてユーザープレーンを選択します。
   - GTP-U セッションを確立します（IPv6/IPv4v6 PDN の場合、RA/RS に必要）。
   - 選択したユーザープレーンと Sxab のインタラクションを実行します。
2. Sx 確立要求には、次の情報が含まれます。

- S-GW アップリンクおよびダウンリンクデータパス（Sxa タイプ PDR）の Create PDR/FAR 情報。
- アップリンクおよびダウンリンクデータパス（Sxb タイプ PDR）の Create PDR/FAR/URR 情報。ダイナミック/事前定義/静的ルールの場合。
- RA/RS（Sxb タイプ PDR）の Create PDR/FAR：IPv6/IPv4v6 PDN タイプに必要。
- さらに、次の目的で F-TEID を割り当てるように、コントロールプレーンがユーザープレーンに要求します。
  - S-GW 入力「S1-U S-GW F-TEID」
  - S-GW 出力「S5/S8-U S-GW F-TEID」
  - P-GW 入力 PDR「S5/S8-U P-GW F-TEID」

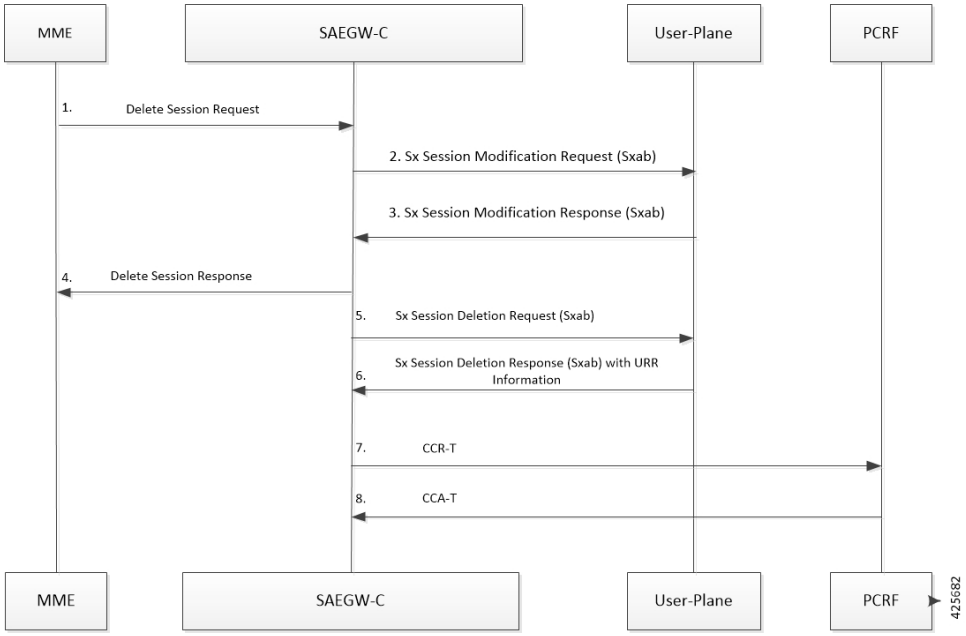
3. ユーザープレーンは、Sx セッション確立応答の一部として次の情報を提供します。
   - 作成された PDR：S-GW 入力 PDR「S1-U S-GW F-TEID」
   - 作成された PDR：S-GW 出力 PDR「S5/S8-U S-GW F-TEID」
   - 作成された PDR：P-GW 入力 PDR「S5/S8-U P-GW F-TEID」
4. 正常な Sx セッション確立応答を受信すると、コントロールプレーンは次の情報を使用して Sx 変更要求をトリガーします。
   - 「S5/S8-U S-GW F-TEID」の IP アドレス情報に基づいて「Outer Header Removal」を使用して P-GW（Sxb）の「アップリンク PDR」を更新
   - 「Outer Header Creation」を「S5/S8-U S-GW F-TEID」として P-GW（Sxb）の「ダウンリンク FAR」を更新
   - 「Outer Header Creation」を「S5/S8-U P-GW F-TEID」として S-GW（Sxa）の「アップリンク FAR」を更新
   - 「S5/S8-U P-GW F-TEID」の IP アドレス情報に基づいて「Outer Header Removal」を使用して S-GW（Sxa）の「ダウンリンク PDR」を更新
5. Sx セッション変更応答を受信すると、SAEGW-C は「S1-U S-GW F-TEID」および「S5/S8-U P-GW F-TEID」を使用してセッション作成応答を MME に送信します。
6. ベアラー変更要求（MBR）を受信すると、SAEGW-C で次の処理が実行されます。
   - Sx セッション変更要求のトリガー：
     - 「Outer Header Creation」を「S1 eNodeB F-TEID」としてダウンリンク FAR を更新します。
     - 「S1 eNodeB F-TEID」の IP アドレス情報に基づいて、「Outer Header Removal」を使用してアップリンク PDR を更新します。

7. Sx セッション変更応答を受信すると、SAEGW-SGW-C は「S1-U S-GW F-TEID」を使用して MBR を送信します。

初回接続解除手順（Collapsedコール）

切断手順（*Collapsed*）：*UE* 開始

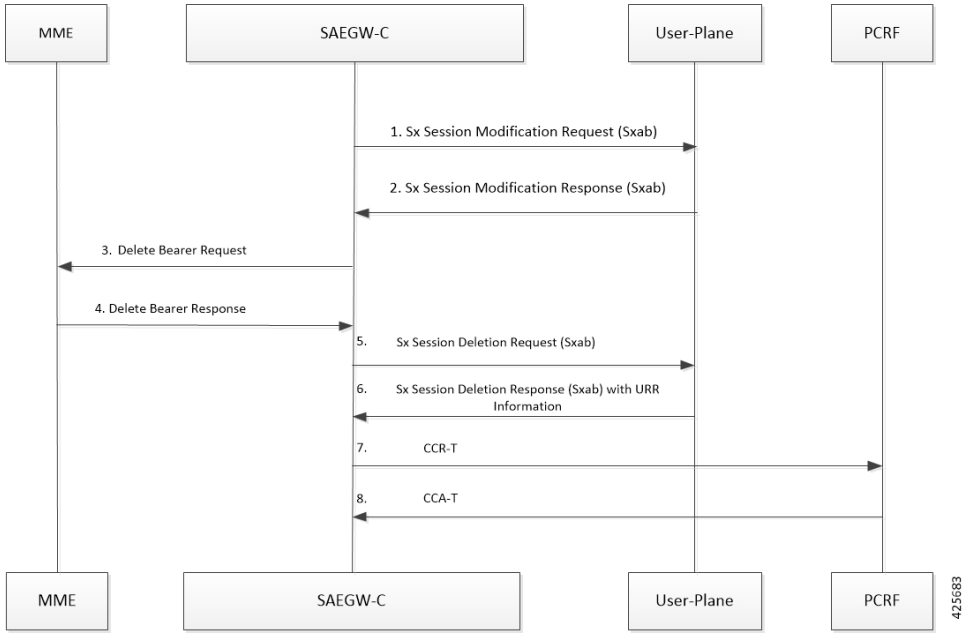
次のコールフローは、UE が開始した Collapsed PDN の切断手順の概要を示しています。



1. セッション削除要求を受信すると、SAEGW-C は Sxab インタラクションを実行し、アップリンクとダウンリンクの両方のデータパスに対する Apply Action を「DROP」として FAR を更新します。
2. Sx セッション変更応答を受信すると、SAEGW-C は MME にセッション削除応答を送信します。
3. CUPS SAEGW Collapsed コールの場合、SAEGW-C で次の処理が実行されます。
   - GTP-U セッションを削除します（IPv6/IPv4v6 PDN の場合は RA/RS に必要）。
   - 選択したユーザープレーンとの Sxab インタラクションを実行します。
4. Sx セッション削除応答を受信すると、SAEGW-C で次の処理が実行されます。
   - Gx 通信（CCR-T および CCA-T）を実行します。
   - 受信した URR 情報に基づいて CDR（Gz）を生成します。

接続解除手順（*Collapsed*）：ネットワーク開始

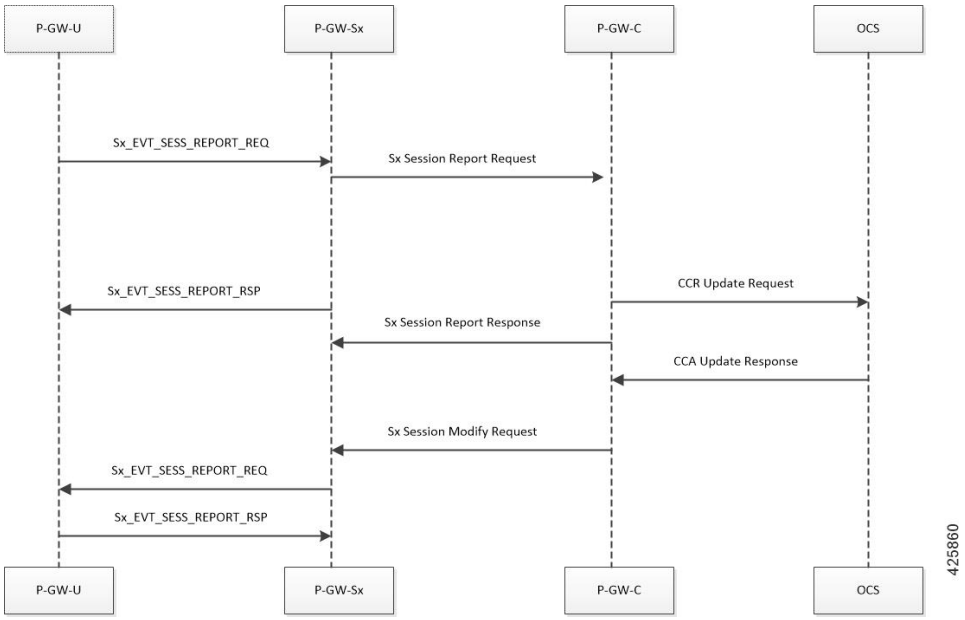
次のコールフローは、ネットワークが開始した Collapsed PDN の接続解除手順の概要を示しています。



1. ベアラー削除要求（RAR により開始されたもの、または **clear sub all** CLI によるもの）を受信すると、SAEGW-C は Sxab インタラクションを実行し、アップリンクとダウンリンクの両方のデータパスに対する適用アクションを「DROP」にして FAR を更新します。
2. Sx セッション変更応答を受信すると、SAEGW-C は MME にベアラー削除要求を送信します。
3. CUPS SAEGW Collapsed コールの場合、SAEGW-C で次の処理が実行されます。
   - GTP-U セッションを削除します（IPv6/IPv4v6 PDN の場合は RA/RS に必要）。
   - 選択したユーザープレーンとの Sxab インタラクションを実行します。
4. Sx セッション削除応答を受信すると、SAEGW-C で次の処理が実行されます。
   - Gx 通信（CCR-T および CCA-T）を実行します。
   - 受信した URR 情報に基づいて CDR（Gz）を生成します。

Gy インターフェイスを使用した P-GW セッションレポート

ここでは、Gyインターフェイスを使用したP-GWセッションのレポートについて説明します。



セッション確立要求での URR サポート

- ユーザープレーンモジュールは、セッション確立要求の一部として受信した URR のリストの保存をサポートします。
- 各 PDR は、1 つ以上の URR に関連付けられます。
- 特定の URR が別の URR にリンクされます。
- 各 URR には、測定方法（時間またはボリューム）と、ユーザープレーンが使用状況レポートを送信する必要があるイベントを示すレポートトリガーが含まれています。
- URR には、Gy-URR のボリュームクォータとボリュームしきい値の両方が存在します。

セッション削除応答

ユーザープレーンから送信されるこのメッセージは、コントロールプレーンからのセッション削除要求への応答です。このメッセージにより、ユーザープレーンで Sx セッションが終了します。使用状況レポートは、Sx セッション削除応答の一部として含まれています。

セッションレポート要求および応答メッセージ

要求メッセージ

- 時間またはボリュームのしきい値制限に達すると、ユーザープレーンは Sx セッションレポート要求メッセージを生成して、コントロールプレーンに送信します。
- このメッセージには、使用状況レポートトリガーで指定された、メッセージの生成理由を示す使用状況レポートが含まれます。
- さらに、使用状況レポートには、時間またはボリュームの測定値が含まれます。

- セッションレポート要求が生成されている URR に他の URR がリンクされている場合、リンクされている URR に対してもセッションレポート要求が生成されます。このリリースでは、Gy-URR はいずれの URR ともリンクされていません。

応答メッセージ

コントロールプレーンからの応答メッセージは、原因コードを含むセッションレポート要求メッセージが正常に配信されたことを示します。現在、障害の原因を受信した場合に実行される特定の障害処理はありません。

Gy のサーバー到達不能サポート

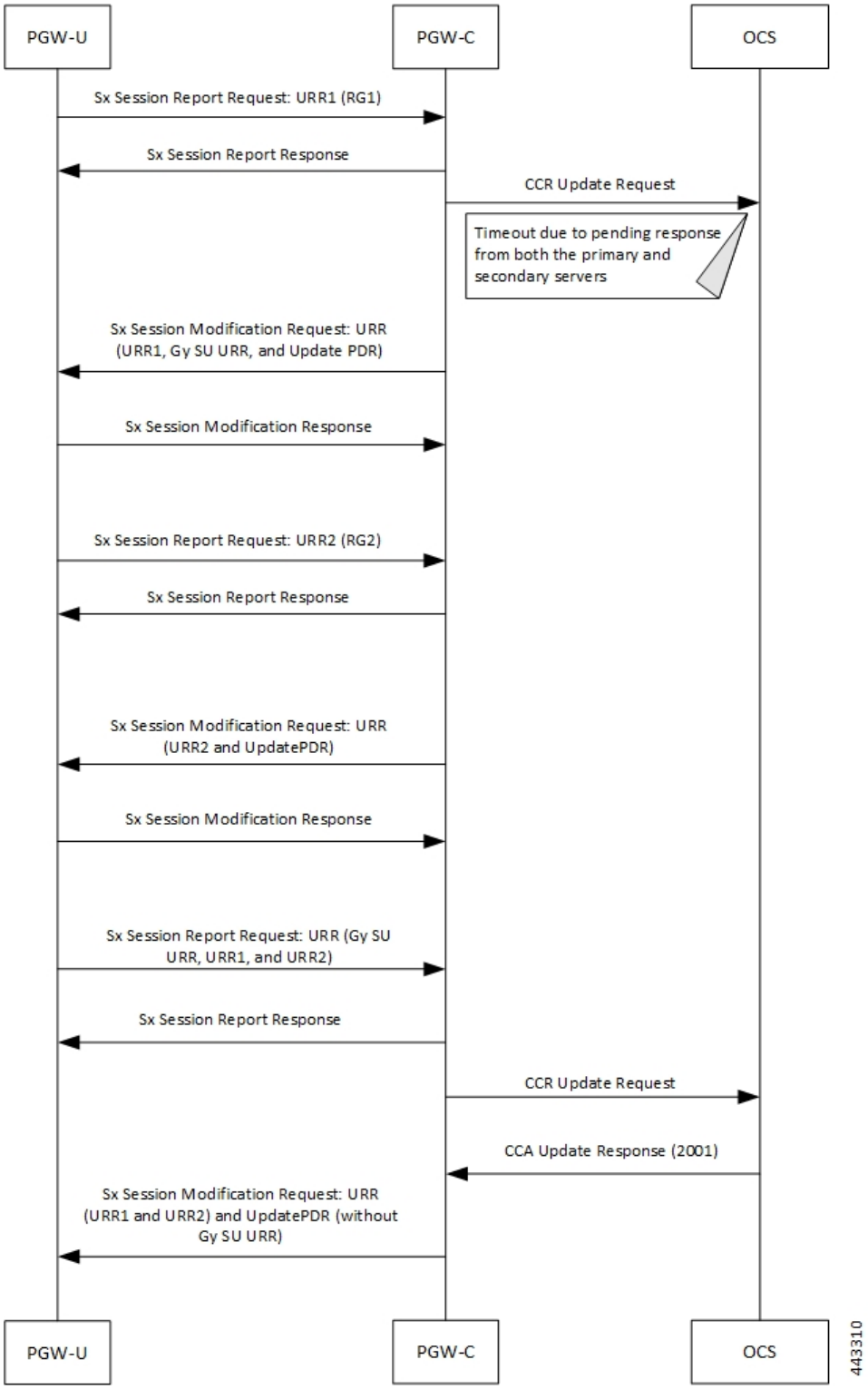
オンライン課金システム（OCS）で発生した問題、またはポリシー/課金適用機能（PCEF）と OCS 間の接続で発生した問題を解決するため、コントロールプレーン（CP）で Gy インターフェイスに対する Server-Unreachable（SU）メカニズムが設定されます。SU 設定により、障害発生後でもセッションを継続できるようになります。そのためのオプションとして、セッションがオフラインに変換されるまたは終了されるまでの暫定クォータ（ボリュームや時間）とサーバー再試行回数を設定できます。

新しい使用状況レポートルール（URR）バケットが作成されます。このバケットには、Gyセッションが SU 状態になったときの SU クォータが含まれます。新しい URR の ID は、SU URR が割り当てられると動的に生成されます。

CUPS ユーザープレーン（UP）ノードでは、既存の Vector Packet Processor（VPP）ストリームが新しい LC レコードによって変更されます。このレコードには、更新された SU URR バケットと既存の課金バケットが含まれます。

VPP ストリームが SU 状態の場合、GyURR と SU URR の 2 つのクォータ行を使用できます。GyURR が [linked-usage-reporting] トリガーが設定された状態で SU 状態になった場合、SU URR のクォータ行は VPP ストリームにリンクされます。

ここでは、CUPS における SU コールフローについて説明します。


PGW-U
PGW-C
OCS
Sx Session Report Request: URR1 (RG1)
Sx Session Report Response
CCR Update Request
Timeout due to pending response from both the primary and secondary servers
Sx Session Modification Request: URR (URR1, Gy SU URR, and Update PDR)
Sx Session Modification Response
Sx Session Report Request: URR2 (RG2)
Sx Session Report Response
Sx Session Modification Request: URR (URR2 and UpdatePDR)
Sx Session Modification Response
Sx Session Report Request: URR (Gy SU URR, URR1, and URR2)
Sx Session Report Response
CCR Update Request
CCA Update Response (2001)
Sx Session Modification Request: URR (URR1 and URR2) and UpdatePDR (without Gy SU URR)
PGW-U
PGW-C
OCS
443310

ステップ	説明
1	PGW-U は、[Time and Volume] または [Quota and Threshold] などの内部トリガー URR1（RG-1）を含む Sx セッションレポート要求メッセージを PGW-C に送信
2	PGW-C は要求を確認し、Sx セッションレポート応答メッセージを PGW-U に す。
3	PGW-C は、プライマリ OCS とセカンダリ OCS の両方に CCR 更新（CCR-U）メッセージを送信します。
4	プライマリ OCS とセカンダリ OCS の両方で CCR-U 要求メッセージが失敗す セッションは SU 状態になります。Gy セッションの SU URR が作成され、関 PDR にリンクされます。PGW-C は、UpdatePDR を含む Sx セッション変更要求 ジを PGW-U に送信します。UpdatePDR の PDR URR リストには Gy SU URR ます。
5	PGW-U は、両方の Gy バケット（URR1 と Gy SU URR1）の使用状況の更新を Sx セッション変更応答メッセージを PGW-C に送信します。
6	Gy URR バケットがクォータを使い切ると、PGW-U は URR2（RG-2）を含む セッションレポート要求メッセージを PGW-C に送信します。
7	PGW-C は要求を確認し、Sx セッションレポート応答メッセージを PGW-U に す。
8	PGW-C は、UpdatePDR および Update RR2 を含む Sx セッション変更要求メッ PGW-U に送信します。UpdatePDR には、URR2 と Gy SU URR の両方を含む URR リストが含まれます。
9	PGW-U は Sx セッション変更応答メッセージを PGW-C に送信します。
10	Gy SU URR クォータを使い切ると、PGW-U は、URR1（RG-1）および URR2 を含む Sx セッションレポート要求メッセージを PGW-C に送信します。
11	PGW-C は要求を確認し、Sx セッションレポート応答を送信します。
12	PGW-C は、SU の再試行後に CCR 更新（CCR-U）要求メッセージを OCS に す。
13	OCS は、[Result-Code] が 2001 の CCA 更新応答メッセージを送信します。
14	PGW-C は、URR1（RG-1）、URR2（RG-2）、および UpdatePDR（Gy SU U を含む Sx 変更要求メッセージを PGW-U に送信します。

CUPS における新しい動作

CUPS の新たな SU メカニズムは次のとおりです。

- 非CUPSアーキテクチャでは、単一のノード（P-GW）によってGyセッション状態とデータトラフィックが処理されるため、メッセージングによる遅延なくSUURRが作成されます。一方、CUPSモードでは、CPは追加のノードとなります。このノードは、セッション状態に関する情報を保持し、ユーザープレーン（UP）からのURR要求を処理します。Gy

セッションを SU URR に関連付けることができるのは、CP だけです。UP と CP 間のこのメッセージングにより遅延が発生し、データパケットは [Pending-Traffic-Treatment] 設定に従って処理され、通信が完了します。

- 非 CUPS アーキテクチャでは、SU 状態タイマーは、Time-Quota タイマーとは異なる方法で処理されます。SU クォータを使い切ると、OCS への再試行が発生し、新たに [next-interim-time-quota] が開始されます。一方、CUPS モードでは、SU 時間クォータを使用する場合、クォータの枯渇が CP に報告され、セッションが再びサーバー到達不能状態になると、前回の使用状況レポートからの経過時間が使用状況に計上されます。
- CUPS で **servers-unreachable after-timer-expiry** *timeout_period* CLI コマンドを使用することは推奨されません。代わりに、**servers-unreachable after-interim-time** *timeout_period* **server-retries** *retry_count* を使用して同様の動作を実現しますが、再試行回数は 1 回です（*retry_count* を「1」に設定）。

制限に達した後処理

制限到達後の後処理は、CUPS と非 CUPS の両方のアーキテクチャでサポートされている 3GPP 非準拠の独自の動作です。この機能により、課金バケットのクォータを使い切った場合に、実装済みのリダイレクトまたは制限操作が可能になります。ただし、OCS サーバーは [FUI-Redirect] または [FUI-Restrict] を付与できません。この機能を使用する場合、オペレータは、使用可能なすべてのルール一致基準を組み合わせて（たとえば、IMSI ベースの一致基準を有効にするなど）、サブスクライバ/トラフィックごとに異なる処理を選択的に適用できます。この機能を有効にするには、次の CLI コマンドを使用します。

```
configure
  active-charging service service_name
    rulebase rulebase_name
      post-processing policy always
      end
```

また、**rule-application post-processing** CLI コマンドは、[ACS Ruledef Configuration] モードで limit-reached に設定する必要があります。

PTT no-quota Limited Pass

この機能により、サブスクライバは OCS からの応答を待機している間にネットワークを使用できます。Limited-Pass 設定では、サブスクライバが OCS からのクォータ応答を待機している間に消費できるボリュームを指定できます。使用量はそれぞれの課金バケットでカウントされ、次のクォータ割り当てに対して調整されます。

この機能を有効にするには、次の CLI コマンドを使用します。

```
configure
  active-charging service service_name
    credit-control
      pending-traffic-treatment noquota limited-pass volume volume
      end
```

Limited Pass Volume は、**noquota** のケース（クォータを初めて要求する評価グループ（RG））にのみ使用され、**quota-exhausted** には使用されません。Limited Pass Volume は、後続のクレジット要求には使用されません。

Limited Pass Volume が使い果たされるまで、トラフィックの通過が許可されます。使用量はそれぞれの課金バケットでカウントされ、付与された「クォータ」に対して調整されます。「クォータ」割り当てが実際の使用量よりも少ない場合、使用状況レポートを使用した OCS への即時レポートが発生し、より多くのクォータ割り当てが要求されます。後続の着信パケットは、「quota-exhausted」PTT 設定に従って処理されます。

OCS がクォータの拒否で応答する前に Limited Pass Volume が使い果たされていない場合、トラフィックはOCS応答後にブロックされます。ゲートウェイは、OCSが応答するまで、CCR-U（FINAL）（CUPS 以外の場合）または CCR-T（CUPS の場合）の Limited Pass Volume の使用状況を報告します。

OCS が応答する前に Limited Pass Volume が使い果たされた場合、OCS からクォータが付与されるまで、セッションの後続の着信パケットはドロップされます。

noquota のデフォルトの pending-traffic-treatment は Drop です。**default pending-traffic-treatment noquota** コマンドは、設定されたすべての Limited Pass Volume サイズを削除します。

PTT クォータ枯渇制限パス

CUPS アーキテクチャの Pending-Traffic-Treatment（PTT）Quota-Exhausted Limited-Pass は、バッファリングオプションの代わりに使用できます。高速ネットワークでは、バッファリングオプションには現実的な制限があります。バッファリングでは、ゲートウェイで多数のパケットをバッファリングする必要があるため、メモリが不足し、帯域幅の速度に影響を及ぼすリスクが発生します。PTT Quota-Exhausted Limited Pass では、クォータ枯渇シナリオで設定された制限に達するまで、トラフィックを通過させます。

PTT は、Limited-Pass ボリュームを使いきるまでトラフィックを許可します。PTT は、付与された「クォータ」を基準に、それぞれの課金バケットの使用状況を計算し、調整します。「クォータ」割り当てが実際の使用量よりも少ない場合は、使用状況レポートを通じてすぐに OCS に報告し、追加のクォータ割り当てを要求します。

OCSによるクォータの拒否応答までにLimited-Passボリュームが枯渇しなければ、OCS応答後にトラフィックがブロックされます。ゲートウェイは、CCR-U（FINAL）で使用状況をレポートします。

OCSからの応答前にLimited-Passボリュームが枯渇した場合、OCSからクォータが付与されるまで、セッションの以降の着信パケットがドロップされます。

クォータが枯渇した場合の pending-traffic-treatment のデフォルト動作は [Drop] です。デフォルトの pending-traffic-treatment quota-exhausted CLI コマンドにより、設定済みの Limited-Pass ボリュームのサイズは削除されます。

この機能を有効にするには、次の CLI コマンドを使用します。

```
configure
  active-charging service service_name
    credit-control
      pending-traffic-treatment quota-exhausted limited-pass volume
```

volume
end

（注） 上記の CLI コマンドは、CUPS アーキテクチャにのみ適用されます。

注：

- **limited-pass**：OCS に到達できない場合に、サブスクライバへの制限付きアクセスを有効にします。
- **volume** *volume*：OCS に到達できない場合に、サブスクライバへの制限付きボリュームアクセスを有効にします。*volume* は、デフォルトのクォータサイズ（バイト単位）を指定します。クォータサイズは 1 ～ 4294967295 までの整数で指定する必要があります。

クォータ有効時間の処理

MSCC バケットのクォータ有効時間が受信されると、同じ情報がユーザープレーンに送信されます。直接使用できる特定の IE がないため、QVT 値が Time-Quota IE に入力され、URR がユーザープレーンに送信されます。QVT またはタイムクォータの小さい方の値が、Time-Quota IE で設定されます。また、Time-Quota でユーザープレーンからの使用状況レポートがトリガーされると、解釈が行われて、Validity-Timeout の CCR-Update が生成されます。

サポートされる機能と制限事項

ボリュームクォータ メカニズムを使用した基本的なコールフローは、Gy インターフェイスでの P-GW セッションレポートに関する次の制限付きでサポートされます。

- CCR/CCA-I、CCR/CCA-U および CCR/CCA-T、RAR/RAA メッセージのみがサポートされます。
- セッションセットアップ時およびセッション中のどちらでも、[Dynamic Rules with Online Enabled] がサポートされます。
- セッションセットアップ時およびセッション中のどちらでも、[Predefined Rules]（ダイナミックのみ）がサポートされます。「プリエンプティブな要求」の設定に制限はありません。
- オンライン課金を使用する静的ルールがサポートされます。
- Ignore-service-id がサポートされます。
- ボリュームクォータ/ボリュームしきい値メカニズムがサポートされます。
- イベントトリガー（クエリ URR が発生するもの）、および OCS への使用状況情報の送信がサポートされます。

重要 RAT 変更機能は、このリリースでは検証されていません。

- OCS が新しいクォータを付与する Sx セッション変更手順を通じた「updateURR」手順がサポートされます。
- ベアラーレベルの Gy とサブスクライバレベルの Gy がサポートされます。
- Pending-Traffic-Treatment（PTT）の [Drop] / [Pass] は、次の制限付きでサポートされます。
  - 現在サポートされているシナリオは、クォータなしとクォータ枯渇です。
  - トリガー/再承認シナリオはサポートされていません。
  - PTT アクション（[Forward] / [Drop]）は、クォータ取得で取得できるクォータが枯渇した後に考慮されます。
- 次のような障害シナリオが認定されています。
  - 障害処理の終了、続行と再試行、および終了：CC グループ/FHT を使用
  - エラー結果コードの処理（MSCC レベルとコマンドレベルの両方）がサポートされます。
- 実測時間クォータメカニズムがサポートされます。
- その他の時間クォータメカニズム（離散期間および連続期間）はサポートされません。
- Final-Unit-Indication Terminate メカニズムがサポートされます。
- [FUI-Restrict] はサポートされません。
- セッション中のルールのインストール/削除/変更はサポートされます。
- RAR メカニズムがサポートされます。
- Server-Unreachable（SU）メカニズムがサポートされたことにより、非 CUPS P-GW と比較して動作が若干変更されました。
  - URR が UP でクォータを必要とする場合、使用状況レポートが CP に生成され、CP がリンクされた SU_URR で応答するまで、この URR に一致するパケットは [Pending-Traffic-Treatment] 設定で処理されます。
  - SU 時間クォータを使用する場合、クォータの枯渇が CP に報告され、セッションが再びサーバー到達不能状態になると、前回の使用状況レポートからの経過時間が使用状況に計上されます。
- Pending-Traffic-Treatment バッファメカニズムはサポートされません。
- [send-ccri on traffic-start] がサポートされます。
- [Quota-Hold-Time] がサポートされます。
- Quota-Consumption-Time メカニズムはサポートされません。
- [Quota-Validity-Time] がサポートされます。

- Gy でイベントが発生した場合の、Gy からの Gz レコードのトリガーがサポートされます。Gy-Gz 同期はサポートされません。
- Gy でイベントが発生した場合の、Gy からの Rf レコードのトリガーはサポートされません。
- [rated-group] 値では、「content-id」以外の値の設定がサポートされます。
  - RG「0」はサポートされません。
- Out-of-Credit、Reallocation-of-Credit イベントの PCRF へのトリガーは認定されていません。

重要 PCRF に対するイベントトリガーの [Out-of-Credit] は、1 回限りの付与クォータ（合計ボリュームと付与ボリュームが同じ値）という制限付きで検証されます。

- CCR-I に関する OCS からの遅延応答がサポートされます。
- [Service-Specific-Units] はサポートされません。
- [Tariff-Time] の変更は、3GPP 仕様に従ってサポートされます。
- [Quota-Retry Timer] がサポートされます。
- **diameter mscc-final-unit-action terminate session** CLI コマンドは、[Credit Control Configuration] モードでサポートされます。
- [FUI-Redirect] は、次の制限付きでサポートされます。
  - HTTP のリダイレクトはサポートされません。
  - フィルタ ID/フィルタルールを使用した FUI リダイレクトはサポートされません。
  - WSP プロトコルはサポートされません。
  - 3GPP 仕様に従って、リダイレクトされたトラフィックは、[FUI-Redirect] のルールにヒットした場合にもリダイレクトされます。リダイレクトされたトラフィックの通過を許可するプロビジョニングはありません。
    - 3GPP 仕様に従って、CUPS アーキテクチャは **no diameter fui-redirected-flow allow** CLI コマンドの動作に準拠しています。
  - **redirect-require-user-agent** CLI コマンドはサポートされません。ユーザーエージェントが存在しない場合でも、リダイレクトは引き続き機能します。
  - 元の URL の追加はサポートされません。
  - **diameter redirect-validity-timer immediate** CLI コマンドがサポートされます。ただし、**diameter redirect-validity-timer traffic-start** CLI コマンドはサポートされません。

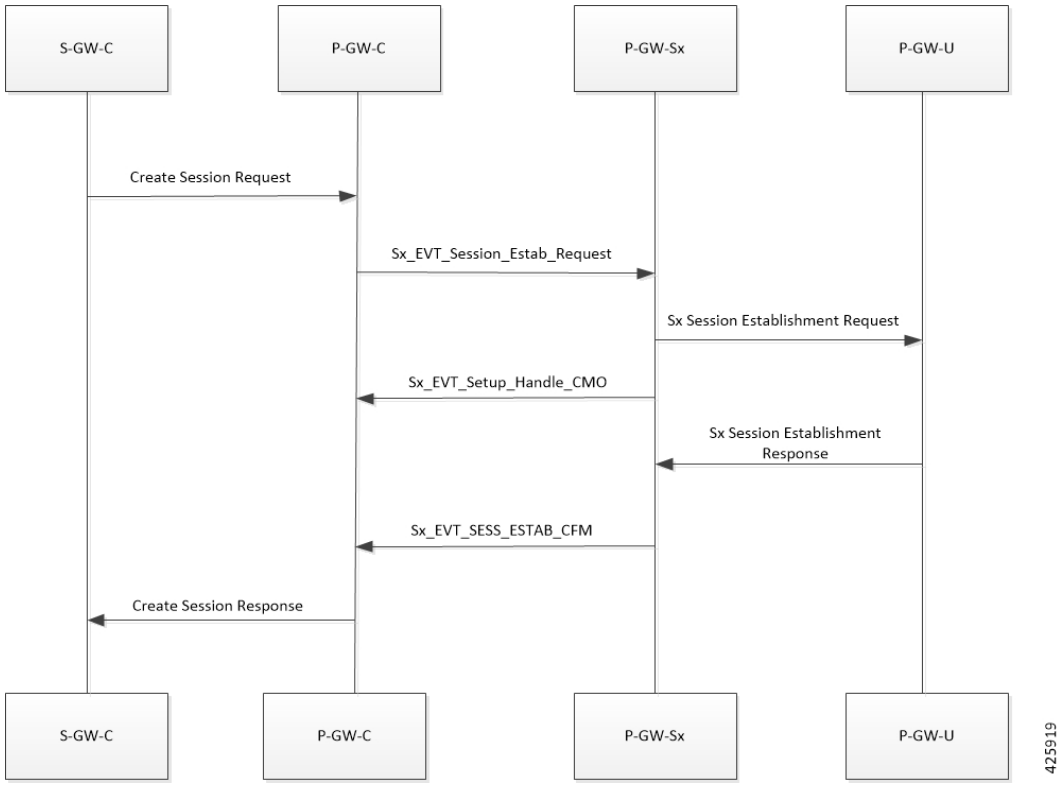
- リダイレクトを脱するトークンベースのメカニズムはサポートされません。CUPS でリダイレクトを終了するには、OCS が Redirect Validity-Time または RAR を送信します。
- FUI リダイレクトは、非 CUPS アーキテクチャでの動作と同様に、URL に対してのみサポートされます。

- PCRF/OCS からの rulebase の変更がサポートされます。

Gz インターフェイスを使用した P-GW セッションレポート

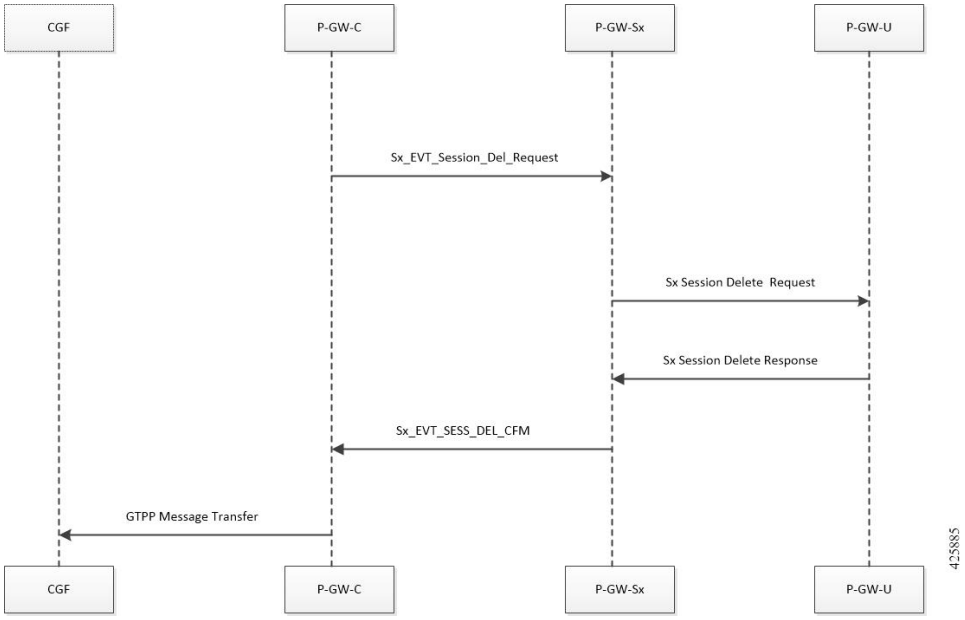
この項では、Gzインターフェイスを使用したP-GWセッションレポートについて説明します。

セッション確立要求での URR サポート



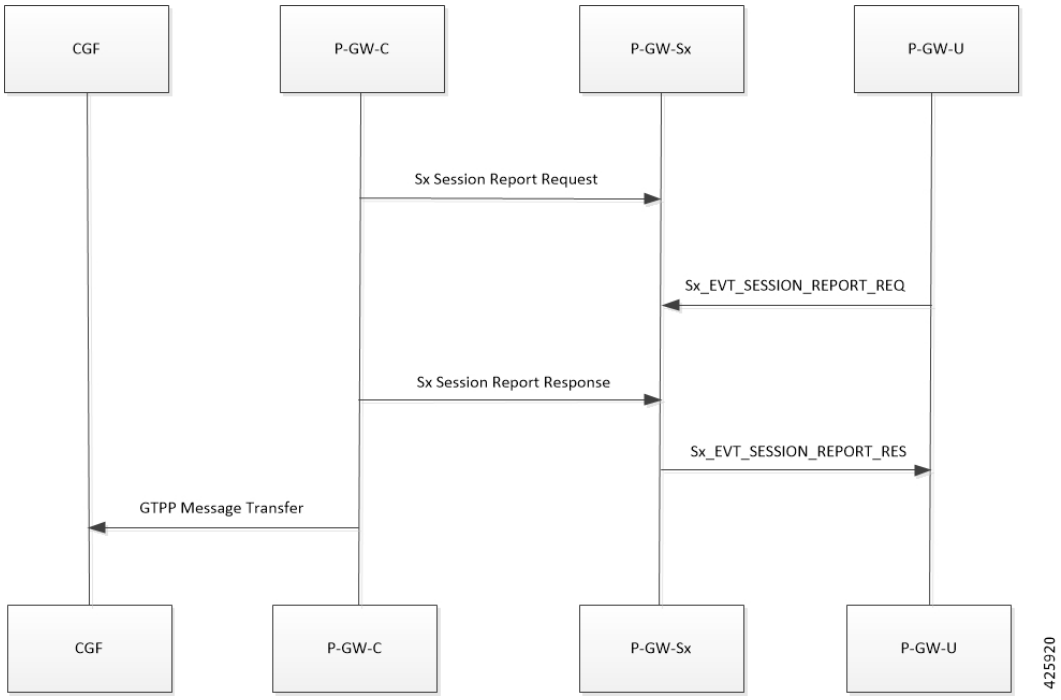
- ユーザープレーンモジュールは、セッション確立要求の一部として受信した URR のリストの保存をサポートします。
- 各 PDR は、1 つ以上の URR に関連付けられます。
- 特定の URR が別の URR にリンクされます。
- 各URRには、測定方法（時間またはボリューム）と、ユーザープレーンが使用状況レポートを送信する必要があるイベントを示すレポートトリガーが含まれています。

セッション削除応答



ユーザープレーンから送信されるこのメッセージは、コントロールプレーンからのセッション削除要求への応答です。このメッセージにより、ユーザープレーンで Sx セッションが終了します。使用状況レポートは、Sx セッション削除応答の一部として含まれています。

セッションレポート要求および応答メッセージ



要求メッセージ

- 時間またはボリュームのしきい値制限に達すると、ユーザープレーンは Sx セッションレポート要求メッセージを生成して、コントロールプレーンに送信します。
- このメッセージには、使用状況レポートトリガーで指定された、メッセージの生成理由を示す使用状況レポートが含まれます。
- さらに、使用状況レポートには、時間またはボリュームの測定値が含まれます。
- セッションレポート要求が生成されている URR に他の URR がリンクされている場合、リンクされている URR に対してもセッションレポート要求が生成されます。

応答メッセージ

コントロールプレーンからの応答メッセージは、原因コードを含むセッションレポート要求メッセージが正常に配信されたことを示します。現在、障害の原因を受信した場合に実行される特定の障害処理はありません。

ビットレートマッピングのサポート

P-GW は、PCRF から受信したビット レート値を bps から kbps に変換します。この変換により、小数値が最も近い整数（floor）値に切り捨てられ、情報が失われる可能性があります。3GPP では、bps から kbps に変換すると小数値になる場合は、最も近い整数値（ceil）値に切り上げてアクセス側に送信することが推奨されています。

（注） bps から kbps への切り捨て（floor）値が PFCP インターフェイスで送信されるように設計が変更されました。

標準準拠

ビットレートマッピング機能は、3GPP TS 29.274 リリース 12 に準拠しています。

ビットレートマッピング機能の設定

P-GW の APN-AMBR、GBR、および MBR で、bps から kbps ビットレートの切り上げ（ceil）値を設定するには、次の手順を実行します。

```
configure
  context context_name
    pgw-service service_name
      [ no ] egtp bitrates-rounded-down-kbps
      end
```

P-GW の APN-AMBR、GBR、および MBR で、bps から kbps ビットレートの切り捨て（floor）値を設定するには、次の手順を実行します。

```
configure
  context context_name
    pgw-service service_name
      egtp bitrates-rounded-down-kbps
      end
```

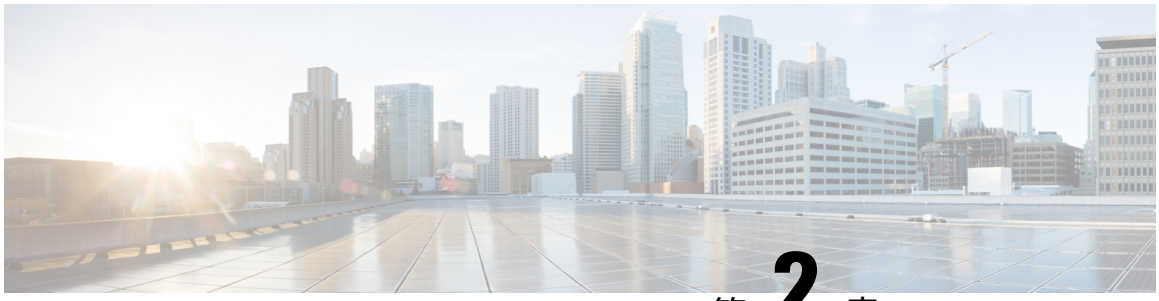
CUPS の新しい動作

デフォルトでは、APN-AMBR、MBR、およびGBR のビットレートの切り上げ値（kbps 単位）が Sx および GTP インターフェイスで送信されます。切り捨て動作を有効にするには、CLI を設定する必要があります。

標準準拠

CUPS のユーザープレーンは、次の標準規格に準拠しています。

- 3GPP 仕様 23.214 リリース 14.0：Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for control and user plane separation of EPC nodes
- 3GPP 仕様 29.244 リリース 14.0：LTE; Interface between the Control Plane and the User Plane of EPC Nodes
- 3GPP 仕様 23.401 リリース 14.0：3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access



第 2 章

CUPS でのユーザープレーンの設定

ここでは、CUPS のユーザープレーンの設定に使用できる CLI コマンドについて説明します。

重要 次の設定に関する情報は、『*Ultra Packet Core CUPS Sx* インターフェイス管理およびリファレンスガイド』を参照してください。

- *CUPS* の *Sx* サービスの設定
- *CUPS* の *Sx-u* インターフェイスの設定
- *CUPS* の *Sx Demux* の設定

重要

- CUPS では、次の設定制限が適用されます。
  - Rulebase - 512
  - Ruledef - 2500
  - Charging-action - 2048
- 次の CLI コマンドは、実稼働環境のアクティブなサブスクライバセッションでの使用は推奨されません：**no active-charging service** *service_name*

ユーザープレーンサービスの設定

ユーザープレーンサービスを設定するには、次の CLI コマンドを使用します。

```
configure
  context context_name
    [ no ] user-plane-service service_name
    end
```

注：

- **user-plane-service** *service_name*：指定したユーザープレーンサービス名を作成して、ユーザープレーンサービスの設定を許可します。*service_name* は、ユーザープレーンサービスを定義するための必須パラメータです。
- **[no] user-plane-service** *service_name*：特定のコンテキストからユーザープレーンサービスを削除します。
- デフォルトでは、CLI は無効になっています。

ユーザープレーンサービスの開始

ユーザープレーンサービスを開始するには、次の最低限かつ重要なパラメータを設定する必要があります。

- 1 つの Sx サービス。
- インターフェイスタイプが P-GW 入力、S-GW 入力、および S-GW 出力の 3 つの GTP-U サービス。

重要 ユーザープレーンサービスの重要なパラメータを削除または変更すると、ユーザープレーンサービスが停止します。

ユーザープレーンサービスに関連付けられているサービスは、実行モードになっている必要があります。他のモードの場合は、関連するサービスが停止すると、ユーザープレーンサービスの停止がトリガーされます。

GTP-U サービスとユーザープレーンサービスの関連付け

GTPU サービスをユーザープレーンサービスに関連付けるには、次の CLI コマンドを実行します。

```
configure
  context context_name
    user-plane-service service_name
    [ no ] associate gtpu-service gtpu_service_name { pgw-ingress |
sgw-ingress | sgw-egress }
    end
```

注：

- **no**：指定されたインターフェイスタイプとのGTP-Uサービスの関連付けをユーザープレーンサービスから削除します。
- **associate**：ユーザープレーンサービスを GTP-U サービスに関連付けます。
- **gtpu-service** *gtpu_service_name*：ユーザープレーンサービスの GTP-U サービスを指定します。
- **pgw-ingress**：インターフェイスタイプを P-GW 入力として設定します。
- **sgw-ingress**：インターフェイスタイプを S-GW 入力として設定します。
- **sgw-egress**：インターフェイスタイプを S-GW 出力として設定します。
- デフォルトでは、このコマンドはディセーブルです。

Sx サービスとユーザープレーンサービスの関連付け

次の CLI コマンドを使用して、Sx サービスをユーザープレーンサービスに関連付けます。

```
configure
  context context_name
    user-plane-service service_name
      associate sx-service sx_service_name
      no associate sx-service
      end
```

注：

- **no** ：ユーザープレーンサービスから Sx サービスの関連付けを解除します。
- Sx サービスとユーザープレーンサービスの関連付けは必須パラメータです。
- デフォルトでは、この CLI は無効になっています。

推奨タイマー

次の表に、IPSec、Sx、および SRP に関連する CLI コマンドの推奨タイマー値を示します。

IPSEC	**CP**	**UP**
ikev2-ikesa max-retransmission	*3*	*3*
ikev2-ikesa retransmission-timeout	*1000*	*1000*
keepalive	**interval** *4* **timeout** *1* **num-retry** *4*	**interval** *5* **timeout** *2* **num-retry** *4*
Sx	**CP**	**UP**

IPSEC	CP	UP
sx-protocol heartbeat interval	*10*	*10*
sx-protocol heartbeat retransmission-timeout	*5*	*5*
sx-protocol heartbeat max-retransmissions	*4*	*4*
sxa max-retransmissions	*4*	*4*
sxa retransmission-timeout-ms	*5000*	*5000*
sxb max-retransmissions	*4*	*4*
sxb retransmission-timeout-ms	*5000*	*5000*
sxab max-retransmissions	*4*	*4*
sxab retransmission-timeout-ms	*5000*	*5000*
sx-protocol association reattempt-timeout	*60*	*60*
SRP	**CP**	**UP**
hello-interval	*3*	*3*
dead-interval	*15*	*15*

推奨設定

以下に、Sx over IPSec および SRP over IPSec に関連する推奨設定と制限事項を示します。

- CP と UP 間のマルチホップ BFD タイマーは 7 秒にする必要があります（データ UP の場合）。
- シングルホップ BFD は、すべてのコンテキスト（CP GW/課金情報および UP Gn/Gi）で有効にする必要があります。
- シャーシ間マルチホップ BFD は、CP-CP ICSR および UP-UP ICSR（IMS UP）に対して有効にする必要があります。
- SRP-IPSec ACL は、IP プロトコルではなく TCP プロトコル用に設定する必要があります。
- Sx-IPSec ACL は、IP プロトコルではなく UDP プロトコル用に設定する必要があります。

CP の設定例

マルチホップ BFD 設定 VPC-DI

次に、7 秒タイマーを使用したマルチホップ BFD の設定例を示します。

```
bfd-protocol
      bfd multihop-peer 209.165.200.226 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.227 interval 350 min_rx 350 multiplier 20
```

```
      bfd multihop-peer 209.165.200.225 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.230 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.228 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.229 interval 350 min_rx 350 multiplier 20
    #exit
```

マルチホップ BFD 設定 VPC-SI

次に、タイマーが 3 秒のマルチホップ BFD 設定の例を示します。

```
bfd-protocol
      bfd multihop-peer 209.165.200.226 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.227 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.225 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.230 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.228 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.229 interval 150 min_rx 150 multiplier 20
    #exit
```

BGP の設定

以下に、推奨タイマーを使用した BGP の設定例を示します。

```
router bgp 1111
      router-id 209.165.200.225
      maximum-paths ebgp 15
      neighbor 209.165.200.250 remote-as 1000
      neighbor 209.165.200.250 ebgp-multihop
      neighbor 209.165.200.250 update-source 209.165.200.225
      neighbor 1111:2222::101 remote-as 1000
      neighbor 1111:2222::101 ebgp-multihop
      neighbor 1111:2222::101 update-source 1111:2222::1
      bgp graceful-restart restart-time 120
      bgp graceful-restart stalepath-time 300
      timers bgp keepalive-interval 30 holdtime-interval 90 min-peer-holdtime-interval
0 server-sock-open-delay-period 10
      address-family ipv4
        redistribute connected
      #exit
      address-family ipv6
        neighbor 1111:2222::101 activate
        redistribute connected
      #exit
    #exit
```

シングルホップ BFD 設定

タイマーが 3 秒のシングルホップ BFD の設定例を以下に示します。

```
interface bgp-sw1-2161-10
      ip address 209.165.200.233 209.165.200.255
      ipv6 address 1111:222::9/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-11
      ip address 209.165.200.234 209.165.200.255
      ipv6 address 1111:222::10/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-12
      ip address 209.165.200.235 209.165.200.255
      ipv6 address 1111:222::11/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
```

```
#exit
interface bgp-sw1-2161-3
  ip address 209.165.200.226 209.165.200.255
  ipv6 address 1111:222::2/112 secondary
  bfd interval 999 min_rx 999 multiplier 3
#exit
interface bgp-sw1-2161-4
  ip address 209.165.200.227 209.165.200.255
  ipv6 address 1111:222::3/112 secondary
  bfd interval 999 min_rx 999 multiplier 3
#exit
interface bgp-sw1-2161-5
  ip address 209.165.200.228 209.165.200.255
  ipv6 address 1111:222::4/112 secondary
  bfd interval 999 min_rx 999 multiplier 3
#exit
interface bgp-sw1-2161-6
  ip address 209.165.200.229 209.165.200.255
  ipv6 address 1111:222::5/112 secondary
  bfd interval 999 min_rx 999 multiplier 3
#exit
interface bgp-sw1-2161-7
  ip address 209.165.200.230 209.165.200.255
  ipv6 address 1111:222::6/112 secondary
  bfd interval 999 min_rx 999 multiplier 3
#exit
interface bgp-sw1-2161-8
  ip address 209.165.200.231 209.165.200.255
  ipv6 address 1111:222::7/112 secondary
  bfd interval 999 min_rx 999 multiplier 3
#exit
interface bgp-sw1-2161-9
  ip address 209.165.200.232 209.165.200.255
  ipv6 address 1111:222::8/112 secondary
  bfd interval 999 min_rx 999 multiplier 3
#exit
```

マルチホップ BFD 設定のスタティックルート

次に、スタティック ルート マルチホップ BFD 設定の例を示します。

```
ip route static multihop bfd UP-5 209.165.200.240 209.165.200.245
    ip route static multihop bfd UP-6 209.165.200.240 209.165.200.246
    ip route static multihop bfd UP-9 209.165.200.240 209.165.200.247
    ip route static multihop bfd UP-10 209.165.200.240 209.165.200.248
    ip route static multihop bfd UP-7 209.165.200.240 209.165.200.249
    ip route static multihop bfd UP-8 209.165.200.240 209.165.200.250
```

シングルホップ BFD 設定用のスタティックルート

次に、スタティックルートのシングルホップ BFD 設定の例を示します。

```
ip route static bfd bgp-sw1-2161-3 209.165.200.230
    ip route static bfd bgp-sw1-2161-4 209.165.200.230
    ip route static bfd bgp-sw1-2161-5 209.165.200.230
    ip route static bfd bgp-sw1-2161-6 209.165.200.230
    ip route static bfd bgp-sw1-2161-7 209.165.200.230
    ip route static bfd bgp-sw1-2161-8 209.165.200.230
    ip route static bfd bgp-sw1-2161-9 209.165.200.230
    ip route static bfd bgp-sw1-2161-10 209.165.200.230
    ip route static bfd bgp-sw1-2161-11 209.165.200.230
    ip route static bfd bgp-sw1-2161-12 209.165.200.230
```

IPSec ACL の設定

以下に、CP での IPSec ACL の設定例を示します。

```
ip access-list UP-1
      permit udp host 209.165.200.225 host 209.165.200.226
    #exit
```

IPSec トランスフォームセットの設定

CP での IPSec トランスフォームセットの設定例を以下に示します。

```
ikev2-ikesa transform-set ikesa-UP-1
      encryption aes-cbc-256
      group 14
      hmac sha2-256-128
      lifetime 28800
      prf sha2-256

    ipsec transform-set A-UP-1
      encryption aes-cbc-256
      hmac sha2-256-128
      group 14
```

IPSec クリプトマップの設定

CP での IPSec クリプトマップの設定例を以下に示します。

```
crypto map UP-1 ikev2-ipv4
      match address UP-1
      authentication local pre-shared-key encrypted key secretkey
      authentication remote pre-shared-key encrypted key secretkey
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 1000
      ikev2-ikesa transform-set list ikesa-UP-1
      ikev2-ikesa rekey
      keepalive interval 4 timeout 1 num-retry 4
      control-dont-fragment clear-bit
      payload foo-sa0 match ipv4
        ipsec transform-set list A-UP-1
        lifetime 300
        rekey keepalive
      #exit
      peer 192.1.1.1
      ikev2-ikesa policy error-notification
    #exit
```

Sx の設定

以下に、CP における Sx の設定例を示します。

```
sx-service SX-1
      instance-type controlplane
      sxa max-retransmissions 4
      sxa retransmission-timeout-ms 5000
      sxb max-retransmissions 4
      sxb retransmission-timeout-ms 5000
      sxab max-retransmissions 4
      sxab retransmission-timeout-ms 5000
      n4 max-retransmissions 4
      n4 retransmission-timeout-ms 5000
      sx-protocol heartbeat interval 10
      sx-protocol heartbeat retransmission-timeout 5
```

```
      sx-protocol heartbeat max-retransmissions 4
      sx-protocol compression
      sx-protocol supported-features load-control
      sx-protocol supported-features overload-control
    exit
end
```

ルータの設定例

インターフェイスのスタティックルート

次に、インターフェイスのスタティックルートの設定例を示します。

```
ip route 209.165.200.224/27 Vlan1111 209.165.200.225
ip route 209.165.200.224/27 Vlan1111 209.165.200.226
ip route 209.165.200.224/27 Vlan1111 209.165.200.227
ip route 209.165.200.224/27 Vlan1111 209.165.200.228
ip route 209.165.200.224/27 Vlan1111 209.165.200.229
ip route 209.165.200.224/27 Vlan1111 209.165.200.230
ip route 209.165.200.224/27 Vlan1111 209.165.200.231
ip route 209.165.200.224/27 Vlan1111 209.165.200.232
ip route 209.165.200.224/27 Vlan1111 209.165.200.233
ip route 209.165.200.224/27 Vlan1111 209.165.200.234
```

シングルホップ BFD のスタティックルート

次に、シングルホップ BFD のスタティックルートの設定例を示します。

```
ip route static bfd Vlan1111 209.165.200.225
ip route static bfd Vlan1111 209.165.200.226
ip route static bfd Vlan1111 209.165.200.227
ip route static bfd Vlan1111 209.165.200.228
ip route static bfd Vlan1111 209.165.200.229
ip route static bfd Vlan1111 209.165.200.230
ip route static bfd Vlan1111 209.165.200.231
ip route static bfd Vlan1111 209.165.200.232
ip route static bfd Vlan1111 209.165.200.233
ip route static bfd Vlan1111 209.165.200.234
```

シングルホップ BFD のインターフェイス

シングルホップ BFD のインターフェイスの設定例を以下に示します。

```
interface Vlan1111
  no shutdown
  bandwidth 10000000
  bfd interval 999 min_rx 999 multiplier 3
  no bfd echo
  ip address 209.165.200.224/27
  ipv6 address 1111:222::1/112
```

BGP の設定

次に、推奨タイマーを使用した BGP の設定例を示します。

```
router bgp 1000
  router-id 209.165.200.226
  timers bgp 30 90
  timers bestpath-limit 300
  timers prefix-peer-timeout 30
  timers prefix-peer-wait 90
  graceful-restart
```

```
  graceful-restart restart-time 120
  graceful-restart stalepath-time 300
```

UP の設定例

IPSec ACL の設定

UP での IPSec ACL の設定例を以下に示します。

```
ip access-list CP-1
      permit udp host 209.165.200.225 host 209.165.200.226
    #exit
```

IPSec トランスフォームセットの設定

以下に、UP での IPSec トランスフォームセットの設定例を示します。

```
ipsec transform-set A-CP-1
      encryption aes-cbc-256
      hmac sha2-256-128
      group 14

    ikev2-ikesa transform-set ikesa-CP-1
      encryption aes-cbc-256
      group 14
      hmac sha2-256-128
      lifetime 28800
      prf sha2-256
```

IPSec 暗号マップの設定

UP での IPSec 暗号マップの設定例を以下に示します。

```
crypto map CP-1 ikev2-ipv4
      match address CP-1
      authentication local pre-shared-key encrypted key secretkey
      authentication remote pre-shared-key encrypted key secretkey
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 1000
      ikev2-ikesa transform-set list ikesa-CP-1
      ikev2-ikesa rekey
      keepalive interval 5 timeout 2 num-retry 4
      control-dont-fragment clear-bit
      payload foo-sa0 match ipv4
        ipsec transform-set list A-CP-1
      #exit
      peer 209.165.200.230
      ikev2-ikesa policy error-notification
    #exit
```

Sx の設定

UP における Sx の設定例を以下に示します。

```
sx-service SX-1
      instance-type userplane
      sxa max-retransmissions 4
      sxa retransmission-timeout-ms 5000
      sxb max-retransmissions 4
      sxb retransmission-timeout-ms 5000
      sxab max-retransmissions 4
      sxab retransmission-timeout-ms 5000
```

```
      n4 max-retransmissions 4
      n4 retransmission-timeout-ms 5000
      sx-protocol heartbeat interval 10
      sx-protocol heartbeat retransmission-timeout 5
      sx-protocol heartbeat max-retransmissions 4
      sx-protocol compression
    exit
```

SRP の設定例

IPSec ACL の設定

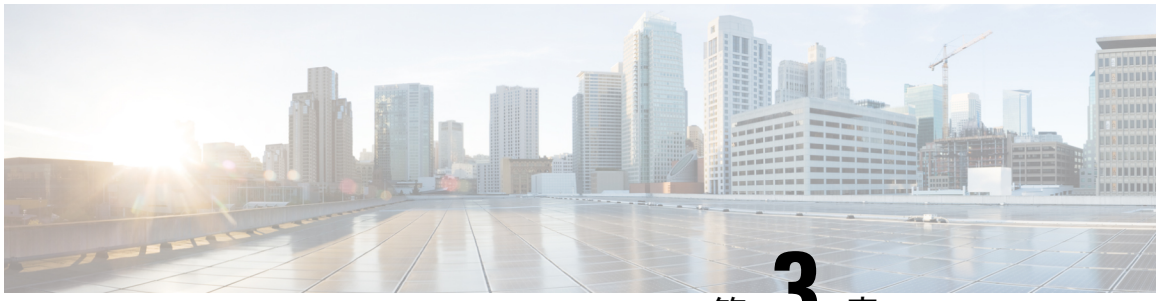
次に、SRP の IPSec ACL 設定の例を示します。

```
ip access-list SRP
      permit tcp host 209.165.200.227 host 209.165.200.228
    #exit
```

SRP の設定

SRP の設定例を以下に示します。

```
configure
  context srp
    bfd-protocol
      bfd multihop-peer 209.165.200.225 interval 999 min_rx 999 multiplier 3
    #exit
configure
  context srp
    service-redundancy-protocol
      chassis-mode primary
      hello-interval 3
      dead-interval 15
      monitor bfd context srp 209.165.200.226 chassis-to-chassis
      monitor bgp context gi-pgw 209.165.200.245
      monitor bgp context gi-pgw 3333:888::1
      monitor bgp context saegw 209.165.200.245
      monitor bgp context saegw 3333:888::2
      peer-ip-address 209.165.200.227
      bind address 209.165.200.228
    #exit
    ip route static multihop bfd srp 209.165.200.229 209.165.200.245
    ip route 209.165.201.1 209.165.202.129 209.165.200.230 SRP-Physical-2102
    ip route 209.165.201.2 209.165.202.130 209.165.200.231 SRP-Physical-2102
    ip route 209.165.201.3 209.165.202.131 209.165.200.232 SRP-Physical-2102
    ip igmp profile default
    #exit
  #exit
end
```



第 3 章

CUPS でのユーザープレーンのモニタリングと障害対応

ここでは、CUPS におけるユーザープレーンのモニターまたは障害対応に使用できる CLI コマンドについて説明します。

CUPS でのユーザープレーンのモニタリングと障害対応

ここでは、CUPS におけるユーザープレーンのモニターまたは障害対応に使用できる CLI コマンドについて説明します。

SNMP トラップ

ユーザープレーンノードでのセッションリカバリ後に、次のトラップを使用できます。

- **StarManagerFailure**：このトラップは、ソフトウェアマネージャで障害が発生した場合に生成されます。
- **StarTaskFailed**：このトラップは、重要ではないタスクが失敗し、適切なリカバリ手順が開始されたときに生成されます。
- **StarTaskRestart**：このトラップは、以前の障害後に重大ではないタスクが再起動したときに生成されます。
- **StarSessMgrRecoveryComplete**：このトラップは、セッションマネージャのリカバリが完了すると生成されます。通常は、セッションマネージャタスクが失敗し、リカバリが正常に完了した場合に発生します。
- **StarManagerRestart**：このトラップは、指定されたマネージャタスクが再起動されたときに生成されます。

コマンドの表示

show configuration

このコマンドを実行すると、次のフィールドが表示されます。

```
saegw-service
associate sgw-service
associate pgw-service
associate gtpu-service up-tunnel
associate sx-service
```

show-gtpu-statistics

この show コマンドを実行すると、次の出力が表示されます。

- セッション統計：
  - Current
  - Current (IMS-media)
  - Total Setup
  - Total Setup (IMS-media)
  - Current gtpu v0 sessions
  - Current gtpu v1 sessions
- 合計データ統計：
  - Uplink Packets
  - Uplink Bytes
  - Downlink Packets
  - Downlink Bytes
  - Packets Discarded
  - Bytes Discarded
  - Uplink Packets (IMS-media)
  - Uplink Bytes (IMS-media)
  - Downlink Packets (IMS-media)
  - Downlink Bytes (IMS-media)
  - Packets Discarded (IMS-media)
  - Bytes Discarded (IMS-media)

- QOS 統計：
  - QCI <n>：
    - Uplink Packets
    - Uplink Bytes
    - Downlink Packets
    - Downlink Byte
    - Packets Discarded
    - Bytes Discarded
  - 非標準 QCI（GBR 以外）：
    - Uplink Packets
    - Uplink Bytes
    - Downlink Packets
    - Downlink Byte
    - Packets Discarded
    - Bytes Discarded
- 非標準 QCI（GBR）：
  - Uplink Packets
  - Uplink Bytes
  - Downlink Packets
  - Downlink Byte
  - Packets Discarded
  - Bytes Discarded
- アップリンクパケットの GBR QCI の合計：
  - Total uplink Bytes GBR QCI's
  - Total Downlink packets GBR QCI's
  - Total Downlink Bytes GBR QCI's
  - Total uplink packets Non-GBR QCI's
  - Total uplink Bytes Non-GBR QCI's
  - Total Downlink packets Non-GBR QCI's
  - Total Downlink Bytes Non-GBR QCI's

- パス管理メッセージ：
  - Echo Request Rx
  - Echo Response Rx
  - Echo Request Tx
  - Echo Response Tx
  - SuppExtnHdr Tx
  - SuppExtnHdr Rx
- ピア統計：
  - Total GTPU Peers
  - Total GTPU Peers with Stats
- トンネル管理メッセージ:
  - Error Indication Tx
  - Error Indication Rx
  - Error Indication Rx Discarded
- 最適化統計：
  - Total Packets Input
  - Total Packets Optimized
  - Total TCP Packets Input
  - Total TCP Packets Optimized
  - Total UDP Packets Input
  - Total UDP Packets Optimized
  - Total Fragments Input
- IPSec データ統計：
  - Discards Due To IPSec Tunnel Not Present
    - Packets Discarded
    - Bytes Discarded
    - Err-Ind Tx Discarded

（注） CUPS では、[Packets Discarded] 統計は、セッションマネージャでドロップされたパケットと VPP でドロップされたパケット数を集約したものです。VPP はパケットの大部分を処理するため、VPP でのパケットドロップは、これらの統計では大まかにしか分類できません。

セッションマネージャでドロップされたパケットについてのみ、具体的なパケットドロップ理由を表示できます。VPP でドロップされたパケットは、**show gtpu statistics** CLI の [Packets Discarded] カウンタで分類されます。

show module p2p user-plane-ipv6-addr

この show コマンドを実行すると、次の出力が表示されます。

- Control-Plane Sx-Service name
  - Priority
  - User-Plane ip
  - version
  - update/rollback time

show saegw-service all

このコマンドの出力範囲が拡張され、 SAEGW サービスと関連する Sx サービスをサポートする次の新しいフィールドが追加されました。

sx-service

show saegw-service name

このコマンドの出力は **show saegw-service all** CLI コマンドと同様で、指定した saegw-service 名のフィールドを表示します。

show service all

このコマンドの出力が変更され、ユーザープレーンサービスとその関連パラメータが追加されました。

- コンテキスト ID
- Service ID
- Context Name
- Service Name
- State

- max-sessions
- Type

show subscriber all

このコマンドの出力範囲が変更され、ユーザープレーンサービスとその関連パラメータが追加されました。

- アクセスタイプ
  - ユーザープレーン
- アクセステクノロジー
- コール状態
- アクセス CSCF ステータス
- リンクステータス
- ネットワークタイプ
- CALLID
- MSID
- ユーザー名
- IP
- アイドル時間

show subscribers user-plane-only all

この show コマンドを実行すると、次の出力が表示されます。

- アクセス タイプ
- インターフェイス タイプ
- コール状態
- コール ID
- ローカル SEID
- IP
- PDN インスタンス
- アイドル時間

show subscribers user-plane-only called/seid *called/seid* flow flow-id *flow-id*

この show コマンドを実行すると、次の出力が表示されます。

- Callid
  - インターフェイス タイプ
  - IP アドレス
  - フロー ID
  - アップリンクパケット数
  - ダウンリンクパケット数
  - アップリンクバイト数
  - ダウンリンクバイト数
  - UE IP アドレス
  - UE ポート
  - サーバの IP アドレス
  - サーバ ポート
  - プロトコル
- 検出されたフローの総数
- 指定した条件に一致するサブスクライバの総数

show subscribers user-plane-only called/seid *called/seid* flows full

この show コマンドを実行すると、次の出力が表示されます。

- Callid
  - インターフェイス タイプ
  - IP アドレス
  - フロー ID
  - アップリンクパケット数
  - ダウンリンクパケット数
  - アップリンクバイト数
  - ダウンリンクバイト数
  - UE IP アドレス

- UE ポート
- サーバの IP アドレス
- サーバ ポート
- プロトコル
- フロー ID
- アップリンクパケット数
- ダウンリンクパケット数
- UE IP アドレス
- UE ポート
- サーバの IP アドレス
- サーバ ポート
- プロトコル

- 検出されたフローの総数
- 指定した条件に一致するサブスクライバの総数

show subscribers user-plane-only called/seid *called/seid* flows

この show コマンドを実行すると、次の出力が表示されます。

- セッションマネージャ インスタンス
  - アプリケーション プロトコル
  - トランスポートプロトコル
    - テザリングされたフロー
      - 回復されたフロー
  - アクティブフローの合計数

show subscribers user-plane-only callid *call_id* pdr all

この show コマンドを実行すると、次の出力が表示されます。

- Source Interface
- Type
- Destination Interface

- Type
- vv
- PDR-ID
- Linked FAR-ID
- Linked URR-ID
- Linked QER-ID
- Total subscribers matching specified criteria

show subscribers user-plane-only callid/seid *callid/seid* pdr full all

この show コマンドを実行すると、次の出力が表示されます。

- Callid
  - インターフェイス タイプ
  - IP アドレス
- PDR-ID
- Hits（ヒット数）
- Match Bypassed
- Matched Bytes
  - Precedence
  - Source Interface
- [Matched Packets]
- SDF Filter(s)
  - Filter 1
    - プロトコル
    - Src IP Addr
    - Src Port
    - Dst IP Addr
    - Dst Port
- SPI
  - Local F-TEID
  - Outer header removal

- アプリケーション ID

- Linked FARID
  - Destination Interface
  - Apply Action
  - Outer Header Creation
  - Remote TEID
  - リモート IP アドレス（Remote IP Address）
  - リモートポート

- Linked QERID
  - PDR-ID
  - Hits（ヒット数）
  - Match Bypassed
  - Matched Bytes
    - Precedence
    - Source Interface
  - SDF Filter(s)
    - Filter 1
      - プロトコル
      - Src IP Addr
      - Src Port
      - Dst IP Addr
      - Dst Port
      - SPI
  - Local F-TEID
  - Outer header removal
  - アプリケーション ID

- Linked FARID
  - Destination Interface
  - Apply Action
  - Outer Header Creation

- Remote TEID
- リモート IP アドレス（Remote IP Address）
- リモートポート

- Total PDRs found
- Total subscribers matching specified criteria

show subscribers user-plane-only callid/seid *callid/seid* pdr id *pdr-id*

この show コマンドを実行すると、次の出力が表示されます。

- Callid
  - インターフェイス タイプ
  - IP アドレス
- PDR-ID
- Hits（ヒット数）
- Match Bypassed
- Matched Bytes
  - Precedence
  - Source Interface
- [Matched Packets]
- SDF Filter(s)
  - Filter 1
    - プロトコル
    - Src IP Addr
    - Src Port
    - Dst IP Addr
    - Dst Port
    - SPI
- Local F-TEID
- Outer header removal
- アプリケーション ID
- Linked FARID

- Destination Interface
- Apply Action
- Outer Header Creation
- Remote TEID

- リモート IP アドレス（Remote IP Address）
- リモートポート
- Linked QERID
- Total PDRs found
- Total subscribers matching specified criteria

show subscribers user-plane-only flows

この show コマンドを実行すると、次の出力が表示されます。

- Sessmgr Instance
  - アプリケーション プロトコル
  - Transport Protocol
    - Tethered Flow
      - Recovered Flow

- Flow-ID
- Bytes-Up
- Bytes-Down
- Pkts-Up
- Total Number of Active flows
- Total subscribers matching specified criteria

show subscribers user-plane-only full all

この show コマンドを実行すると、次の出力が表示されます。

- ローカル SEID
- リモート SEID
- 状態
- Connect Time

- Idle time
- アクセス タイプ（Access Type）
- ネットワークタイプ
- user-plane-service-name
- Callid
- インターフェイス タイプ
- Card/Cpu
- IP 割り当てタイプ
- IP アドレス
- 送信元コンテキスト
- 接続先コンテキスト
- PDN-Instance
- User-plane-Sx-addr
- Control-plane-Sx-addr
- 関連付けられた PDR の数
- 関連付けられた FAR の数
- 関連付けられた QER の数
- 関連付けられた URR の数
- input pkts
- output pkts
- input bytes
- output bytes
- input bytes dropped
- output bytes dropped
- input pkts dropped
- output pkts dropped
- pk rate from user(bps)
- pk rate to user(bps)
- ave rate from user(bps)
- ave rate to user(bps)
- sust rate from user(bps)

- sust rate to user(pps)
- pk rate from user(pps)
- pk rate to user(pps)
- ave rate from user(bps)
- ave rate to user(pps)
- sust rate from user(pps)
- sust rate to user(pps)
- ipv4 bad hdr
- ipv4 ttl exceeded
- ipv4 fragments sent
- ipv4 could not fragment
- ipv4 bad length trim
- ipv4 input mcast drop
- ipv4 input bcast drop
- input pkts dropped (0 mbr)
- output pkts dropped (0 mbr)
- ip source violations
- ipv4 output no-flow drop
- ipv6 bad hdr
- ipv6 bad length trim
- ipv4 input mcast drop
- ipv4 input bcast drop
- input pkts dropped (0 mbr)
- output pkts dropped (0 mbr)
- ip source violations
- ipv4 output no-flow drop
- ipv6 bad hdr
- ipv6 bad length trim
- ipv4 icmp packets dropped
- APN AMBR 入力パケットドロップ
- APN AMBR 出力パケットドロップ
- APN AMBR 入力バイトドロップ

- APN AMBR 出力バイトドロップ
- 指定した条件に一致するサブスクライバの総数

show subscribers user-plane-only seid *seid* pdr all

この show コマンドを実行すると、次の出力が表示されます。

- Source Interface
  - Type
- Destination Interface
  - Type
- vv
- PRD-ID
- リンクされた FAR-ID
- リンクされた URR-ID
- リンクされた QER-ID
- 指定した条件に一致するサブスクライバの総数

show user-plane-service [all | name *name*]

この show コマンドを実行すると、次の出力が表示されます。

- サービス名
- Service-Id
- Context
- ステータス
- PGW Ingress GTPU Service
- SGW Ingress GTPU Service
- SGW Egress GTPU Service
- Control Plane Tunnel GTPU Service
- Sx Service

（注） ユーザープレーンで QCI レベルの統計情報をモニターするには、ユーザープレーンで GTPU スキーマを設定します。この情報は、「show user-plane-service gtpu statistics」 CLI で確認できます。

show user-plane-service statistics all

この show コマンドを実行すると、次の出力が表示されます。

- VPN 名
- サブスクライバの総数
  - PDN の総数
    - アクティブ
    - 設定
    - リリース日
    - Rejected
  - PDN タイプ別の PDN
    - IPv4 PDN
      - アクティブ
      - 設定
      - リリース日
    - IPv6 PDN
      - アクティブ
      - 設定
      - リリース日
    - IPv4v6 PDN
      - アクティブ
      - 設定
      - リリース日
  - インターフェイスタイプ別の PDN

- Sxa インターフェイスタイプの PDN
  - アクティブ
  - リリース日
- Sxb インターフェイスタイプの PDN
  - アクティブ
  - 設定
  - リリース日

- 理由別の拒否された PDN
  - リソースなし（No Resource）
  - Missing or unknown APN
  - アドレスが割り当てられていない
  - アドレスが存在しない
  - No memory available
  - システム障害
  - PDR インストールのエラー
- 理由別のリリースされた PDN
  - ネットワーク開始型リリース
  - 管理者接続解除
- 合計データ統計
  - アップリンク
    - パケットの総数
    - Total Bytes
    - ドロップされたパケットの総数
    - 合計廃棄バイト数
  - ダウンリンク
    - パケットの総数
    - Total Bytes
    - ドロップされたパケットの総数

- 合計廃棄バイト数

- PDN タイプごとのデータ統計
  - IPv4 PDN
    - アップリンク
      - パケットの総数
      - Total Bytes
    - ダウンリンク
      - パケットの総数
      - Total Bytes
  - IPv6 PDN データ統計
    - アップリンク
      - パケットの総数
      - Total Bytes
    - ダウンリンク
      - パケットの総数
      - Total Bytes
  - IPv4v6 PDN データ統計
    - アップリンク
      - パケットの総数 v4
      - バイトの総数 v4
      - パケットの総数 v6
      - バイトの総数 v6
    - ダウンリンク
      - パケットの総数 v4
      - バイトの総数 v4
      - パケットの総数 v6
      - バイトの総数 v6

- フロー統計
  - 最大フローに到達
  - ドロップされたパケット数：システム制限（L4）
  - IP フロー統計
    - フローの総数 v4
      - アップリンク
        - パケットの総数 v4
        - バイトの総数 v4
        - エラーパケットの総数 v4
        - エラーバイトの総数 v4
    - アクティブフロー数 v4
      - ダウンリンク
        - パケットの総数 v4
        - バイトの総数 v4
        - エラーパケットの総数 v4
        - エラーバイトの総数 v4
    - フローの総数 v6
      - アップリンク
        - パケットの総数 v6
        - バイトの総数 v6
        - エラーパケットの総数 v6
        - エラーバイトの総数 v6
    - アクティブフロー数 v6
      - ダウンリンク
        - パケットの総数 v6
        - バイトの総数 v6
        - エラーパケットの総数 v6
        - エラーバイトの総数 v6

- UDP フロー統計
  - UDP フローの総数
    - アップリンク
      - UDP パケットの総数
      - UDP バイトの総数
      - UDP エラーパケットの総数
      - UDP エラーバイトの総数
    - ダウンリンク
      - UDP パケットの総数
      - UDP バイトの総数
      - UDP エラーパケットの総数
      - UDP エラーバイトの総数
- TCP フロー統計
  - TCP フローの総数
    - アップリンク
      - TCP パケットの総数
      - TCP バイトの総数
      - TCP エラーパケットの総数
      - TCP エラーバイトの総数
    - ダウンリンク
      - TCP パケットの総数
      - TCP バイトの総数
      - TCP エラーパケットの総数
      - TCP エラーバイトの総数

show user-plane-service statistics charging action

このコマンドは、Active Charging Service（ACS）で設定されているすべてまたは指定された課金アクションの課金アクション統計を表示します。課金アクションは、設定されたルールに一

致したときに実行されるアクションを意味します。アクションの範囲として、アカウンティングレコードの生成から IP パケットのドロップなどまでが含まれます。また、課金アクションによって、使用量計算の原則を規定します。再送信されたパケットをカウントするかどうか、および課金情報にどのプロトコルフィールド（L3/L4/L7など）を使用するかがこれに当たります。

構文

show user-plane-service statistics charging-action
{ all [debug-info | verbose] | name *charging_action_name* **[debug-info | verbose] } [| { grep** *grep_options* **| more }]**

注：

- **all**：ACS で設定されているすべての課金アクションの情報を表示します。
- **name** *charging_action_name*：1 ～ 63 文字の英数字で指定された既存の課金アクションの情報を表示します。

この show CLI コマンドは、次の統計情報をサポートしていません。サポートされない統計のカウンタ値はそれぞれ *0* と表示されます。

```
PP Flows Readdressed:0
Bytes Charged Yet Packet Dropped:0
Predef-Rules Deactivated:0
Outer IP header dscp marked Pkts:0

Tethering Blocking Statistics:
   TTL Modified downlink packets:0

Throttle-Suppress Stats:
   Uplink Bytes:0    Downlink Bytes:0

XHeader Information:
IP Frags consumed by XHeader:0 IP Frags consumed by XHeader:0

Strip URL:
   Successful Token stripped:0
   Total strip URL failure:0
   Failure - Missing config:0
   Failure - Existing flow bid:0
   Failure - Token matching failed:0
   Failure - Empty packet:0
   Failure - Req end not found:0
   Failure - Subset of big token:0

URL-Readdressing:
   Requests URL-Readdressed:0
   Total Charging action hit - Req. Readdr.:0
   Proxy Disable Success:0
```

```
  Flows connected to URL Server:0


URL-Readdressing Error Conditions:
  Total connect failed to URL Server:0
  URL Readdress- pipelined case:0
  URL Readdress- Socket Mig. Failed:0
  Proxy Disable Failed:0

CAE-Readdressing:
  Requests CAE-Readdressed:0
  Responses CAE-Readdressed:0
  Requests having MVG xheader inserted:0
  Total CAE-Readdressed Uplink Bytes:0
  Total CAE-Readdressed Uplink Packets:0
  Total CAE-Readdressed Downlink Bytes:0
  Total CAE-Readdressed Downlink Packets:0
  Total Charging action hit - Req. Readdr.:0
  Total Charging action hit - Resp. Readdr:0
  Proxy Disable Success:0
  Flows connected to CAE:0

CAE Readdressing Error Conditions:
  Total connect failed to CAE:0
  Req. Readdr. - pipelined case:0
  Skipped Resp. Readdr. - pipelined req:0
  Req. Readdr. - Socket Mig. failed:0
  Skipped Resp. Readdr. - partial resp hdr:0
  Resp. Readdr. - Socket Mig. failed:0
  Total CAE load balancer failed:0
  Total MVG xheader insertion failed:0
  Proxy Disable Failed:0

  Rulebase Changed by flow action:0
  Terminate Session:0
  P2P random dropped packets:0
```

show user-plane-service statistics group-of-ruledefs

このコマンドは、アクティブ課金サービスで設定されている **ruledef** のすべてのグループまたは指定されたグループの統計を表示します。**group-of-ruledefs** は、アクセスポリシーの作成に使用できるルール定義のコレクションです。

構文

show user-plane-service statistics group-of-ruledefs { all | name *group_of_ruledefs_name* **} [| { grep** *grep_options* **| more }]**

注：

- **all**：ACS で設定されているすべての **groups of ruledefs** の情報を表示します。
- **name** *group_of_ruledefs_name*：1 ～ 63 文字の英数字で指定された既存の **group of ruledefs** の詳細情報を表示します。
- **{ grep** *grep_options* **| more } Pipes**：このコマンドの出力を指定されたコマンドに送信します。
- 次の clear CLI コマンドを使用できます。

  clear user-plane-service statistics group-of-ruledefs { all | name *group_of_ruledefs_name* **}**

show user-plane-service statistics ruledef

このコマンドは、アクティブな課金サービスで設定されているすべてまたは指定された **ruledef** の統計情報を表示します。**ruledef** は、プロトコルフィールドと状態情報に基づいた複数の L3 ～ L7 プロトコルにおける一連の一致条件を表します。各 **ruledef** は、アクティブな課金サービス内の複数のルールベースで使用できます。

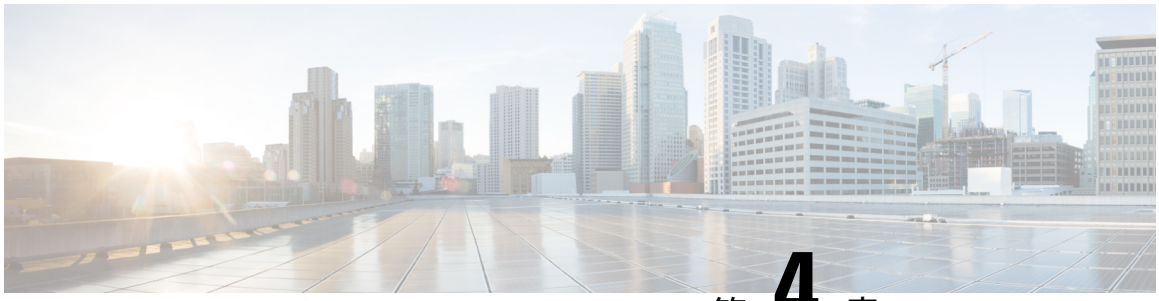
構文

show user-plane-service statistics ruledef { all { charging | firewall [wide] | post-processing } | name *ruledef_name* **[wide] } [| { grep** *grep_options* **| more }]**

注：

- **all**：ACS で設定されている指定したタイプの **all ruledef** の統計情報を表示します。
- **charging**：ACS で設定されているすべての **charging ruledef** の統計情報を表示します。
- **firewall**：サービスで設定されているすべての **firewall ruledef** の統計情報を表示します。
- **post processing**：ACS で設定されているすべての **post processing ruledef** の統計情報を表示します。
- **name** *ruledef_name*：1 ～ 63 文字の英数字文字列として指定された既存の **ruledef** の統計情報を表示します。
- **wide**：使用可能なすべての情報を 1 行で表示します。
- 次の clear CLI コマンドを使用できます。

  clear user-plane-service statistics ruledef { all | charging | firewall | name *group_of_ruledefs_name* **}**



第 4 章

4G CUPS の 1:1 ユーザープレーン冗長性

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

4G CUPS の 1:1 ユーザープレーン冗長性機能は、障害が発生したユーザープレーン（UP）の検出をサポートし、障害が発生した UP の機能をシームレスに処理します。各アクティブ UP には専用のスタンバイ UP があります。1:1 UP 冗長性アーキテクチャは、UP から UP へのシャーシ間セッションリカバリ（ICSR）接続に基づいています。

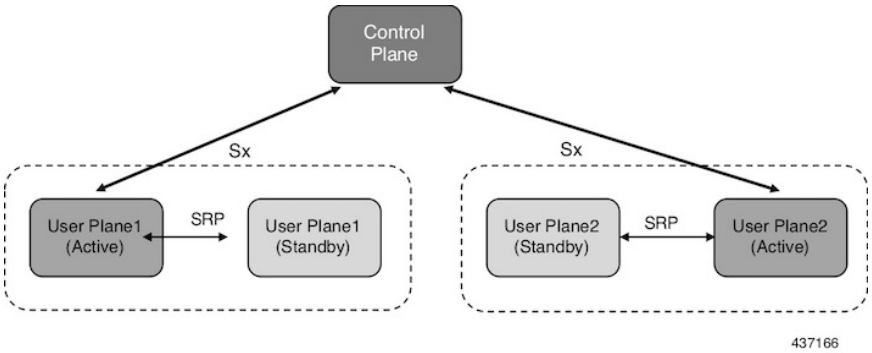
機能の仕組み

ここでは、4G CUPS ユーザープレーンの 1:1 冗長性機能の仕組みについて簡単に説明します。

4G CUPS 展開では、次の図に示すように、ICSR フレームワーク インフラストラクチャを活用して UP ノードのチェックポインティングとスイッチオーバーを実現します。アクティブ UP

は、UP 間でプロビジョニングされたサービス冗長性プロトコル（SRP）リンクを介して専用のスタンバイ UP と通信します。

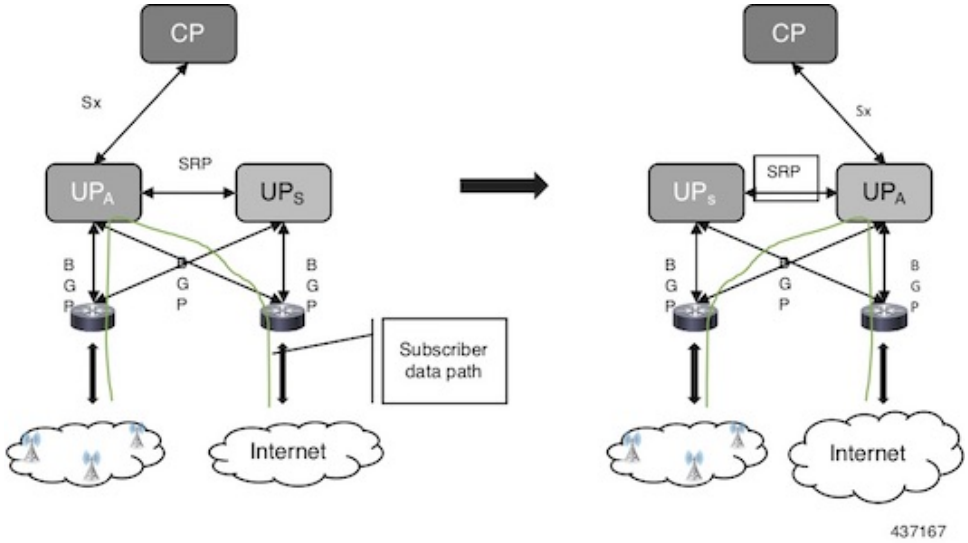
図 *1 : SRP* を使用した *UP* の *1:1* 冗長性



コントロールプレーン（CP）ノードには、UP グループ設定で使用可能なスタンバイ UP 情報がありません。このため、UP の冗長性設定と UP 間のスイッチオーバーイベントは CP には認識されません。

アクティブ UP は、UP で設定された Sx インターフェイスアドレスを介して CP と通信します。スタンバイ UP は、スイッチオーバーイベント中にアクティブに移行する際に、同じ Sx インターフェイスアドレスを引き継ぎます。これは、Sx インターフェイスが SRP によってアクティブ化され、既存の設定方法に準拠していることを意味します。したがって、UP スイッチオーバーは CP に対して透過的です。

図 *2 : UP* の *1:1* 冗長性スイッチオーバー



1:1 の冗長性に完全に準拠するため、CUPS 環境の SRP ベースの ICSR に対する次の依存関係に対応します。

- PFD 設定の同期

- Sx 関連付けチェックポイント
- Sx リンクのモニタリング

上記の依存関係に加えて、UP は UP ノードに固有のデータ収集およびチェックポイント手順を実装します。たとえば、IP プールチャンクのチェックポインティングなどです。UP は、これらの手順を既存の ICSR チェックポインティング フレームワークに統合します。

図 *3 : UP* の *1:1* 冗長性設定時の *CP-CP ICSR*（*CP* スイッチオーバー前）

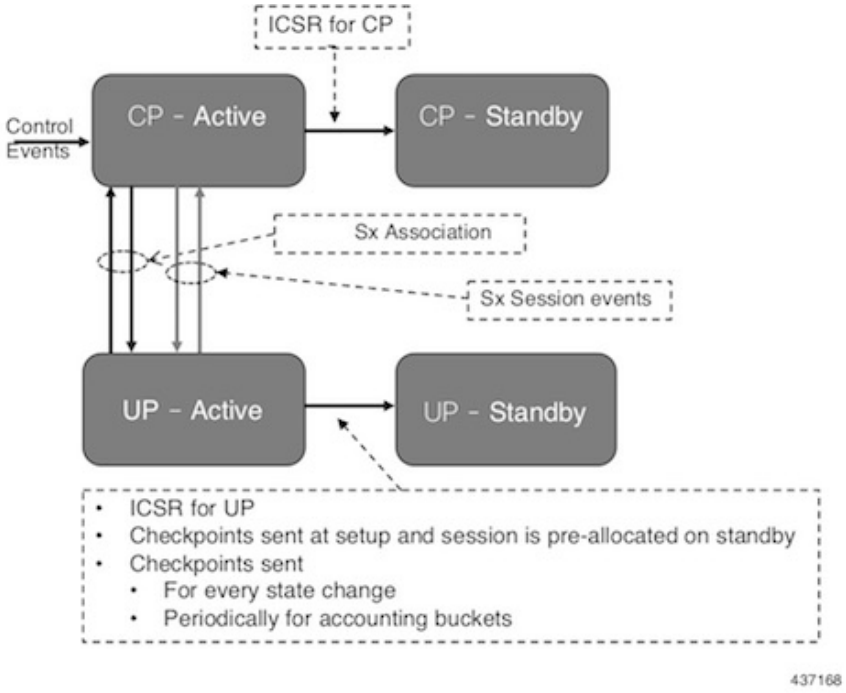
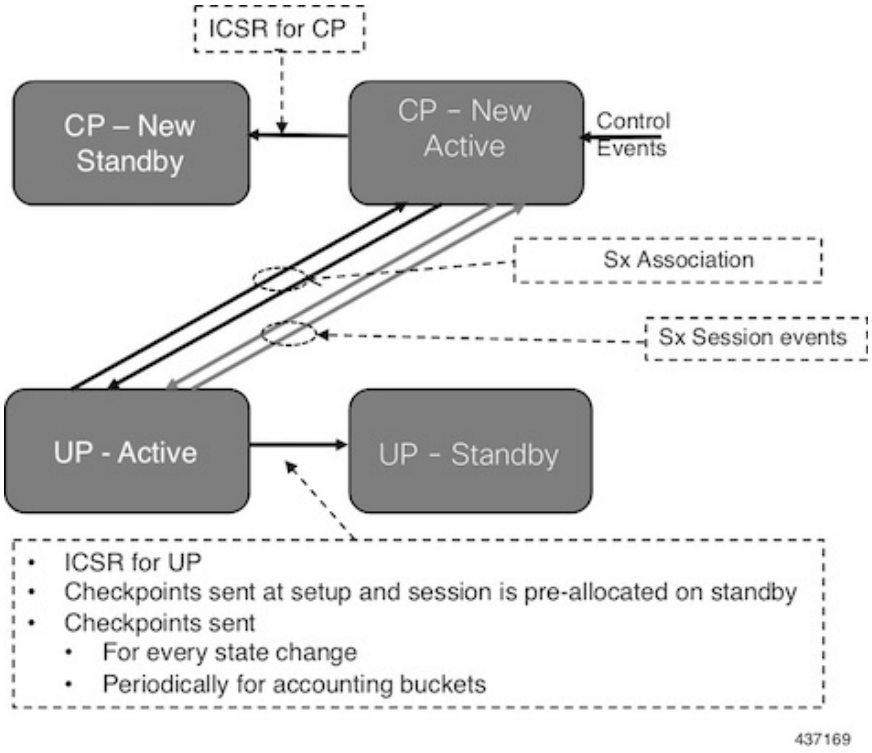


図 *4 : UP* の *1:1* 冗長性設定時の *CP-CP ICSR*（*CP* スイッチオーバー後）

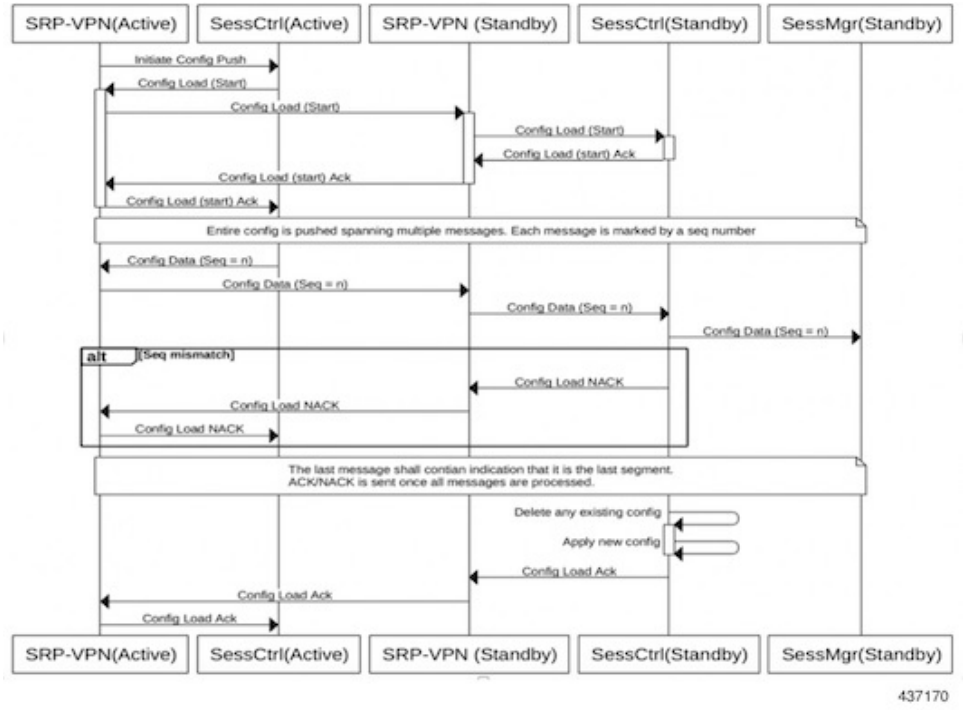


PFD 設定の同期

CP ノードは、パケットフロー記述（PFD）メッセージを介して UP 設定をプッシュします。UP の Sx IP アドレスはアクティブ UP およびスタンバイ UP を介して SRP によってアクティブ化されるため、CP はアクティブ UP からスタンバイ UP に PFD 設定を送信します。

SRP VPN マネージャが UP 間のトランスポートを提供し、アクティブ UP のセッションコントローラが設定のプッシュをアンカーします。次の図にイベントのシーケンスを示します。

図 *5 : PFD* 設定の同期



アクティブ UP とスタンバイ UP 間の BFD モニター

BFD は、アクティブ UP とスタンバイ UP 間の SRP リンクをモニターして、迅速な障害検出とスイッチオーバーを実現します。スタンバイ UP がこのリンクで BFD 障害を検出すると、アクティブ UP を引き継ぎます。

BFD リンクは、シングルホップまたはマルチホップが可能です。

（注） SRP バインドインターフェイスには、カードサービスポートに接続するイーサネットインターフェイスを推奨します。ループバックアドレスでは、BFD 制御パケットが 1 つのサービスポートのみを通過するようにすることを推奨します。ECMP の場合は、ルートコンバージェンス時間が BFD タイムアウトを超えないようにします。

アクティブ UP とスタンバイ UP 間の BFD モニターを設定するには、「アクティブ UP とスタンバイ UP 間の BFD モニタリングの設定」を参照してください。

マルチホップ BFD モニタリングの設定例

プライマリ UP：

```
config
  context srp
    bfd-protocol
      bfd multihop-peer 209.165.200.225 interval 50 min_rx 50 multiplier 20
    #exit
    service-redundancy-protocol
```

```
      monitor bfd context srp 209.165.200.225 chassis-to-chassis
      peer-ip-address 209.165.200.225
      bind address 209.165.200.227
    #exit
    interface srp
      ip address 209.165.200.227 255.255.255.224
    #exit
    ip route static multihop bfd bfd1 209.165.200.227 209.165.200.225
    ip route 192.168.210.0 255.255.255.224 209.165.200.228 srp
  #exit
end
```

バックアップ UP：

```
config
  context srp
    bfd-protocol
      bfd multihop-peer 209.165.200.227 interval 50 min_rx 50 multiplier 20
    #exit
    service-redundancy-protocol
      monitor bfd context srp 209.165.200.227 chassis-to-chassis
      peer-ip-address 209.165.200.227
      bind address 209.165.200.225
    #exit
    interface srp
      ip address 209.165.200.225 255.255.255.224
    #exit
    ip route static multihop bfd bfd1 209.165.200.225 209.165.200.227
    ip route 192.168.209.0 255.255.255.224 209.165.200.226 srp
  #exit
End
```

プライマリ UP とバックアップ UP 間のルータ：

```
config
  context one
    interface one
      ip address 209.165.200.228 255.255.255.224
    #exit
    interface two
      ip address 209.165.200.226 255.255.255.224
    #exit
  #exit
end
```

シングルホップ BFD モニタリングの設定例

プライマリ UP：

```
config
  context srp
    bfd-protocol
    #exit
    service-redundancy-protocol
      monitor bfd context srp 255.255.255.230 chassis-to-chassis
      peer-ip-address 255.255.255.230
      bind address 209.165.200.227
    #exit
    interface srp
      ip address 209.165.200.227 255.255.255.224
      bfd interval 50 min_rx 50 multiplier 10
    #exit
    ip route static bfd srp 255.255.255.230
```

```
  #exit
end
```

バックアップ UP：

```
config
  context srp
    bfd-protocol
    #exit
    service-redundancy-protocol
      monitor bfd context srp 209.165.200.227 chassis-to-chassis
      peer-ip-address 209.165.200.227
      bind address 255.255.255.230
    #exit
    interface srp
      ip address 255.255.255.230 255.255.255.224
      bfd interval 50 min_rx 50 multiplier 10
    #exit
    ip route static bfd srp 209.165.200.227
  #exit
end
```

VPP モニター

VPP サブシステムに障害が発生すると、SRP VPP モニターはスタンバイ UP へのスイッチオーバーを開始します。

（注） VPP モニターは、VPC-SI インスタンス UP でのみ使用できます。ASR 5500 の VPP 障害はカードレベルの冗長性によって対処されるため、VPP モニターは、ハイブリッド CUPS ASR 5500 UP では使用できません。VPP によって複数のカード障害が発生する場合は、SRP カードモニターを使用する必要があります。

VPP モニターを設定するには、「アクティブ UP およびスタンバイ UP での VPP モニターの設定」を参照してください。

Sx 関連付けチェックポイント

アクティブ UP が設定済み CP ノードへの Sx 関連付けを開始すると必ず、スタンバイ UP がこのデータのチェックポイントを生成します。これにより、UP スイッチオーバー後も関連付け情報が保持されます。

Sx ハートビートメッセージが送信され、アクティブ UP は連続した UP スイッチオーバー後であっても応答する必要があります。

Sx モニター

UP と CP 間の Sx インターフェイスのモニタリングは重要です。Sx ハートビート機能を有効にすることは、モニター障害の検出に役立つため不可欠です。

（注） Sx モニタリングは UP でのみ使用できます。

アクティブ UP の Sx インターフェイスは障害を検出し、SRP VPN マネージャに通知して、スタンバイ UP による引き継ぎに向けた UP スイッチオーバーイベントがトリガーされるようにします。

CP Sx ハートビートタイムアウトが、UP Sx ハートビートタイムアウトと UP ICSR スイッチオーバー時間の合計よりも大きくなるようにすることが重要です。これは、UP Sx モニター障害が原因で、UP スイッチオーバー中に CP が Sx パス障害を検出しないようにするためです。

コントロールプレーンのハートビートタイムアウトの防止

UP ICSR スイッチオーバー中に CP ハートビートがタイムアウトする可能性はわずかながらあります。これを軽減するには、次の手順を実行します。

1. CP から UP への Sx ハートビートを削除します。
2. 上記が不可能な場合は、CP から UP への Sx ハートビートに複数の再試行タイムアウトを設けるようにします。また、この再試行回数が UP Sx ハートビートタイムアウトと UP ICSR スイッチオーバー時間の合計よりも大きくなるようにします。

   次に例を示します。

   A = CP ハートビート間隔（*sx-protocol Heartbeat interval*）

   B = CP ハートビートの最大再送信回数（*sx-protocol Heartbeat max-retransmissions*）

   C = CP ハートビート再送信タイムアウト（*sx-protocol Heartbeat retransmission-timeout*）

   D = UP ハートビート間隔（*sx-protocol Heartbeat interval*）

   E = UP ハートビートの最大再送信回数（*sx-protocol Heartbeat max-retransmissions*）

   F = UP ハートビート再送信タイムアウト（*sx-protocol Heartbeat max-retransmissions*）

   G = スイッチオーバー時間（BGP ルートコンバージェンス時間を含む）

   したがって、Sx モニター障害スイッチオーバーを成功させるための式は次のようになります。

   B * C > D + (E * F) + G

   値の例：

   CP：

   A：

   ```
   sx-protocol heartbeat interval 60
   ```

   B：

   ```
   sx-protocol heartbeat max-retransmissions 10
   ```

   C:

   ```
   sx-protocol heartbeat retransmission-timeout 10
   ```

   UP：

   D：

sx-protocol heartbeat interval 30

E：

sx-protocol heartbeat max-retransmissions 3

F：

sx-protocol heartbeat retransmission-timeout 3

BGP：

G：ルートコンバージェンス時間の例 = 30 秒

したがって、B * C > D + (E * F) + G

=> 10 * 10 > 30 + (3 * 3) + 30

=> 100 > 69

B の最大値は 15 で、C の最大値は 20 です。したがって、Sx モニター障害検出と UP スイッチオーバー（D +（E * F）+ G）を設定して、15 * 20 = 300 秒（5 分）の最大遅延に耐えられるようにします。

BGP ルートコンバージェンス時間（G）を最小限に抑えるには、BFD フェールオーバーを使用して BGP を実行します。

Sx モニターを設定するには、「アクティブ UP およびスタンバイ UP での Sx モニタリングの設定」を参照してください。

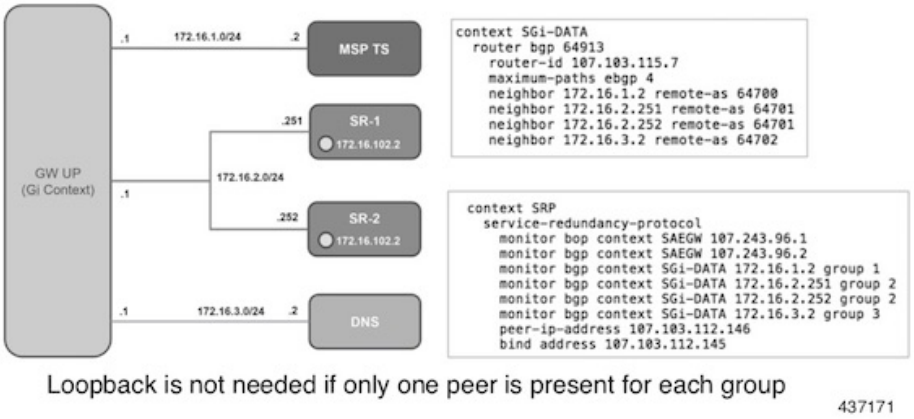
スタンバイ UP 自体に CP との独立した接続はありません。アクティブ UP の Sx コンテキストがスタンバイ UP に複製され、SRP スイッチオーバー時のテイクオーバーの準備が整います。これは、Sx モニター障害のためにアクティブ UP がスタンバイに切り替わった場合、新しいスタンバイは UP から CP へのリンクが機能しているかどうかを把握できないことを意味します。新しいアクティブ UP での Sx モニター障害が原因で、新しいスタンバイ UP が再びアクティブ状態にスイッチバックされないようにするには、新たな **monitor sx** CLI コマンドで **disallow-switchover-on-peer-monitor-fail** キーワードを使用します。

Sx モニタリング障害が原因でシャーシがスタンバイになった後、Sx UP チェックポイントが新しいアクティブ UP から受信されても、Sx 障害ステータスはリセットされません。これは、前回のスイッチオーバーを引き起こしたそもそもの原因が Sx モニター障害であった場合に、Sx モニター障害によって、再び新しいアクティブの計画外のスイッチバックが起こるのを防ぐためです。これにより、CP のダウン時に、連続したピンポン方式のスイッチオーバーが起こるのを防ぎます。Sx モニター障害ステータスは、ネットワーク接続が正常であるという確信が得られたら、オペレータが手動でリセットする必要があります。リセットするには、スタンバイシャーシで新しい **srp reset-sx-fail** CLI コマンド（「Sx モニター障害のリセット」を参照）を使用します。

BGP モニター

次の図に示すように、UP（Gi 側と Gn 側の両方）からネクストホップルータの BGP ピアモニターとピアグループモニターを設定します。これは既存の ICSR 設定です。BGP は、迅速な BGP ピア障害の検出のため、BFD によるサポートと併せて実行できます。

図 *6 : BGP* ピアグループと回送



BGP モニタリングを設定し、BPG モニタリング障害にフラグを設定するには、BGP モニタリング障害のフラグ付け （87 ページ）を参照してください。

UP セッションチェックポイント

アクティブシャーシは、次のシナリオで、UP データのコレクションをチェックポイントとしてピアスタンバイシャーシに送信します。

- 新しいコールのセットアップ時
- コールの状態が変化するたびに
- アカウンティングバケット用に定期的に

これらのチェックポイントを受信すると、スタンバイシャーシはデータに基づいて動作し、コールレベルまたはノード/インスタンスレベルで必要な情報を更新します。

VPN IP プールのチェックポイント

PFD 設定メッセージとともに、CP は IP プール割り当てを各 UP に送信します。VPN マネージャは、UP でこのメッセージを受信し、SRP が設定されている場合、スタンバイ UP で同じ情報を使ってチェックポイントを生成します。

IP プール情報は、SRP VPNMGR の再起動中、および SRP リンクのダウンおよびアップシナリオ中にも送信されます。

スイッチオーバーの前に、スタンバイに IP プール情報が存在することを検証することが重要です。IP プール情報が存在しない場合、ルートアドバタイズメントができないため、トラフィックは UP に到達しません。

外部監査と PFD 設定監査のインタラクション

アクティブ UP は、外部監査と PFD 設定監査のインタラクションを実行します。セッションマネージャが PFD 設定監査の開始通知と完了通知を受け取ります。PFD 設定監査の進行中は、セッションマネージャは外部監査を開始しません。外部監査の進行中に PFD 設定監査の開始

通知が届いた場合、セッションマネージャは PFD 設定監査の完了後に外部監査を再開するようにフラグを立てます。PFD監査の進行中に外部監査が発生しても目的を達成できないため、外部監査の再開が必要です。

ユーザープレーンのゼロアカウンティング損失

アカウンティングデータ/課金情報の損失が 18 秒より小さくなるよう、ゼロアカウンティング損失機能がユーザープレーン（UP）に実装されます。この時間は、アクティブUPからスタンバイ UP へのデフォルトチェックポイント時間、または設定されるアカウンティング チェックポイント時間のデフォルトチェックポイント時間です。

UP でのこの変更は、Gz、Gy、VoGx、および RADIUS URR をサポートするためです。ゼロアカウンティング損失/URR データカウンタ損失では、計画的スイッチオーバーのみがサポートされます。この機能は、現行の ICSR フレームワークや、チェックポイントの生成およびリカバリ方法には影響しません。

Sx 使用状況レポートは、シャーシが [pending active] 状態から [Active] になるまでブロックされます。

UP セッション回復のための早期 PDU リカバリ

早期 PDU リカバリ機能は、これまでのセッションリカバリ機能が抱えていた、リカバリ対象として選択された CRR に優先順位付けが行われないという制限を克服します。これまでは、すべての CRR が AAAMgr から取得され、コールが順番に回復されていました。すべての CRR を取得するのにかかる時間が、セッションリカバリ中に認識される遅延の主な要因でした。障害が発生した際に、セッションマネージャに多数のセッションがあると、遅延が非常に長くなることがありました。また、コールのリカバリに特定の順序がないため、アクティブセッションよりも前にアイドルセッションが回復されることもありました。

（注） 早期 PDU リカバリ機能は、最大 5% のセッションを回復できます。

リカバリ中のセッションの優先順位付け

このリリース以前は、セッションリカバリ機能はリカバリ対象として選択されたセッションに優先順位を付けず、コールリカバリリスト内のすべてのコールをループ処理し、セッションリカバリがトリガーされると順番に回復していました。

リカバリにおけるセッションの優先順位付けの一環として、優先コールのみを対象に別途スキップリストを保持します。該当するレコードがループ処理によらず、AAAMgrからすぐに送信できるようにするためです。その結果、優先コールの迅速なリカバリとデータ停止時間の短縮につながります。

ユーザープレーンには、優先セッションと通常セッションの2種類のセッションがあります。セッションが優先セッションかどうかは、コントロールプレーンから受信したメッセージの優先順位フラグに基づいて判別され、優先セッションがまず回復され、その後に通常のコールが続きます。

これらの優先セッションは、早期 PDU 処理でも優先されます。通常コールの早期 PDU リカバリは、すべての優先セッションのリカバリが完了してはじめて開始されます。

クリティカルフラッシュ（GR）の場合、まず優先セッションのチェックポイントが送信され、その後に通常のコールが送信されます。スイッチオーバー中は、すべてのコール（通常コールと優先コールの両方）のデータが許可されます。

（注） コントロールプレーンがすべてのコールに優先順位フラグを設定します。ユーザープレーンは、コントロールプレーンから受信した優先コールの詳細を、セッションの優先順位付け機能に使用します。

4G CUPS の 1:1 ユーザープレーン冗長性の設定

以下の項では、機能を有効または無効にするために使用できる CLI コマンドについて説明します。

アクティブ UP とスタンバイ UP 間の BFD モニタリングの設定

アクティブ UP およびスタンバイ UP で Bidirectional Forwarding Detection（BFD）のモニタリングを設定するには、次のコマンドを使用します。このコマンドは、SRP コンフィギュレーション モードで設定します。

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor bfd context context_name { ipv4_address | ipv6_address
} { chassis-to-chassis | chassis-to-router }
      exit
```

注：

- **no**：アクティブおよびスタンバイ UP で BFD モニタリングを無効にします。
- **context** *context_name* ：使用するコンテキストを指定します。BFD ピアが設定されているコンテキスト（SRP コンテキスト）を参照します。

  context_name は、1 ～ 79 文字の英数字で表される既存のコンテキストである必要があります。
- *ipv4 _address* | *ipv6_address*：モニターする BFD ネイバーの IP アドレスを定義します。これは、IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記を使用して入力します。

  設定された BFD（ICSR）ピアの IP アドレスを参照します。
- **chassis-to-chassis** | **chassis-to-router**：

chassis-to-chassis：非 SRP リンク上のプライマリシャーシとバックアップシャーシの間で BFD を実行できるようにします。

chassis-to-router：BFD はシャーシとルータの間で動作します。

⚠

注意　アクティブ UP とスタンバイ UP 間の SRP リンクでは、BFD モニタリングに **chassis-to-router** キーワードを使用しないでください。

- このコマンドは、デフォルトで無効になっています。

BGP モニタリング障害のフラグ付け

単一の BGP ピア（ユーザープレーン）障害時に BGP モニター障害のフラグを設定するには、次のコマンドを使用します。このコマンドは、SRP コンフィギュレーション モードで設定します。

（注）

- このリリースでは、**exclusive-failover** キーワードが既存の **monitor bgp** CLI コマンドに追加され、BGP モニタリング障害にフラグを立てるための代替（新しい）アルゴリズムとして使用されます。
- **monitor bgp** CLI コマンドの詳細については、『Command Reference Guide』の「Service Redundancy Protocol Configuration Mode Commands」の項 [英語] を参照してください。
- **exclusive-failover** キーワードを既存の **monitor bgp** CLI コマンドに追加する前に **monitor bgp** コマンドを実装すると、次のように動作しました。
  - BGP ピアグループ内のいずれかの BGP ピアが稼働している場合、BGP ピアグループは稼働していました。
  - BGP モニターのグループ設定を省略すると、そのモニターがグループ 0 に含まれていました。
  - BGP グループ 0 は暗黙的なグループからのコンテキストでモニターされました。各コンテキストは、個別の BGP グループ 0 の暗黙的モニターグループを形成しました。
  - いずれかの BGP ピアグループがダウンしている場合、BGP モニターはダウンしていました。

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor bgp exclusive-failover
      end
```

注：

- **no**：単一の BGP ピア障害時の BGP モニター障害のフラグ設定を無効にします。
- 新しい **exclusive-failover** キーワードを実装すると、動作は次のようになります。
  - BGP ピアグループ内のいずれかの BGP ピアが稼働している場合、BGP ピアグループは稼働します。
  - BGP ピアをグループ 0 に含めることは、非グループ化（グループを省略する）と同じです。
  - いずれかの BGP ピアグループまたは非グループ BGP ピアがダウンすると、BGP モニターはダウンします。
  - モニター対象の BGP ピアを削除すると、BGP モニター障害が発生します。
- このコマンドは、デフォルトで無効になっています。

アクティブ UP とスタンバイ UP での Sx モニタリングの設定

アクティブ UP およびスタンバイ UP で Sx モニタリングを設定するには、次のコマンドを使用します。このコマンドは、[SRP Configuration] モードで設定します。

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor sx [ { context context_name | bind-address
{ipv4_address |ipv6_address } | { peer-address {ipv4_address | ipv6_address } }
 ]
       exit
```

注：

- **no**：アクティブおよびスタンバイ UP で Sx モニタリングを無効にします。
- **context***context_name*：Sx サービスのコンテキストを指定します。

  context_name は、1 ～ 79 文字の英数字で表される既存のコンテキストである必要があります。
- **bind-address {** *ipv4 _address* **|** *ipv6_address***}**：Sx サービスのサービス IP アドレスを定義します。IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記を使用して入力します。

（注） **bind-address** および **peer-address** の IP アドレスファミリは同じである必要があります。

- **peer-address {** *ipv4 _address* **|** *ipv6_address***}**：Sx ピアの IP アドレスを定義します。IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記を使用して入力します。
- **disallow-switchover-on-peer-monitor-fail** ：

UP から CP へのリンクの動作ステータスが不明な場合に、UP がアクティブ状態にスイッチバックされるのを防止します。

- 複数の Sx 接続をモニタリングする場合には、この CLI コマンドを複数回実装できます。
- モニター対象の Sx 接続のいずれかがダウンすると、Sx のモニター状態も停止します。
- このコマンドは、デフォルトで無効になっています。

アクティブ UP とスタンバイ UP での SRP over IPSec の設定

IPSec は、IP ネットワーク全体でセキュアなプライベート通信を提供するために相互にデータをやり取りする一連のプロトコルです。これらのプロトコルにより、システムはピアセキュリティ ゲートウェイとセキュアなトンネルを確立して維持できます。IPSec は、IP データグラムに機密性、データの完全性、アクセス制御、およびデータソース認証を提供します。

CUPS アーキテクチャでは IPSec プロトコルを使用して、アクティブ UP とスタンバイ UP 間のシャーシ間セッションリカバリ（ICSR）接続を介して送信されるパケットを暗号化します。この暗号化を実現するために、Service Redundancy Protocol（SRP）ピア間のすべてのトラフィックを照合するアクセスリストが定義され、このリストがクリプトマップに関連付けられます。このクリプトマップは、UP に存在する IPSec ピア間のセキュリティ アソシエーションを確立するために使用されます。

（注） IPSec、その機能、および該当する CLI 設定の詳細については、StarOS の『*IPSec Reference*』[英語] を参照してください。

CLI コマンドを使用して UP で SRP over IPSec を設定する例を以下に示します。

```
context srp
   ip access-list srp-acl
   permit tcp host 209.165.200.225 host 209.165.200.226
   #exit
   ipsec transform-set A-foo
   #exit
   ikev2-ikesa transform-set ikesa-foo
   #exit
   crypto map srp-cm ikev2-ipv4
   match address srp-acl
   authentication local pre-shared-key key local key
   authentication remote pre-shared-key key remote key
   ikev2-ikesa transform-set list ikesa-foo
   payload foo-sa0 match ipv4
   ipsec transform-set list A-foo
   #exit
   peer 209.165.200.227
   #exit
   service-redundancy-protocol
   checkpoint session duration non-ims-session 30
   checkpoint session duration ims-session 30
   route-modifier threshold 18
   delta-route-modifier 2
   audit periodicity 60
   priority 2
```

```
monitor bgp context isp 209.165.200.228
monitor sx context EPC2 bind-address bbbb:abcd::77 peer-address bbbb:abcd::10
peer-ip-address 209.165.200.226
bind address 209.165.200.225
#exit
interface ike-lb loopback
ip address 209.165.200.228 255.255.255.224
crypto-map srp-cm
#exit
interface srp-rtr
ip address 209.165.200.229 255.255.255.224
#exit
interface srp-loopback loopback
ip address 209.165.200.225 255.255.255.224
#exit
ip route 209.165.200.226 255.255.255.224 209.165.200.231 srp-rtr
ip route 209.165.200.227 255.255.255.224 209.165.200.231 srp-rtr
#exit
```

（注） IKEv1：認証ヘッダー（AH）プロトコルを使用したトランスポートモードは推奨されません。ESP では認証と暗号化の両方が実行されるため、Encapsulating Security Payload（ESP）が推奨されます。

アクティブ UP およびスタンバイ UP での VPP モニターの設定

次のコマンドを使用して、VPP がダウンした場合にアクティブ UP で UP スイッチオーバーをトリガーするように Vector Packet Processing（VPP）モニターを設定します。このコマンドは、SRP コンフィギュレーション モードで設定します。

```
configure
  context context_name
    service-redundancy-protocol
      monitor system vpp delay-period 0-300 seconds
      exit

no monitor system vpp
```

注：

- **no**：アクティブおよびスタンバイ UP で VPP モニタリングを無効にします。
- **vpp delay-period***0-300 seconds* ：VPP 障害後のスイッチオーバーの遅延時間を秒単位で指定します。

  遅延時間が 0 より大きい値の場合、VPP に障害が発生すると、指定された遅延時間の後にスイッチオーバーが開始されます。遅延時間内の最後の VPP ステータス通知が、スイッチオーバーアクションの最終トリガーです。デフォルト値は 0 秒で、すぐにスイッチオーバーが開始されます。

  遅延は、VPP が一時的にダウンし、回復が進行中のシナリオに対処するために必要です。これは、スイッチオーバーが不要な場合があることを意味します。

- このコマンドは、デフォルトで無効になっています。

LZ4 圧縮アルゴリズムの設定

必要に応じて、RCM ソリューションの LZ4 圧縮アルゴリズムを有効にすることができます。zlib アルゴリズムはデフォルトのままになります。この設定は、セッション関連のチェックポイントにのみ適用されます。

Zlib アルゴリズムはデータのパッケージングに優れていますが、CPU 使用率が高くなります。それに対して、LZ4 圧縮アルゴリズムは CPU 使用率を抑えますが、データ圧縮率は低くなります。したがって、LZ4 圧縮アルゴリズムが有効になっている場合、UP でのセッションマネージャの CPU 使用率は名目上減少します。ただし、RCM に保存される各チェックポイントのサイズがわずかに増加するため、使用される RCM メモリが多くなります。

LZ4 圧縮アルゴリズムの使用を有効にするには、RCM コンフィギュレーション モードで **checkpoint session compression lz4** CLI コマンドを使用します。**checkpoint session compression zlib** CLI コマンドを使用して、圧縮アルゴリズムを zlib に戻すこともできます。

次のコマンドシーケンスは、LZ4 圧縮の使用を有効にします。

```
configure
  context context_name
    redundancy-configuration-module rcm_name
      checkpoint session compression lz4
      end
```

RCM システムレベルの MOP :

1. UP(F) スイッチオーバーを防ぐには、RCM オペレーションセンターで **rcm pause switchover true** CLI コマンドを使用します。
2. すべての UP で、冗長グループレベル全体の圧縮アルゴリズムを LZ4 に更新します（Day-0.5 設定および実行中の設定）。

   show config context *context_name* または **show config url** *url* CLI コマンドを使用して、**checkpoint session compression lz4** CLI コマンドが有効になっているかどうかを確認します。
3. すべてのチェックポイント マネージャ コンテナを再起動し、すべてのチェックポイントが再同期するのを待つか、RCM 高可用性を実行します。

   次の例を参考にしてください。

   ```
   kubectl -n rcm get pod rcm-checkpointmgr-0 -o yaml | grep -i
   "containerID:  docker
   - containerID:
   docker://3f7e6b10a1be3005424eae148cca2905df8e24e0a549069dfacba533c7b57bf3
   sudo docker restart
   3f7e6b10a1be3005424eae148cca2905df8e24e0a549069dfacba533c7b57bf3
   [sudo] password: 3f7e6b10a1be3005424eae148cca2905df8e24e0a549069dfacba533c7b57bf3
   ```

   RCM 高可用性の場合は、プライマリ RCM オペレーションセンターで **rcm migrate primary** CLI コマンドを実行します。
4. **rcm pause switchover false** CLI コマンドを使用して、**rcm pause switchover** の値を **false** に戻します。

冗長グループレベルの MOP：

1. UP(F) スイッチオーバーを防ぐには、RCM オペレーションセンターで **rcm pause switchover true red-group** *red_group_number* CLI コマンドを使用します。
2. すべての UP で、冗長グループレベル全体の圧縮アルゴリズムを LZ4 に更新します（Day-0.5 設定および実行中の設定）。

   show config context *context_name* または **show config url** *url* CLI コマンドを使用して、**checkpoint session compression lz4** CLI コマンドが有効になっているかどうかを確認します。
3. UP で、RCM インターフェイスを停止してから起動します。

   RCM インターフェイスを停止するための設定例を以下に示します。

```
Configure
  port ethernet 1/10
    vlan 2199
      shutdown
```

4. RCM オペレーションセンターで **rcm pause switchover false red-group** *red_group_number* CLI コマンドを使用して **rcm pause switchover** 値を **false** に戻します。

（注） 同じ MOP に従って、圧縮アルゴリズムを LZ4 から zlib に変更し、キーワード **lz4** を **zlib** に置き換えます。

ユーザー プレーン スイッチバックの防止

次のコマンドを使用して、新しいアクティブ UP での Sx モニター障害が原因で、新しいスタンバイ UP が再びアクティブ状態にスイッチバックされないようにします。このコマンドは、SRP Configuration モードで設定します。

```
configure
  context context_name
    service-redundancy-protocol
      monitor sx disallow-switchover-on-peer-monitor-fail [ timeout
seconds ]
      exit
```

次のいずれかの CLI を使用して、新しいスタンバイ UP からアクティブ状態へのスイッチバックを許可します。

```
no monitor sx disallow-switchover-on-peer-monitor-fail
```

または

```
monitor sx disallow-switchover-on-peer-monitor-fail timeout 0
```

注：

- **no**：スイッチオーバー防止を無効にします。
- **disallow-switchover-on-peer-monitor-fail [timeout** *seconds* **]**：UP から CP へのリンクの動作ステータスが不明な場合に、UP のアクティブ状態へのスイッチバックを防止します。

  timeout *seconds*：スタンバイピアで Sx 障害ステータスがリセットされない場合でも、このタイムアウトの経過後にスイッチバックを許可します。有効な値の範囲は 0 ～ 2073600（24 日）です。

（注） タイムアウトを「0」秒に指定すると、計画外のスイッチオーバーが可能になります。

  timeout キーワードが指定されていない場合、アクティブシャーシはスタンバイピアで Sx 障害ステータスがリセットされるまで無期限に待機します。

- デフォルト設定では、あらゆる条件において、Sx モニター障害による計画外のスイッチオーバーが許可されます。

（注） 手動による計画的スイッチオーバーは、この CLI が設定されているかどうかに関係なく許可されます。

デュアル アクティブ エラー シナリオの防止

CP で次の CLI 設定を使用して、UP 1:1 冗長性のデュアル アクティブ エラー シナリオを回避します。

```
configure
    user-plane-group group_name
       sx-reassociation disabled
       end
```

注：

- **sx-reassociation disabled**：CP との関連付けがすでに存在する場合、UP Sx の再関連付けを無効にします。

Sx モニター障害のリセット

サービス冗長性プロトコル（SRP）の Sx モニター障害情報をリセットするための次のコマンドは、スタンバイシャーシでのみ使用できます。このコマンドは、EXEC モードで設定します。

```
srp reset-sx-fail
```

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングとトラブルシューティングのサポートに使用できるCLIコマンドに関する情報を提供します。

コマンドや出力の表示

この項では、この機能のサポートにおけるshowコマンドまたはその出力について説明します。

show srp monitor bfd

この CLI コマンドの出力には、4G CUPS 1:1 UP 冗長性機能に関する次のフィールドが含まれています。

- タイプ
- 状態
- GroupId
- IP Addr
- Port
- Context（VRF Name）
- Last Update

show srp monitor bgp

この CLI コマンドの出力には、4G CUPS 1:1 UP 冗長性機能に関する次のフィールドが含まれています。

- タイプ
- 状態
- GroupId
- IP Addr
- ポート
- Context (VRF Name)
- Last Update

show srp monitor sx

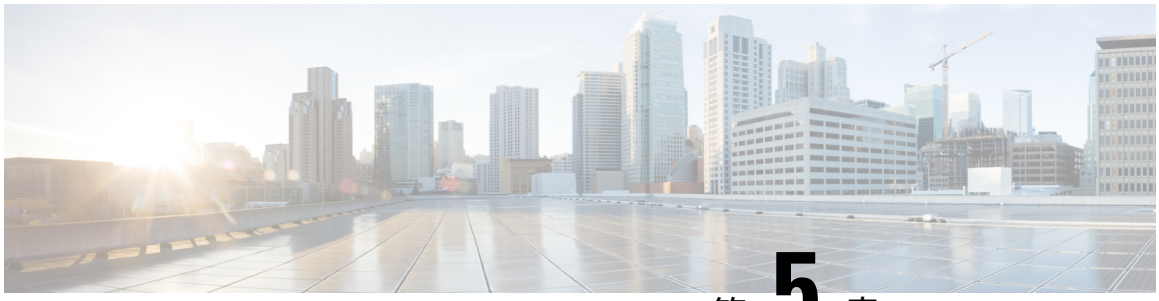
この CLI コマンドの出力には、4G CUPS 1:1 UP 冗長性機能に関する次のフィールドが含まれています。

- タイプ
- 状態
- GroupId
- IP Addr
- ポート
- Context（VRF Name）
- Last Update

show srp monitor vpp

この CLI コマンドの出力には、4G CUPS 1:1 UP 冗長性機能に関する次のフィールドが含まれています。

- タイプ
- 状態
- GroupId
- IP Addr
- ポート
- コンテキスト（VRF 名）
- Last Update



第 5 章

CUPS の SAEGW 向け 5G NSA

機能説明

Cisco 5G Non Standalone（NSA）ソリューションは、既存の LTE 無線アクセスとコアネットワーク（EPC）をモビリティ管理とカバレッジのアンカーとして活用します。このソリューションにより、オペレータは Cisco EPC Packet Core を使用して 5G サービスをより短時間で開始し、既存のインフラストラクチャを活用できます。こうして、NSA はネットワークの中断を最小限に抑えながら 5G サービスを展開するためのシームレスなオプションを提供します。

5G は 4G/LTE の次世代となる 3GPP テクノロジーであり、ワイヤレスモバイルデータ通信向けに定義されています。5G 標準は、5G ネットワークのニーズに応えるために 3GPP リリース 15 で導入されました。

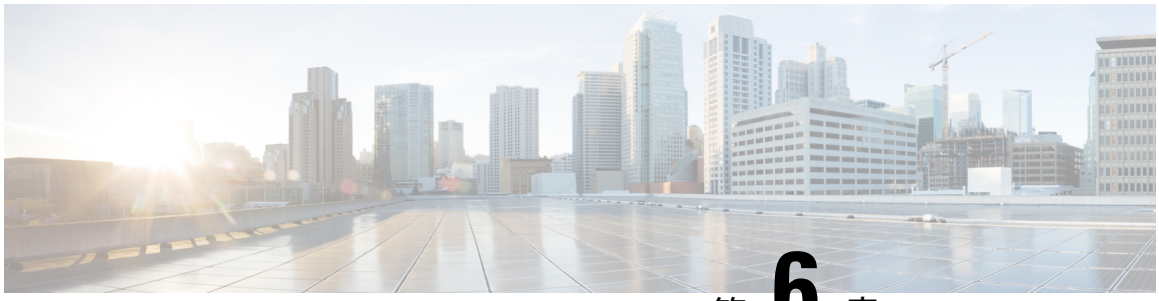
5G 非スタンドアロン（NSA）：既存の LTE 無線アクセスおよびコアネットワーク（EPC）を活用して、デュアル接続機能を使用して 5G NR を固定します。このソリューションにより、通信事業者はより短い時間とより少ないコストで 5G サービスを提供できます。

制限事項

- CUPS アーキテクチャでは、DCNR に基づいて SGW-U/PGW-U を選択する SGW-C/PGW-C は、このリリースではサポートされていません。
- このリリースでは、APNMBR レート制限の設定はサポートされていません。APNMBR ポリサーは、内部で自動再調整を使用します。

  制限事項の詳細については、『*5G Non Standalone Solution Guide*』の「*5G NSA for SAEGW*」の章 [英語] を参照してください。

5G NSA for SAEGW の詳細については、『*5G Non Standalone Solution Guide*』の「*5G NSA for SAEGW*」の章 [英語] を参照してください。



第 6 章

アクセス コントロール リスト

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

CUPS アーキテクチャは、ユーザープレーンのアクセス制御リストをサポートします。この機能により、ユーザープレーンがサブスクライバの IP アクセス権限を作成、管理できます。

アクセス コントロール リストの設定

この機能には、非 CUPS アーキテクチャの一部である既存の設定が実装されています。**ip access-list** コマンド（コンテキスト コンフィギュレーション モードの一部）は、アクセス制御リストを実装するために使用されます。

（注） CUPS の場合、同じ設定がユーザープレーンの APN コンフィギュレーション モードで実装されます。

IP ベースのユーザーアクセス権限を作成および管理するには、次の設定を使用します。

```
configure
  context context_name
    ip access-list acl_name
      { deny | permit } [ log ] source_address source_wildcard
      no { deny | permit } [ log ] source_address source_wildcard
      end
```

注：

- **no**：指定したオプションに完全に一致するルールを削除します。
- **deny|permit**：ルールがブロック（deny）または許可（permit）フィルタであることを指定します。
  - **deny**：ルールが一致した場合、対応するパケットをドロップすることを示します。
  - **permit**：ルールが一致した場合、対応するパケットを許可することを示します。
- **log**：フィルタに一致するすべてのパケットがログに記録されることを示します。デフォルトでは、パケットはログに記録されません。
  - *source_address*：パケットの送信元の IP アドレス。IP アドレスは、IPv4 ドット付き 10 進表記で入力する必要があります。

    このオプションは、特定の IP アドレスや IP アドレスグループからのすべてのパケットをフィルタ処理するために使用されます。

    アドレスのグループを指定する場合、初期アドレスはこのオプションを使用して設定されます。アドレスの範囲は、*source_wildcard* パラメータを使用して設定できます。
  - *source_wildcard*：このオプションは、*source_address* オプションとともに使用して、パケットをフィルタ処理するアドレスのグループを指定します。

    マスクは補数として入力する必要があります。
    - このパラメータの 0 ビットは、*source_address* パラメータに設定されている対応するビットが同一である必要があることを意味します。
    - このパラメータの 1 ビットは、*source_address* パラメータに設定されている対応するビットを無視する必要があることを意味します。

（注） マスクには、最下位ビット（LSB）からの連続した1ビットのセットが含まれている必要があるため、許可されるマスクは0、1、3、7、15、31、63、127、および255です。使用可能なワイルドカードの例は、0.0.0.3、0.0.0.255、および0.0.15.255です。ワイルドカード0.0.7.15は、1ビットが連続していないため使用できません。

モニタリングおよびトラブルシューティング

ここでは、アクセス制御リスト機能のモニタリングと障害対応について説明します。

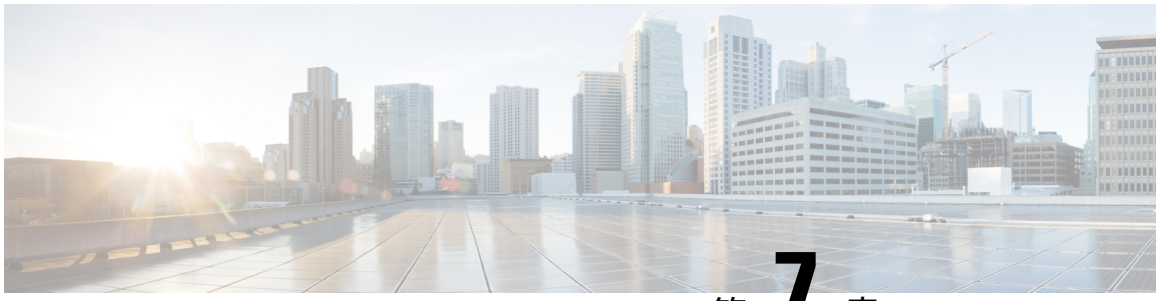
コマンドや出力の表示

この項では、この機能のサポートにおけるshowコマンドまたはその出力について説明します。

show sub user-plane-only full all

上記のコマンドを実行すると、この機能に関する次のフィールドが表示されます。

- active input acl
- active output acl
- ipv4 input acl drop
- ipv4 output acl drop



第 7 章

ADC Over Gx

機能説明

3GPP TS 29.244 V15.0.0 に準拠している、ADC Over Gx 機能は CUPS 環境で次の機能をサポートします。

- インスタンスレベルでのアプリケーションの開始/停止イベントレポート。セッション使用状況レポート要求の一部として、Sx インターフェイスを介して提供。
- フローが Ruledef のグループに一致すると、アプリケーションの開始/停止が Ruledef のグループに送信されます。
- ルールラインの AND ロジックをサポート、および ADC ルール定義の照合。
- ADC アプリケーション検出通知に使用されるパケット転送制御プロトコル（PFCP）メッセージの新しい情報要素（IE）のサポート。

重要 このリリースでは、ADC Over Gx 機能は、ADC L3/L4 ルールに適用されます。

重要 非 CUPS 環境での ADC Over Gx 機能の補足情報については、次を参照してください。

- ADC アドミニストレーション ガイド [英語] の「Application Detection and Control Overview」の章にある「ADC Support over Gx」の項。
- P-GW アドミニストレーション ガイド [英語] の「Gx Interface Support 」の章にある「Support ADC Rules over Gx Interface」の項。

機能の仕組み

CUPS 環境の ADC Over Gx 機能については、次のサポートが追加されています。

- アプリケーション ID/TDF アプリケーション識別子は、Sx 確立要求または Sx セッション変更要求における PDR の PDI の一部です。
- U プレーンで ADC ルールの照合を処理します。
- アプリケーションの開始/停止イベントが U プレーンで発生したときにセッション使用状況レポート要求を生成します。
- 使用状況レポート要求の一部としての新しい IE：
  - アプリケーション ID
  - アプリケーション インスタンス ID
  - フロー情報
- 新しい IE を復号するためのモニタープロトコル。
- 受信した使用状況レポート要求を処理し、C プレーンで PCRF への CCR-U をトリガーします。

ADC Over Gx 機能は次のコンポーネントで構成されており、この項では各コンポーネントについて説明します。

ADC ルールの照合

従来のルール照合の後に、ADC ルールの照合が呼び出されます。L3/L4 フィルタが照合されると、ルール照合エンジンがベアラーに設定されている ADC ルールをチェックします。ADC ルールが存在する場合は、ADC ルールの照合が行われます。

L3/L4 フィルタを持たない ADC ルールがベアラーにあり、それが非 GBR ベアラーである場合、ADC ルールの照合はすべての非 GBR ベアラーで行われます。課金は、ルール照合の課金およびアクションポリシーに対して行われます。

ADC 動的ルールの場合、L3/L4 フィルタが一致しても、ADC ルールが一致しない場合、ルールは不一致と見なされます。

セッション使用状況レポート要求の生成

U プレーンで ADC ルールが一致し、アプリケーションが検出されると、U プレーンが Sx インターフェイスを介して、次の状況のセッション使用状況レポートとしてアプリケーションの開始通知をトリガーします。

- 測定方法が [Event] に設定されている
- 使用状況レポートのトリガーが [Start of Traffic] に設定されている

- アプリケーション ID、アプリケーション インスタンス ID、アプリケーションフロー情報などのアプリケーション検出情報と方向。

アプリケーションのティアダウンが正常に行われるか、アプリケーションがタイムアウトになるか、ルール照合が変更されると、次の状況のセッション使用状況レポートとしてUプレーンからCプレーンにアプリケーションの停止がトリガーされます。

- 測定方法が [Event] に設定されている
- 使用状況レポートのトリガーが [Stop of Traffic] に設定されている
- アプリケーション ID
- アプリケーション インスタンス ID

アプリケーションの停止は、次の場合にはトリガーされません。

- 「ミュート」が有効になっている。
- コールがダウンしている。
- ルールや PDR が削除されている。
- ベアラーやトンネルの削除が発生している。

C プレーンでのセッション使用状況レポートの処理

Cプレーンでセッション使用状況レポートを受信すると、イベントが検出され、送信する必要がある属性とともに PCRF に向けて CCR-U がトリガーされます。

動的 HTTP リダイレクト

Gx を介して受信されるリダイレクトルールとアクションは、動的ルールの RAR および CCA-U メッセージの一部です。CUPS は、C プレーンから U プレーンに伝達され、U プレーンに適用されるリダイレクトルールとアクションをサポートします。次のフィールドが変換され、U プレーンと U プレーンのリダイレクトに適宜送信されます。

```
[V] Redirect-Information:
   [V] Redirect-Support:
   [M] Redirect-Address-Type:
   [M] Redirect-Server-Address:
```

C プレーンの場合：

- PDR に関連付けられた FAR は、Gx を介した ADC 動的ルールの「Redirect-Information」AVP をサポートするために入力されます。
- PDR と FAR は、「Redirect-Information」IE とともに U プレーンに送信されます。
  - CCA-I の Gx を介した ADC 動的ルールで PCRF からの「Redirect-Information」AVP を受信した場合の Sx セッション確立要求。
  - CCA-U の Gx を介した ADC 動的ルールで PCRF からの「Redirect-Information」AVP を受信した場合の Sx セッション変更要求。

- RAR の Gx を介した ADC 動的ルールで PCRF からの「Redirect-Information」AVP を受信した場合の Sx セッション変更要求。

- ADC 動的ルールの削除のサポートが追加されています。

U プレーンの場合：

- サブスクライバの ADC 動的ルールがインストールされます。
- パケットは、ADC 動的ルールが一致した場合にリダイレクトされます。

制限事項

次に、ADC Over Gx 機能の既知の制限事項を示します。

- U プレーンの TDF アプリケーション識別子と「**policy-control bypass TDF-ID-validation** CLI コマンドが存在しない場合、コールはドロップされ、適切な切断理由は表示されません。
- 「ミュート」から「ミュート解除」や「ミュート解除」から「ミュート」への変更シナリオなど、事前定義された ADC ルールの設定の変更は、このリリースではサポートされていません。
- セッション中の ADC ルールの更新や変更（設定の変更または RAR を介した PDN 更新）はサポートされていません。
- デフォルトベアラーの L3/L4 ルールでは、ADC がサポートされます。
- HTTP リダイレクト用の ADC Over Gx は、専用ベアラーに適していません。

ライセンス

ADC Over Gx 機能にはアプリケーション検出制御ライセンスが必要です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

ADC over Gx の設定

非 CUPS 環境の ADC Over Gx で使用可能な CLI コマンドは、CUPS 環境でも使用できます。

以下に設定例を示します。

- [Policy Control Configuration] モードでこの機能を有効にする場合：

```
diameter encode-supported-features adc-rules
```

- [ACS Rulebase Configuration] モードで ADC の定義済みルールを設定する場合：

```
action priority 55 dynamic-only adc ruledef qci5 charging-action charge-action-qci5
action priority 56 dynamic-only adc mute group-of-ruledefs qci5_gor charging-action
 charge-action-qci5
```

重要 ADC Over Gx 機能が有効で、アプリケーションの開始/停止イベントトリガーが登録されていない場合、アプリケーションの開始/停止は PCRF に送信されません。

重要 CLI コマンドの詳細については、『*Command Line Interface Reference*』[英語] を参照してください。

モニタリングおよびトラブルシューティング

ここでは、この機能のモニタリングや障害対応に使用できる CLI コマンドについて説明します。

モニタープロトコル

monitor protocol コマンドを使用する場合は、オプション 49 を有効にして、Sx メッセージの ADC 関連パラメータを表示します。

コマンドや出力の表示

コントロールプレーン

show active-charging subscribers callid <callid> urr-info

この show コマンドの出力が変更され、ボリュームや期間関連の URR とともに ADC の URR が表示されるようになりました。

U プレーン上

show subscribers user-plane-only full all

この show コマンドの出力は、「関連付けられた ADC PDR の数」を表示するように変更されました。

show subscribers user-plane-only callid <callid> pdr full all

この show コマンドの出力は、次の新しいフィールドを表示するように変更されました。

- TDF アプリケーション ID
- TDF 通知
- 検出された ADC PDR の総数

show subscribers user-plane-only callid <callid> urr full all

この show コマンドの出力は、ボリュームおよび期間関連の URR とともに ADC URR を表示するように変更されました。

show user-plane-service rulebase name <rulebase_name>

この show コマンドの出力が拡張され、この機能がサポートされるようになりました。ADC ルールと「ミュート」を使用する ADC ルールを識別するために、次の 2 つの新しいタイプ文字が導入されました。

- RDA：A は ADC ルール用
- GDAM：AM は「ミュート」を使用する ADC ルール用

show sub user-plane-only full all

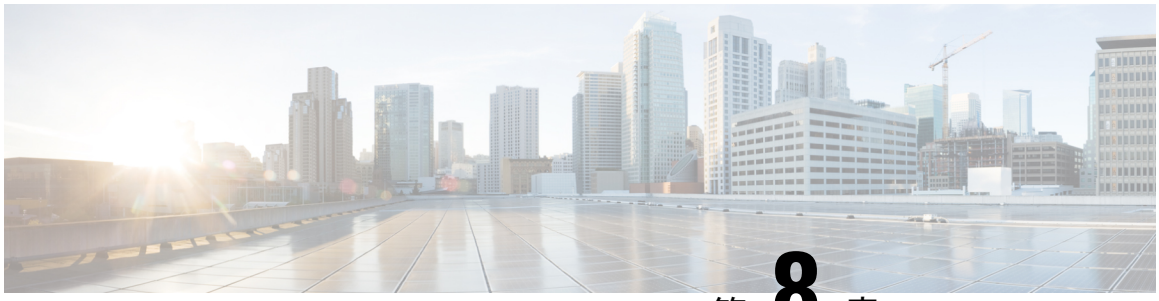
この show コマンドの出力が拡張され、ADC PDR およびリダイレクトフローに関する情報を表示するようになりました。

- Flow Action Redirected フロー
- 関連付けられた ADC PDR の数

show user-plane-service statistics all

この show コマンドの出力が拡張され、ADC Redirect Stats の下に次の新しいフィールドが表示されるようになりました。

- ADC リダイレクトフロー



第 8 章

IP グループでの IP プールの追加

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

既存の CUPS プラットフォームでは、新しい IP プールが追加されると、この新しいプールの作成後に登録されたユーザープレーン（UP）のみが該当するプールを使用できます。既存の UP で新しいプールを使用するには、UP のリロードまたは UP の再関連付けを実行する必要があります。

IP グループへの IP プールの追加機能により、新しい IP プールが追加されると、APN 設定をもとに、既存の各 UP にこの新しいプールからチャンクを取得する資格があるかどうかが評価されます。UP に新しいプールからチャンクを取得する資格があれば、チャンクが UP に割り当てられ、以降のコール割り当てに使用されます。

次のシナリオで、UP は資格ありと判断されます。

- APN にプールグループが設定されている。新しいプールは、このプールグループに追加される。

- APNにプール名およびプールグループが設定されていない。新しいパブリックプールが追加される。

（注） APN で実施された変更は、UP が再関連付けまたはリロードされるまで有効になりません。

機能の仕組み

ここでは、IP グループに IP プールを追加する機能の仕組みについて簡単に説明します。

CP-CP ICSR 環境での新しいプールの追加

1. スタンバイ コントロール プレーン（CP）に新しいプールを追加します。
2. アクティブ CP に新しいプールを追加します。

   チャンクは適格な UP に割り当てられ、同じものがスタンバイ CP にチェックポイントされます。
3. 両方の CP に対する **show { ip | ipv6 } pool-chunks pool-name** <*name*> コマンドが同期されているかを確認します。

CP-CP ICSR 環境でのプールの削除

1. アクティブ CP のプールを削除します。
2. **show { ip | ipv6 } pools** コマンドを使用して、すべての IP がスタンバイ CP の削除されたプールから解放されていることを確認します。
3. スタンバイ CP のプールを削除します。

（注） 同じ IP プールの IP Pool コマンドと Busyout コマンドを同時に追加すると、競合状態が発生します。この問題を回避するには、IP Pool コマンドと Busyout コマンドを別々に実行します。

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングとトラブルシューティングのサポートに使用できる CLI コマンドに関する情報を提供します。

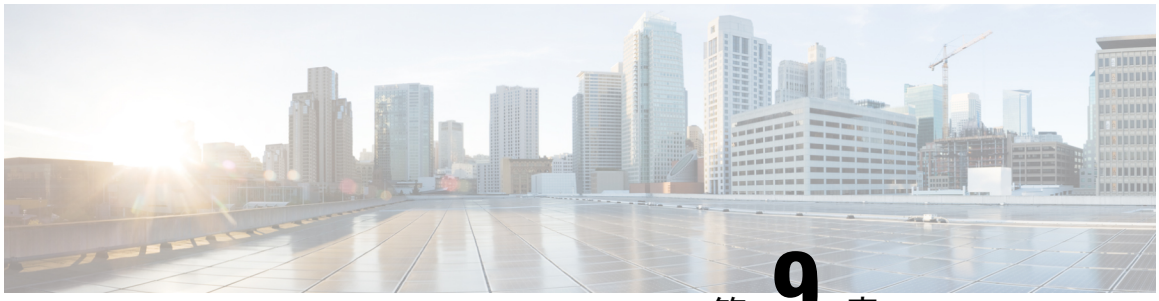
コマンドや出力の表示

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show ip user-plane verbose

この CLI コマンドの出力には、CUPS モードでの IP グループへの IP プールの追加機能をサポートする次のフィールドが表示されます。

- 動的プール数
- apn-without-pool-name-v4
- apn-without-pool-name-v6
- プールグループ
- プールグループ名



第 9 章

APN ACL のサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

現在、CUPS（21.19.x より前のリリース）では、APN レベルの ACL 定義が UP で設定されています。

この機能により、CP で設定された ACL は UP にプッシュされます。この機能を使用することで、すべての UP ノードで ACL 定義を個別に設定するコストや労力を削減できます。

（注）
- このリリースへのアップグレードに進む前に、CP 設定で APN ACL を確認します。
- CP と UP の両方で同じコンテキスト名が設定されている必要があります。CP は、UP よりも多くのコンテキストを持つことができます。コンテキスト名が一致しない場合、それぞれの ACL は UP でドロップされます。
- CP と UP の両方で APN ACL を定義しないことを推奨します。ただし、必要な場合は、競合を回避するために、UP と CP の ACL 名を互いに異なるものにする必要があります。
- 下位互換性を確保するために、UP 設定でローカルに作成された ACL が優先されます。
- APN が特定のユーザープレーングループに属している場合、同じ APN の ACL は、同じユーザープレーングループに属する UP にのみプッシュされます。
- 最大 64 のコンテキストが許可され、コンテキストごとに最大 16 の ACL が許可されます。
- 複数の APN が同じコンテキストで ACL を共有できます。
- ACL の変更内容は、新しいセッションにのみ適用され、進行中のセッションには適用されません。
- IPv6 の ACL で **deny any** ルールが設定されている場合は、ルータアドバタイズメント（RA）とルータ要請（RS）メッセージを ACL で明示的に許可する必要があります。

トラブルシューティング

ここでは、この機能の障害対応について説明します。

（注） この機能は、デフォルトでイネーブルにされています。

show コマンド

ここでは、この機能の show コマンドについて説明します。

show user-plane-service ip-access-list name *access list name*

このコマンドは、ユーザープレーンの ACL ルールを表示するために使用されます。

show user-plane-service pdn-instance name *apn name*

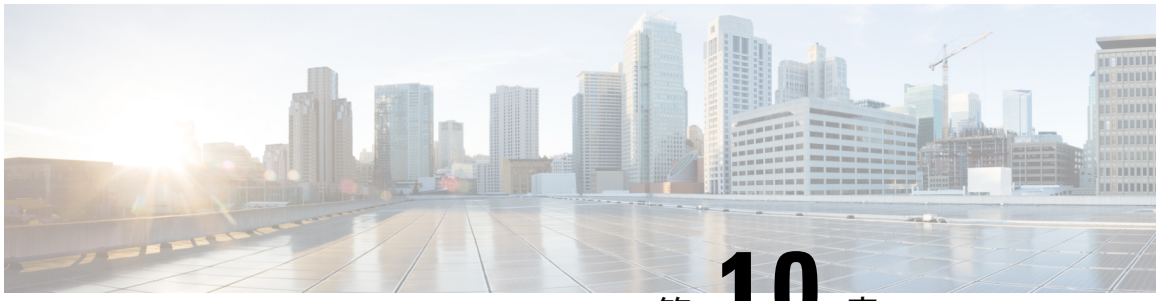
このコマンドは、ユーザープレーンの apn のアクセスグループを表示するために使用されます。

show srp statistics

このコマンドは、SRP を介した APN ACL の送信、受信、および廃棄されたパケット数を表示するために使用されます。

show demux-mgr statistics sxdemux all

この show コマンドは、CP から送信された PFD ACL_INFO パケット数を表示するために使用されます。



第 10 章

APN AMBR トラフィックポリシング

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

APN-AMBR は、HSS の APN ごとに保存されるサブスクリプション パラメータです。S-GW は、デフォルトベアラーの確立手順において APN-AMBR を提供します。APN-AMBR により、すべての GBR 以外のベアラーと同じ APN のすべての PDN 接続にわたって提供されることが予想される集約ビットレートが制限されます。これらの GBR 以外のベアラーのそれぞれが APN-AMBR 全体を利用する可能性があります。たとえば、他の GBR 以外のベアラーがトラフィックを伝送しない場合などです。P-GW は、ダウンリンクおよびアップリンク方向に APN-AMBR を適用します。

この CLI 制御機能の一環として、CLI パラメータをコントロールプレーンで設定し、Sx インターフェイスを介してユーザープレーンに伝達する必要があります。

制限事項

以下に、APN-AMBR トラフィックポリシング機能の既知の制限事項を示します。

- **token-replenishment-interval** および **violate-action shape** CLI の設定はサポートされません。

APN AMBR トラフィックポリシング機能の設定

ここでは、APN-AMBR トラフィックポリシングの設定方法について説明します。

```
configure
         context context_name
           apn apn_name
      apn-ambr rate-limit direction { downlink | uplink } [ burst-size
 { auto-readjust duration { milliseconds msecs | seconds } |
violate-action { drop | lower-ip-precedence | transmit }
               end
```

注：

- **rate-limit direction { downlink | uplink }**：ダウンリンク（ネットワークからサブスクライバ）トラフィック、アップリンク（サブスクライバからネットワーク）トラフィックのどちらにレート制限を適用するかを指定します。
- **burst-size { auto-readjust duration milliseconds msecs | seconds }**：このパラメータは、トラフィックのショートバーストが許容データレートを超えないようにするために、ポリシングアルゴリズムで使用されます。トークンバケットの最大サイズです。
  - **auto-readjust duration***seconds*：バーストサイズの計算（バーストサイズ＝ピークデータレート/8 * 自動再調整期間）で使用される期間（秒単位）。
    - 秒は 1 ー 30 の整数値である必要があります。デフォルトは 1 秒です。
  - **milliseconds**：*msecs* は 100 ～ 900 の整数値で、100 ミリ秒単位で指定する必要があります。たとえば、100、200、300 などです。
- **violate-action { drop | lower-ip-precedence | transmit }**：ベアラーコンテキストのデータレートが AMBR を超えた場合に P-GW が実行するアクション。
  - **drop**：違反パケットをドロップします。
  - **lower-ip-precedence**：違反パケットの DSCP 値をゼロ（「ベストエフォート」）に設定します。
  - **transmit**：違反パケットを送信します。これは、この機能のデフォルト動作です。
- この機能が導入される前は、デフォルト動作では違反パケットはドロップされました。

モニタリングおよびトラブルシューティング

この項では、APN-AMBR トラフィックポリシング機能のモニターや障害対応に使用できるコマンドについて説明します。

show コマンドと出力

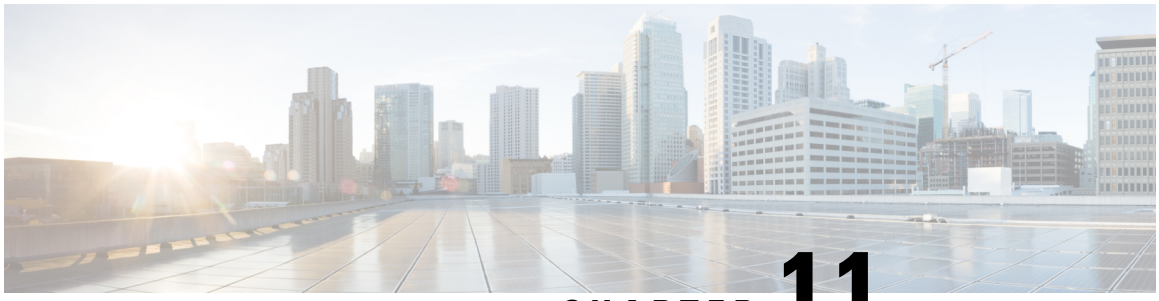
この項では、APN-AMBR トラフィックポリシング機能のモニタリングや障害対応に使用できる show コマンドについて説明します。

- **show user-plane-service pdn-instance name <apn_name>**：APN-AMBR CLI がコントロールプレーンで設定され、ユーザープレーンへの PFD プッシュが完了すると、次の APN-AMBR 情報がユーザープレーンで使用可能になります。
  - APN-AMBR
    - [Downlink Apn Ambr]：ダウンリンクトラフィックのレート制限が有効か無効かを示します。
      - [Burst Size]：ダウンリンクトラフィックのバーストサイズを示します。
      - [Auto Readjust]：ダウンリンクバーストサイズの自動再調整が有効か無効かを示します。
      - [Auto Readjust Duration]：ダウンリンクバーストサイズの計算に使用される期間を示します。
      - [Burst Size(bytes)]：バーストサイズをバイト単位で示します。
      - [Violate Action]：ベアラーコンテキストのデータレートがダウンリンクトラフィックの AMBR を超えた場合に P-GW が実行するアクションを示します。
    - [Uplink Apn Ambr]：アップリンクトラフィックのレート制限が有効か無効かを示します。
      - [Burst Size]：アップリンクトラフィックのバーストサイズを示します。
      - [Auto Readjust]：アップリンクバーストサイズの自動再調整が有効か無効かを示します。
      - [Auto Readjust Duration]：アップリンクバーストサイズの計算に使用される期間を示します。
      - [Burst Size(bytes)]：バーストサイズをバイト単位で示します。
      - [Violate Action]：ベアラーコンテキストのデータレートがアップリンクトラフィックの AMBR を超えた場合に P-GW が実行するアクションを示します。
    - [Token Replenishment Interval]：トークンの補充間隔を示します。

- **show sub user-plane-only full all**:

  ユーザープレーンでこの show コマンドを使用すると、ドロップされたパケットの数と、APN-AMBR ポリサーが原因で IP プレシデンスが低下したことを確認できます。この機能をサポートするために、次のフィールドが導入されました。

  - [APN AMBR Uplink Pkts Drop]：アップリンクトラフィックでドロップされた APN-AMBR パケット数を示します。
  - [APN AMBR Uplink Bytes Drop]：アップリンクトラフィックでドロップされた APN-AMBR バイト数を示します。
  - [APN AMBR Uplink Pkts IP pref lowered]：IP プレシデンスが低下する APN-AMBR アップリンクパケット数を示します。
  - [APN AMBR Uplink Bytes IP pref lowered]：IP プレシデンスが低下する APN-AMBR アップリンクのバイト数を示します。
  - [APN AMBR Downlink Pkts Drop]：ダウンリンクトラフィックでドロップされた APN-AMBR パケット数を示します。
  - [APN AMBR Downlink Bytes Drop]：ダウンリンクトラフィックでドロップされた APN-AMBR バイト数を示します。
  - [APN AMBR Downlink Pkts IP pref lowered]：IP プレシデンスが低下する APN-AMBR ダウンリンクパケット数を示します。
  - [APN AMBR Downlink Bytes IP pref lowered]：IP プレシデンスが低下する APN-AMBR ダウンリンクバイト数を示します。



CHAPTER 11

APN データトンネル MTU サイズの設定

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

拡張パケットコア（EPC）により、IPv4 および IPv6 データパケットのカプセル化を必要とするさまざまなインターフェイスが定義されます。EPC はヘッダーをカプセル化して追加するため、IPv4 および IPv6 パケットをフラグメント化する場合はさらに注意する必要があります。

適切な設定により、EPC のどのノードでもフラグメンテーションが発生しないようにする必要があります。この機能は、MTU に基づいて IPv6 および IPv4 パケットをフラグメント化します。

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 に送信するようサポートします。（インターネットでは）ダウンリンクデータパケットの送信が可能になっているため、設定された MTU に基づいて、必要に応じて送信元でデータのフラグメンテーションが実行されます。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、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。

制限事項

- P-GW/SAEGW IPv6セッションの場合、パケットがAPN MTU値を超えると、ICMPがVPPで使用できないため、CLI **policy ipv6 tunnel mtu exceed notify-sender** はサポートされません。
- GGSN/P-GW/SAEGW IPv4 セッションの場合、パケット（df ビット付き）が APN MTU 値を超えると、ICMP が VPP で使用できないため、CLI **access-link ip-fragmentation df-fragment-and-icmp-notify** はサポートされません。
- GGSN/P-GW/SAEGW IPv4 セッションの場合、パケット（df ビット付き）が APN MTU 値を超えると、ICMP が VPP で使用できないため、CLI **access-link ip-fragmentation normal** はサポートされません。

MTU の設定

次のCLIコマンドは、P-GWとモバイルノード間のIPv4およびIPv6トンネルで送信されるデータの最大伝送ユニット（MTU）を設定します。

```
configure
  context context_name
    apn apn_name
      ppp mtu bytes
      data-tunnel mtu bytes
      policy ipv6 tunnel mtu exceed { fragment inner | notify-sender
 | fragment }
      access-link ip-fragmentation { df-ignore  | normal |
df-fragment-and-icmp-notify }
      end
```

注：

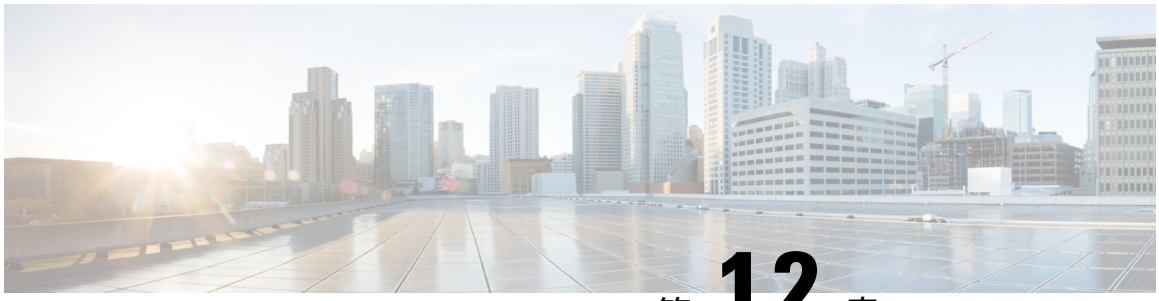
- *bytes*：P-GW とモバイルノード間の IPv6 トンネルの MTU を指定します。bytes は 1,280 ～ 2,000 の整数で指定する必要があります。デフォルト：1,500。
- **ppp**：P-GW とモバイルノード間の IPv4 トンネルで送信されるデータを指定します。
- **data-tunel mtu**：P-GW とモバイルノード間の IPv6 トンネルで送信されるデータを指定します。
- **fragment internal**：GTP トンネルイニシエータでフラグメントを 1 回実行します。
- **notify-sender**：システムは着信パケットをドロップし、元の送信者に「ICMPv6 Packet Too Big」を送信します。

（注） これはデフォルトのCLI設定でもあるため、明示的に設定されていない場合はデフォルトの動作になります。

- **fragment**：中間 GTP ホップでフラグメンテーションまたはリアセンブルを実行します。
- **df-ignore**：DF（Don't Fragment）ビット設定を無視し、アクセスリンクを介してパケットをフラグメント化して転送します。

（注） これはデフォルトの CLI 設定でもあるため、明示的に設定されていない場合はデフォルトの動作になります。

- **df-fragment-and-icmp-notify**：DF ビットを部分的に無視し、パケットをフラグメント化して転送します、また、パケットの送信元に ICMP エラーメッセージを返します。このように送信される ICMP エラーの数は、セッションごとに 1 秒あたり 1 つの ICMP エラーパケットにレート制限されます。
- **normal**：パケットをドロップし、ICMP 到達不能メッセージをパケットの送信元に送信します。



第 12 章

ユーザープレーンでのアプリケーションベースのテザリング検出

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

重要 アプリケーションベースのテザリング検出は、非CUPSアーキテクチャでサポートされている既存の機能です。このリリースでは、この機能はCUPSアーキテクチャでサポートされています。

アプリケーションベースのテザリング検出ソリューションは、アプリケーション識別用の既存の ADC プラグインを中心に構築されています。テザリング固有のパターンは、認識されたアプリケーションプラグインの上に追加されます。これらのプラグインは、アプリケーションフローがテザリングされているかどうかに応じて連続して返されます。アプリケーションベースのテザリング検出は、他の既存のサポートされているテザリング技術と連動します。

非 CUPS アーキテクチャと同様に、テザリング検出は現在 Netflix と YouTube でのみサポートされています。

CUPS のこの機能は、CUPS 以外のテザリングパターン検出技術と同等です。

アプリケーションベースのテザリング検出の詳細については、『*ADC Administration Guide*』の「*App-based Tethering Detection*」の章 [英語] を参照してください。

制限事項

CUPS のこの機能は、CUPS 以外のテザリングパターン検出技術と同等のため、ネットワーク内のテザリングされたデバイスで使用される新しい TLS パターンがある場合、新しいパターンはテザリング検出で識別されません。

アプリケーションベースのテザリング検出の設定

この項では、アプリケーションベースのテザリング検出のサポートを有効にする方法について説明します。

ルールベースレベルでのアプリケーションベースのテザリング検出の有効化

重要　テザリング設定はコントロールプレーンで実行し、ユーザープレーンにプッシュする必要があります。

ACS ルールベースコンフィギュレーション モードで、ADC トラフィックのアプリケーションベースのテザリング検出を有効にするには、次のコマンドを使用します。

```
configure
  active-charging service service_name
    rulebase rulebase_name
      tethering-detection application
      exit
    exit
  exit
```

注：

- **default tethering-detection** コマンドにより、デフォルト値が設定されます。

  デフォルト：デフォルトでは、テザリング検出機能は無効になっています。

重要　OS および UA ベースのテザリング検出は、現在 CUPS ではサポートされていません。

- 以前に設定済みの場合は、**no tethering-detection** コマンドを使用して、ルールベースからテザリング検出設定を削除します。

ruledefレベルにおけるアプリケーションベースのテザリング検出の有効化

[Ruledef Configuration] モードでアプリケーションベースのテザリング検出を有効にするには、次の設定を使用します。

```
configure
  active-charging service service_name
    ruledef ruledef_name
      tethering-detection application { flow-tethered |
flow-not-tethered }
      exit
    exit
  exit
```

注：

- 以前に設定済みの場合は、**no tethering-detection** コマンドを使用して、ruledef からテザリング検出設定を削除します。

アプリケーションベースのテザリング検出のモニタリングと障害対応

この項では、アプリケーションベースのテザリング検出のモニタリングと障害対応に使用できる CLI コマンドに関する情報について説明します。

show コマンドと出力

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show user-plane-service statistic tethering-detection

この CLI コマンドの出力範囲が拡張され、この機能をサポートする次のフィールドが追加されました。

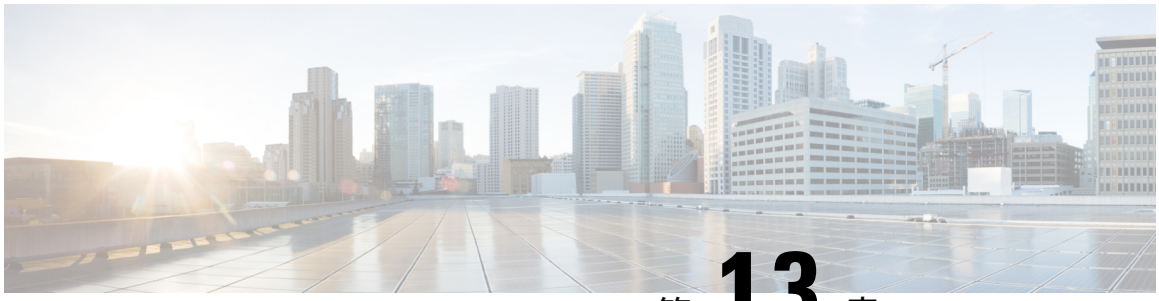
- テザリング検出統計（アプリケーション）：
  - スキャンされたフローの総数
  - テザリングされたフローの検出数
  - テザリングされたアップリンクパケット

- テザリングされたダウンリンクパケット

show user-plane-service statistic rulebase name <rulebase_name>

このCLIコマンドの出力範囲が拡張され、この機能をサポートする次のフィールドが追加されました。

- テザリング検出（アプリケーション）：
  - スキャンされたフローの総数
  - テザリングされたフローの検出数
  - テザリングされたアップリンクパケット
  - テザリングされたダウンリンクパケット



第 13 章

VPP による Cisco Ultra Traffic Optimization

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

Cisco Ultra Traffic Optimization は、CUPS アーキテクチャの VPP でサポートされています。

Cisco Ultra Traffic Optimization は、軋轢状態のセルのサブスクライバ接続速度を向上させることにより、セル容量を大幅に増やす RAN 最適化テクノロジーです。これにより、RAN の最適化が実現します。モバイルネットワーク事業者（MNO）はネットワーク品質の目標を達成する一方で、展開するセルの数を継続的に削減したり、トラフィックの増加に対応したりできます。

アダプティブビットレート（ABR）ビデオなどの大規模なトラフィックフローは、無線リソースを飽和させ、eNodeB スケジューラのメモリを大量に消費します。Cisco Ultra Traffic Optimization は、機械学習アルゴリズムを使用してネットワーク内の大規模なトラフィックフロー（ビデオ

など）を検出して、それらのフローデリバリを最適化し、ユーザーに提供する品質を変えることなくネットワークの輻輳を軽減します（ビデオのエンドユーザーエクスペリエンスが維持されます）。つまり、Cisco Ultra Traffic Optimization は、ネットワークの中核部分にソフトウェアインテリジェンスを取り入れることで、ビデオが RAN に与える多大な影響を軽減します。

その結果、輻輳した状態のネットワークでも Web サイトの閲覧が可能になります。Cisco Ultra Traffic Optimization：

- 平均ユーザースループットが向上します。
- 輻輳状態にあるセルサイトのキャパシティを増やします。
- スケジューラの遅延を削減します。
- セルを共有するユーザーやトラフィックが増えた場合にも、ユーザーエクスペリエンスの品質を維持します。
- eNodeB パフォーマンスカウンタ（平均 UE スループット、スケジューラ遅延など）によって直接測定されます。これらは、ネットワーク キャパシティ プランニングに使用される重要なパフォーマンス指標です。
- RAN の投資要件を永続的に節約します。
- Cisco StarOS P-GW に統合されます。
- 新しいハードウェアやケーブル配線の煩雑な作業は必要ありません。すぐに利用できます。
- HTTP(s) および SSH トラフィックに対応しています。

ライセンス

VPP を使用した Cisco Ultra Traffic Optimization は、シスコのライセンスソリューションです。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

RCM のサポート

この機能により、Cisco Ultra Traffic Optimization（CUTO）の Redundancy and Configuration Management（RCM）のサポートが有効になります。ユーザープレーンの Cisco Ultra Traffic Optimization（CUTO）プロファイルやポリシーのサービススキームとアプリケーションを使用して Cisco Ultra Traffic Optimization（CUTO）を有効にするために必要なすべての関連設定は、RCM を使用してサポートされます。

Cisco Ultra Traffic Optimization への GBR または MBR 値の送信

ストリームの作成や更新中に、有効な QER を持つベアラーが GBR ベアラーである場合、それぞれのベアラーレベルのダウンリンク GBR/MBR 値は、下限値または上限値として Cisco Ultra Traffic Optimization（CUTO）ライブラリに送信され、それ以外の場合は下限値または上限値はゼロになります。下限値と上限値は、1 秒あたりのビット数（BPS）です。RCM サポート後、P-GW はベアラーレベルの GBR と MBR ではなく、ダウンリンクフローレベルの GBR と MBR 値を最適化ライブラリに送信します。GBR ベアラーの場合、Cisco Ultra Traffic Optimization（CUTO）ライブラリにはフローレベルの GBR が下限値として、フローレベルの MBR が上限値として 送信されます。GBR ベアラー以外の場合、Cisco Ultra Traffic Optimization（CUTO）ライブラリには 0 が下限値として、フローレベルの MBR が上限値として送信されます。フローレベルの MBR が GBR ベアラー以外の APN-AMBR より大きい場合、トラフィックは APN-AMBR でスロットリングされます。このような場合、APN-AMBR が上限値として Cisco Ultra Traffic Optimization（CUTO）ライブラリに送信されます。フローに固有の有効なフローレベルの MBR がない場合、APN-AMBR が Cisco Ultra Traffic Optimization（CUTO）ライブラリに上限値として送信されます。最適化ライブラリは、3 タプル（送信元 IP、宛先 IP、プロトコル）に基づいて論理フローを維持しますが、非 CUPS アーキテクチャはフローを 5 タプル（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）として扱います。したがって、複数の非 CUPS アーキテクチャの 5 タプルエントリは、最適化ライブラリの同じ 3 タプルエントリに属することができます。PG-W は 5 タプルに基づいて GBR および MBR 値を最適化ライブラリに提供します。この機能の一部として、次の処理が実行されます。

- 最適化ライブラリは、同じ 3 タプルエントリに属するすべての MBR 値の最小値を上限値として使用します。
- 最適化ライブラリは、同じ 3 タプルエントリに属するすべての GBR 値の最大値を下限値として使用します。

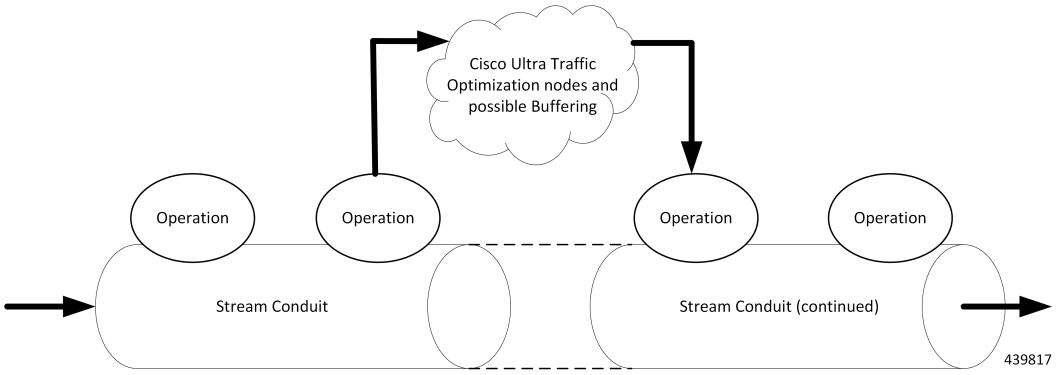
Cisco Ultra Traffic Optimization ライブラリの初期化解除

この機能は現在、初期化解除をサポートしていません。初期化解除は、Cisco Ultra Traffic Optimization（CUTO）ライセンスがシステムから削除されたときに発生します。

機能の仕組み

アーキテクチャ

次の図は、CUPS の VPP における Cisco Ultra Traffic Optimization のアーキテクチャを示しています。



Cisco Ultra Traffic Optimization は、コントロールプレーンとユーザープレーンに分割されます。

CUTO-CTRL

- CUTO-CTRL は、East-West API（EWAPI）を介して SMGR からガイダンスと要求を受信します。その結果、クライアント（SMGR インスタンス）が登録および登録解除され、新しいストリームやフローが作成および終了されます。
- CUTO-CTRL は、シスコが提供する SHM インフラストラクチャで構成される North-South API（NSAPI）を使用して、一連の共有メモリ（SHM）テーブルを管理します。
- CUTO-VPP は、この SHM 環境を通じて、CUTO-VPP と CUTO-CTRL の両方に表示されるコンテンツを読み取りおよび書き込みできます。
- SHM は、VPP での CUTO ソリューションの高性能設定と管理に必要な、すべての大容量かつスケーラブルで変更可能なコンテンツに使用されます。

CUTO-VPP

- CUTO-VPP は、ユーザープレーンのパケット処理エンジンです。
- fastpath では、Cisco Ultra Traffic Optimization は、その動作で設定されたストリーム上のパケットに適用されます。
- パケットはストリームコンジットから特定の CUTO-VPP 操作に送信され、潜在的な遅延（0 ～ N ミリ秒）の後、同じコンジットにトラフィックが返されます。
- Cisco Ultra Traffic Optimization アプリケーションによってパケットがドロップされることはありません。

制限事項

CUPS の Cisco Ultra Traffic Optimization 機能には、次の制限事項があります。

- サービススキーマで行われた CUTO 設定の変更は、既存のフローに対してはすぐに有効になりません。
- Cisco Ultra Traffic Optimization VPP のグローバルな初期化解除はサポートされていません。

- SMGR と CUTO-VPP 間の動的なメモリ割り当て。
- Cisco Ultra Traffic Optimization を有効にするためのベアラー関連のトリガーはサポートされていません。
- ルール照合変更トリガーは、CUPS の CUTO に対して設定する必要があります。
- トラフィック最適化の無効化は、「loc-update」トリガーではサポートされていません。
- Gx を介した Cisco Ultra Traffic Optimization の有効化はサポートされていません。
- CUTO ライセンスを削除しても、グローバルな初期化解除はトリガーされません。新しいフローの CUTO 機能を解除するには、CUTO 設定を削除する必要があります。

show コマンドと出力

この項では、CUPS での Cisco Ultra Traffic Optimization のサポートにおける show コマンドおよびコマンドの出力について説明します。

その他のサポートされている show コマンドの詳細については、P-GW アドミニストレーション ガイド [英語] の「Cisco Ultra Traffic Optimization」の章にある「Monitoring and Troubleshooting」の項を参照してください。

show コマンドと出力

show user-plane-service traffic-optimization counters sessmgr all

このコマンドの出力には、次のフィールドが含まれています。

TCP トラフィック最適化フロー：

- Active Normal Flow Count
- Active Large Flow Count
- Active Managed Large Flow Count
- Active Unmanaged Large Flow Count
- Total Normal Flow Count
- Total Large Flow Count
- Total Managed Large Flow Count
- Total Unmanaged Large Flow Count
- Total IO Bytes
- Total Large Flow Bytes
- Total Recovered Capacity Bytes

- Total Recovered Capacity ms

UDP トラフィック最適化フロー：

- Active Normal Flow Count
- Active Large Flow Count
- Active Managed Large Flow Count
- Active Unmanaged Large Flow Count
- Total Normal Flow Count
- Total Large Flow Count
- Total Managed Large Flow Count
- Total Unmanaged Large Flow Count
- Total IO Bytes
- Total Large Flow Bytes
- Total Recovered Capacity Bytes
- Total Recovered Capacity ms

show user-plane-service traffic-optimization info

このコマンドの出力には、次のフィールドが含まれています。

- CUTO Ctrl Library Version
- CUTO VPP Library Version
- Mode
- Configuration

show user-plane-service traffic-optimization policy all

このコマンドの出力には、次のフィールドが含まれています。

- Policy Name
- Policy-Id
- 帯域幅管理：
  - Backoff-Profile
  - Min-Effective-Rate
  - Min-Flow-Control-Rate
- 抑制制御：
  - Time

- Rate
- Max-Phases
- Threshold-Rate

- ヘビーセッション：
  - Threshold
  - Standard-Flow-Timeout

- リンクプロファイル：
  - Initial-Rate
  - Max-Rate
  - Peak-Lock

- Session-Params:
  - Tcp-Ramp-Up
  - Udp-Ramp-Up

バルク統計情報

CUPS の Cisco Ultra Traffic Optimization では、次の既存のバルク統計情報がサポートされています。

バルク統計情報	説明
cuto-uplink-drop	CUTO ライブラリによってドロップされたアップリンクパケットの合計数を示します。
cuto-uplink-hold	CUTO ライブラリによって保持されているアップリンクパケットの合計数を示します。
cuto-uplink-forward	CUTO ライブラリによって転送されたアップリンクパケットの合計数を示します。
cuto-uplink-rx	CUTO ライブラリが受信したアップリンクパケットの合計数を示します。
cuto-uplink-tx	CUTO ライブラリが送信したアップリンクパケットの合計数を示します。
cuto-dnlink-drop	CUTO ライブラリによってドロップされたダウンリンクパケットの合計数を示します。

バルク統計情報	説明
cuto-dnlink-hold	CUTO ライブラリによって保持されているダウンリンクパケットの合計数を示します。
cuto-dnlink-forward	CUTO ライブラリによって転送されたダウンリンクパケットの合計数を示します。
cuto-dnlink-rx	CUTO ライブラリが受信したダウンリンクパケットの合計数を示します。
cuto-dnlink-tx	CUTO ライブラリが送信したダウンリンクパケットの合計数を示します。
cuto-todrs-generated	生成された TODR の合計数を示します。
tcp-active-normal-flow-count	Cisco Ultra Traffic Optimization の TCP active-normal-flow カウントの数値を示します。
tcp-active-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-large-flow カウントの数値を示します。
tcp-active-managed-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-managed-large-flow カウントの数値を示します。
tcp-active-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-unmanaged-large-flow カウントの数値を示します。
tcp-total-normal-flow-count	Cisco Ultra Traffic Optimization の TCP total-normal-flow カウントの数値を示します。
tcp-total-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-large-flow カウントの数値を示します。
tcp-total-managed-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-managed-large-flow カウントの数値を示します。
tcp-total-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-unmanaged-large-flow カウントの数値を示します。
tcp-total-io-bytes	Cisco Ultra Traffic Optimization の TCP total-IO のバイト数を示します。
tcp-total-large-flow-bytes	Cisco Ultra Traffic Optimization の TCP total-large-flow のバイト数を示します。
tcp-total-recovered-capacity-bytes	Cisco Ultra Traffic Optimization の TCP total-recovered キャパシティのバイト数を示します。

バルク統計情報	説明
tcp-total-recovered-capacity-ms	Cisco Ultra Traffic Optimization の TCP total-recovered キャパシティをミリ秒単位で示します。
udp-active-normal-flow-count	Cisco Ultra Traffic Optimization の UDP active-normal-flow カウントの数値を示します。
udp-active-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-large-flow カウントの数値を示します。
udp-active-managed-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-managed-large-flow カウントの数値を示します。
udp-active-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-unmanaged-large-flow カウントの数値を示します。
udp-total-normal-flow-count	Cisco Ultra Traffic Optimization の UDP total-normal-flow カウントの数値を示します。
udp-total-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-large-flow カウントの数値を示します。
udp-total-managed-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-managed-large-flow カウントの数値を示します。
udp-total-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-unmanaged-large-flow カウントの数値を示します。
udp-total-io-bytes	Cisco Ultra Traffic Optimization の UDP total-IO のバイト数を示します。
udp-total-large-flow-bytes	Cisco Ultra Traffic Optimization の UDP total-large-flow のバイト数を示します。
udp-total-recovered-capacity-bytes	Cisco Ultra Traffic Optimization の UDP total-recovered キャパシティのバイト数を示します。
udp-total-recovered-capacity-ms	Cisco Ultra Traffic Optimization の UDP total-recovered キャパシティをミリ秒単位で示します。

レガシー（StarOS）実装に含まれる Cisco Ultra Traffic Optimization の次の統計は、CUPS 実装には適用されません。

- tcp-uplink-drop
- tcp-uplink-hold
- tcp-uplink-forward
- tcp-uplink-forward-and-hold

- tcp-uplink-hold-failed
- tcp-uplink-bw-limit-flow-sent
- tcp-dnlink-drop
- tcp-dnlink-hold
- tcp-dnlink-forward
- tcp-dnlink-forward-and-hold
- tcp-dnlink-hold-failed
- tcp-dnlink-bw-limit-flow-sent
- tcp-dnlink-async-drop
- tcp-dnlink-async-hold
- tcp-dnlink-async-forward
- tcp-dnlink-async-forward-and-hold
- tcp-dnlink-async-hold-failed
- tcp-process-packet-drop
- tcp-process-packet-hold
- tcp-process-packet-forward
- tcp-process-packet-forward-failed
- tcp-process-packet-forward-and-hold
- tcp-process-packet-forward-and-hold-failed
- tcp-pkt-copy
- tcp-pkt-Copy-failed
- tcp-process-pkt-copy
- tcp-process-pkt-copy-failed
- tcp-process-pkt-no-packet-found-action-forward
- tcp-process-pkt-no-packet-found-forward-and-hold
- tcp-process-pkt-no-packet-found-action-drop
- tcp-todrs-generated
- udp-uplink-drop
- udp-uplink-hold
- udp-uplink-forward
- udp-uplink-forward-and-hold
- udp-uplink-hold-failed

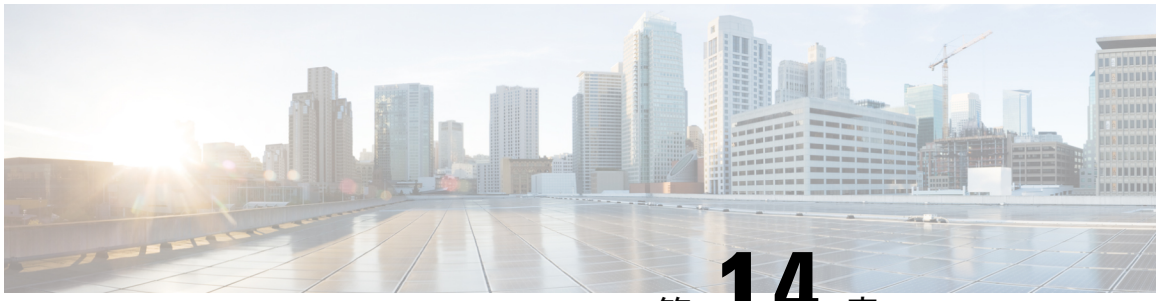
- udp-uplink-bw-limit-flow-sent
- udp-dnlink-drop
- udp-dnlink-hold
- udp-dnlink-forward
- udp-dnlink-forward-and-hold
- udp-dnlink-hold-failed
- udp-dnlink-bw-limit-flow-sent
- udp-dnlink-async-drop
- udp-dnlink-async-hold
- udp-dnlink-async-forward
- udp-dnlink-async-forward-and-hold
- udp-dnlink-async-hold-failed
- udp-process-packet-drop
- udp-process-packet-hold
- udp-process-packet-forward
- udp-process-packet-forward-failed
- udp-process-packet-forward-and-hold
- udp-process-packet-forward-and-hold-failed
- udp-pkt-copy
- udp-pkt-Copy-failed
- udp-process-pkt-copy
- udp-process-pkt-copy-failed
- udp-process-pkt-no-packet-found-action-forward
- udp-process-pkt-no-packet-found-forward-and-hold
- udp-process-pkt-no-packet-found-action-drop
- udp-todrs-generated

設定例

CUPS CUTO 機能を有効にするための設定例：

```
configure
  active-charging service ACS
    trigger-action TA1
       traffic-optimization policy custom1
```

```
    #exit
    trigger-condition TC1
      rule-name = dynamic-rule2
    #exit
    service-scheme SS1
      trigger rule-match-change
        priority 5 trigger-condition TC1 trigger-action TA1
      #exit
    subs-class SB1
      rulebase = cisco
    #exit
    subscriber-base default
      priority 5 subs-class SB1 bind service-scheme SS1
    #exit
    traffic-optimization-profile
      mode active
      data-record
    #exit
    traffic-optimization-policy custom1
      bandwidth-mgmt min-effective-rate 300 min-flow-control-rate 150
      heavy-session threshold 200000
      link-profile max-rate 20000
    #exit
    traffic-optimization-policy default
    #exit
end
```



第 14 章

既存のセッション Gy および Gz インターフェイスの課金アクション設定変更のサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

設定のギャップにより、CDR の Gy と Gz に不適切な使用状況レポートが送信され、チェックポイントの遅延により、SR/ICSR プロセスによるデータ損失も発生します。

Gy/Gz 課金に関する既存の Pure-P コールと Collapsed コールのギャップを解消するために、次の設定の変更が実装されています。

- 課金アクションにおける通話中の「Rated to Free」および「Free to Rated」。
- 異なる評価グループを持つ異なる課金アクションを使用した、通話中の優先順位の高いルールの追加。
- ruledef の課金アクションの通話中。

機能の仕組み

Rulebase 内の課金アクションと高優先順位ルールの追加に関連する設定変更のための既存のコールに、次のサポートが追加されました。

課金アクションでの従量制から無料および無料から従量制への通話の設定変更

課金アクションで「無料から従量制」への設定変更が生じた場合、コントロールプレーン（CP）が変更を適用し、Gy/Gz コンポーネントで必要となる URR を作成します。また、ユーザープレーンが使用状況レポートを報告すると、同じレポートが新しい変更内容に基づいて Gy インターフェイスと CDR に送信されます。

課金アクションで「従量制から無料」に設定が変更されると、ユーザープレーン（UP）は、使用状況レポートの従量制設定についてのみデータ通信量を CP に送信します。使用状況レポートを受信すると、必要に応じて Gy/Gz インターフェイスに報告されます。

異なる料金設定グループで異なる課金アクションを使用する優先度の高いルールを追加するための設定変更

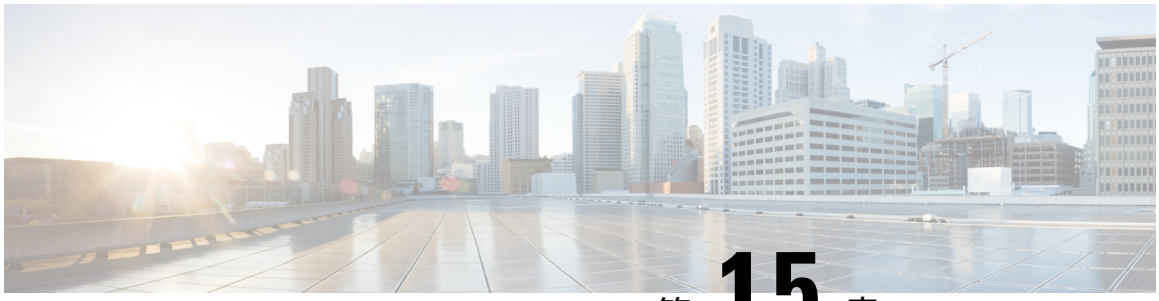
異なる課金アクションおよび異なる料金設定グループを使用する優先度の高いルールを追加することで、rulebase に設定変更を適用すると、ユーザープレーンは新しい課金アクションルールに個別の URR を送信し、CP は URR を設定と比較して新しい URR を処理します。CP は、該当する場合には、対応する情報を Gy/Gz インターフェイスに送信します。

Ruledef の課金アクション通話の設定変更

Rulebase の設定を変更するには、charging-action を別の charging-action や別の評価グループに変更します。CP は受信した新しい URR を処理し、正しい評価グループを含む CDR で適切な LOSDV を送信します。また、設定変更後にユーザープレーンがトラフィックの開始を CP に送信すると、CP は CCR-U に Gy を送信してクォータを要求します。

Gy の URR バケットチェックポイントの機能拡張

チェックポイントは「sx-session-usage-report」がユーザープレーンからコントロールプレーンに送信されてもすぐには実行されず、フルチェックポイントの一部として実行されます。その間、セッションがリカバリされると、チェックポイント間の詳細は失われます。この問題を回避するには、「sx-session-usage-report」がコントロールプレーンに到達したときにマイクロチェックポイントを実行する必要があります。



第 15 章

PCRF なしでの専用ベアラーの確立

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

P-GW は VoLTE 非対応の UE に IMS サービスを 提供するために、ディープ パケット インスペクション（DPI）機能を使用して、PCRF と連携せずに専用ベアラーを作成します。インターネット APN のデフォルトベアラーは PCRF との連携により作成されますが、この機能は音声サービスの高い QoS を維持するのに役立ちます。

SBC の IP アドレス（IPv4 または IPv6）とプロトコル RTP/RTCP は ruledef で設定され、サブスクライバトラフィックが PCRF との連携なしで ruledef と一致すると、音声サービスを検出するための専用ベアラーが作成されます。データフローがない場合、専用ベアラーは設定された時間制限後に削除されます。このとき、PCRF とは連携しません。

機能の仕組み

CUPS のサービス スキーマ フレームワークは、デフォルトのベアラーが PCRF を介して作成された場合に、GW での専用ベアラーの確立をサポートします。トリガー条件とトリガーアクションは、新しいトラフィックフローを作成するためにサービススキーマで設定されます。専用ベアラーを確立する場合、トリガー条件で設定されたルール名が、デフォルトのベアラールール名であるルールベース設定のルール名と一致する必要があります。

トラフィックがルール内で対応する IP や設定されたポート範囲と一致すると、事前定義されたルールトリガーアクションがアクティブになります。これにより、PCRF と連携しなくても、新しい専用ベアラーがアクティブ化されます。事前に設定された時間制限が経過しても、このベアラーにデータが流れない場合、ベアラーは削除されます。

主な特長は次のとおりです。

- VoLTE 以外の UE には別の APN が用意されており、VoLTE UE 専用ベアラーの作成が試みられないようにします。
- 専用ベアラーの作成に失敗した場合、コールは続行され、トラフィックはこのベアラーに流れ続けます。
- 専用ベアラーの作成を目的とした SX_Session_Report_Request の再送信は、既存の動作に従って実行されます。
- 機能のサポートは、P-GW/SAEGW CUPS コールに対してのみ提供されます。GGSN CUPS は、このリリースでは専用ベアラーをサポートしていません。

ここでは、PCRF を使用せずに専用ベアラーを確立する方法のコールフローと手順について説明します。

図 *7*: 通話フロー

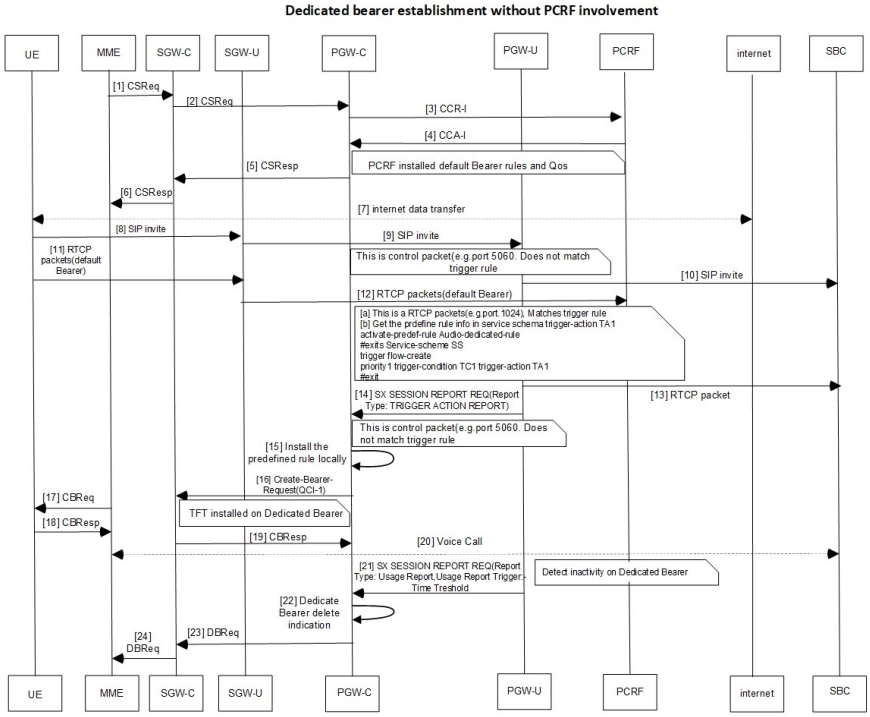


表 *1*: 手順

ステップ	説明
1	PCRF を使用してインターネット APN でデフォルトのベアラーを確立します。
2	デフォルトベアラーは SIP INVITE を受信すると、SBC に転送します。 （注）　ポート 5060/5061 は、専用ベアラーのポート範囲外にある SIP INVITE を受信します。
3	SBC アドレスやポート範囲がトリガールールに一致する RTCP パケットが受信されます。
4	ルールが一致すると、UP はサービススキーマを読み取り、専用ベアラーの作成に必要な事前定義されたルール情報を識別します。

ステップ	説明
5	UP は **SX_Session_Report_Request** （レポートタイプが Trigger Action Report の場合）を介してルール情報を CP と共有します。CP は要求メッセージを処理し、ルールのインストールをトリガーします。
6	専用ベアラーは、パケットフィルタ tft1 および tft2 で定義されているように、事前定義された **Audio_dedicated_rule** と複数のポート範囲を持つ TFT で作成されます。 （注） このようなルールの課金アクションには、**billing-action egcdr** と **content-id** が設定されています。
7	UE は、指定されたポート範囲のパケットを専用ベアラーにプッシュし、Audio_dedicated_rule と照合します。
8	300 秒後、またはしきい値の設定に照らして、非アクティブのタイムアウト値を過ぎた後、ベアラーが削除され、対応するデータカウントを持つベアラーに対して PGWCDR が生成されます。 • このしきい値は、キープアライブ/ウォッチドッグメッセージに基づいて調整できます。 • 音声コールフロー後の SIP 制御メッセージは、専用ベアラー TFT に定義されたポート範囲外のポートに送信されます。 （注） UE はデフォルトのベアラーで SIP 制御メッセージを送信するため、専用ベアラーアクティビティでは考慮されません。**AF-Charging-Id** は専用ベアラー PGWCDR に入力されません。

Sx インターフェイスの変更

UP でのルールの照合後アクティビティ中に、専用ベアラーの作成に必要な事前定義されたルール情報を取得するためにサービススキーマがチェックされます。この情報は、SX_Session_Report_ Request メッセージを介して CP と共有され、CP が専用ベアラー作成ルールのインストールをトリガーできるようにします。

以下で説明されているように、ルール情報は、新しく導入されたセッションレポートタイプ「Trigger Action Report」および SX プライベート IE を介して SX_Session_Report_ Request で送信されます。

表 *2:* セッションレポートタイプ *IE*

		ビット	

	オクテット	8	7	6	5	4	3	2	1	
	1 ～ 2	タイプ = 39（10 進数）								
	3 ～ 4	長さ = n								
	5	GTER	SRIR	予備	SPTIR	UPIR	ERIR	USAR	DLDR	
	6	予備				TAR	NBUR	UPRR	STS	
	7 ～（n + 4）	これらのオクテットは、明示的に指定されている場合にのみ存在します。								

オクテット 6（長さ > 1 の場合に存在）は次のようにエンコードされます。

- ビット 1：STS（サブスクライバ トレース ステータス レポート）：1 に設定されている場合、サブスクライバ トレース ステータス レポートを表します。
- ビット 2：UPRR。
- ビット 3：NBUR。
- ビット 4：TAR（Trigger Action Report）：1 に設定されている場合、Trigger Action Report IE を表します。
- ビット 5 ～ 8：スペア。

トリガーアクションレポート IE（プライベート IE）

これは、Pure-P および Collapse コールタイプにのみ適用される条件付き IE です。

表 *3:* トリガーアクションレポート *IE*

		ビット							
	オクテット	8	7	6	5	4	3	2	1
	1 ～ 2	タイプ = 256（10 進数）							
	3 ～ 4	長さ = n							
	5 ～ n+2	トリガーアクション							

複数の Trigger Action IE が TAR IE で指定されます。現行では、トリガーアクション内にパッキングされるトリガーアクションタイプは 1 つのみです。

トリガーアクション

次のフォーマットでエンコードされます。

表 *4:* トリガーアクション

		ビット								
	オクテット	8	7	6	5	4	3	2	1	
	1	トリガーアクションタイプ								
	2 ～ 3	長さ = p								
	4 ～ (4+p)	トリガーアクション BLOB								

トリガーアクションタイプ：現在許可される値 = 1（Rule Activate）。今後、さまざまなトリガーアクションタイプに拡張される可能性があります。

トリガーアクションBLOB：トリガーアクションタイプごとに一意。トリガーアクションタイプが [Activate Rule] の場合、次のようになります。

表 *5:* トリガーアクション *BLOB*

		ビット								
	オクテット	8	7	6	5	4	3	2	1	
	1 ～ p	ルール名								

N-1 互換性マトリックス

次の情報は、N-1 互換性マトリックスの一部を示しています。

番号	CP – UP	動作
1	CP と UP は同じバージョン	SX_Session_Report_Request が CP で処理され、トリガーアクションが実行されます。 CP は IE を検証し、TAR IE が正しくパッキングされていない場合には、Offending IE を使って拒否する必要があります。
2	CP の方がバージョンが古い（Sx セッションレポート要求の TAR を認識しない）	UP は、TAR ビットを含む SX_Session_Report_Request を送信します。CP はこの SX_Session_Report_Request を無視し、成功として UP に送信します。

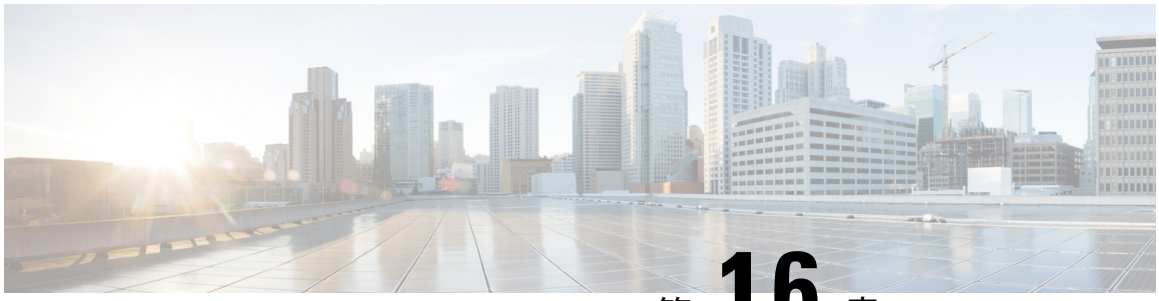
番号	CP – UP	動作
3	CP の方がバージョンが新しい	古いバージョンの UP は、TAR ビット = 1 の SX_Session_Report をトリガーしないため、処理は必要ありません。 ただし、CP は IE を検証し、TAR IE が正しくパッキングされていない場合には、Offending IE を使って拒否する必要があります。

active-charging-services の設定

PCRF と連携せずに専用ベアラーを確立するには、次の設定例を使用します。

```
config
  active-charging service acs
    ruledef Audio_dedicated_rule
      ip dst-address = 209.165.200.224/27
    #exit
    ruledef trigger_rule
      ip dst-address = 209.165.200.224/27
      udp either-port range 1024 to 5059
      udp either-port range 5062 to 43672
    #exit
    packet-filter tft1
      ip remote-port range 1024 to 5059
      ip remote-address = 209.165.200.224/27
    #exit
    packet-filter tft2
      ip remote-port range 5062 to 43672
      ip remote-address = 209.165.200.224/27
    #exit
    charging-action no_charge
    #exit
    charging-action ca_audio
      content-id 2
      billing-action egcdr
      qos-class-identifier 1
      flow limit-for-bandwidth direction downlink peak-data-rate 256000 peak-burst-size
 32000 violate-action discard
      flow limit-for-bandwidth direction uplink peak-data-rate 256000 peak-burst-size
300000 violate-action discard
      allocation-retention-priority 4 pvi 1 pci 1
      tft packet-filter tft1
      tft packet-filter tft2
    #exit
    rulebase prepaid
       billing-records egcdr
  #Install Audio_dedicated_rule on dedicated bearer to cater to VoLTE traffic
     action priority 1 dynamic-only ruledef Audio_dedicated_rule charging-action ca_audio

  #Use traffic matching to trigger_rule on default bearer as trigger condition
action priority 2 ruledef trigger_rule charging-action no_charge
    #exit
    trigger-action TA1
      #activate-predef-rule Audio_dedicated_rule
    #exit
    trigger-condition TC1
```

```
      rule-name = trigger_rule
    #exit
    trigger-condition tc
      rulebase = prepaid
    #exit
    service-scheme SS
      trigger flow-create
        priority 1 trigger-condition TC1 trigger-action TA1
      #exit
    subs-class SC1
      rulebase = prepaid
    #exit
    subscriber-base sb
      priority 1 subs-class SC1 bind service-scheme SS
    #exit
  #exit
context egress
    apn internet
 #Remove dedicated bearer after 300 seconds of inactivity
      timeout bearer-inactivity gbr 300 volume-threshold total 1
 active-charging rulebase prepaid
    exit
  exit
end
```



第 16 章

Pure-P セッションと Collapsed セッションのデフォルトおよび専用ベアラーのサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

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。

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。

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。

この機能により、UDP、TCP、および HTTP データは、デフォルトおよび専用ベアラーの fastpath にオフロードされます。

サポートされる機能

Pure-P およびコラスプセッションの場合：

1. デフォルトのベアラー確立には以下が含まれます（CCA-I）。
   - ルールを使用した場合と使用しない場合のデフォルトのベアラー確立。
   - 事前定義されたルール/ルールグループ（GoR）。
2. デフォルトのベアラー更新には以下が含まれます（CCA-U/RAR）。
   - 新しいルールのインストール。
   - 既存のルールの変更（TFT の変更、MBR/GBR の変更、フローステータスの変更）。
   - 既存のルールの削除。
   - デフォルトベアラー QoS の変更
   - APN-AMBR の変更。
   - 事前定義されたルール/GoR。
3. デフォルトのベアラー削除には以下が含まれます（CCA-U/RAR）。
   - 既存のルールの削除。

4. 専用ベアラーの確立には以下が含まれます（CCA-I/CCA-U/RAR）。
   - 新しい専用ベアラーの確立。
   - 事前定義されたルール/GoR。
5. 専用ベアラーの更新には以下が含まれます（CCA-U/RAR）。
   - インストール済みの専用ベアラーに新しいルールを追加。
   - 既存のルールの変更（TFT の変更、MBR/GBR の変更）。
   - 既存のルールの削除。
   - ルールの QCI の変更。
   - 事前定義されたルール/GoR
   - 専用ベアラーを介した ADC の基本サポート
   - 専用ベアラーのアイドルモードからアクティブモードへの移行（SAEGW、DDN）のサポート。
6. 専用ベアラーの削除には以下が含まれます。
   - MME/PCRF および **clear subscribers imsi** *imsi_id* **ebi** *ebi_id* CLI コマンドによる専用ベアラーの削除。
7. ユーザープレーンでの Pure-P および Collapsed セッションのリカバリ中に、ユーザープレーンの課金データがリカバリされます。
8. MME および eNodeB のハンドオーバー（HO）：
   - Pure-P コールタイプ：
     - Gx の新しいポリシー（作成、更新、削除、および作成、更新、削除の任意の組み合わせ）がある場合とない場合の MME と eNodeB の HO。
   - Collapsed コールタイプ：
     - Gx の新しいポリシー（作成、更新、削除）がある場合とない場合の MME と eNodeB の HO。
9. S-GW のハンドオーバー（HO）：
   - Pure-P から Pure-P への HO：
     - Gx の新しいポリシー（作成、更新、削除、および作成、更新、削除の任意の組み合わせ）がある場合の専用ベアラーを使用または使用しない Pure-P から Pure-P への HO。
     - HO 中に削除対象のマークが付けられたベアラーによる Pure-P から Pure-P への HO。

- Collapsed から Pure-P および Pure-P から Collapsed への HO：
  - Gx の新しいポリシー（新しいルールのインストール、デフォルトのベアラーQCI の変更、ルールの更新、ルールの削除）がある場合の専用ベアラーを使用しない Collapsed から Pure-P および Pure-P から Collapsed への HO。
  - Gx の新しいポリシーがある場合とない場合の専用ベアラーによる Collapsed から Pure-P および Pure-P から Collapsed HO への HO。

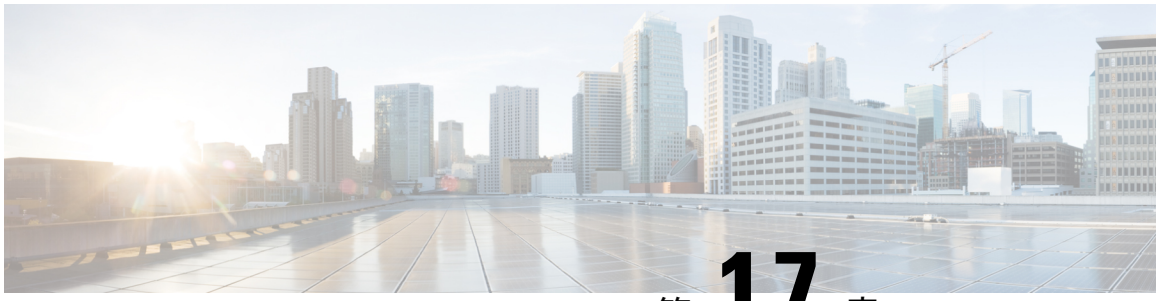
制限事項

このリリースでは、次の機能はサポートされません。

- デフォルトベアラーにインストールされているダイナミックルールの優先順位の更新。
- デフォルトベアラーおよび専用ベアラーにおける、ルールの時間ベースのアクティブ化と非アクティブ化。
- コリジョン処理はまだサポートされていません。

  コリジョンは、PCRF からの制御メッセージとアクセス側からの制御メッセージ間で発生する可能性があります。PCRF が開始する単一のメッセージ（CCA-U/RAR）内の複数の手順により、制御外のコリジョンが発生します。たとえば、同じ RAR 内のあるベアラーの作成と別のベアラーの削除などです。
- セッション中の ADC ルールの更新や変更（設定の変更または RAR を介した PDN 更新）はサポートされていません。
- MME および eNodeB のハンドオーバー（HO）：
  - Pure-P コールタイプ：
    - HO 中に発生した障害処理またはコリジョン。
  - Collapsed コールタイプ：
    - Gx からの新しいポリシー（作成、更新、および削除の任意の組み合わせ）を含む MME および eNodeB のハンドオーバー。
    - HO 中に発生した障害処理またはコリジョン。
- S-GW のハンドオーバー（HO）：
  - Pure-P から Pure-P への HO：
    - HO 中に発生した障害処理またはコリジョン。
    - ベアラーEBIが変更されないように、専用ベアラーにインストールされたダイナミックルール QCI の変更。
  - Collapsed から Pure-P および Pure-P から Collapsed への HO：

• HO 中に発生した障害処理またはコリジョン。



第 17 章

EDNS0 レコードのデバイス ID

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

表 *6*：マニュアルの変更履歴

改訂の詳細	リリース
この機能は、21.25 以降のリリースでサポートされています。	21.25
最初の導入。	21.24 より前

機能説明

EDNS0 のデバイス ID を使用すると、カスタマイズされたドメインを Cisco Umbrella を介してブロッキングできます。

EDNS0 機能でデバイス ID を有効にするには、次の手順を実行します。

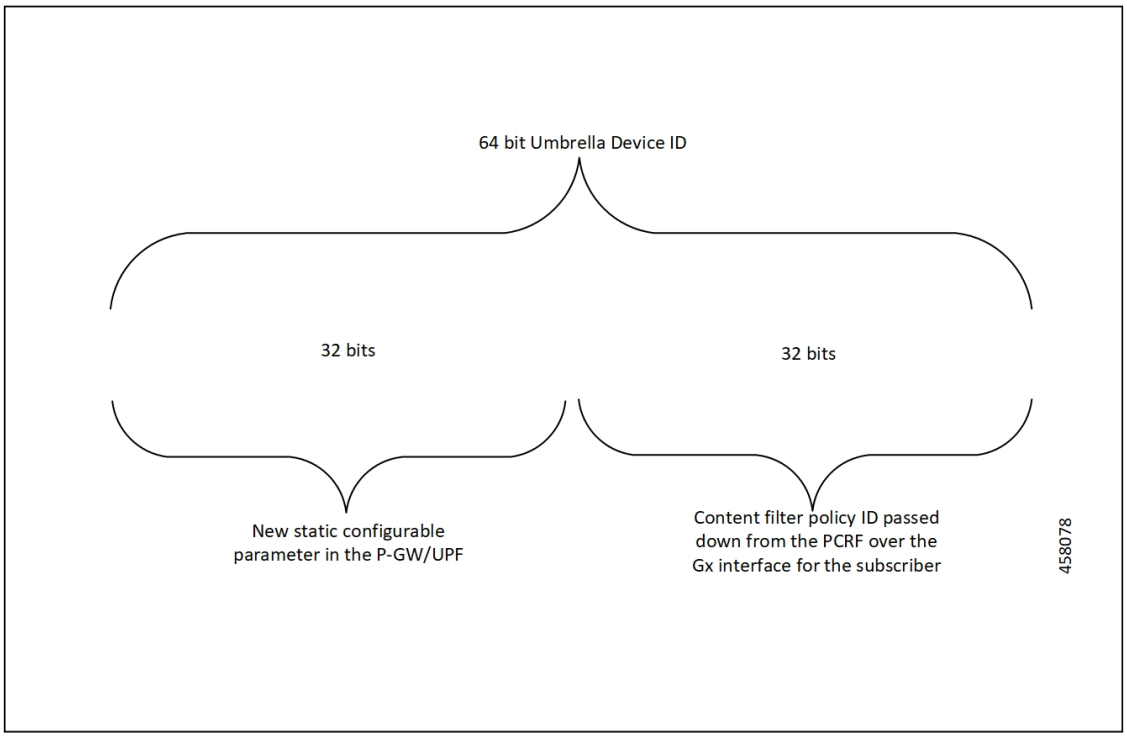
- UP はサブスクライバ DNS 要求を EDNS0 要求に再フォーマットする必要があります。
- UP では EDNS0 パケットに Cisco Umbrella の「デバイス ID」を含める必要があります。Cisco Umbrella DNS リゾルバはデバイス ID を使用して、EDNS0 パケット内のデバイス ID に関連付けられた、または設定されたドメインフィルタを適用できます。

コントロールプレーン（CP）は、PCRF または PCF からドメイン フィルタリング ポリシー ID を受信します。CP はドメイン フィルタリング ポリシー ID をサブスクライバパラメータでユーザープレーン（UP）に渡します。UP はドメイン フィルタリング ポリシー ID を使用して、ドメインフィルタリング機能をサブスクライバに適用します。

機能の仕組み

EDNS0 パケットが OPT RR データとして 64 ビットのデバイス ID を受信します。すべてのデバイス ID の最初の 32 ビットは、UP で設定された固定値です。サブスクライバデバイス ID の最後の 32 ビットは、PCRF または PCF から受信したコンテンツフィルタ ID 値です。UP はこの 2 つの 32 ビット値を連結して、サブスクライバ EDNS0 クエリに入力するための 64 ビットからなる完全なサブスクライバデバイス ID を作成します。CLI コマンドによって、静的デバイス ID 値の最初の 32 ビットを設定します。32-bit static prefix CLI コマンドを設定しない場合、発信パケットには device-ID = 32 ビット CF PolicyID が表示されます。

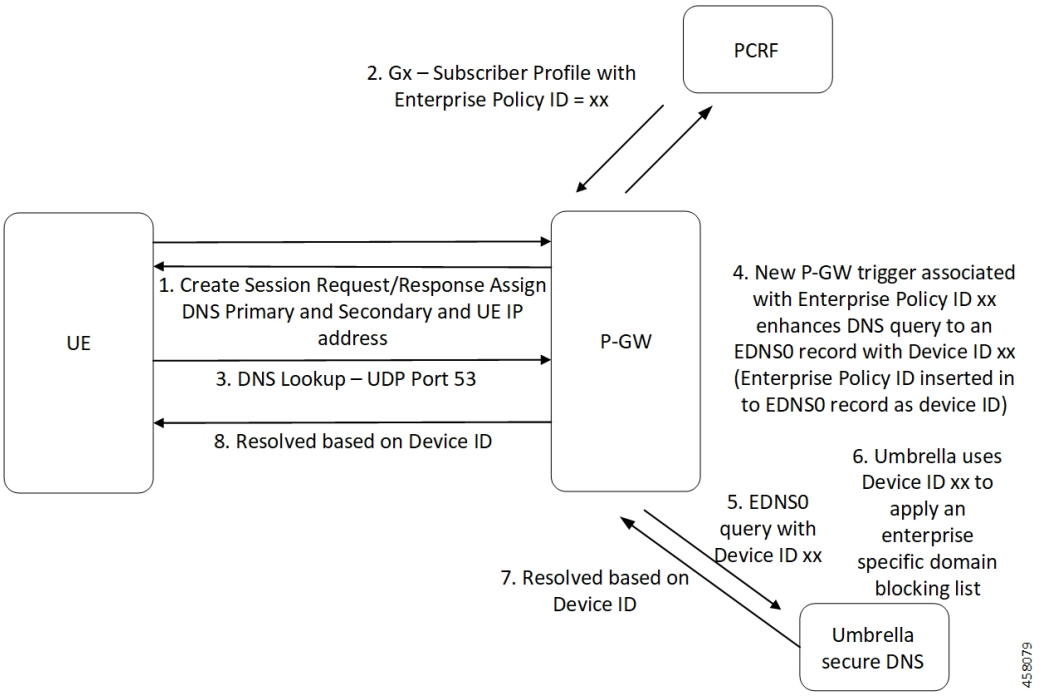
EDNS0 レコードのデバイス ID 番号により、Cisco Umbrella DNS システムは EDNS0 クエリにドメインフィルタのカスタムセットを適用できます。



プロセス フロー

次のプロセスフローは、EDNS0 レコードにデバイス ID を挿入するためのコンテンツフィルタリングの拡張機能を示しています。

図 *8 : EDNS* レコードへのデバイス *ID* の挿入



EDNS0 パケット形式

PCRF からのエンタープライズポリシー ID（CF_POLICY_ID）は、デバイス ID の作成に役立ちます。CP はデバイス ID を UP に送信します。DNS パケットにデバイス ID を追加すると、EDNS0 パケットの作成に役立ちます。EDNS0 パケットの形式は RFC2671 で指定されています。

次に、パケット形式の仕様を示します。

- 次に、OPT RR の固定部分の構造を示します。

```
Field Name   Field Type     Description
-------------------------------------------------
NAME         domain name    empty (root domain)
TYPE           u_int16_t          OPT
CLASS          u_int16_t          sender's UDP payload size
TTL            u_int32_t          extended RCODE and flags
RDLEN          u_int16_t          describes RDATA
RDATA          octet stream       {attribute, value} pairs
```

- 次に、RDATA でエンコードされた OPT RR の可変部分を示します。

```
      +0 (MSB)                            +1 (LSB)
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
  0: |                         OPTION-CODE                           |
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
  2: |                         OPTION-LENGTH                         |
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
  4: |                                                               |
    /                         OPTION-DATA                           /
```

```
/                                                               /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

- OPTION-CODE：IANA によって割り当て済み
- OPTION-LENGTH：OPTION-DATA のサイズ（オクテット単位）
- OPTION-DATA：OPTION-CODE によって異なる

例：

PCF または PCRF から受信したポリシー ID が「1234」で、UP で設定された静的プレフィックスが「5678」の場合、64 ビットのデバイス ID は「0000162e000004d2」になります。

- 0000162e：5678（10 進数）
- 000004d2：1234（10 進数）

RDATA 69 42 00 0f 4f 70 65 6e 44 4e 53 00 00 16 2e 00 00 04 d2

- 6942：option-code
- 000f：option-length
- 4f70656e444e53：OpenDNS（文字列）
- 0000162e：5678（MSB）
- 000004d2：1234（LSB）

IP 再アドレス指定を使用した EDNS0

トリガーアクション内で設定された CLI コマンドにより、DNS トラフィックは Umbrella DNS に再びアドレス指定されます。この CLI は、ACS サービスの既存の再アドレスサーバーリスト設定を使用します。パケットの宛先 IP アドレスに基づいてパケットを再アドレス指定することで、再アドレス指定されたサーバーリスト内の設定済みサーバーやポートにゲートウェイトラフィックをリダイレクトできます。

動作と制限事項

この機能の動作と制約事項は以下のとおりです。

- フロー作成時にトリガー条件を評価します。フロー間のトリガー条件の変更は、既存のフローには影響しませんが、新しいフローに影響します。
- トリガーアクションの変更は、同じフローに適用されます。
- CF ポリシーの ID 範囲は定義されているが、サービススキーマが定義されていない場合、または EDNS に関連するトリガー条件が設定されていない場合、CF も EDNS も適用されません。

- Gx から CF ポリシー ID を受信しない場合、範囲チェックは実行されず、コンテンツフィルタリングはルールベースで定義されているとおりに機能します。
- 「security-profile」CLI コマンドがトリガーアクションで EDNS 形式の CLI に関連付けられていない場合、EDNS 送信パケットのデバイス ID は 32 ビットの CF ポリシー ID でのみ送信されます。
- A、AAAA、CNAME、NS、PTR、SRV、TXT、NULL 以外のタイプの DNS クエリは、EDNS に変換することはできません。
- インフロー間の Gx に対する CF ポリシー ID の変更は、現在のフローには適用されません。現在のフローでは、フローの作成時に存在する CF ポリシー ID が引き続き挿入されます。

制限事項

この機能には、次の制限事項があります。

- EDNS 応答パケットの再フォーマットはサポートしていません。
- UP では、EDNS0 クエリに IMSI MSISDN タグ値を含めることができるようにする必要があります。この機能は、EDNS0 パケットの暗号化された IMSI と、次の設定の EDNS フィールドもサポートしていません。

```
configure
  active-charging-service service_name
    edns
      fields fields_name
        tag default device-id
        tag 101 imsi encrypt
        tag 102 pgw-address
        end
```

EDNS フォーマットとトリガーアクションの設定

DNS フィルタの設定

DNS フィルタリングを有効または無効にするには、次の設定を使用します。

```
configure
  active-charging-service service_name
    content-filtering range start_min_val to end_max_val
    no content-filtering range
    end
```

注：

- range パラメータが 10 ～ 1000 に設定されている場合、コンテンツ フィルタリング ポリシー ID が 10 ～ 1000 のサブスクライバプロファイルは、標準コンテンツフィルタリング

機能を使用します。コンテンツ フィルタリング ポリシー ID が 1000 より大きい、または 10 より小さいサブスクライバプロファイルは、EDNS0 機能をトリガーします。

- DNS フィルタリングが無効になっている場合、標準コンテンツ フィルタリング ポリシーは、設定または PCF からの受信内容に応じて再開されます。

EDNS パケットの設定

アクティブ課金サービスで EDNS パケットアクションおよびフォーマットを設定するには、次の設定を使用します。

```
configure
  active-charging-service service_name
    trigger-condition trigger_condition_name
      external-content-filtering
        app-proto = dns
        end
```

注：

- **external-content-filtering**：このフラグが「true」に設定され、範囲条件が指定されている場合に、EDNS0 機能を有効にします。デフォルトでは、このフラグは無効です。
- **app-proto = dns**：DNS 以外のトラフィックの IP アドレスの再指定を回避します。このコマンドが multiline-or CLI で有効になっている場合、すべての DNS トラフィックが EDNS でエンコードされます。

次の設定により、EDNS パケットに挿入される EDNS フォーマットを定義します。

```
configure
  active-charging-service service_name
    trigger-action trigger_action_name
      edns-format format_name
        security-profile profile_name
          flow action readdress server-list server_list_name [ hierarchy
 ] [ round-robin ] [ discard-on-failure ]
           end
```

注：

- **trigger-action** *trigger_action_name*：トリガーアクションで flow-action CLI を有効にします。
- **edns-format** *format_name*：EDNS が適用されている場合に EDNS フォーマットを使用します。
- **security-profile** *profile_name*：EDNS のセキュリティプロファイル設定を定義して、デバイス ID マッピングを追加します。

（注） この機能は、複数のセキュリティプロファイルをサポートします。

- **flow action readdress server-list** *server_list_name* **[hierarchy] [round-robin] [discard-on-failure]** : EDNS を IP アドレス再指定に関連付けます。IP アドレス再指定は、設定済みのサーバー IP 宛てにパケットのアドレスを再指定するために使用されます。トリガーアクションのこの CLI は、サーバーリスト設定のみをサポートします。単一サーバーの IP やポート設定（charging-action など）はサポートされません。

CF ポリシー ID の挿入

次の設定を使用して、EDNS に CF ポリシー ID を挿入します。

```
configure
  active-charging-service service_name
    edns
      fields fields_name
        tag { val { imsi | msisdn | cf-policy-id } }
        end
```

注：

- 32 ビットを設定するため、セキュリティプロファイルを含む静的な値が EDNS レベルで提供されます。

  security-profile *security_profile* **cf-policy-id-static-prefix** *value*

- 新しいタグを挿入するには、ペイロード長の値を 576 ～ 4096 までの整数で指定します。

  tag default payload-length [tcp | udp] *value*

設定例

以下に、EDNS パケットを設定するための設定例を示します。

```
configure
   active-charging service ACS
      content-filtering range 10 to 100

      ruledef dns-port
         udp either-port = 53
         tcp either-port = 53
         multi-line-or all-lines
         rule-application routing
      #exit

      readdress-server-list re_adr_list_ta
         server 100.100.100.14
         server 2001::14
         server 100.100.100.15
         server 2001::15
       #exit

      rulebase test
         route priority 20 ruledef dns-port analyzer dns
         #exit

      edns
         security-profile sec_profile cf-policy-id-static-prefix 123456
         fields test_fields
```

```
            tag 26946 cf-policy-id
          #exit

          format test_format
            fields test_fields encode
          #exit

          trigger-action TA1
            edns format test_format security-profile sec_profile
            flow action readdress server-list re_adr_list_ta hierarchy
           #exit

          trigger-condition TC1
            external-content-filtering
            app-proto = dns
            #exit

          service-scheme SS1
            trigger flow-create
               priority 1 trigger-condition TC1 trigger-action TA1
          #exit

          subs-class SC1
            rulebase = test
            multi-line-or all-lines
          #exit

          subscriber-base SB1
            priority 1 subs-class SC1 bind service-scheme SS1
          #exit
end
```

モニタリングおよびトラブルシューティング

以下に、EDNS0 レコードにデバイス ID を挿入するための拡張コンテンツフィルタリングをサポートする show コマンドとその出力を示します。

show コマンドと出力

この機能をサポートする、次の show コマンドと出力が変更されました。

show user-plane-service inline-services info

```
CF Range: Enabled
  Start Value:  1
  End Value:    1000
```

show user-plane-service statistics analyzer name dns

```
EDNS Over UDP:
EDNS Encode Success:            0         EDNS Encode Failed:      0
EDNS Encode Success Bytes:      0
EDNS Response Received:         0

EDNS Over TCP:
EDNS Encode Success:            0         EDNS Encode Failed:      0
```

```
EDNS Encode Success Bytes:      0
EDNS Response Received:         0
```

show subscribers user-plane-only full callid <call_id>

```
DNS-to-EDNS Uplink Pkts:     0       DNS-to-EDNS Uplink Bytes:     0
EDNS Response Received:      0
```

show user-plane-service edns all

```
Fields:
    Fields Name: fields_1
    tag 26946 cf-policy-id

    Fields Name: fields_2
    tag 2001 imsi
    tag 2002 msisdn
    tag 26946 cf-policy-id

    Format:
    Format Name: format_1
    fields fields_1 encode

    Format Name: format_2
    fields fields_2 encode

    Security-profile Name: high
    CF Prefix Policy ID: 1234
```

トリガーアクション統計

トリガーアクションの統計を表示するには、次の show コマンドを使用します。

- **show user-plane-service statistics trigger-action all**

```
Trigger-Action: TA1
  Total EDNS PKTS           :  1
  Total readdressed Flows   :  1
  Total Trigger action(s)   :  1
```

- **show user-plane-service statistics trigger-action name** *trigger_action_name*

```
Trigger-Action: TA1
  Total EDNS PKTS           :  1
  Total readdressed Flows   :  1
  Total Trigger action(s)   :  1
```

- **show user-plane-service trigger-condition all**

```
Trigger-Condition: TC1
       External-content-filtering : Enabled
       App-proto : dns
       Multi-line-OR All lines : Disabled
```

- **show user-plane-service trigger-action all**

```
Trigger-Action: TA1
       HTTP Response Based TRM      : none
       HTTP Response Based Charging : none
       Throttle Suppress            : Disabled
       Flow Recovery                : Disabled
       Traffic Optimization         : Disabled
       Step Up GBR                  : Disabled
       Step Down GBR                : Disabled
```

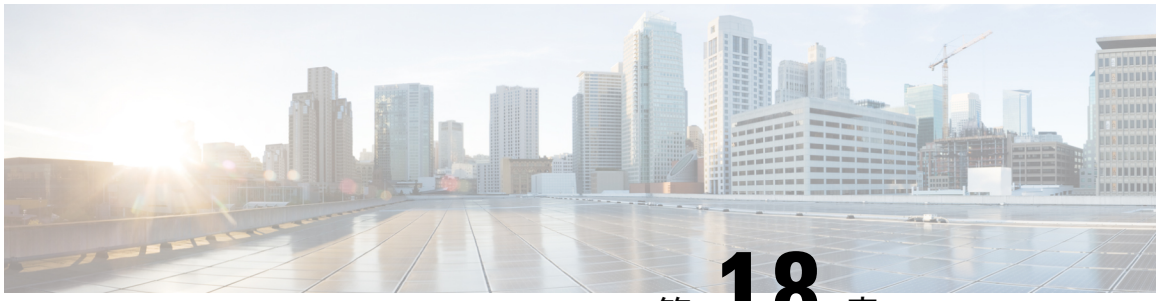
```
TCP Acceleration             : Disabled
TCP Acceleration Threshold   : Disabled
Service-Chain                : none
UP-Service-Chain             : none
EDNS-Encode                  : Enabled
Flow-IP-Readdressing         : Enabled
```

バルク統計情報

この機能では、ECS スキーマで次のバルク統計がサポートされます。

表 *7: ECS* スキーマ

統計	説明
ecs-dns-udp-edns-encode-succeed	UDP を介して DNS から EDNS に変換されたパケットの数。
ecs-dns-udp-edns-encode-failed	UDP を介した DNS から EDNS への変換に失敗した回数。
ecs-dns-udp-edns-encode-response	UDP を介した EDNS クエリに対して受信された応答の数。
ecs-dns-tcp-edns-encode-succeed	TCP を介して DNS から EDNS に変換されたパケットの数。
ecs-dns-tcp-edns-encode-failed	TCP を介した DNS から EDNS への変換に失敗した回数。
ecs-dns-tcp-edns-encode-response	TCP を介した EDNS クエリに対して受信された応答の数。



第 18 章

DI-Net 暗号化

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.27.4

機能説明

VPC-DI システムは、Advanced Encryption Standard 暗号ブロック連鎖（AES CBC）アルゴリズムを使用して、異なるカード間を流れるトラフィックを暗号化します。ただし、CBC アルゴリズムには 1 つデメリットがあります。認証されていない暗号化モードを使用するため、攻撃者によってどこかの時点で暗号化トラフィックが改ざんされる可能性があるからです。この問題を回避するため、より優れた保護を提供し、データの完全性を促進する認証付き暗号化アルゴリズムが使用されます。

ガロア/カウンタモード（GCM）暗号化アルゴリズムは、この脆弱性の克服に有効な認証付き暗号化モードをサポートしています。また、復号側では、GCM は追加認証データ（AAD）を使用してペイロードを認証します。

機能の仕組み

GCM 暗号化アルゴリズムは認証されるため、DI-Net トラフィック暗号化プロセスで使用されます。これは非常に安全で、特定のキー値に対して同じ初期化ベクトル（IV）が繰り返されることはありません。*param.cfg* ファイルは、暗号化アルゴリズムの設定に使用されます。

暗号ブロック連鎖（CBC）アルゴリズムと GCM アルゴリズムではどちらも、異なる内部機能を備えたブロック暗号と排他的論理和（XOR）ロジックが使用されます。

CBC暗号化プロセスは、暗号テキストと呼ばれる以前に暗号化されたブロックとプレーンテキストと呼ばれる暗号化されていないブロックの XOR 演算、および結果のブロックのブロック暗号による暗号化から成ります。ブロック暗号を使用し、結果のブロックを前の暗号テキストブロックと XOR 演算することで、暗号化されたデータまたは暗号テキストを復号すると、プレーンテキストデータが生成されます。

（注） 最初のブロックは、前のブロックに属さず、前のブロックデータの代わりに IV を使用するため、特殊なケースとして扱われます。

GCM アルゴリズムは、カウンタモードの暗号化と認証（CTR + Auth）の組み合わせです。このアルゴリズムは、ガロア体乗算とブロック暗号のカウンタモードの動作を組み合わせ、ブロック暗号からストリーム暗号への変換を支援します。各ブロックは、キーストリームの疑似ランダム値で暗号化されます。IV 値が連続的に増加するため、各ブロックは重複しない一意の値で暗号化されます。

ガロア体乗算コンポーネントは、各ブロックを Advanced Encryption Standard（AES）標準に基づく暗号化の独自の有限体と見なします。AES GCM には、ハンドシェイク認証と追加のデータ認証が組み込まれています。また、GCM 暗号化や復号プロセスはいつでも並列化でき、組み込みの認証により、ペイロードの改ざんやパドルオラクル攻撃に対する耐性があり、CBC アルゴリズムよりも優先されます。

AES-CBC-256

マスター制御機能（CF）カードでは、**openssl** を使用して暗号化されたパスワードが生成されます。CF カード単独で、起動プロセス中にすべてのカードが使用するパスワードとシークレットコードが作成されます。すべてのパスワードには、キーと IV の生成プロセス中にスロット番号が付加されます。任意のカードで他のカードのキーと IV を生成できます。ダイナミック IV テーブルを作成する場合も、同じプロセスに従います。キーの長さはそれぞれ 256 ビットで、IV の長さは 128 ビットです。

暗号化プロセス中、送信元カードでは独自のキーが使用されますが、IV はランダムに生成されます。送信元カードの対応する IV は、IP ヘッダーの送信元アドレスと宛先アドレス、および乱数を含むハッシュ関数の出力に基づいて選択された動的 IV テーブルからの IV と XOR 演算されます。この乱数は、暗号ヘッダーに含まれます。

復号プロセス中に、接続先カードで送信元カードのスロット番号を使用して、ヘッダーからの宛先アドレスと乱数に加えて、キーと送信元アドレスが選択されてから、IVが選択されます。

AES-GCM-256

暗号化アルゴリズムを **aes-gcm-256** に変更するには、暗号化アルゴリズムの追加入力として、追加認証データ（AAD）が暗号化関数に必要です。送信元と宛先の間で転送されるものであれば、キーとIVのペアが再利用されないようにすることができます。GCMセキュリティは、この機能に準拠している必要があります。万が一、キーを持つ認証済みの暗号化関数のいずれかまたはすべてのインスタンスに対してIVが繰り返されると、実装全体が偽造攻撃に対して脆弱になります。

GCMでパケットを暗号化する際、送信元カードはCBCアルゴリズムに似たキーを選択しますが、IVは、選択されたIVが特定のキーに対して一意であり、これまでに使用されたことがないことを保証するメカニズムに基づいて選択されます。AADは暗号ヘッダーに含まれ、暗号化が完了すると、ペイロードとともに送信される前に、暗号化されたデータに認証タグ「T」が追加されます。

復号プロセス中に、GCM、キー、およびIVを使用するパケットは、暗号化プロセスと同様のメカニズムを使用して選択され、認証タグは暗号化されたデータから削除されます。AAD、キー、およびIVはすべて、ペイロードの復号に使用されます。復号後に生成された認証タグが送信元から受信した認証タグと一致する場合、データの完全性が保証され、復号プロセスは成功します。

暗号化方式（iftask_aes_gcm_encrypt）

新しい暗号化方式は次のとおりです。

- 送信元カードのスロット番号を確認します。
- 保存されている値から、このスロットのキーとIVを選択します。
- 乱数を生成します。
- 送信元IPアドレス、宛先IPアドレス、乱数を使用して、ダイナミックIVテーブルからの選択用に *hash_index* を生成します。
- 送信元カードのIVとダイナミックIVテーブルのIVのXOR演算を行い、次にそれを乱数とOR演算することで、最終的なIVを生成します。これにより、最終的なIVがキーに対して一意になるため、同じキーであるIVペアが再利用されることはありません。

（注） ダイナミックIVテーブルのサイズは64で、乱数は *uint16_t* です。

- 追加の認証データとしてIPフラグメントオフセット値を選択します。
- 選択または生成されたキー、IV、およびAADを使用して暗号化します。

- 生成された乱数を暗号ヘッダーに入力します。

復号方式（iftask_aes_gcm_decrypt）

新しい復号方式は次のとおりです。

- 送信元カードのスロット番号を確認します。
- 保存されている値から、送信元スロットのキーと IV を選択します。
- 暗号ヘッダーから乱数を取得します。
- 送信元 IP アドレス、宛先 IP アドレス、および乱数を使用して、ダイナミック IV テーブルから選択する *hash_index* を作成します。
- 送信元カードの IV とダイナミック IV テーブルの IV の XOR 演算を行い、乱数と OR 演算することで、最終的な IV を生成します。
- 追加の認証データとして IP フラグメントオフセット値を選択します。
- AAD を使用して、受信したペイロードを認証します。
- 選択または生成されたキー、IV、および AAD を使用して暗号化を続行します。

制限事項

この機能の既知の制限事項と制約事項は次のとおりです。

- この機能は、すべての VPC-DI システムではなく、CUPS-DI システムのみに限定されます。
- 暗号化アルゴリズムを変更するには、リロードする必要があります。アルゴリズムは、リロードする前に、*/boot1/param.cfg* ファイルを手動で変更するか、アルゴリズム変更のための新しい CLI を使用して変更できます。その後リロードを開始します。
- 暗号化アルゴリズムはカードの起動プロセスの前に設定する必要があるため、リロード前に変更を行わずに起動設定に優先アルゴリズム含めてリロードするだけでは、アルゴリズムは変更されません。
- 小さいパケットに対する **aes-gcm-256** のコンピューティング オーバーヘッドにより、認証アルゴリズムによるパフォーマンスへの影響を評価する必要があります。

暗号化アルゴリズムの設定

暗号化アルゴリズムは、カードの起動プロセス中に、起動パラメータファイルを使用して設定されます。新しい起動フラグ値 *DI_NET_ENC_ALG* は、設定時に、起動オプションとして */boot1/param.cfg* ファイルで使用できます。

このフラグは、次の CLI を使用するか、/boot1/param.cfg ファイルを手動で編集して設定できます。手動で設定する場合は、アクティブとスタンバイのすべての CF および SF カードで同じ値に設定する必要があります。デフォルトでは、「0」は CBC で、「1」は GCM です。

（注） 変更を有効にするには、暗号化アルゴリズムを変更するたびに CP をリロードする必要があります。

CUPS で暗号化アルゴリズムを設定するには、次の設定を使用します。

```
configure
   iftask di-net-encrypt-alg di_net_encrypt_alg
end
```

注：

- **di-net-encrypt-alg**：Di-LAN トラフィックの暗号化アルゴリズムを設定します。これは、暗号化アルゴリズム名を表します。

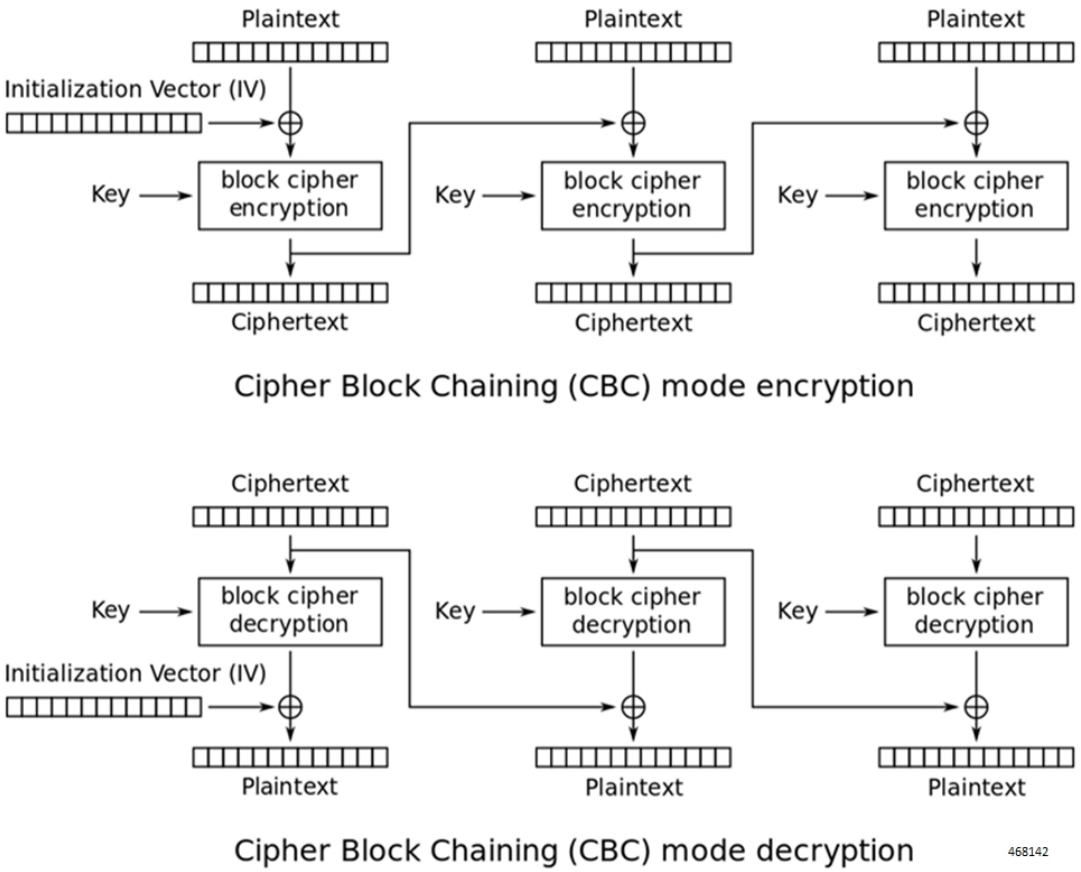
付録

暗号ブロック連鎖

暗号化中にプレーンテキストブロックと暗号テキストブロックと組み合わせる場合、機密モードでは CBC と呼ばれます。CBC には予測不能な IV が必要ですが、最初のプレーンテキストブロックと組み合わせるために、常にシークレットである必要はありません。

各プレーンテキストブロックは、前の暗号テキストブロックと XOR 演算されます。各暗号テキストブロックは、任意の時点における暗号化前のプレーンテキストブロックによって決まります。一意のテキストブロックにするためには、各メッセージ IV を最初のブロックで使用する必要があります。

図 *9:* 暗号ブロック連鎖メソッド



ガロア/カウンタモード

GCM は、暗号化のカウンタモードと新しいガロア認証モードを組み合わせたものです。主な特徴として、認証に使用されるガロア体乗算を簡単に並列化できます。

GCM を構成する 2 つの関数は、認証付き暗号化および復号と呼ばれます。認証付き暗号化関数は、機密データを暗号化し、機密データとそれ以外の非機密データの両方で認証タグを計算します。認証付き復号関数は、タグの検証を条件として、機密データを復号します。

ブロック暗号とキーが選択され承認されると、暗号化関数は次の 3 つの入力文字列を受け付けます。

- 「P」で表されるプレーンテキスト
- 追加認証付きデータ（AAD）
- 初期化ベクトル（IV）

GCM は、プレーンテキストと AAD の 2 種類のデータを、その真正性を確保することで保護します。また、AAD の透過性を維持しながら、プレーンテキストの機密性を保護します。IV は、保護する入力データに対する認証付き暗号化関数を呼び出す一意の値です。

暗号化アルゴリズムの入力文字列のビット長は、次の制限内である必要があります。

- P の長さ 239 ～ 256 以下
- A の長さ 264-1 以下
- IV の長さ 1 以上 264-1 以下

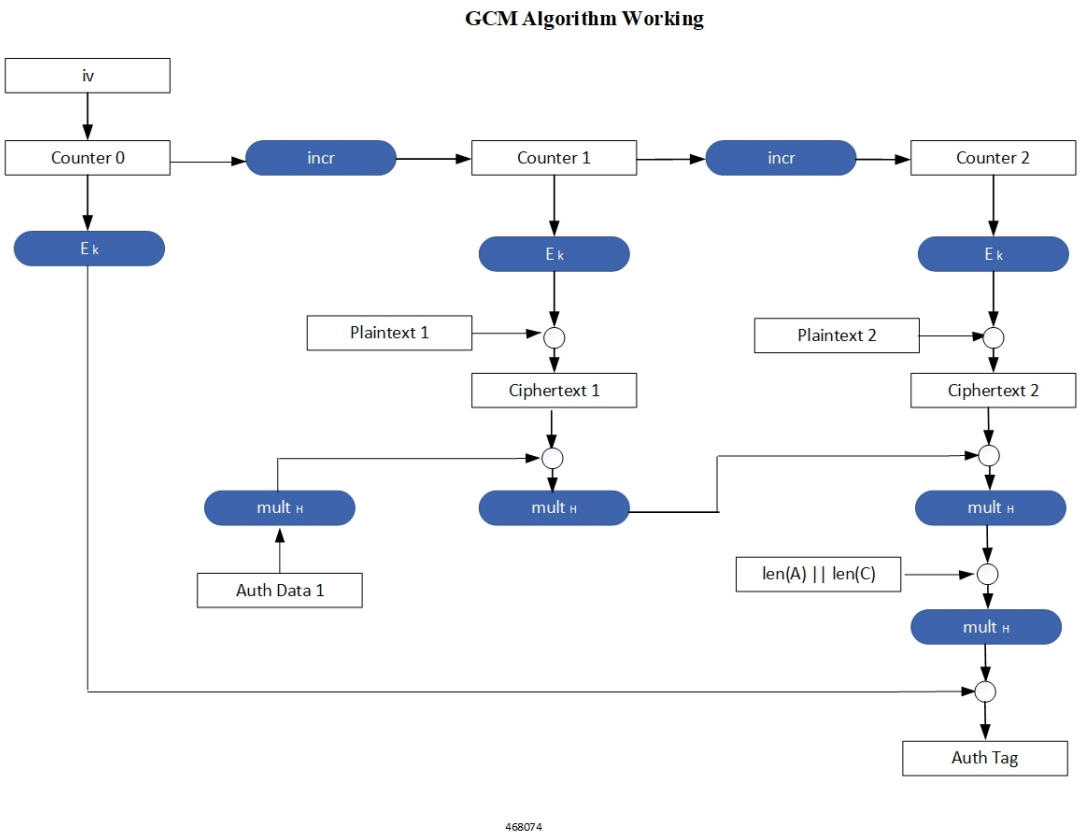
認証付き暗号化関数の入力は、IV、AAD、秘密鍵、およびプレーンテキストであり、出力は、認証タグ「T」を含むプレーンテキストと同じビット長の暗号テキストです。

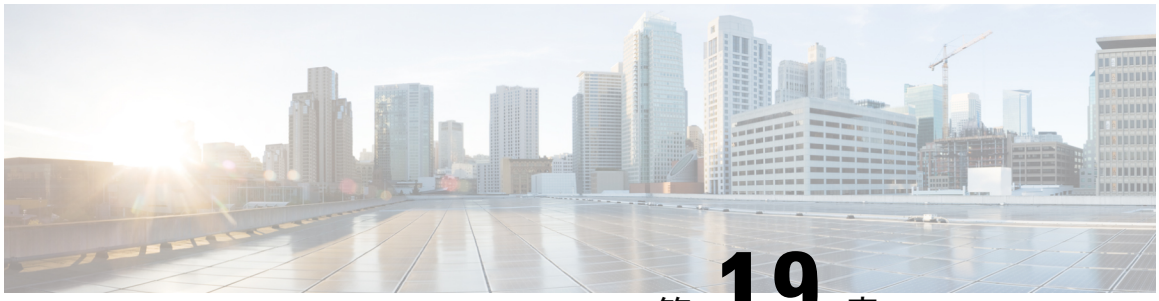
ブロック暗号、鍵、および関連するタグ長を承認し選択した後、IV、追加認証付きデータ「A」、暗号テキスト「C」、および認証タグ「T」が認証付き復号関数への入力として供給されます。復号プロセスにより、次のような出力が生成されます。

- 暗号テキスト「C」に対応するプレーンテキスト「P」
- 特殊なエラーコード

（注） 出力「P」は、IV、「A」、および「C」の認証タグ「T」が成功したかどうかを示します。成功していない場合は、復号プロセスは失敗と見なされます。

図 *10 :* ガロア/カウンタモードメソッド





第 19 章

RADIUS アカウンティングの無効化

マニュアルの変更履歴

Note リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアントまたはサーバーシステムです。シスコの実装では、RADIUS クライアントはシスコデバイス上で実行され、すべてのユーザー認証およびネットワーク サービス アクセス情報を持つ中央の RADIUS サーバーに認証要求を送信します。

CUPS では、RADIUS サーバー専用ベアラーの RADIUS アカウンティングの無効化がサポートされます。

CUPS は、次の機能をサポートしています。

- すべてのベアラーの RADIUS アカウンティングの有効化
- QCI および ARP 値に基づいて特定の専用ベアラーの RADIUS アカウンティングを無効にする
- すべての専用ベアラーの RADIUS アカウンティングを無効にし、デフォルトベアラーのみ RADIUS アカウンティングを有効にする

- RADIUS アカウンティングが無効になっているベアラーの URR は作成されません。
- CLI 設定の変更は、設定変更後に発生した新しいコールにのみ適用され、既存のコールには影響しません。
- 特定のベアラーの RADIUS アカウンティングが無効化または有効化された場合、これは無効化/有効化後に作成されたベアラーに適用され、既存のベアラーには適用されません。

注：この機能は、非 CUPS アーキテクチャで RADIUS を使用する製品でも使用できます。

専用ベアラー機能での RADIUS アカウンティングの設定

ここでは、次の場合の CLI 設定について説明します。

- すべてのベアラーの RADIUS アカウンティングの有効化
- QCI および ARP 値に基づいて特定の専用ベアラーの RADIUS アカウンティングを無効にする
- すべての専用ベアラーの RADIUS アカウンティングを無効にし、デフォルトベアラーのみ RADIUS アカウンティングを有効にする

すべてのベアラーの RADIUS アカウンティングの有効化

すべてのベアラーで RADIUS アカウンティングを有効にするには、次の CLI 設定を使用します。

```
configure
   context context_name
      aaa group group_name
         radius accounting mode all-bearers
         end
```

注：

- **radius accounting mode all-bearers** CLI コマンドは、デフォルトで有効になっています。

特定のベアラーの RADIUS アカウンティングの無効化

QCI 値と ARP 値に基づいて特定の専用ベアラーの RADIUS アカウンティングを無効にするには、次の CLI 設定を使用します。

```
configure
   context context_name
      aaa group group_name
        radius accounting disable-bearer qci qci_value arp-priority-level
```

```
arp_value
        end
```

注：

- **radius accounting disable-bearer qci** *qci_value* **arp-priority-level** *arp_value* CLI コマンドは、指定された QCI 値と ARP 値を持つ専用ベアラーに対してのみ RADIUS アカウンティングを無効にします。他の専用ベアラーのアカウンティングは影響を受けません。
- 専用ベアラーで RADIUS アカウンティングを無効にできる QCI と ARP の組み合わせ設定の最大数は 16 です。16 を超える組み合わせを設定しようとすると、次のエラーメッセージが表示されます。

```
Failure: Error!!! Maximum 16 qci and arp combinations allowed.
```

デフォルトベアラーのみの RADIUS アカウンティングの有効化

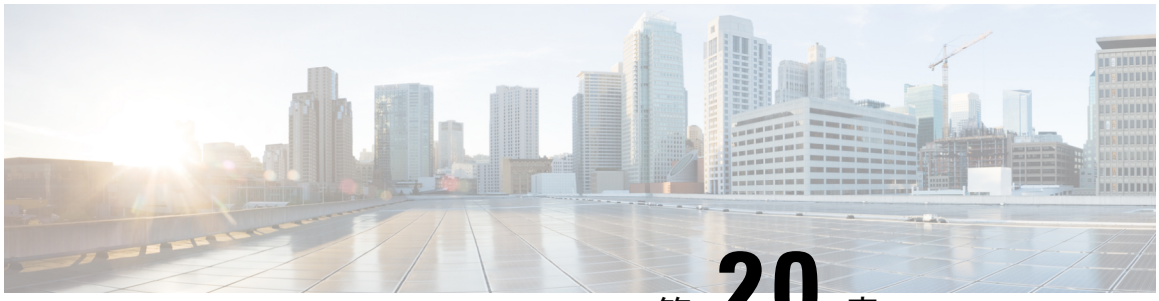
デフォルトベアラーのみを対象に RADIUS アカウンティングを有効にし、すべての専用ベアラーで RADIUS アカウンティングを無効にするには、次の CLI 設定を使用します。

```
configure
   context context_name
      aaa group group_name
         radius accounting mode default-bearer-only
         end
```

注：

- **radius accounting mode default-bearer-only** CLI コマンドは、デフォルトベアラーのみを対象に RADIUS アカウンティングを有効にし、すべての専用ベアラーで RADIUS アカウンティングを無効にします。
- 特定の専用ベアラーの **radius accounting disable-bearer qci** *qci_value* **arp-priority-level** *arp_value* 設定を削除し、その専用ベアラーで RADIUS アカウンティングを許可するには、**no radius accounting disable-bearer qci** *qci_value* **arp-priority-level** *arp_value* CLI コマンドを使用します。
- RADIUS アカウンティングモードが [default-bearer-only] に設定されている場合、専用ベアラーで RADIUS アカウンティングを無効にすることはできません。**radius accounting disable-bearer qci** *qci_value* **arp-priority-level** *arp_value* CLI コマンドを実行すると、次のエラーメッセージが表示されます。

```
Failure: Error!!! Radius accounting mode is set to default-bearer-only. Change the
mode to all-bearers and run this CLI again
```



第 20 章

Collapse コールの DSCP マーキング

機能の概要と変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

現在、QCI ベースの DSCP マーキングは Pure-S および Pure-P コールに適用されます。DSCP マーキングは、それぞれの S-GW サービスまたは P-GW サービスに関連付けられた QCI-QOS マッピングに基づいています。Collapse コールの場合、PGW サービスに関連付けられた QCI-QOS マッピングが適用されます。この機能は、アップリンクおよびダウンリンクトラフィックに関連付けられた S-GW および P-GW サービスに基づいて、Collapse コールに DSCP マーキングを適用するのに役立ちます。アップリンクトラフィックには、論理 P-GW サービスに関連付けられた DSCP マーキングが適用されます。ダウンリンクトラフィックには、論理 S-GW サービスに関連付けられた DSCP マーキングが適用されます。DSCP マーキングは、GTPU ヘッダーおよび内部 IP の一部としてデータトラフィックの IP ヘッダーに存在します。CLI 設定でこの機能を有効または無効にするオプションがあります。この機能を有効にすると、新しい機能のみ

が適用され、有効にしない場合は既存の機能も動作します。デフォルトでは、この機能は無効になっているため、この機能にアップグレードしてもユーザーに影響はありません。

機能の仕組み

以下に、Collapse コールの DSCP マーキングに関する手順を示します。

- Collapse コールの場合：
  - アクセス側では、SGW サービスに関連付けられている QCI-QOS マッピングテーブルが使用されます。
  - コア側では、PGW サービスに関連付けられた QCI-QOS マッピングテーブルが使用されます。
- これは、機能を有効にすると適用されます。機能を有効にしていない場合は、アクセス側およびコア側ともに PGW サービスに関連付けられた QCI-QOS マッピングテーブルが使用されます。
- APN に関連付けられた QCI-QOS マッピングテーブルは、P-GW サービス QCI-QOS マッピングテーブルよりも優先されます。
- APN プロファイルに関連付けられた QCI-QOS マッピングテーブルは、アクセス側の DSCP マーキングでは、SGW サービス QCI-QOS マッピングテーブルよりも優先されます。
- P-GW サービスのみに QCI-QOS マッピングテーブル設定がある場合、これらの DSCP マーキングは Collapse コールのアクセス側とコア側の両方に適用されます。
- S-GW サービスのみに QCI-QOS マッピングテーブル設定がある場合、これらの DSCP マーキングは Collapse コールのアクセス側に適用されます。
- SAE-GW サービス内に、この機能が有効か無効かを示す新しい設定可能なパラメータがあります。
- Pure-P から Collapse およびその逆の HO の場合、トランスポート層マーキングは Sx 変更要求の一部として FAR で更新されます。
- レイヤ 2 マーキングも、アクセス側およびコア側で選択された QCI-QOS マッピングテーブルに基づいて変更されます。
- DSCP マーキングは、セッション回復後に既存のベアラーに引き続き適用されます。
- DSCP マーキングは、スタンバイシャーシがアクティブモードに切り替わると、そのシャーシのベアラーで継続されます。

設定

この機能を有効または無効にするには、SAE-GW サービス内で次のコマンドを設定します。

```
configure
          context egress
             saegw_service saegw_service
             downlink-dscp-per-call-type enabled/disabled
             end
```

（注） 機能を有効にすると、コールタイプがCollapsedの場合、ダウンリンクにはS-GWサービスQCI-QoSマッピングDSCPマーキングが使用されます。デフォルトでは、downlink-DSCP-per-call-typeは [Disabled] です。

モニタリングおよびトラブルシューティング

ここでは、Collapse コールの DSCP マーキングのモニタリングと障害対応に使用できる CLI コマンドについて説明します。

show コマンドの出力

ここでは、Collapse コールの DSCP マーキングをサポートするために使用できる show CLI コマンドについて説明します。

show saegw-service all

この show コマンドにより、この機能が有効か無効かを確認できます。

```
Service name : SAEGW11
Service-Id : 47
Context : EPC1
Status : STARTED
sgw-service : SGW11
pgw-service : PGW11
sx-service : SX11C
User Plane Tunnel GTPU Service : SAEGW11SXU
Newcall policy : n/a
downlink-dscp-per-call-type : enabled
CUPS Enabled : Yes
Service name : SAEGW21
Service-Id : 25
Context : EPC2
Status : STARTED
sgw-service : SGW21
pgw-service : PGW21
sx-service : SX21C
User Plane Tunnel GTPU Service : SAEGW21SXU
Newcall policy : n/a
downlink-dscp-per-call-type : disabled
CUPS Enabled : Yes
```

show sub user-plane-only callid <call_id> far full all

このユーザープレーン CLI を使用して、アップリンク/ダウンリンク FAR のトランスポートレベルのマーキングオプションと内部パケットマーキングを検証します。

SMGR CP の変更

アップリンク/コアおよびダウンリンク/アクセスの DSCP マーキングは、sessmgr_sub_session_t → sessmgr_qci_tab_t 内にベアラーレベルで存在します。

ユーザーデータグラムの DSCP マーキングは、内部パケットの IP ヘッダーで更新されます。つまり、UE からインターネットに、またはその逆に送信されるパケットです。

カプセル化ヘッダーの DSCP マーキングは、GTPU ヘッダー（外部ヘッダー）を持つ外部 IP レイヤの IP ヘッダーで更新されます。

DSCP マーキングは、次のように FAR IE 内で CP から UP に送信されます。

- トランスポート レベル マーキング：DSCP マーキングは、アクセス側のカプセル化ヘッダーと、コア側の Collapse コールのユーザーデータグラムで設定されます。
- トランスポート レベル マーキング オプション：2 つのオプションがあり、外部ヘッダーにのみ適用されます。
  - Copy-inner：内部パケットのマーキングを外部ヘッダーにコピーします。
  - Copy-outer：外部ヘッダーの DSCP マーキングをリレーします。

内部パケットマーキング：DSCP マーキングは、アクセス側のユーザーデータグラムで設定されます。コア側の場合、Collapse コールには適用されません。

Collapse コールを対象に、変更された DSCP マーキングを取得するロジック：

- アクセス/ダウンリンク側では、関連付けられた SGW サービスから、セッションの qci および qrp_pl に基づいて DSCP マーキングを取得します。
- コア/アップリンク側では、関連付けられた PGW サービスから、セッションの qci および qrp_pl に基づいて DSCP マーキングを取得します。
- アクセス/ダウンリンク側では、APN プロファイルに関連付けられた qci-qos マッピングテーブルが SGW-Service qci-qos-mapping テーブルよりも優先されます。
- コア/アップリンク側では、APN 設定に関連付けられた qci-qos マッピングテーブルが PGW-Service qci-qos-mapping テーブルよりも優先されます。
- SGW-service qci-qos マッピングテーブルが設定されていない場合、PGW-service qci-qos-mapping テーブルがアクセス側とコア側の両方に適用されます。
- PGW-service qci-qos マッピングテーブルが設定されていない場合、SGW-service qci-qos mapping table がアクセス側に適用され、コア側には DSCP マーキングは適用されません。

- DSCP マーキングは、CP から UP への SX 確立/変更要求の一部として送信される Create/Update FAR によって UP で更新されます。
- Pure-P から Collapse への HO の場合、またはその逆の場合に、Update FAR IE の一部として Sx 変更要求で TLM、IPM、および TLMO を更新します。
- Pure-P から Collapse への HO の場合、またはその逆の場合に、Update FAR IE の一部として Sx 変更要求でレイヤ 2 マーキングを更新します。

次の表に、Collapse コールのアクセス側およびコア側に適用される DSCP マーキングのさまざまな設定の組み合わせと結果を示します。

S. No.	機能の有効/無効	PGW サービス QOS-QCI テーブルの設定（Q1）	SGW サービス QOS-QCI テーブルの設定（Q2）	APN QOS-QCI テーブルの設定（Q3）	APN-Profile QOS-QCI テーブルの設定（Q4）	Collapse コールのアクセス/ダウンリンク DSCP マーキング	Collapse コールのコア/アップリンク DSCP マーキング
1	有効	対応	対応	対応	対応	Q4（APN プロファイル）	Q3（APN）
2	有効	対応	対応	対応	非対応	Q2（SGW サービス）	Q3（APN）
3	有効	対応	対応	非対応	対応	Q4（APN プロファイル）	Q1（PGW サービス）
4	有効	対応	対応	非対応	非対応	Q2（SGW サービス）	Q1（PGW サービス）
5	有効	対応	非対応	対応	対応	Q4（APN プロファイル）	Q3（APN）
6	有効	対応	非対応	対応	非対応	Q3（APN）	Q3（APN）
7	有効	対応	非対応	非対応	対応	Q4（APN プロファイル）	Q1（PGW サービス）
8	有効	対応	非対応	非対応	非対応	Q1（PGW サービス）	Q1（PGW サービス）
9	有効	非対応	対応	対応	対応	Q4（APN プロファイル）	Q3（APN）
10	有効	非対応	対応	対応	非対応	Q2（SGW サービス）	Q3（APN）
11	有効	非対応	対応	非対応	対応	Q4（APN プロファイル）	N/A（DSCP なし）
12	有効	非対応	対応	非対応	非対応	Q2（SGW サービス）	N/A（DSCP なし）

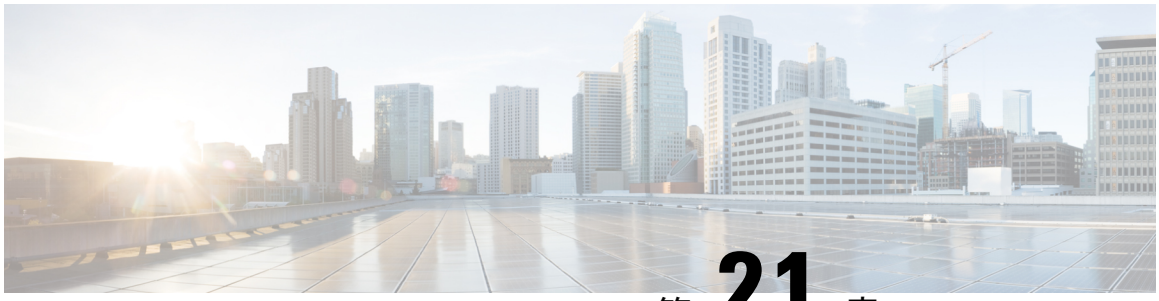
S. No.	機能の有効/無効	PGW サービス QOS-QCI テーブルの設定（Q1）	SGW サービス QOS-QCI テーブルの設定（Q2）	APN QOS-QCI テーブルの設定（Q3）	APN-Profile QOS-QCI テーブルの設定（Q4）	Collapse コールのアクセス/ダウンリンク DSCP マーキング	Collapse コールのコア/アップリンク DSCP マーキング
13	有効	非対応	非対応	対応	対応	Q4（APN プロファイル）	Q3（APN）
14	有効	非対応	非対応	対応	非対応	Q3（APN）	Q3（APN）
15	有効	非対応	非対応	非対応	対応	Q4（APN プロファイル）	N/A（DSCP なし）
16	有効	非対応	非対応	非対応	非対応	N/A（DSCP なし）	N/A（DSCP なし）
17	無効	対応	対応	対応	対応	Q3（APN）	Q3（APN）
18	無効	対応	対応	対応	非対応	Q3（APN）	Q3（APN）
19	無効	対応	対応	非対応	対応	Q1（PGW サービス）	Q1（PGW サービス）
20	無効	対応	対応	非対応	非対応	Q1（PGW サービス）	Q1（PGW サービス）
21	無効	対応	非対応	対応	対応	Q3（APN）	Q3（APN）
22	無効	対応	非対応	対応	非対応	Q3（APN）	Q3（APN）
23	無効	対応	非対応	非対応	対応	Q1（PGW サービス）	Q1（PGW サービス）
24	無効	対応	非対応	非対応	非対応	Q1（PGW サービス）	Q1（PGW サービス）
25	無効	非対応	対応	対応	対応	Q3（APN）	Q3（APN）
26	無効	非対応	対応	対応	非対応	Q3（APN）	Q3（APN）
27	無効	非対応	対応	非対応	対応	N/A（DSCP なし）	N/A（DSCP なし）
28	無効	非対応	対応	非対応	非対応	N/A（DSCP なし）	N/A（DSCP なし）
29	無効	非対応	非対応	対応	対応	Q3（APN）	Q3（APN）
30	無効	非対応	非対応	対応	非対応	Q3（APN）	Q3（APN）
31	無効	非対応	非対応	非対応	非対応	N/A（DSCP なし）	N/A（DSCP なし）

S. No.	機能の有効/無効	PGW サービス QOS-QCI テーブルの設定（Q1）	SGW サービス QOS-QCI テーブルの設定（Q2）	APN QOS-QCI テーブルの設定（Q3）	APN-Profile QOS-QCI テーブルの設定（Q4）	Collapse コールのアクセス/ダウンリンク DSCP マーキング	Collapse コールのコア/アップリンク DSCP マーキング
32	無効	非対応	非対応	非対応	非対応	N/A（DSCP なし）	N/A（DSCP なし）

統計

U/L および D/L の TOS マーク付きパケット数を表示するには、次のユーザープレーン CLI を使用します。

show sub user-plane-only full all



第 21 章

ダイナミックおよび ADC 課金ルール名

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

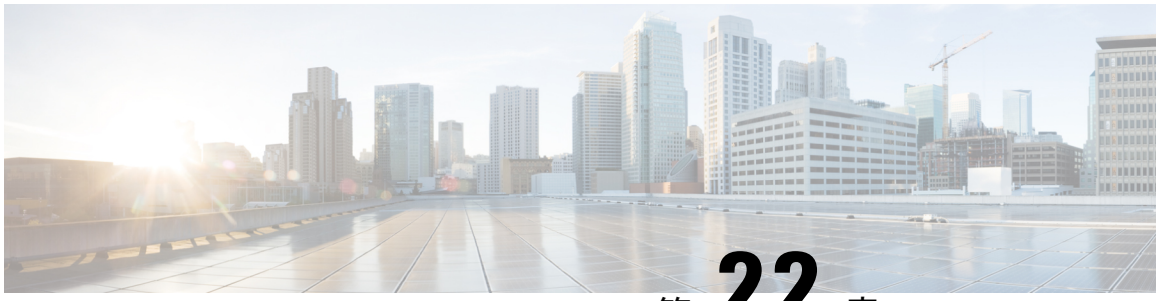
機能説明

この機能により、オペレータは Mobility Services Platform（MSP）機能の使用例をサポートできます。

この機能は、次の要件に対応します。

- 64 個のルールのサポート：
  - フローの説明を含むデフォルトベアラーの動的ルール。
  - フローの説明がある場合とない場合の ADC ルール。
- 最大 174 の PDR とそれぞれに対応する FAR、URR、および QER が静的ルール、事前定義されたルール、動的ルール、および ADC ルールでサポートされます。
  - 静的ルール、事前定義されたルール、動的ルール、および ADC ルールでは、最大 206 の URR がサポートされます。

- すべてのルール情報は、Create PDR、Create URR、Create FAR、および Create QER を使用してユーザープレーンに伝達されます。
- すべての Sx メッセージでは、必要な数の PDR、URR、FAR、QER、使用状況レポート、および Query URR がサポートされます。
- モニタープロトコルは、すべての Sx メッセージを表示します。
- モニターサブスクライバは、すべての Sx メッセージを表示します。



第 22 章

ダイナミック APN および IP プールのサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

ダイナミック APN および IP プールのサポート機能により、次の機能が有効になります。

- 以前は IP プールが設定されていなかった APN への IP プールの追加。
- APN 内にある既存 IP プールの設定の変更または削除、および別の設定の追加。
- APN 内にある既存 IP プールの設定の削除。

この機能は、APN IP プールとグループの動的設定の変更をサポートし、Sx の再関連付けなしでチャンクをユーザープレーン（UP）に割り当てます。

機能の仕組み

この項では、ダイナミック APN および IP プールのサポート機能の仕組みについて簡単に説明します。

Demux は、動的に追加された APN および IP プールの設定を VPN Manager に伝達します。この情報により、Sx リンクが切断されることなくリソースが割り当てられます。コントロールプレーン（CP）は、Sx 関連付け更新メッセージを介して設定をユーザープレーンにプッシュします。

APN IP プール追加要求を動的にトリガーする

新規または既存の APN に関連付けられた APN および IP プールを動的に追加できます。ランタイム時に、新しい APN と IP プールが設定に追加されます。設定の更新は、CP と UP 間の Sx 関連付けを中断することなく実行されます。

ダイナミック APN および IP プールのサポート機能は、次の機能もサポートしています。

- 既存の APN への新しい IP プールまたは UP グループの追加
- 既存の UP グループへの新しい APN の追加

この機能は、次のシナリオをサポートしています。

APN での操作	IP プールやグループでの操作	UP グループでの操作	既存のコールへの影響
新しい APN の追加	新しいプールまたは新しいグループ	新しい UP グループ（未登録）	影響なし
新しい APN の追加	新しいプールまたは新しいグループ	既存の UP グループ（すでに少数の UP が登録済み）	影響なし
新しい APN の追加	デフォルトプール	既存の UP グループ（すでに少数の UP が登録済み）	影響なし
既存の APN	既存の IP プールまたはグループを削除し、新しい IP プールまたはグループを追加する	既存の UP グループ（すでに少数の UP が登録済み）	削除された IP プールからは割り当てられません。コールへの影響はありません。
既存の APN	既存の IP プールまたはグループを削除し、新しい IP プールまたはグループを追加する	デフォルトの UP グループ	削除された IP プールからは割り当てられません。コールへの影響はありません。

APN での操作	IP プールやグループでの操作	UP グループでの操作	既存のコールへの影響
既存の APN	APN から既存の IP プールまたはグループを削除する	デフォルトの UP グループ	削除された IP プールからは割り当てられません。コールへの影響はありません。
APN の削除	影響を受ける UP ごとに、一連の新しい IP プールまたはグループを VPNMgr-C に渡す	既存の UP グループ（すでに少数の UP が登録済み）	当該 APN に関連付けられている既存のコールはすべて影響を受けませんが、新しいコールは接続されません。

図 *11 : APN* および *IP* プールの動的な追加

新たに追加された UP 登録が成功すると、VPN Manager が IP チャンク情報をプールから UP にプッシュします。

- CP Sx-demux は、新しい APN または IP プールを追加、変更、または削除するためのトリガーを CLI から受信します。
- CP の Sx-C demux により、影響を受ける UP のリストが決まります。APN IP プールの変更要求を使用して、影響を受ける各 UP の情報を CP の VPN Manager に渡します。
- VPN Manager が IP チャンクを割り当て、Sx-C demux に成功または失敗で応答します。
- 新しい APN または IP プールが既存の設定に適用されます。「show config」CLI コマンドを使用して、設定を表示します。
- 既存の APN に新しい IP プール名や UP グループを追加しても、その APN の既存のコールには影響しません。
- すべての IP プール（IPv4 または IPv6）は、APN に動的に追加でき、同じ実行で変更（削除および新しい IP プールの追加）できます。この変更は、既存のコールにはまったく影響しません。変更された設定は、APNに対する新しいコールが行われた後にのみ適用されます。
- 特定の APN でコールが実行されている場合、その APN の削除を試みるとエラーがスローされます。
- コールが実行されていない APN のみ削除できます。この APN に関連付けられている IP プールチャンクは、他の APN で使用できます。

割り当てられたチャンク情報の UP への受け渡し

- Sx 関連付け更新要求または応答メッセージを受信すると、独自またはカスタム IE は IP チャンク情報を UP にプッシュします。
- UP の S1-U demux は、この情報を UP の VPN Manager に渡します。

- VPN Manager は、チャンクごとにアナウンスする BGP ルートを受信します。

制限事項

ダイナミック APN および IP プールのサポート機能には以下の制限事項があります。

- 既存の APN に関連付けられている IP プールと UP グループに対する操作は、このリリースではサポートされていません。
- このリリースの一部として、複数の UP が同じ IP プールにアクセスすることはできません。
- 新しい IP プールを設定せずに新しい UP グループが APN に対して追加された場合、コールはデフォルトではなく新しい UP グループで開始されます。これにより、コールが中止されます。

ダイナミック APN および IP プールのサポートの設定

この項では、ダイナミック APN および IP プールのサポート機能の設定方法について説明します。

次の一連のコマンドを実行して、新しい APN を追加します（IP プールの追加は任意です）。

- 新しい IP プールを作成します。詳細については、『コマンドリファレンスガイド』の **ip address** *ip_ pool_name* CLI コマンドを参照してください。

  IP プールを IP プールグループに追加するには、**ip pool** *ip_pool_name* **static group-name** *ip_pool_group_name* CLI コマンドを使用します。詳細については、『コマンドリファレンスガイド』を参照してください。

- 新しい APN を追加し、新しい IP プールをこの APN に関連付けます。詳細については、『コマンドリファレンスガイド』の **apn** *apn_name* CLI コマンドを参照してください。

  IP プールグループを APN に追加するには、**ip address pool name** *ip_pool_group_name* CLI コマンドを使用します。詳細については、『コマンドリファレンスガイド』を参照してください。

- 設定を UP にプッシュします。
- VPN Manager に対する IP プール情報を更新します。
- attach コールを実行します。

APN 設定の更新

Exec モードで次のコマンドを使用して VPN マネージャを更新し、APN 設定の変更を反映します。

設定されたすべての APN を VPN マネージャで更新する場合：

```
update ip-pool apn all
end
```

特定の APN 設定を VPN マネージャで更新する場合：

```
update ip-pool apn name apn_name
end
```

注：

- この CLI コマンドは、UP に対して SX_ASSOCIATION_UPDATE をトリガーし、新しく追加された IP プールに割り当てられたすべての IP プールチャンクを転送します。

例

次の CLI コマンドは、VPN マネージャで特定の APN 設定を更新します。

```
update ip-pool apn name cisco.com
```

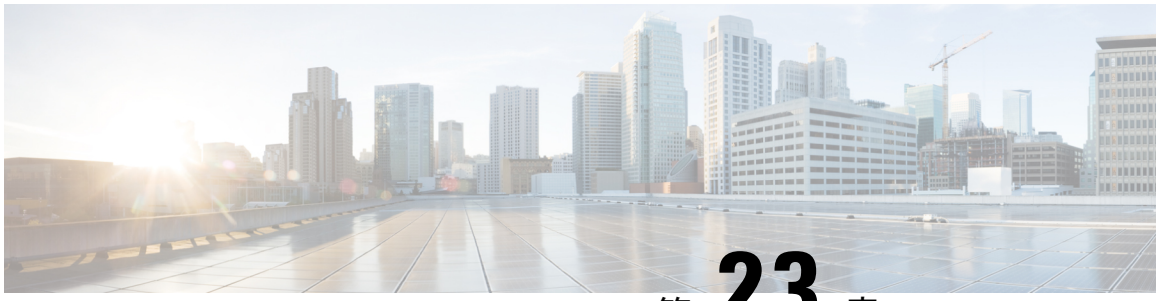
ダイナミック APN および IP プールのサポートの確認

ダイナミック APN および IP プールのサポート機能を確認するには、次のコマンドを使用します。

```
show config apn intershat
```

次に、show コマンドの出力例を示します。

```
config
  context ingress
    apn intershat
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode subscribed sent-by-ms chosen-by-sgsn
      ims-auth-service ims-ggsn-auth
      ip access-group acl4-1 in
      ip access-group acl4-1 out
      ip context-name egress
      ip address pool name ipv4-test
      ipv6 access-group acl6-1 in
      ipv6 access-group acl6-1 out
      active-charging rulebase prepaid
    exit
  #exit
end
```



第 23 章

ECS 正規表現のサポート

機能の概要と変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

この機能は、正規表現（regex）ルールの照合に Enhanced Charges Support（ECS）を提供します。この機能の目的は、ユーザープレーンに正規表現エンジンを実装して、RCM および PFD ベースの正規表現の設定や照合を有効にすることです。ユーザープレーンは、正規表現エンジンの再構築とルールマッチングの一環として、次のプロトコルをサポートします。

- HTTP
  - URL
  - URI
  - HOST
- WWW

- URL
- URI

- RTSP
  - URL
  - URI

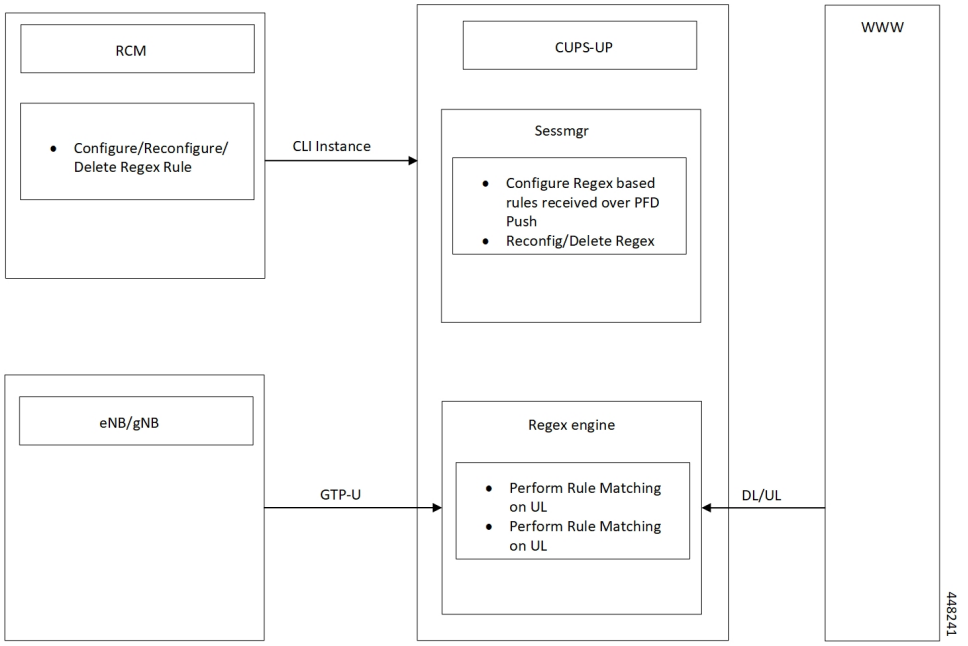
機能の仕組み

次の表に、正規表現ルールで使用できる特殊文字を示します。

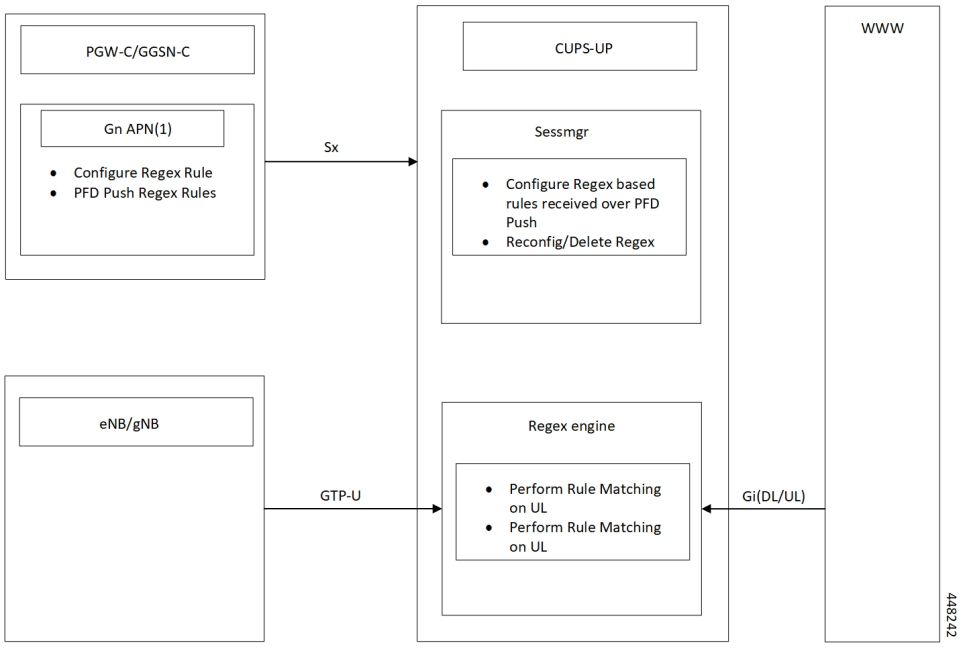
表記法	説明
*	0 字以上の文字
+	+ の前のトークンを 0 回以上繰り返すインスタンス
?	0 または 1 文字
\ 記号	エスケープ文字
\?	疑問符に相当（\<ctrl-v>?）
\+	プラス記号に相当
*	アスタリスクに相当
\a	アラート（ASCII 7）
\b	バックスペース（ASCII 8）
\f	改ページ（ASCII 12）
\n	改行（ASCII 10）
\r	改行（ASCII 13）
\t	タブ（ASCII 9）
\v	垂直タブ（ASCII 11）
\0	Null（ASCII 0）
\\	バックスラッシュ
角カッコで囲まれた範囲 [0-9]	範囲内のいずれか 1 文字と一致する。
範囲の先頭の ^	範囲内に一致するものなし。他のすべての文字はそのものを表す。
.\x##	2 桁の 16 進表記で指定された任意の ASCII 文字。たとえば、\x5A は「Z」となる。

以下に、正規表現ルールを設定する 2 つの方法を示します。

- RCM による正規表現ルールの設定：



- PFD プッシュによる正規表現ルールの設定：



正規表現ルールの設定

次に、正規表現ルールの 2 つの設定方法を示します。

RCM を介した正規表現ルールの設定

ユーザープレーン CLI インスタンスから RCM を介して、または CLI を介してユーザープレーンで直接正規表現ルールを設定します。

```
configure
          require rcm-configmgr
          end
```

PFD プッシュを介した正規表現ルールの設定

PFDプッシュを介しユーザープレーンを経由してコントロールプレーンで正規表現ルールを設定します。

```
configure
        push config-to-up all
        end
```

設定例

次に、正規表現ルールを設定するための設定例を示します。

```
configure
   active-charging service <service_name>
      ruledef <ruledef_name>
         http url regex <regex_url>
         rtsp uri regex <regex_uri>
         www url regex <regex_url>
         end
```

（注）
- RCM の場合：ユーザープレーン CLI インスタンスを使用して正規表現ルールの設定を実行します。
- PFD の場合：コントロールプレーンを介して正規表現ルールの設定を実行し、PFD プッシュを実行します。

モニタリングおよびトラブルシューティング

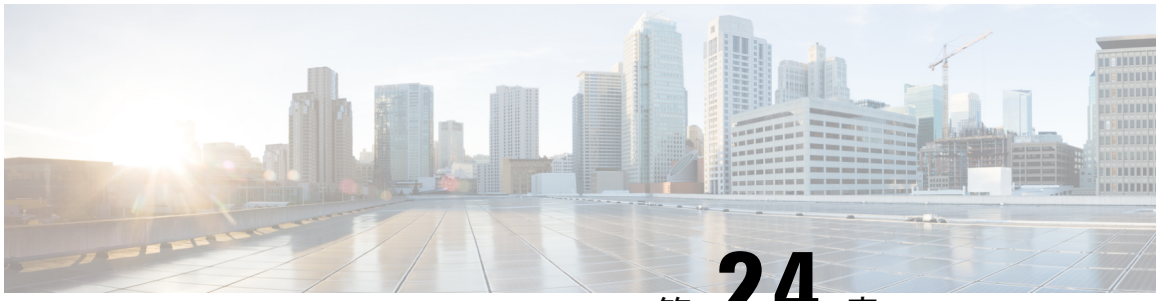
ここでは、ユーザープレーンの正規表現サポートのモニタリングと障害対応で使用できる CLI コマンドについて説明します。

show コマンドと出力

この項では、ユーザープレーンでの正規表現をサポートするために使用可能な show CLI コマンドについて説明します。

- **show user-plane-service regex status**：このコマンドを使用して、SessMgr インスタンスのエンジンステータスを表示します。
- **show user-plane-service regex statistics memory**：このコマンドを使用して、SessMgr インスタンスのメモリ統計情報を表示します。
- **show user-plane-service regex statistics memory summary**：このコマンドを使用して、SessMgr の合計メモリサマリーを表示します。
- **show user-plane-service regex statistics ruledef**：このコマンドを使用して、SessMgr の正規表現 ruledef 統計情報を表示します。
- **show user-plane-service regex statistics ruledef summary**：

  このコマンドを使用して、SessMgr の結合された正規表現 ruledef 統計情報サマリーを表示します。



第 24 章

EDNS エンリッチメント

マニュアルの変更履歴

表 *8*: マニュアルの変更履歴

改訂の詳細	リリース
追加の RR を含む DNS 要求のエンリッチメントのサポートを追加。	21.28.m23
最初の導入。	21.28.m10

機能説明

CUPS は、ペアレント コントロール サービスに登録されているサブスクライバの DNS 要求を拡充して再アドレス指定するための EDNS 要求の機能拡張をサポートしています。

サブスクライバがペアレントコントロールサービスに登録すると、サブスクライバによる DNS 要求は OPT RR フィールドの追加情報（IMSI、MSISDN、APN）で拡充され、適切な分析と処理のために専用 DNS サーバーに再アドレスされます。この追加情報は、タグ値を指定する EDNS 形式を使用して設定できます。各フィールドはエンコードされ、DNS 要求ヘッダーに追加されます。追加の RR を含む着信 DNS 要求は、サブスクライバのブロックを解除するために正確に拡充されます。

機能の仕組み

ここでは、この機能の仕組みを説明します。

PCRF または PCF は、サブスクライバに対して事前定義されたルールをアクティブ化します。

- 事前定義されたルールがアクティブ化されると、事前定義されたルールに一致する新しい DNS フローに EDNS エンリッチメント機能が適用されます。事前定義されたルールに一致するすべての DNS 要求に対し、DNS ヘッダーの設定済みフィールド（IMSI、MSISDN、APN）によるエンリッチメントが行われます。
- 事前定義されたルールが非アクティブ化されると、ルールの非アクティブ化後に作成された新しいフローには、EDNS エンリッチメント機能が適用されなくなります。非アクティブ化の前に作成された DNS フローに対しては、引き続きエンリッチメントが行われ、アドレスが再指定されます。

アクティブ課金サービス設定の service-scheme は、ペアレント コントロール サービスに登録している一連のサブスクライバにのみ選択的に機能を適用します。トリガー条件の評価に rule-match-change トリガータイプを使用し、適切な EDNS トリガーアクションを実行することでこれを実現します。

IP アドレス再指定の設定は、EDNS 要求のエンリッチメントに使用される EDNS フォーマットを含むものと同一のトリガーアクションで設定する必要があります。課金アクションとトリガーアクションの両方でアドレスの再指定が設定されている場合は、トリガーアクションが優先されます。

DNS 要求に対して、次のシナリオで設定された EDNS フォーマットに基づいて [Option-Codes] フィールドと [Option-Data] フィールドを追加するエンリッチメントが行われます。

- 受信した DNS 要求に [OPT RR] タイプの追加 RR が存在する

  受信した要求に OPT RR が存在する場合、その OPT RR は削除され、設定された EDNS フォーマットに基づいて、新しい OPT RR が最初の追加 RR として追加されます。

- DNS 要求に追加の RR がない

  DNS 要求に追加の RR がない場合、要求に OPT RR を追加するエンリッチメントが行われます。

- DNS 要求に [OPT RR] タイプ以外の追加の RR が存在する

制限事項

この機能には、次の制限事項があります。

- オンボックス データベースに対する外部コンテンツ フィルタリングとコンテンツ フィルタリングは、この機能とシームレスに相互作用せず、各機能は相互に排他的です。

- 受信 DNS 要求は、RFC 準拠をチェックするために検証されません。DNS 要求が無効で、複数の OPT RR が含まれている場合でも、EDNS の機能拡張で受け入れられます。着信 DNS 要求に複数の OPT RR が存在する場合、最初の OPT RR が拡充され、要求が DNS サーバーに転送されます。

設定例

次に、EDNS の機能拡張に関する CLI 設定の例を示します。

```
configure
   active-charging service ACS

      ruledef dns-port
         udp either-port = 53
         tcp either-port = 53
         multi-line-or all-lines
         rule-application routing
      #exit

      ruledef dns_traffic
         ip server-ip-address = 213.158.199.1
         ip server-ip-address = 213.158.199.5
         multi-line-or all-lines
      #exit

      charging-action ca
         content-id 1000
         billing-action egcdr
      #exit

      readdress-server-list test_edns_servers
         server 100.100.100.14
         server 100.100.100.15
         #exit

      rulebase test
         action priority 50 dynamic-only ruledef dns_traffic charging-action ca
         route priority 10 ruledef dns-port analyzer dns
         #exit

      edns
         fields test_fields
            tag 1 imsi
            tag 2 msisdn
            tag 3 apn-name
            #exit

         format test_format
            fields test_fields encode
         #exit

         trigger-action TA1
            edns format test_edns_format
           flow action readdress server-list test_edns_servers [ hierarchy | round-robin
 | discard-on-failure …]
          #exit

         trigger-condition TC1
            rule-name = dns_traffic
          #exit
```

```
            service-scheme SS1
               trigger rule-match-change
                  priority 1 trigger-condition TC1 trigger-action TA1
            #exit

            subs-class SC1
               rulebase = test
               multi-line-or all-lines
            #exit

            subscriber-base SB1
               priority 1 subs-class SC1 bind service-scheme SS1
            #exit
end
```

モニタリングおよびトラブルシューティング

EDNS エンリッチメント機能は、次の show コマンドと出力をサポートします。

show コマンドと出力

この機能をサポートする、次の show コマンドと出力が変更されました。

show user-plane-service statistics analyzer name dns

```
EDNS Over UDP:
EDNS Encode Success:            0         EDNS Encode Failed:      0
EDNS Encode Success Bytes:      0
EDNS Response Received:         0

EDNS Over TCP:
EDNS Encode Success:            0         EDNS Encode Failed:      0
EDNS Encode Success Bytes:      0
EDNS Response Received:         0
```

show subscribers user-plane-only full callid <call_id>

```
DNS-to-EDNS Uplink Pkts:     0       DNS-to-EDNS Uplink Bytes:     0
EDNS Response Received:      0
```

show user-plane-service edns all

```
Fields:
    Fields Name: fields_1
    tag 26946 cf-policy-id

    Fields Name: fields_2
    tag 2001 imsi
    tag 2002 msisdn
    tag 26946 cf-policy-id

    Format:
    Format Name: format_1
    fields fields_1 encode
```

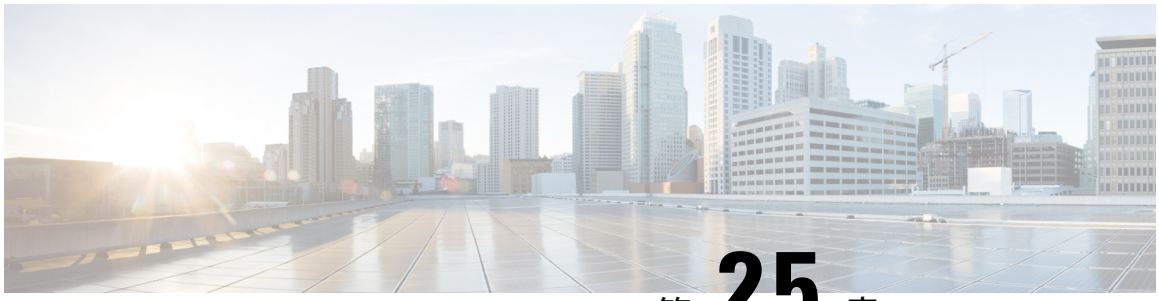
```
    Format Name: format_2
    fields fields_2 encode
```

show user-plane-service statistics trigger-action all

```
Trigger-Action: TA1
  Total EDNS PKTS           :  1
  Total readdressed Flows   :  1
  Total Trigger action(s)   :  1
```

show user-plane-service statistics trigger-action name <trigger_action_name>

```
Trigger-Action: TA1
  Total EDNS PKTS           :  1
  Total readdressed Flows   :  1
  Total Trigger action(s)   :  1
```



第 25 章

終了マーカーパケット

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

SGW-U を変更せずにハンドオーバー手順中に eNodeB を再配置する場合、SGW-C は eNodeB の新しい F-TEID-u を使用して Sx セッション変更要求メッセージを送信することによって、S1 パスの切り替えを SGW-U に指示します。さらに、古いパスで終了マーカーパケットを送信するように SGW-U に指示します。SGW-U はこの指示を受信すると、終了マーカーパケットを作成し、古いパスで最後の PDU を送信した後、送信元 eNodeB に向けて S1 GTP-U トンネルごとに送信します。

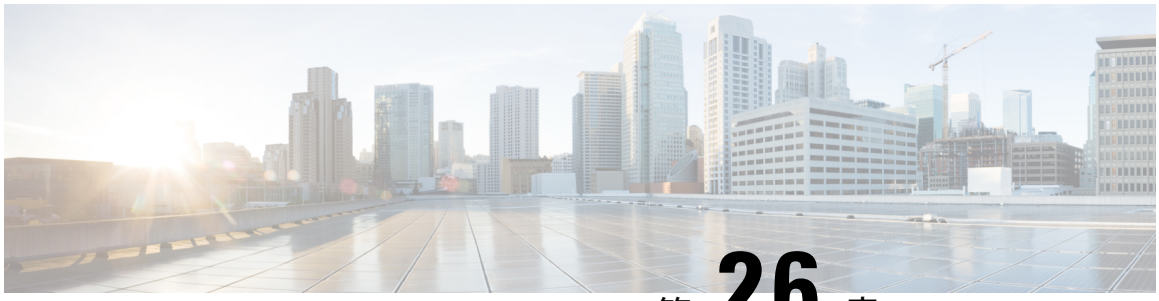
上記のシナリオで、終了マーカー パケットは GTP-U TEID ごとに送信されます。

コントロールプレーンは、新しいダウンストリーム F-TEID と SNDEM（修了マーカーパケットの送信）フラグが設定された FAR を含むセッション変更要求を送信することによって、終了マーカーパケットを作成して送信するようにユーザープレーンに要求します。

Information Element（情報要素）	P	条件/コメント
PFCPSMReq フラグ	C	SNDEM（Send End Marker Packets）：この IE が存在するのは、CP 機能が Outer Header Creation IE でダウンストリームノードの F-TEID を変更した場合や、CP 機能が UP 機能に GTP-U 終了マーカーメッセージを作成してダウンストリームノードの古い F-TEID に送信することを要求した場合です。

制限事項

P-GW でのハンドオフは、終了マーカーの送信ではサポートされていません。この動作は、非 CUPS に似ています。



第 26 章

CUPS でのエンタープライズオンボーディング

機能変更履歴

Note リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

CUPS アーキテクチャでは、ユーザープレーン（SAEGW-U）は、ユーザープレーングループ（UP グループ）と呼ばれる論理概念にグループ化され、コントロールプレーン（CP）ノードによって制御されます。APN は UP グループに関連付けられ、IP プールの UP は、使用頻度が最も低いユーザープレーンに基づいて選択されます。

新しい APN と IP プールの設定時に、オペレータは使用する UP グループを決定する必要があります。UP グループを決定するために必要な情報はシステムによって公開されず、このプロセスは煩雑でエラーが発生しやすくなります。また、ASR 5500 と比較して、CUPS アーキテクチャの CP と UP の両方でコンテキスト、APN、VRF、および IP プールの数は少なくなります。これにより、新しい APN と IP プールを適切なコンテキストと UP グループに追加することも制限されます。

インテリジェント オンボーディング（IOB）ツールは、追加する新しい APN に適した UP グループと SGi コンテキストを選択する手順を自動化します。このツールは、CUPS システムで設定されている現在のリソース情報（UP グループの数、グループごとの UP、既存のコンテキスト、APN、および IP プール）を収集します。次に、システムが新しい設定に対応できるかどうかを判断し、システムの制限に違反することなくサポートできる UP グループを決定します。これに伴い、新しい設定がツールによって適用されます。

運用ユースケース

企業は、APN および IP プールに基づく情報を使用して、オペレータを通じたユーザーの追加、変更、削除を行う必要があります。このツールは、CUPS 環境で APN を追加、変更、または削除するために必要な設定を生成して適用します。

次の操作を実行できます。

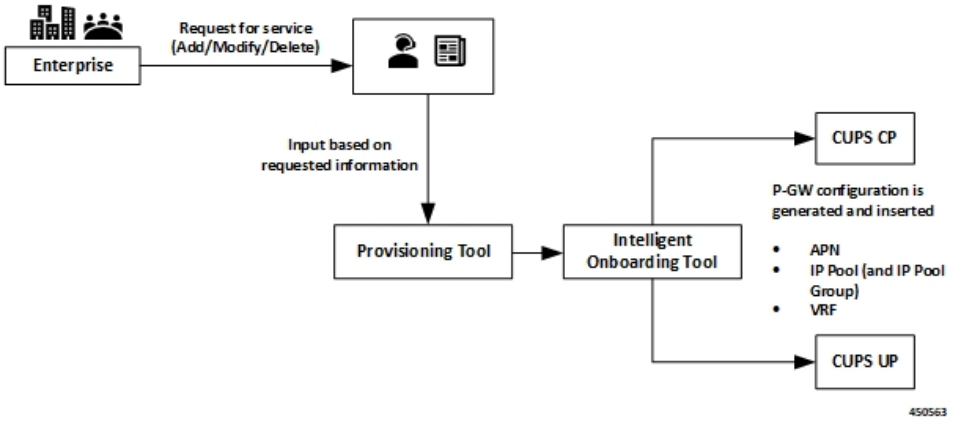
- 企業の追加：必要な数の IPv4/IPv6 プールを持つ新しい APN が追加されます。
- 企業の変更：既存の APN の IP プールを追加/削除できます。
- 企業の削除：APN が削除されます。

21.20.13 以降のリリースでは、IOB ツールは、1 回の操作で 1 つまたは複数の仮想 APN のオンボーディングが可能です。この操作の一環として、1 つまたは複数の既存の APN を変更して、これらの新しい仮想 APN を参照できます。同様に、このツールは、一緒にオンボードされた一連の仮想 APN を削除し、同時に他の APN からそれらの APN への既存の参照を削除することもできます。

アーキテクチャ

ASR 5500 では、エンタープライズの追加は新しい APN の追加で構成されます。CUPS には、APN の設定だけでなく、正しい UP グループと SGi コンテキストの設定を含める必要があります。

IOB ツールはプロビジョニングツールから入力データを取得し、APN に最適な UP グループと SGi コンテキストを選択し、CP と UP を設定します。IOB ツールでは、APN 設定の変更（IP プールの追加/削除）と APN の削除もできます。



複数の APN をオンボーディングする場合は、APN 設定セクションに以下を指定する必要があります。

- すべてのオンボーディング対象 APN
- それらを参照する APN（仮想 APN の場合）

前述のシナリオでは、すべての APN が同じ UP グループと SGi コンテキストにオンボーディングされます。

インストール

IOB ツールは、Linux 実行ファイルとして出荷されます。Pexpect や接続管理ライブラリなど、依存関係があるものはすべて、スタンドアロンの .exe ファイルにパッケージ化されます。

このツールは StarOS イメージに付属しており、StarOS VPC-SI イメージに使用されるキーと同じキーで署名されています。

実行可能ツールには、次の環境が必要です。

- RedHat Enterprise Linux 7.6（または同等の CentOS）64 ビットのインストール
- OpenSSL バージョン 1.0.2.k-fips
- 次の共有ライブラリは、/lib64 の下にインストールされます（共有ライブラリは通常、標準の RHEL または CentOS インストールに存在します）。
  - libdl.so.2
  - libz.so.1
  - libc.so.6
  - ld-linux-x86-64.so.2
- */tmp* ディレクトリの読み取り、書き込み、実行権限。実行中、ツールは */tmp* の下に一時ディレクトリを作成し、実行ファイルのセクションをこの一時ディレクトリに抽出し、セクションを実行します。

- ツールとログファイル用の十分なディスク容量（現在の使用量は約 10 MB）
- オンボーディングが実行される CP および UP への IP 接続。パスワードベースの SSH は接続に使用されます。

機能の仕組み

IOB ツールはスタンドアロン アプリケーションで、StarOS CLI を活用してシステムレベルのリソースの収集、設定の読み取り、エラーや SRP 情報の確認などを行います。IOB ツールへの入力パラメータには、CP および UP のアドレス指定とログイン情報、操作の詳細（追加/変更/削除）、適用される特定の設定が含まれます。設定を適用するコンテキストは事前に認識されていない可能性があるため、入力設定ではプレースホルダとしてダミーコンテキストを指定します。IOB ツールは、設定を適用する前に、そのダミーコンテキストを、選択された特定のコンテキストに置き換えます。

また、エンタープライズ オンボーディング ソリューションの一部として、新しい CLI コマンドが導入され、既存の CLI コマンドが変更されました。詳細については、「CUPS OAM におけるエンタープライズ オンボーディングのサポート」 の項を参照してください。

IOB ツールは、次の手順を実行します。

- **前処理**：オンボーディング操作を続行するにあたり、システムが安定した状態であることを確認するために実行されます。検証に成功すると、IOB ツールはシステムから現在のリソース使用状況情報を収集します。
- **コンテキストと UP グループの選択**：IOB ツールは、オンボーディング アルゴリズムを適用してコンテキストと UP グループを選択し、APN をオンボーディングします。
- **設定**：実行する操作に応じて、前処理ステップで収集したデータを使ってアルゴリズムが適用されます。その後、設定が CP および UP に適用されます。障害が発生した場合、IOB ツールは以前の設定へのロールバックを試行します。
- **後処理**：設定後のチェックが実行され、システムのエラーが検証されます。障害が発生した場合、IOB ツールは以前の設定へのロールバックを試行します。
- **ロギング**：操作全体がログに記録されます。ロギングメカニズムは、操作の出力、操作の履歴、警告/エラーメッセージ、およびデバッグに役立つその他の情報をキャプチャします。

前処理

前処理の手順は、オンボーディング操作が実行されている CUPS システムのステータスを理解するのに役立ちます。前処理段階では、操作に関係なく次のチェックが実行されます。

- すべての CP および UP 管理 IP が到達可能かどうかを確認します。
  - すべての CP のアクティブ/スタンバイ管理 IP に ping を実行します。

- すべての UP のアクティブ/スタンバイ管理 IP に ping を実行します。

- 次の出力に基づいて、リソース情報（APN、IP プール、VRF、コンテキスト）を収集します。
  - **show ip user-plane verbose**
  - **show cups-resources session summary**

- **追加操作**：
  - コントロールプレーンノードでは、次のチェックが実行されます。
    - オンボーディングする VRF、APN、および IP プールがシステムで設定されていないことを確認します。1つ以上の仮想 APN をオンボーディングする場合、これらの仮想 APN を参照する APN がシステムにすでに存在している必要があります。このツールは、APN 内の次の設定の存在を使用して、これらの APN を区別します。

      ```
      virtual-apn gcdr apn-name-to-be-included Gn
      ```

      そのため、1つ以上の APN を含む入力設定がある場合、システムにすでに存在する APN には前述の設定が含まれている必要があります。それ以外の場合、ツールは APN が存在しないと見なし、事前監査手順に失敗します。
    - **show srp info** を使用して、アクティブおよびスタンバイ CP 間に設定の違いがないことを確認します。
  - コンテキストと UP グループの選択後、ユーザープレーンノードでは、選択した UP グループのすべての UP に対して次の前処理チェックが実行されます。
    - オンボーディングする VRF がシステムに存在しないことを確認します。存在する場合、前処理は失敗し、オンボーディングは中止されます。
    - **show srp info** を使用して、アクティブおよびスタンバイ UP 間に設定の違いがないことを確認します。
    - SGi コンテキストが UP グループにマッピングされているかどうかを確認します。

- **変更操作**:
  - コントロールプレーンノードでは、次のチェックが実行されます。
    - 変更する VRF がシステムに存在することを確認します。
    - 変更する APN がシステムに存在することを確認します。
    - 変更操作の一部として削除された IP プールがシステムに存在することを確認します。変更操作の一部として追加された IP プールは、システムに存在しません。
    - **show srp info** を使用して、アクティブおよびスタンバイ CP 間に設定の違いがないことを確認します。

- **削除操作**：
  - コントロールプレーンノードでは、次のチェックが実行されます。
    - 削除する VRF がシステムに存在することを確認します。
    - 削除する APN がシステムに存在することを確認します。
    - **show srp info** を使用して、アクティブおよびスタンバイ CP 間に設定の違いがないことを確認します。
  - ユーザープレーンノードでは、次のチェックが実行されます。
    - 削除する VRF がシステムに存在することを確認します。
    - **show srp info** を使用して、アクティブおよびスタンバイ UP 間に設定の違いがないことを確認します。

CP および UP の設定

前処理が成功すると、ツールは入力内容に従って追加/変更/削除操作を実行し、CP および UP に設定を適用します。ICSR セットアップの場合、設定はアクティブとスタンバイの両方の CP と UP に適用されます。

- 追加操作：アルゴリズムは、追加する APN の適切な SGi コンテキストと UP グループを選択します。
  - コントロールプレーンノードでは、次の手順が実行されます。
    - 選択された SGi コンテキストと UP グループが APN 設定に追加され、ツールへの入力データとして使用されます。仮想 APN をオンボーディングする場合、オンボードの対象の仮想 APN のみで、UP グループと IP コンテキストが更新されます。それらを参照する APN（システムにすでに存在する）は、入力ファイル内にある **virtual-apn preference ..** の設定により更新されます。
    - その後、更新された設定が CP ノードに適用されます。
  - ユーザープレーンノード：
    - IOB ツールは、ダミーの SGi コンテキストを選択されたコンテキストに置き換え、選択された UP グループ内のすべての UP に最終的な設定を適用します。
    - UP グループ内のすべての UP に VRF 設定を適用します。
  - 障害が発生した場合、IOB ツールは以前の設定へのロールバックを試行します。
- 変更操作：IP プールを追加または削除するように設定が変更されます。
  - コントロールプレーンノード：

- 特定の APN 設定については、IP プールを追加/削除するために IP プールの設定が変更されます。IP プールが削除される場合、削除前にツールは次の処理を実行します。
  - プールをビジーアウトします。
  - ペースアウト間隔ごとに、そのプールの既存のサブスクライバをクリアします。ペースアウト間隔は、プールのサイズに基づいて計算されます。

    IPv6 プールの場合、式は次のとおりです。

    ペースアウト間隔 = (2^(64 - プールサイズ) * 2 - 2) / 500

    したがって、/48 プールのペースアウト間隔は、(2^(64 - 48) * 2 - 2) / 500 = (2^16 * 2 - 2) / 500 = 131070 / 500 = 262 秒になります。

    IPv4 プールの場合、式は次のとおりです。

    ペースアウト間隔 = (2^(32 - プールサイズ) * 2 - 2) / 500

    したがって、/21 プールのペースアウト間隔は、(2^(32 - 21) * 2 - 2) / 500 = (2^11 * 2 - 2) / 500 = 4094 / 500 = 8 秒になります。

- 障害が発生した場合、IOB ツールは以前の設定へのロールバックを試行します。

- 削除操作：APN を削除します。
  - コントロールプレーンノード：
    - APN に関連付けられている IP プールと VRF が削除されます。

      APN を削除する前に、IOB ツールは指定された APN にユーザーがアタッチされているかどうかを確認します。ユーザーが存在する場合は、ツールが終了して「サブスクライバをクリアしてから DELETE_ENTERPRISE を実行してください。そうしない場合は APN が削除されます」という内容のエラーメッセージが表示されます。

    - APN 設定が削除されます。
    - 仮想 APN を削除すると、仮想 APN と仮想 APN への参照のみが削除されます。それらを参照する APN は、システムに残ります。そうでなければ、監査情報の送信に失敗します。
  - ユーザープレーンノードでは、VRF 設定が削除されます。

  障害発生時に IOB ツールは以前の設定にロールバックしませんが、手動クリーンアップが必要になる容量を最小限に抑えるために、関連設定をできるだけ多く削除しようとします。

後処理

設定が CP および UP にプッシュされると、設定変更を検証するためのチェックが実行されます。

- 追加操作：
  - コントロールプレーンノードでは、次のチェックが実行されます。
    - **show ip vrf** *vrf_name* を使用して設定済みの VRF を検証します。VRF 設定が CUPS システムに適用されているかどうかを確認します。
    - **show configuration apn** *apn_name* を使用して、選択したコンテキストが表示されるかを検証します。これにより、コンテキストが追加された APN に関連付けられているかどうかを確認します。この検証は、オンボードされている APN ごとに行われます。仮想 APN がオンボードされている場合、この検証は各仮想 APN に対してのみ実行されます。
    - **show configuration apn** *apn_name* を使用して、選択した UP グループが表示されるかを検証します。これにより、UP グループが追加された APN に関連付けられているかどうかを確認します。
    - 仮想 APN がオンボードされている場合、ツールは、入力設定（**virtual-apn preference** <*preference*> **apn** <*virtual apn*> など）に従った他の APN から仮想 APN へのすべての参照が存在し、正しいことを確認します。
    - **save configuration** *file_path* / *file_name* を使用して設定を保存します。新しい企業が正常に追加された後、それぞれの構成ファイルが「CUPSinfo.txt」ファイルで指定されたパスに保存されているかどうかを確認します。
    - **filesystem synchronize** を使用して CP の設定を同期します。新しい企業が正常に追加された後、ファイルの同期を確認します。
    - **show srp info**を使用して CP 間で設定の違いがないことを確認します。ICSR セットアップでの SRP 検証：新しい企業が正常に追加された後、IOB ツールは [Primary] および [secondary] ステータス、[Last Peer Configuration Error]、[Connection State]、および [Number of Sessmgrs] の SRP 検証を確認します。
  - ユーザープレーンノードでは、次のチェックが実行されます。
    - **show ip vrf** *vrf_name* を使用して設定済みの VRF を検証します。CUPS システムに適用される VRF 設定を確認します。
    - **show ip vrf** *vrf_name* を使用してルート識別子を検証します。CUPS システムに適用されるルート識別子の設定を確認します。
    - **save configuration** *file_path* / *file_name* を使用して設定を保存します。
    - **srp validate-configuration**を使用した SRP 検証の呼び出し：**show srp info** を使用して UP 間で設定の違いがないことを確認します。ICSR セットアップでの SRP 検証。

- 障害が発生した場合、IOB ツールは以前の設定へのロールバックを試行します。

- 変更操作：
  - コントロールプレーンノードでは、次のチェックが実行されます。
    - 変更内容が CUPS システムに適用されていることを確認します。
    - IP プールへの変更がシステムに反映されていることを確認します。
    - **save configuration** *file_path* / *file_name* を使用して設定を保存します。
    - **srp validate-configuration**を使用した SRP 検証の呼び出し：**show srp info** を使用して UP 間で設定の違いがないことを確認します。ICSR セットアップでの SRP 検証
  - 障害が発生した場合、IOB ツールは以前の設定へのロールバックを試行します。

- 削除操作：
  - コントロールプレーンノードでは、次のチェックが実行されます。
    - この検証は、削除操作後に APN ごとに行われます。仮想 APN の削除操作では、仮想 APN への参照のみが削除され、それを参照する APN は保持されます。後者の APN を削除すると、後処理が失敗します。
    - VRF 設定が CUPS システムから削除されているかどうかを確認します。
    - **save configuration** *file_path* / *file_name* を使用して設定を保存します。
    - **srp validate-configuration**を使用した SRP 検証の呼び出し：**show srp info** を使用して UP 間で設定の違いがないことを確認します。ICSR セットアップでの SRP 検証
  - ユーザープレーンノードでは、次のチェックが実行されます。
    - VRF 設定が CUPS システムから削除されているかどうかを確認します。
    - **save configuration** *file_path* / *file_name* を使用して設定を保存します。
    - **srp validate-configuration**を使用した SRP 検証の呼び出し：**show srp info** を使用して UP 間で設定の違いがないことを確認します。ICSR セットアップでの SRP 検証。

追加操作

追加操作では、企業顧客の新しい APN を設定します。このツールを使用すると、同じ SGi コンテキストと VRF 設定を共有している場合、1 回の操作で複数の APN のオンボーディングもサポートできます。この場合、オンボーディング APN は IP プール情報を共有する場合と共有しない場合があります（両方の条件をサポートします）。すべてのオンボーディング APN は、

前述のシナリオで同じ SGi コンテキストと UP グループにマッピングされます。アルゴリズムによってシステムパラメータを考慮して適切な SGi コンテキストと UP グループが選択され、APN にマッピングされます。

アルゴリズムロジック：

- システム制限を確認します（システム制限, on page 229 に記載されている CP 制限について確認）。仮想 APN をオンボーディングする場合、ツールでは仮想 APN のみが APN 制限の計算対象の新しい APN と見なされます。仮想 APN を参照する APN はすでにシステムに存在しているため、システムの現在の APN 数にすでに含まれています。
- 上位の低い数値で設定された APN の数に基づいて UP グループをランク付けします。
- 設定された VRF の数に基づいて SGi コンテキストを昇順でソートします。
- リストから VIP UP グループとコンテキストを除外します。
- リストの一番上から（使用頻度が最も低い）UP グループを選択します。
  - UP グループにマッピングされているコンテキストを取得します（コンテキストがマッピングされていない場合は、ソート済みリストから選択します）。
  - VRF、IPv4、IPv6 プールの数、および合計プールサイズをチェックします。
  - 結果がしきい値内に収まっている場合は、コンテキストを選択します。収まっていない場合は、次のコンテキストに対してチェックを繰り返します。
  - 制限内で適切なコンテキストを選択します。適切なコンテキストが見つからない場合は、アルゴリズムを終了します。
  - この UP グループについて、UP を反復処理し、合計 IP プールの制限を確認します。
  - 成功した場合は、UP グループとコンテキストを選択します。
- すべての UP グループを反復処理します。
- 各ステップで、しきい値をチェックしながら、エラーメッセージを出力します。
- 選択したコンテキストと UP グループを使用して設定を準備し、適用します。

変更操作

変更操作により、導入準備を終えた企業のお客様は、IP プールを追加するか、既存の IP プールを削除することでサブスクライバを増減できます。

削除操作

削除操作では、以前にオンボーディングしたエンタープライズが削除されます。この操作中に、IOB ツールはエンタープライズで使用される IP プール、VRF、および APN をクリーンアップします。

エンタープライズを削除する際は、システムにアクティブなサブスクライバが存在する可能性があるため、次の手順に従う必要があります。

- IP プールのビジーアウト：これは、新しいサブスクライバをブロックするために実行します。IOB ツールを呼び出し、MODIFY 操作を使用してビジーアウト操作を実行します。
- サブスクライバのクリア：プロビジョニングツールを使用して、アクティブなサブスクライバをクリアします。
- エンタープライズの削除：IOB ツールを呼び出し、DELETE 操作を使用してエンタープライズの削除を実行します。

パスワード暗号化

IOB ツールを使用すると、「CUPSInfo.txt」入力ファイル内のパスワードが RSA 暗号化され、Base64 形式に変換されます。暗号化は、OpenSSL コマンド（現在バージョン 1.0.2.k をサポート）と RSA 公開キーを使用して行われます。パスワードを復号できるように、IOB ツールに対応する RSA 秘密キーへのパスを指定する必要があります。復号されたパスワードは、IOB ツールの RAM にのみ保存されます。暗号化と復号の詳細な手順を以下に示します。

1. 正しいバージョンの OpenSSL がターゲットマシンにインストールされていることを確認します。
   - 「openssl version」に、バージョンが 1.0.2.k-fips と表示されている必要があります。
2. RSA の秘密キーと公開キーのペアを生成します。
   a. RSA 秘密キー：

      ```
      openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:4096
      ```

      それぞれの説明は次のとおりです。
      - 「private_key.pem」には、生成された秘密キーファイルが PEM 形式で表示されます。これは復号に使用されるため、安全に保存する必要があります。
      - 4,096 はビット単位のキーの長さです。2,048 または 4,096 を使用できます。場合によっては、複数のパスワードを暗号化する必要があるため、4,096 を推奨します。一般に、キーサイズが大きいほど、暗号化できるデータのサイズも大きくなりますが、暗号化と復号にも時間がかかります。

   b. RSA 公開キー：

      ```
      openssl rsa -pubout -in private_key.pem -out public_key.pem
      ```

      それぞれの説明は次のとおりです。
      - 「private_key.pem」は、ステップ（a）で生成された秘密キーです。
      - 「public_key.pem」は、対応する公開キーを含むファイルです。

3. 暗号化する必要があるパスワードごとに、次の手順を実行します。

   a. エディタを使用して、テキストファイルにプレーンテキストでパスワードを入力します。行の最後で Enter を押さないでください。1 行にパスワードのみを含める必要があります。この例では、ファイルの名前は「pp1」です。

   b. 実行：

   ```
   openssl pkeyutl -encrypt -inkey public_key.pem -pubin -in pp1 -out encrypted_pp1
   ```

   それぞれの説明は次のとおりです。

   - 「public_key.pem」は、ステップ 2b で生成された公開キーです。
   - 「pp1」は、プレーンテキストの単一のパスワードを含むファイルです。
   - 「encrypted_pp1」には、暗号化形式のパスワードが含まれています。

   誤って公開されないように、ステップ 3a で作成した「pp1」は削除します。

   c. 「encrypted_pp1」には、raw バイナリ形式のキーが含まれています。次のように Base64 に変換します。

   ```
   base64 encrypted_pp1
   ```

   d. 前述のコマンド（ステップ 3c）を実行すると、Base64 でエンコードされた暗号化パスワードが端末に出力されるので、そのパスワードをコピーして、IOB ツールに提供されるログイン情報を含む「CUPSinfo.txt」ファイルに貼り付けます。コピー時に、改行文字やスペースはすべて削除してください。パスワード全体を 1 行にする必要があります。

   e. 「encrypted_pp1」はこの時点で削除できます。

Note ステップ 3 は、すべてのパスワードに同じ公開キー/秘密キーのペアを使用して、パスワードごとに 1 つずつ実行する必要があります。

「CUPSinfo.txt」ファイルが暗号化されたすべての Base64 パスワードで更新されると、IOB ツールを実行できます。スクリプトを実行するときに、ステップ 2a で作成した追加のパラメータ（**-k** *absolute path to private_key.pem*）を指定します。

オンボーディング アプリケーション：使用状況と入力パラメータ

このアプリケーションは、スタンドアロンの .exe を作成するためにコンパイルされ、RedHat Enterprise Linux マシンで実行できます。

オンボーディング アプリケーションは、次の構文で実行できます。

```
./intelligent_onboarding -o <OP_Type_Parameter_File> -i <CUPS_Info_File> -k
<Path_to_Pvt_Key_file> [ -l <Path_to_store_logfiles> ] [ -p ] [ --context_selection_from_cp
 ] [ -v ]
```

次のオプションがあります。

- **-o**：（必須）呼び出される操作に固有の入力パラメータファイルを指定します。

  オンボーディングが成功すると、IOB ツールによってファイルが削除されます。

- **-i**：（必須）このオプションは、CUPS システムの詳細を含む「CUPSinfo.txt」ファイルに使用されます。

- **-k**：（必須）秘密キーファイルへの絶対パス。ツールはこのパスを使用して、以前に暗号化されたパスワードを復号します。この秘密キーファイルは、パスワードの暗号化に使用される公開キーに対応している必要があります。

- **-p**：（任意）このキーワードを含めると、追加/変更/削除操作にかかる時間を短縮するために、いくつかの事前監査および事後監査チェックがバイパスされます。

- **-l**：（任意）ログを保存する絶対パスを指定します。

  このキーワードが指定されていない場合、ログファイルはIOBツールが呼び出されたディレクトリに作成されます。

- **--context_selection_from_cp**：（任意）指定すると、ツールは CP で使用可能なコンテキストのリストのみに基づいてコンテキストを選択します。このツールでは、選択したコンテキストが UP でも使用可能であると想定されているため、コンテキストは検証されません。つまり、最適化されています。デフォルトの動作では、CP と UP で設定されたコンテキストが検査され、両方に共通のコンテキストから選択されます。

- **-v**：（任意）IOB 実行ファイルのバージョンを表示します。

  -v オプションを指定せずに IOB ツールを実行すると、次のようなバージョンが表示されます。

  ```
  ################################################################
  #                                                              #
  #             WELCOME TO ENTERPRISE ONBOARDING                 #
  #                   Version 21.20.9.private                    #
  #                                                              #
  ################################################################
  ```

  注：バージョンは、ログファイルと端末出力に表示されます。

CUPSinfo.txt

オンボーディングアプリケーションは、オンボーディング操作を実行するためにシステムレベルの詳細を認識している必要があります。「CUPSinfo.txt」ファイルには、CP ノードと UP ノードの IP アドレスと設定可能なしきい値が含まれています。「Skip_UPGroup」と「Skip_Context」は、オンボーディング アルゴリズムで考慮すべきではない UP グループとコンテキストを指します。たとえば、他の企業には使用できない VIP グループやコンテキストです。ファイルで、設定を保存する必要があるパスを指定します。このファイルのパスワードは、RSA 暗号化された Base64 形式で指定する必要があります。

21.20.9 以前のリリースでは、CP および UP 入力のエントリ順序は次のとおりでした。

```
//Control_Plane:
Host,Node,Primary_IP,Secondary-IP,Login,Password,Primary_config_path,Secondary_config_path
//User_Plane:
Host,Node,Primary_IP,Secondary-IP,Login,Password,Sx-IP-Address,Primary_config_path,Secondary_config_path
```

21.20.10 以降のリリースでは、CP および UP 入力のエントリ順序は次のとおりです。

```
//Control_Plane:
Host,Node,Primary_IP,Secondary-IP,Primary_config_path,Secondary_config_path,Login,Password
//User_Plane:
Host,Node,Primary_IP,Secondary-IP,Sx-IP-Address,Primary_config_path,Secondary_config_path,Login,Password
```

CUPSinfo.txt ファイルの例

21.20.9 以前のリリース：

```
//Threshold for Warning, input as percentage values

CPContext_threshold = {vrf_threshold:80, ipv4_threshold:80, ipv6_threshold:80}
CPSystem_threshold = {vrf_threshold:80, total_pool_threshold:80, apn_threshold:80}
UPContext_threshold = {vrf_threshold:80, ipv4_threshold:80, ipv6_threshold:80}
UPSystem_threshold = {vrf_threshold:80, apn_threshold:80, total_pool_threshold:80}
UPBudgeted_Sessions_threshold = {budgeted_threshold:80}

SKIP_UPGroup =
SKIP_Context =

//Control_Plane:
Host,Node,Primary_IP,Secondary-IP,Login,Password,Primary_config_path,Secondary_config_path
cups_di_cp1,Control_Plane,209.165.200.225,209.165.200.225,<login_id>,<password>,
/flash/209.165.200.225-cups-vpp-saegw-global-control-plane.cfg,
/flash/209.165.200.225-cups-vpp-saegw-global-control-plane.cfg

//User_Plane:
Host,Node,Primary_IP,Secondary-IP,Login,Password,Sx-IP-Address,Primary_config_path,Secondary_config_path
cups_di_up0,User_Plane,209.165.200.230,209.165.200.230,<login_id>,<password>,
209.165.200.238,/flash/209.165.200.230-cups-vpp-saegw-global-user-plane-.cfg,
/flash/209.165.200.230-cups-vpp-saegw-global-user-plane.cfg
cups_di_up1,User_Plane,209.165.200.235,209.165.200.235,<login_id>,<password>,
209.165.200.242,/flash/209.165.200.235-cups-vpp-saegw-global-user-plane.cfg,
/flash/209.165.200.235-cups-vpp-saegw-global-user-plane.cfg
```

21.20.10 以降のリリース：

```
//Threshold for Warning, input as percentage values

CPContext_threshold = {vrf_threshold:98, ipv4_threshold:98,ipv6_threshold:98}
CPSystem_threshold = {vrf_threshold:98, total_pool_threshold:98, apn_threshold:98}
UPContext_threshold = {vrf_threshold:98, ipv4_threshold:98, ipv6_threshold:98}
UPSystem_threshold = {vrf_threshold:98, apn_threshold:98, total_pool_threshold:98}
UPBudgeted_Sessions_threshold = {budgeted_threshold:80}

SKIP_UPGroup =
SKIP_Context =

//Control_Plane: Host,Node,Primary_IP,Secondary-IP,Primary_config_path,
Secondary_config_path,Login,Password
cups_di_cp1,Control_Plane,209.165.200.225,209.165.200.225,/flash/209.165.200.225-CP01.cfg,
 /flash/209.165.200.225-CP02.cfg,<login_id>,<password>
//User_Plane: Host,Node,Primary_IP,Secondary-IP,Sx-IP-Address,Primary_config_path,
Secondary_config_path,Login,Password
```

```
cups_si_up1,User_Plane,209.165.200.235,209.165.200.235,209.165.200.242,/flash/209.165.200.235-UP01.cfg,
 /flash/209.165.200.235-UP02.cfg,<login_id>,<password>
```

ADD_ENTERPRISE_INPUT_PARAMETERS.txt

このファイルには、APN 追加時の設定情報が含まれ、IP プール情報と VRF 情報を提供します。提供されるコンテキストはダミーであり、実際のコンテキストはアルゴリズムの一部として決定されます。IP プールはチャンクをサポートしていません。

ADD_ENTERPRISE_INPUT_PARAMETERS.txt の例

次に、単一の APN をオンボーディングするための設定例を示します。

```
OpType = "ADD_ENTERPRISE"

CP_APN_Config  = '''Config
context APN
        apn starent.com
ip address pool name starent_ipv4_pool_group_01
ipv6 address prefix-pool starent_ipv6_pool_group_01
        exit
    exit
exit'''

// script will replace the dummy-SGI context with the chosen context
CP_SGi_Context = '''Config
    context dummy-SGi
ip vrf MPN00001
ip pool starent_ip_pool_v4_001 209.165.200.225 255.255.255.250 private 0 no-chunk-pool
group-name starent_ipv4_pool_group_01 vrf MPN00001
ip pool starent_ip_pool_v4_002 209.165.200.228 255.255.255.250 private 0 no-chunk-pool
group-name starent_ipv4_pool_group_01 vrf MPN00001

ipv6 pool starent_ip_pool_v6_001 prefix 2001:1:1::/48 private 0 no-chunk-pool group-name
 starent_ipv6_pool_group_01 vrf MPN00001

    exit
exit'''

// UP VRF config
// script will replace the dummy-SGI context with the chosen context
UP_VRF_Config= '''config
context dummy-SGI
ip vrf MPN00001
ip maximum-routes 100
exit
router bgp 65101
ip vrf MPN00001
route-distinguisher 65101 11100001
route-target both 65101 11100001
exit
address-family ipv4 vrf MPN00001
redistribute connected
exit
address-family ipv6 vrf MPN00001
redistribute connected
exit
exit
exit
exit'''
```

次に、1 回の追加操作で複数の仮想 APN をオンボーディングするための設定例を示します。

```
OpType = "ADD_ENTERPRISE"

CP_APN_Config  = '''Config
        context APN
        apn virtual1
                        ip address pool name apn2_ipv4_pool_group_01
                        ipv6 address prefix-pool apn2_ipv6_pool_group_01
        exit
        apn virtual2
                        ip address pool name apn2_ipv4_pool_group_02
                        ipv6 address prefix-pool apn2_ipv6_pool_group_02
        exit
        apn virtual3
                        ip address pool name apn2_ipv4_pool_group_03
                        ipv6 address prefix-pool apn2_ipv6_pool_group_03
        exit
        apn virtual4
                        ip address pool name apn2_ipv4_pool_group_04
                        ipv6 address prefix-pool apn2_ipv6_pool_group_04
        exit
        apn virtual5
                        ip address pool name apn2_ipv4_pool_group_05
                        ipv6 address prefix-pool apn2_ipv6_pool_group_05
        exit
        apn virtual6
                        ip address pool name apn2_ipv4_pool_group_06
                        ipv6 address prefix-pool apn2_ipv6_pool_group_06
        exit
        apn virtual7
                        ip address pool name apn2_ipv4_pool_group_07
                        ipv6 address prefix-pool apn2_ipv6_pool_group_07
        exit
        apn virtual8
                        ip address pool name apn2_ipv4_pool_group_08
                        ipv6 address prefix-pool apn2_ipv6_pool_group_08
        exit
        apn virtual9
                        ip address pool name apn2_ipv4_pool_group_09
                        ipv6 address prefix-pool apn2_ipv6_pool_group_09
        exit
        apn virtual10
                        ip address pool name apn2_ipv4_pool_group_10
                        ipv6 address prefix-pool apn2_ipv6_pool_group_10
        exit
        apn real1
            virtual-apn preference 1 apn virtual2 domain virtual2
            virtual-apn preference 2 apn virtual3 domain virtual3
            virtual-apn preference 3 apn virtual4 domain virtual4
        exit
        apn real2
            virtual-apn preference 3 apn virtual5 domain virtual5
            virtual-apn preference 6 apn virtual6 domain virtual6
            virtual-apn preference 9 apn virtual7 domain virtual7
        exit
        apn real3
            virtual-apn preference 2 apn virtual6 domain virtual6
            virtual-apn preference 5 apn virtual7 domain virtual7
            virtual-apn preference 8 apn virtual8 domain virtual8
        exit
        apn real4
            virtual-apn preference 2 apn virtual8 domain virtual8
            virtual-apn preference 3 apn virtual9 domain virtual9
```

```
            virtual-apn preference 5 apn virtual10 domain virtual10
        exit
        apn real5
            virtual-apn preference 7 apn virtual10 domain virtual10
            virtual-apn preference 8 apn virtual1 domain virtual1
            virtual-apn preference 9 apn virtual2 domain virtual2
        exit
        apn real6
            virtual-apn preference 11 apn virtual10 domain virtual10
            virtual-apn preference 12 apn virtual1 domain virtual1
            virtual-apn preference 13 apn virtual2 domain virtual2
        exit
        apn real7
            virtual-apn preference 12 apn virtual2 domain virtual2
            virtual-apn preference 13 apn virtual3 domain virtual3
        exit
        apn real8
            virtual-apn preference 12 apn virtual7 domain virtual7
        exit
        apn real9
            virtual-apn preference 12 apn virtual5 domain virtual5
            virtual-apn preference 13 apn virtual6 domain virtual6
            virtual-apn preference 14 apn virtual7 domain virtual7
            virtual-apn preference 15 apn virtual8 domain virtual8
            virtual-apn preference 16 apn virtual9 domain virtual9
            virtual-apn preference 17 apn virtual10 domain virtual10
            virtual-apn preference 18 apn virtual2 domain virtual2
            virtual-apn preference 19 apn virtual3 domain virtual3
        exit
        apn real10
            virtual-apn preference 1 apn virtual1 domain virtual1
        exit
    exit
exit'''

// script will replace the dummy-SGI context with the chosen context
CP_SGi_Context = '''Config
    context dummy-SGi
        ip vrf MPN00002
        ip pool apn2_ip_pool_v4_001 209.165.201.1 255.255.255.224 private 0 group-name
apn2_ipv4_pool_group_01 vrf MPN00002 no-chunk-pool
       ip pool apn2_ip_pool_v4_002 209.165.201.3 255.255.255.224 private 0 no-chunk-pool
 group-name apn2_ipv4_pool_group_02 vrf MPN00002
       ip pool apn2_ip_pool_v4_003 209.165.201.5 255.255.255.224 private 0 no-chunk-pool
 group-name apn2_ipv4_pool_group_03 vrf MPN00002
       ip pool apn2_ip_pool_v4_004 209.165.201.7 255.255.255.224 private 0 no-chunk-pool
 group-name apn2_ipv4_pool_group_04 vrf MPN00002
       ip pool apn2_ip_pool_v4_005 209.165.201.9 255.255.255.224 private 0 no-chunk-pool
 group-name apn2_ipv4_pool_group_05 vrf MPN00002
       ip pool apn2_ip_pool_v4_006 209.165.201.11 255.255.255.224 private 0 no-chunk-pool
 group-name apn2_ipv4_pool_group_06 vrf MPN00002
       ip pool apn2_ip_pool_v4_007 209.165.201.13 255.255.255.224 private 0 no-chunk-pool
 group-name apn2_ipv4_pool_group_07 vrf MPN00002
       ip pool apn2_ip_pool_v4_008 209.165.201.15 255.255.255.224 private 0 no-chunk-pool
 group-name apn2_ipv4_pool_group_08 vrf MPN00002
       ip pool apn2_ip_pool_v4_009 209.165.201.17 255.255.255.224 private 0 no-chunk-pool
 group-name apn2_ipv4_pool_group_09 vrf MPN00002
       ip pool apn2_ip_pool_v4_010 209.165.201.19 255.255.255.224 private 0 no-chunk-pool
 group-name apn2_ipv4_pool_group_10 vrf MPN00002

        ipv6 pool apn2_ip_pool_v6_001 prefix 2001:268:1::/48 private 0 no-chunk-
pool group-name apn2_ipv6_pool_group_01 vrf MPN00002
        ipv6 pool apn2_ip_pool_v6_002 prefix 2001:278:1::/48 private 0 no-chunk-
pool group-name apn2_ipv6_pool_group_02 vrf MPN00002
```

```
        ipv6 pool apn2_ip_pool_v6_003 prefix 2001:288:1::/48 private 0 no-chunk-
pool group-name apn2_ipv6_pool_group_03 vrf MPN00002
        ipv6 pool apn2_ip_pool_v6_004 prefix 2001:298:1::/48 private 0 no-chunk-
pool group-name apn2_ipv6_pool_group_04 vrf MPN00002
        ipv6 pool apn2_ip_pool_v6_005 prefix 2001:2A8:1::/48 private 0 no-chunk-
pool group-name apn2_ipv6_pool_group_05 vrf MPN00002
        ipv6 pool apn2_ip_pool_v6_006 prefix 2001:2B8:1::/48 private 0 no-chunk-
pool group-name apn2_ipv6_pool_group_06 vrf MPN00002
        ipv6 pool apn2_ip_pool_v6_007 prefix 2001:2C8:1::/48 private 0 no-chunk-
pool group-name apn2_ipv6_pool_group_07 vrf MPN00002
        ipv6 pool apn2_ip_pool_v6_008 prefix 2001:2D8:1::/48 private 0 no-chunk-
pool group-name apn2_ipv6_pool_group_08 vrf MPN00002
        ipv6 pool apn2_ip_pool_v6_009 prefix 2001:2E8:1::/48 private 0 no-chunk-
pool group-name apn2_ipv6_pool_group_09 vrf MPN00002
        ipv6 pool apn2_ip_pool_v6_010 prefix 2001:2F8:1::/48 private 0 no-chunk-
pool group-name apn2_ipv6_pool_group_10 vrf MPN00002
    exit
exit'''

// UP VRF config
// script will replace the dummy-SGI context with the chosen context
UP_VRF_Config   = '''config
                context dummy-SGI
                        ip vrf MPN00002
                                ip maximum-routes 100
                        exit
                        router bgp 65101
                                ip vrf MPN00002
                                        route-distinguisher 65101 11100002
                                        route-target both 65101 11100002
                                exit
                                address-family ipv4 vrf MPN00002
                                        redistribute connected
                                exit
                                address-family ipv6 vrf MPN00002
                                        redistribute connected
                                exit
                        exit
                exit
        exit'''
```

MODIFY_ENTERPRISE_INPUT_PARAMETERS.txt

このファイルは、既存のエンタープライズの追加または削除対象の IP プールを提供します。コンテキスト名は、プール名に基づいて決定されます。

MODIFY_ENTERPRISE_INPUT_PARAMETERS.txt の例

```
OpType = "MODIFY_ENTERPRISE"
CP_APN_Config  = '''Config
     context APN
            apn cisco.com
            exit
     exit
  exit'''
CP_SGi_Context = '''Config
    context dummy-SGi
      no ip pool cisco_ip_pool_v4_002 209.165.202.129 255.255.255.224 private 0
no-chunk-pool group-name starent_ipv4_pool_group_01 vrf MPN00001
      ip pool starent_ip_pool_v4_003 209.165.202.132 255.255.255.224 private 0
no-chunk-pool group-name starent_ipv4_pool_group_01 vrf MPN00001
```

```
    exit
exit'''
```

DELETE_ENTERPRISE_INPUT_PARAMETERS.txt

エンタープライズを削除する要求の場合、この入力ファイルにはAPN、SGiコンテキスト、および VRF の詳細が含まれている必要があります。

DELETE_ENTERPRISE_INPUT_PARAMETERS.txt の例

単一の APN を削除するための設定例を以下に示します。

```
OpType= "DELETE_ENTERPRISE"

CP_APN_Config = '''config
     context APN
         no apn cisco.com
     exit
exit'''

// script will replace the dummy-SGI context with the chosen context
CP_SGi_Context = '''config
    context dummy-SGi
no ip vrf MPN00001

    exit
exit'''

// UP VRF config
// script will replace the dummy-SGI context with the chosen context
UP_VRF_Config = '''config
      router bgp 65101
          no ip vrf MPN00001
      exit
exit'''
```

1 回の削除操作で複数の仮想 APN を削除するための設定例を以下に示します。

```
CP_APN_Config = '''config
     context APN
         no apn virtual1
         no apn virtual2
         no apn virtual3
         no apn virtual4
         no apn virtual5
         no apn virtual6
         no apn virtual7
         no apn virtual8
         no apn virtual9
         no apn virtual10

         apn real1
            no virtual-apn preference 1
            no virtual-apn preference 2
            no virtual-apn preference 3
         exit
         apn real2
            no virtual-apn preference 3
            no virtual-apn preference 6
            no virtual-apn preference 9
         exit
         apn real3
```

```
            no virtual-apn preference 2
            no virtual-apn preference 5
            no virtual-apn preference 8
         exit
         apn real4
            no virtual-apn preference 2
            no virtual-apn preference 3
            no virtual-apn preference 5
         exit
         apn real5
            no virtual-apn preference 9
            no virtual-apn preference 8
            no virtual-apn preference 7
         exit
         apn real6
            no virtual-apn preference 13
            no virtual-apn preference 11
            no virtual-apn preference 12
         exit
         apn real7
            no virtual-apn preference 12
            no virtual-apn preference 13
         exit
         apn real8
            no virtual-apn preference 12
         exit
         apn real9
            no virtual-apn preference 19
            no virtual-apn preference 17
            no virtual-apn preference 13
            no virtual-apn preference 12
            no virtual-apn preference 15
            no virtual-apn preference 14
            no virtual-apn preference 16
            no virtual-apn preference 18
         exit
         apn real10
            no virtual-apn preference 1
         exit
     exit
exit'''


// script will replace the dummy-SGI context with the chosen context
CP_SGi_Context = '''config
    context dummy-SGi
        no ip vrf MPN00002

    exit
exit'''


// UP VRF config
// script will replace the dummy-SGI context with the chosen context
UP_VRF_Config = '''config
      router bgp 65101
          no ip vrf MPN00002
      exit
exit'''
```

システム制限

ASR 5500 および CUPS の制限事項を次の表に示します。

表 *9:* システム制限

パラメータ	ASR 5500	コントロール プレーン	ユーザープレーン
VRF 制限	コンテキストあたり 300 シャーシあたり 2,048	• コンテキストあたり 300：**show ip user-plane verbose** CLI コマンドの出力から取得されます。 • シャーシあたり 1500：すべてのコンテキストに追加される **show ip user-plane verbose** CLI コマンドの出力から取得されます。	205 VRF（デフォルトルートあり）：**show ip user-plane verbose** CLI コマンドの出力から取得されます。UP ごとに計算する必要があります。
IP プールの制限	IPv4：コンテキストあたり 2,000 IPv6：コンテキストあたり 256 IPv6 シャーシあたり 5,000（IPv4 と IPv6 の組み合わせ）	IPv4：コンテキストあたり 2,000：**show ip user-plane verbose** CLI コマンドの出力から取得されます。 IPv6：コンテキストあたり 256 IPv6 シャーシあたり 3400（IPv4 と IPv6 の組み合わせ）：**show ip user-plane verbose** CLI コマンドの出力から取得されます。	UP グループごとのコンテキストあたり合計600個の IP プール： • 合計 600 個の IP プールは、最大 256 個の IPv6 IP プールで構成できます。 • 合計 600 個の IP プールは、最大 600 個の IPv4 IP プールで構成できます。 **show ip user-plane verbose** CLI コマンドの出力から取得されます。出力から値を計算する必要があります（最大 600 個の IPv4 プール、最大 256 個の IPv6 プール）。

パラメータ	ASR 5500	コントロール プレーン	ユーザープレーン
APN 制限	2048	システムの合計 1500：**show cups-resource session summary** CLI コマンドの出力から取得されます。	UP あたり 205：**show cups-resource session summary** CLI コマンドの出力から取得されます。UP ごとに計算する必要があります。

（注）

- IOB ツールを使用すると、すべての APN が入力ファイルの「CP_SGi_Context」および「UP_VRF_Config」セクションを共有している場合、複数の APN をオンボーディング（OpType：ADD_ENTERPRISE）できます。APN は複数の IP プールグループを使用する可能性がありますが、それらのプールグループはすべて、入力ファイルの「CP_SGi_Context」セクションの単一のコンテキストに存在する必要があります。また、APN は単一の VRF を共有する必要があります。このような場合、すべての APN が同じ UP グループと SGi コンテキストにオンボードされます。
- このツールを使用すると、すべての APN が入力設定の「UP_VRF_Config」および「CP_SGi_Context」セクションを共有している場合、複数の APN を削除（OpType：DELETE_ENTERPRISE）できます。ツールは操作の終了時に VRF とプールを削除します。複数の APN を削除する目的は、一緒にオンボーディングされた APN を削除することです。一緒にオンボードされた APN は一緒に削除する必要があります。このツールは、一緒にオンボードされた APN の個別の削除をサポートしていません。
- また、1 回の操作で複数の APN を変更（OpType：MODIFY_ENTERPRISE）することはできません。一度に変更できる APN は 1 つだけです。
- CUPSinfo.txt ファイルは、プライマリ UP 情報と見なされます。システムに追加された UP グループがファイルに存在しない場合、それらはオンボーディングの対象外となります。

CUPS OAM サポートでのエンタープライズ オンボーディング

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

コマンドの表示

show cups-resource session summary

この CLI コマンドは、CUPS ソリューションでのエンタープライズ オンボーディングをサポートするために導入されました。この CLI コマンドの出力には、CP のシステムレベルのリソースが表示されます。

注：

- 出力に表示される [Group Name] 列は、UP グループの名前です。
- Sx-IP には、UP グループで設定された UP の IP アドレスが表示されます。
- APN、アクティブセッション、および LCI の詳細は UP グループに関する内容です。

show ip user-plane verbose

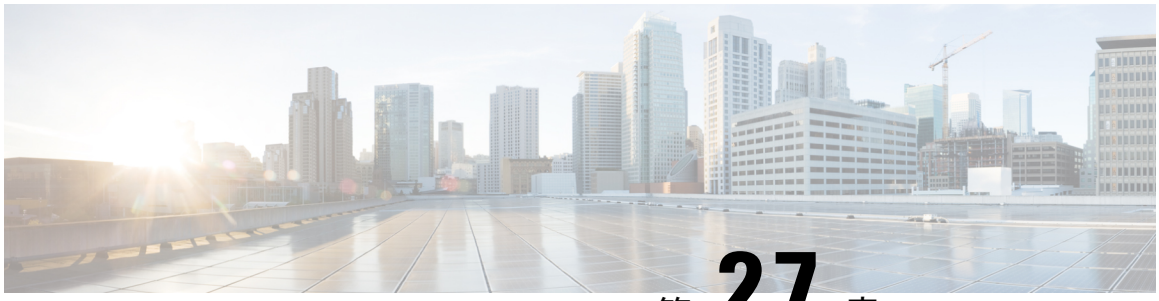
この CLI コマンドの出力は、[Total Pool Kernel Routes] フィールドと [Max Pool Kernel Routes] フィールドを表示するように拡張されています。動的 IPv4 および IPv6 プール数は、IPv4 および IPv6 プールの合計数に置き換えられます。この CLI コマンドの出力には、コンテキストとコンテキストが属する UP グループが表示され、その UP の IP プールと VRF の数に関する情報も追加されます。

エラー コード

次のエラーコードのリストは、CUPS機能でのエンタープライズ オンボーディングのサポートで使用できます。

エラー コード	説明
1001	入力ファイルの解析が失敗したことを示します。
1002	Input_parameters ファイルの解析が失敗したことを示します。
1003	CUPSinfo ファイルの解析が失敗したことを示します。
1004	パスワードを復号できないことを示します。
1005	OpType が入力パラメータに存在しないことを示します。
1006	必要な設定が、特定の OpType の Input_parameters ファイルで使用できないことを示します。
1101	システムの前処理が失敗したことを示します。
1102	特定の OpType に対する CP の事前監査が失敗したことを示します。
1103	<UP_name> に対する UP の事前監査が失敗したことを示します。
1107	選択した SGi コンテキストと UP グループがある CP_APN_Config セクションを、ツールで更新できないことを示します。これは、入力構成ファイルにエラーがあることを示します。
1108	MODIFY_ENTERPRISE 操作で指定された複数の APN が入力ファイルに含まれていることを示します。そのようなポリシーはサポートされていません。
1301	CONTEXT および UPGROUP は選択できないことを示します。

エラー コード	説明
1401	<context_name> および <group_name> が CUPS システムで見つからないことを示します。
1501	**show apn** CLI コマンドの出力から <context_name> を取得できないことを示します。
1601	<control/user plane name> <connection state> の設定が失敗したことを示します。
1602	<control/user plane name> のロールバック設定が失敗したことを示します。
1701	<control plane name> <connection state> の CP 事後監査が失敗したことを示します。
1702	<user plane name> <connection state> の UP 事後監査が失敗したことを示します。
1703	Sx の再関連付けが失敗したことを示します。



第 27 章

CUPS のイベントベースの CDR

この章では、次の事項について説明します。

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

CUPS のイベントベースの CDR

この章では、次の事項について説明します。

機能説明

CUPS アーキテクチャでは、サブスクライバのデータ使用状況を計上するためのイベントベースのコールデータレコード（CDR）の生成がサポートされるようになりました。個別のノードとしてのユーザープレーンとコントロールプレーンで構成される EPC ネットワークでは、デー

タ使用状況を計上するために、これらのエンティティ間のインタラクションが必要になります。

CDR の生成は、コントロールプレーンに不可欠な機能です。コントロールプレーンは、ユーザープレーンとのやり取りを通じて、アップリンクバイト、ダウンリンクバイトなどの使用状況データを受信し、CDR を生成します。これらの CDR は、イベントトリガーに基づいて生成されます。イベントトリガーは、コントロールプレーンのアクセス側または生成された PCRF のいずれかから発生します。ユーザープレーンからこれらのイベントを通じて取得した使用状況データは、CDR で更新されます。

この機能では、次の機能がサポートされます。

- Packet Flow Control Plane（PFCP）セッション変更要求および PFCP セッション変更応答メッセージの交換。
- 設定されたタリフ時間に基づく、ユーザープレーンからコントロールプレーンへの使用状況データのレポート。

（注） この機能の範囲は、P-GW および SAE-GW にのみ制限されます。

機能の仕組み

サブスクライバの使用状況データレポートは、次のメカニズムを使用してユーザープレーンから取得されます。

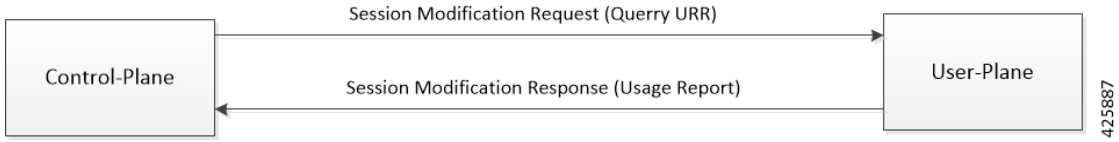
- **プルメカニズム**：コントロールプレーンは、ユーザープレーンに対して使用状況データレポートを照会します。このメカニズムでは、PFCP セッション変更要求 または PFCP セッション変更応答メッセージが使用されます。
- **プッシュメカニズム**：ユーザープレーンが使用状況データレポートをコントロールプレーンに送信します。既存の時間やボリュームベースのプッシュメカニズムと連携するタリフ時間設定が実装されています。このメカニズムでは、PFCP セッションレポート要求またはセッションレポート応答メッセージが使用されます。

使用状況レポートの取得

CUPS アーキテクチャでは、ユーザープレーンは別のノードであるため、コントロールプレーンノードは Sx インターフェイスを介し PFCP プロトコルを使用してユーザープレーンノードと通信し、サブスクライバの使用状況データレポートを取得します。

コントロールプレーンノードは、使用状況データレポートが報告される URR を含む PFCP セッション変更要求を送信します。ユーザープレーンノードは、要求された URR の使用状況データレポートを提供する PFCP セッション変更応答で応答します。

次の図は、コントロールプレーンとユーザープレーン間の相互作用を示しています。



Sx セッション変更交換メッセージの一部として、次の IE がサポートされています。

- **Query URR**：この IE は、コントロールプレーン機能がユーザープレーン機能に即時使用状況レポートを要求する場合に表示されます。同じ IE タイプ内の複数の IE は、即時レポートが要求される URR のリストを表すために存在する場合があります。
- **使用状況レポート**：この IE は、Query URR IE が PFCP セッション変更要求に存在し、その URR のトラフィック使用状況の測定値がユーザープレーン機能で使用可能な場合に存在します。使用状況レポートのリストを表すために、同じ IE タイプ内に複数の IE が存在する場合があります。

タリフ時間

タリフ時間の設定は、非CUPSアーキテクチャですでにサポートされています。CUPSの場合、コントロールプレーンは既存の設定を使用します。コールのセットアップ中、PFCP セッション確立要求は、Monitoring Time IE のタリフ時間を伝送します。これは、SDF URR にのみ適用されます。ベアラーレベル URR にはこの IE はありません。

Monitoring Time IE には、サブスクライバの使用状況データレポートをコントロールプレーンに送信する設定時間が含まれています。設定されたモニタリング時間を経過すると、使用状況データレポートが送信され、次の使用状況データレポートの送信時刻まで自動的に 24 時間進みます。

（注） モニタリングタイマーの次の期限が切れる前に、時間/ボリュームしきい値（設定されている場合）、または PFCP セッション変更要求（Query URR）を使用したコントロールプレーンによる明示的な要求によって、使用状況データが継続的に報告されます。

ユーザープレーンでは、URR のモニタリング時間が経過すると、使用状況レポート IE がコントロールプレーンに送信されます。場合によっては、複数のサブスクライバのモニタリング時間が同時に期限切れになることがあります。コントロールプレーンに送信される使用状況レポートのフラッディングを回避するために、ユーザープレーンはレポートの代わりに、使用状況レポートを伝送する次の発信メッセージ（PFCP セッションレポート要求または PFCP セッション変更応答）で使用状況データをピギーバックします。

PFCPセッション変更要求内のCreate URR IEの一部として、次のIEがサポートされています。

- [Monitoring Time]：この IE には、ユーザープレーン機能がボリュームまたは時間しきい値を再適用する時間が含まれています。
- [Subsequent Volume Threshold]：この IE は、Monitoring Time IE が存在し、ボリュームベースの測定が使用されている場合に存在する可能性があります。存在する場合、トラフィッ

ク量の値を示します。この値を経過すると、モニタリング時間後の期間に、ユーザープレーン機能がそれぞれの URR のコントロールプレーン機能にネットワークリソースの使用状況を報告します。

- [Subsequent Time Threshold]：この IE は、Monitoring Time IE が存在し、時間ベースの測定が使用されている場合に存在する可能性があります。存在する場合、トラフィック時間の値を示します。この値を経過すると、モニタリング時間後の期間に、ユーザープレーン機能がそれぞれの URR のコントロールプレーン機能にネットワークリソースの使用状況を報告します。

（注） 非 CUPS アーキテクチャでは、P-GW はタリフ時間設定で 4 つのタリフ時間インスタンスをサポートしますが、CUPS では、1 つのタリフ時間インスタンスのみがサポートされます。

イベント トリガー

この機能では、イベントトリガーによって部分的な CDR または永続的な CDR が生成されます。部分的なイベントの場合、CDR バケットのみが更新され、実際の CDR は生成されません。ただし、永続的なイベントトリガーでは、完全な CDR が生成されます。

この機能では、次のイベントトリガーがサポートされています。

- ULI の変更（部分的なイベント）
- タイムゾーンの変更（永続的なイベント）
- デフォルトベアラー QoS の変更
- APN-AMBR の変更

（注） このリリースでは、GTPP トリガー **egcdr max-losdv** はサポートされません。

標準準拠

CUPS のイベントベースの CDR は、次の標準規格に基づいています。

- 3GPP TS 29.244: LTE; Interface between the Control Plane and the User Plane of EPC Nodes（3GPP TS 29.244 バージョン 14.0.0 リリース 14）

モニタリングおよびトラブルシューティング

ここでは、CUPS のイベントベースの CDR をサポートするために使用できる show コマンドについて説明します。

show コマンドと出力

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show active-charging subscribers full callid *call_id* urr-info

前述のコマンドを実行すると、次の新しいフィールドが表示されます。

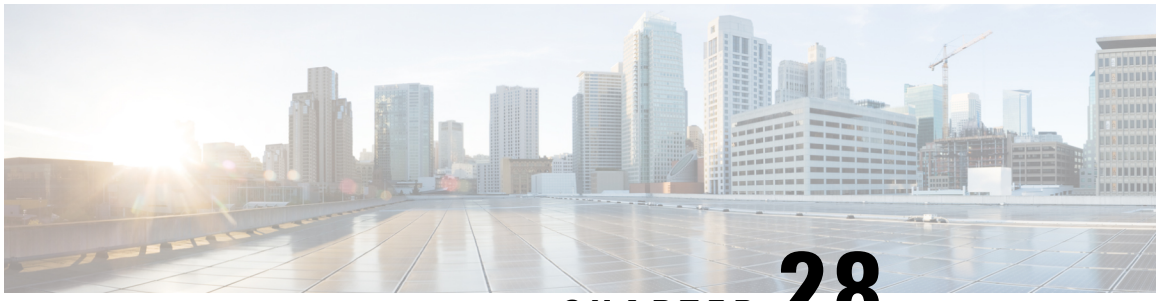
- 次のモニタリング時間
  - 後続時間のしきい値
  - 後続ボリュームのしきい値

show subscribers user-plane-only callid *call_id* urr full all

前述のコマンドを実行すると、次の新しいフィールドが表示されます。

- 次のモニタリング時間
  - 後続時間のしきい値
  - 後続ボリュームのしきい値

show subscribers user-plane-only callid call_id urr full all



CHAPTER 28

CUPS でのイベントデータレコード

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
暫定 EDR 生成のサポートを追加。	21.23.6
初版	21.24 より前

機能説明

イベントデータレコード（EDR）の生成は、CUPS アーキテクチャでサポートされています。

EDR はフローの終了時に生成され、すべてのフローの詳細情報は、フローの終了後に生成されます。

以下は、フローの終了、トランザクションの完了などにより EDR が生成された場合、または必要な条件を満たした場合に入力される EDR フィールドです。

- P2P 期間
- 評価グループ
- RADIUS NAS 識別子

- 3GPP Charging-id
- SN-Parent Protocol-id

LTE ネットワークに接続されたサブスクライバに対して TCP を使用したデータトラフィックが開始された場合は、EDR の TCP フローの制御パケット間の時間差を計算して記録する必要があります。また、次のパケット間の違いを記録する必要があります。

- SYN および SYN-ACK パケット
- SYN-ACK および ACK パケット

TCP Fast Open

TCP Fast Open（TFO）は、2 つのエンドポイント間の連続する TCP 接続をより迅速に開始するための拡張機能です。そのためにこの機能では、クライアントに保存され、サーバーとの初回接続時に設定される暗号化 Cookie である TFO Cookie（TCP オプション）を使用します。その後クライアントが再接続する際、認証のために初回 SYN パケットとともに TFO Cookie データも送信します。認証が成功すると、サーバーは、3 ウェイハンドシェイクの最後の ACK パケットを受信する前であっても、クライアントへのデータ送信を開始できます。このため、SYN-ACK と ACK 間のラウンドトリップ時間（RTT）は、SYN-ACK パケットと最初のアップリンク ACK パケットの差をもとに計算されます。

機能の仕組み

EDR は、フロー終了時に UP から生成されます。コールのセットアップおよびコールの変更時に、EDR 生成に必要なすべてのコール固有の属性が、Sx 確立または変更要求メッセージ内の Subscriber Params IE の一部として CP から UP に送信されます。

フローの終了時に、VPP から課金カウンタが取得されます。EDR 形式の設定で設定されたすべてのコールレベル属性は、課金やボリュームカウンタの属性とともに CDRMOD proclet に送信されます。この proclet により、該当レコードがファイルまたはディスクに書き込まれ、設定された外部サーバーに転送されます。

（注） User-Location-Information は 16 進形式で記述されます。

トランザクション完了 EDR

HTTP トランザクションが完了すると、HTTP EDR に対してトランザクション完了 EDR が生成されます。完了すると、VPP から課金カウンタが取得されます。EDR 形式の設定で設定されたすべてのコールレベル属性は、課金やボリュームカウンタの属性とともに CDRMOD proclet に送信されます。この proclet により、該当レコードがファイルまたはディスクに書き込まれ、設定された外部サーバーに転送されます。

次の EDR 属性のリストがサポートされています。

- attribute sn-start-time
- attribute sn-end-time
- attribute sn-start-time format MM/DD/YYYY-HH:MM:SS:sss
- attribute sn-end-time format MM/DD/YYYY-HH:MM:SS:sss
- attribute radius-calling-station-id
- attribute radius-called-station-id
- rule-variable bearer 3gpp imsi
- rule-variable bearer 3gpp imei
- rule-variable bearer 3gpp rat-type
- rule-variable bearer 3gpp user-location-information
- rule-variable ip subscriber-ip-address
- rule-variable ip dst-address
- attribute sn-ruledef-name
- attribute sn-subscriber-port
- attribute sn-server-port
- attribute sn-app-protocol
- attribute sn-volume-amt ip bytes uplink
- attribute sn-volume-amt ip bytes downlink
- attribute sn-flow-start-time format seconds
- attribute sn-flow-end-time format seconds
- attribute sn-volume-amt ip pkts uplink
- attribute sn-volume-amt ip pkts downlink
- attribute sn-direction
- rule-variable traffic-type
- rule-variable p2p protocol
- rule-variable p2p app-identifier tls-cname
- rule-variable p2p app-identifier tls-sni
- rule-variable p2p app-identifier quic-sni
- rule-variable bearer 3gpp sgsn-address
- attribute sn-rulebase
- attribute sn-charging-action
- rule-variable flow tethered-ip-ttl

- rule-variable flow ttl
- rule-variable flow ip-control-param
- rule-variable bearer qci
- rule-variable tcp flag
- rule-variable ip server-ip-address
- attribute sn-flow-id
- attribute sn-closure-reason
- attribute sn-duration
- rule-variable ip src-address
- rule-variable ip protocol
- attribute sn-charge-volume ip bytes uplink
- attribute sn-charge-volume ip bytes downlink
- tcp-state
- tcp-prev-state

次の HTTP EDR 属性がサポートされています。

- rule-variable http url length 2000
- rule-variable http request method
- rule-variable http content type
- rule-variable http user-agent length 255
- rule-variable http reply code
- rule-variable http referer
- rule-variable http host
- rule-variable http cookie
- rule-variable http header-length
- attribute transaction-uplink-bytes
- attribute transaction-downlink-bytes

暫定 EDR のサポート

ECSは、暫定EDR（設定可能なタイマーに基づいて進行中のフローに対して生成されるEDR）の生成をサポートします。

通常は、フローが終了した場合、またはフローが設定されたフローのアイドルタイムアウト値に達した場合にのみ、フローに対してEDRが生成されます。フローの期間は最大48時間にも

なることがあるため、EDRが生成されるまでサブスクライバのアクティビティの追跡が困難になります。

そのため、暫定 EDR では、フローの暫定タイムアウト値を設定することで、進行中のフローアクティビティが追跡されます。暫定タイマーが期限切れになると、EDR が生成されます。

暫定 EDR を設定するために、新しい CLI キーワード **interim** が導入されました。設定に基づいて、新たに作成されたフローに暫定タイマーが適用されます。タイマーの期限が切れると、暫定EDRが生成され、理由：**sn-closure-reason (23)** が表示されます。タイマーの期限が切れるまで使用可能な情報量が、それぞれのタイムスタンプとともに EDR に入力されます。

制限事項

CUPS のイベントデータレコード機能には、次の制限があります。

- EDR は、フロー終了条件（アイドルタイムアウト、hagr、通常フロー終了、およびセッション終了時）に対してのみ生成されます。
- 課金アクションベースの EDR 設定はサポートされません。
- EDR のレポートはサポートされません。

CUPS でのイベントデータレコードの設定

EDR を UP にプッシュするための CP の設定

PFD メカニズムを使用して CP から UP に EDR をプッシュするには、次の設定を使用します。

（注） この設定で使用される CLI コマンドは、既存の非 CUPS アーキテクチャの一部です。

```
active-charging service service_name
   rulebase rulebase_name
     flow end-condition { timeout | normal-end-signaling | session-end
 | interim  } charging-edr charging_edr_format_name
     edr transaction-complete http charging-edr charging_edr_format_name
     exit
     edr-format format_name
        attribute attribute_name
        end
```

注：

- **flow end-condition**：このコマンドを使用すると、ユーザーセッションに関連するセッションフローの終了条件を設定し、EDR 生成をトリガーできます。

- **timeout**：タイムアウト条件が原因でフローが終了するたびに、指定された EDR 形式で EDR を作成します。
- **normal-end-signaling**：フロー終了が正常に通知されるたびに、指定された EDR 形式で EDR を作成します。
- **session-end**：サブスクライバセッションが終了するたびに、指定された EDR 形式で EDR を作成します。このオプションを使用すると、セッションマネージャは、セッション終了時にフローに対して最後の EDR が作成されてからアクティビティがあったすべてのフローに対して、指定された形式名で EDR を作成します。
- **charging-edr** *charging_edr_format_name*：課金 EDR 形式を指定します。
- **interim**：この条件で、設定されたタイマー値に基づいて EDR が生成されるフローの暫定しきい値条件を指定します。*interim_timer_value* は分単位で設定され、設定可能な範囲は 15 ～ 1,440 分です。
- **interim** キーワードは、新たに作成されたフローにのみ適用され、既存のフローには適用されません。
- **http**：HTTP プロトコル関連の設定を指定します。

UP で EDR モジュールを有効にするための設定

UP で EDR モジュールを有効にするには、次の設定を使用します。

（注） この設定で使用される CLI コマンドは、既存の非 CUPS アーキテクチャの一部です。

```
configure
  context context_name
    edr-module active-charging-service
    end
```

追加の TCP フィールドの設定

次の CLI コマンドを使用して EDR に追加の TCP フィールドを設定する前に、他のすべての EDR 設定が完了していることを確認します。

（注） CUPS セットアップの場合、CP 側の設定が完了したら、CP から **push config-to-up all** コマンドを使用して該当する変更を UP にプッシュします。

```
configure
  active-charging service service_name
    edr-format edr_format_name
      [ no ] rule-variable tcp syn_synack_rtt priority 3
```

```
[ no ] rule-variable tcp syn_synack_ack_rtt priority 4
end
```

モニタリングおよびトラブルシューティング

show user-plane-service statistics rulebase name *rulebase_name*

この機能をサポートするために、次のフィールドが表示されます。

- Rulebase Name
  - EDR
  - Charge Volume
    - Uplink Pkts
    - Uplink Bytes
    - Downlink Pkts
    - Downlink Bytes
  - Charging EDRs
    - Total Charging EDRs generated
    - EDRs generated for handoff
    - EDRs generated for timeout
    - EDRs generated for normal-end-signaling
    - EDRs generated for session end
    - EDRs generated for rule match
    - EDRs generated for hagr
    - EDRs generated for flow-end content-filtering
    - EDRs generated for flow-end url-blacklisting
    - EDRs generated for content-filtering
    - EDRs generated for url-blacklisting
    - EDRs generated for any-error packets
    - EDRs generated for firewall deny rule match
    - EDRs generated for transaction completion
    - EDRs generated for voip call end
    - EDRs generated for dcca failure handling
    - EDRs generated for TCP optimization on

- EDRs generated for tethering signature change
- EDRs generated for interim interval
- Total Flow-Overflow EDRs
- Total zero-byte EDRs suppressed

- EDRs generated for interim
  - Interval

- Total Rulebases

show active-charging rulebase statistics real-time

この機能をサポートするために、次のフィールドが表示されます。

- Rulebase Name
- Charging EDRs
  - Total Charging EDRs generated
    - EDRs generated for handoff
    - EDRs generated for timeout
    - EDRs generated for normal-end-signaling
    - EDRs generated for session end
    - EDRs generated for rule match
    - EDRs generated for hagr
    - EDRs generated for flow-end content-filtering
    - EDRs generated for flow-end url-blacklisting
    - EDRs generated for content-filtering
    - EDRs generated for url-blacklisting
    - EDRs generated for any-error packets
    - EDRs generated for firewall deny rule match
    - EDRs generated for transaction completion
    - EDRs generated for voip call end
    - EDRs generated for dcca failure handling
    - EDRs generated for TCP optimization on
    - EDRs generated for tethering signature change
    - EDRs generated for interim interval

- EDRs generated for audio-end Sessions
- EDRs generated for video-end Sessions
- EDRs generated for voipout-end Sessions
- Total Flow-Overflow EDRs
- Total zero-byte EDRs suppressed

show active-charging edr-format all

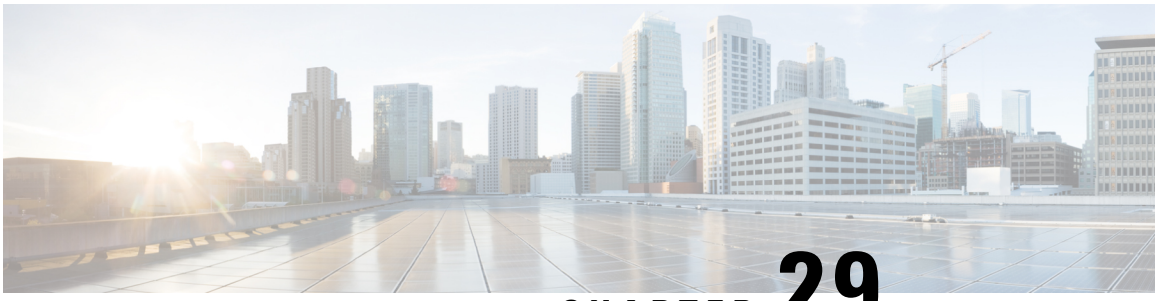
EDR 機能の追加の TCP フィールドをサポートするために、次のフィールドが表示されます。

- サービス名
  - EDR 形式名
    - rule-variable tcp syn-synack-rtt priority 3
    - rule-variable tcp synack-ack-rtt priority 4

バルク統計情報

CUPS のイベントデータレコードをサポートするために、次のバルク統計情報が ECS スキーマに追加されました。

- edrs-generated：生成された EDR の総数を示します。



CHAPTER 29

エラー表示と GTPU パス障害検出

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

ユーザープレーン（UP）機能は、存在しない TEID を持つ GTP-PDU を受信したときに、GTPU ピアの Error Indication メッセージを送信者に通知します。この通知により、古いセッションやベアラーがなくなり、ネットワーク内の一貫性が維持されます。

CP ノードと UP ノード間の Error Indication と GTPU パス障害は、SxA、SxB、および SxAB を介してサポートされます。ネイバーノードの場合は、S1u/S5u インターフェイスでサポートされます。

この実装では、Error Indication および GTPU パス障害用の local-purge または signal-peer の動作のバリエーションが考慮されます。

- Error Indication を受信すると、UP は TEID および GTPU ピア情報を CP に伝達して、GTPU ピアの削除または変更を確認します。

- 存在しない TEID を持つ GTPU パケットを受信すると、UP は Error Indication を生成し、TEID および GTPU ピアエントリを使用して送信します。
- セッションやベアラーの削除は、CP または UP でのパス障害検出に基づいて判断されます。
- GTPU パス障害は、UP ノード間、および UP ノードと CP ノード間の GTPU エコーメッセージを使用して検出されます。

3GPP TS 29.244 に従って、この機能には次のものが実装されています。

- PFCP セッションレポート要求は、PFCP セッションに関連する情報を CP 機能に報告するために、UP 機能によって Sxa および Sxb インターフェイスを介して送信されます。
- PFCP セッションレポート応答は、PFCP セッションレポート要求への応答として、CP 機能によって Sxa および Sxb インターフェイスを介して UP 機能に送信されます。
- レポートタイプが Error Indication Report を示している場合は Error Indication Report IE が存在する必要があります。
- リモート F-TEID は、UP 機能で Error Indication を受信した GTP-U ベアラーのリモート F-TEID を識別するために Error Indication Report で送信されます。
- PFCP ノードレポート要求は、PFCP セッションに固有ではない情報を CP 機能に報告するために、UP 機能によって Sxa および Sxb インターフェイスを介して送信されます。
- PFCP ノードレポート応答は、PFCP ノードレポート要求への応答として、CP 機能によって Sxa、Sxb、Sxc、および N4 インターフェイスを介して UP 機能に送信されます。
- UP パス障害レポートは、ノードレポートタイプがユーザープレーンパス障害レポートを示している場合に表示されます。
- リモート GTP-U ピアには、UP パス障害が検出されたリモート GTP-U ピアの IP アドレスが含まれます。

機能の仕組み

エラー表示のサポート

CP でのエラー表示の処理

CP は、ネイバー UP から UP で受信した Error Indication によってトリガーされた PFCP セッションレポート要求を受信すると、PFCP セッションレポート応答で応答し、PDR、削除用に識別された専用ベアラーの FAR を削除するために PFCP セッション変更要求を UP に送信します。 または、セッションを削除するための PFCP セッション削除要求を送信します。

- セッションまたはベアラーは、それぞれ UP からの PFCP セッション削除応答または PFCP セッション変更応答の受信時に PGW-C でローカルに消去されます。

- SAEGW-C の場合、EGTP を介したシグナリングは、S1u の **local purge** および **page-ue** の設定に基づいています。
- SGW-C の場合、CP 上の EGTP を介したシグナリングは、S1u の **local purge** および **page-ue** 設定、S5u の local-purge および信号ピアに基づいています。

UP でのエラー表示の処理

UP はエラー表示を受信すると 、リモート FTEID を含むエラー通知レポートを使用して PFCP セッションレポート要求を開始します。このリモート FTEID には TEID と GTPU ピアアドレスが含まれます。

- PGW-U の場合、エラー通知メッセージは S5u を介して送受信されます。
- SAEGW-U の場合、エラー通知メッセージは S1u を介して送受信されます。
- SGW-U の場合、エラー通知メッセージは S1u および S5u を介して送受信されます。

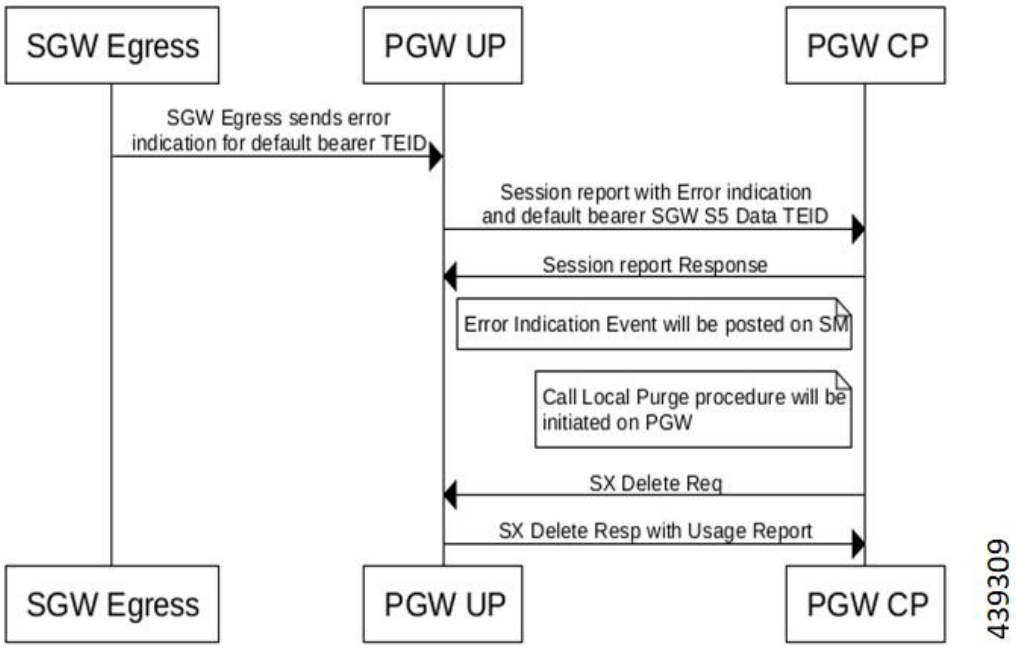
UP でのエラー表示の生成

セッションまたはベアラーが存在しない TEID を使用してデータパケットを受信すると、UP はピアに対して TEID および GTPU ピアアドレスを含む Error Indication を生成します。

エラー表示コールフロー

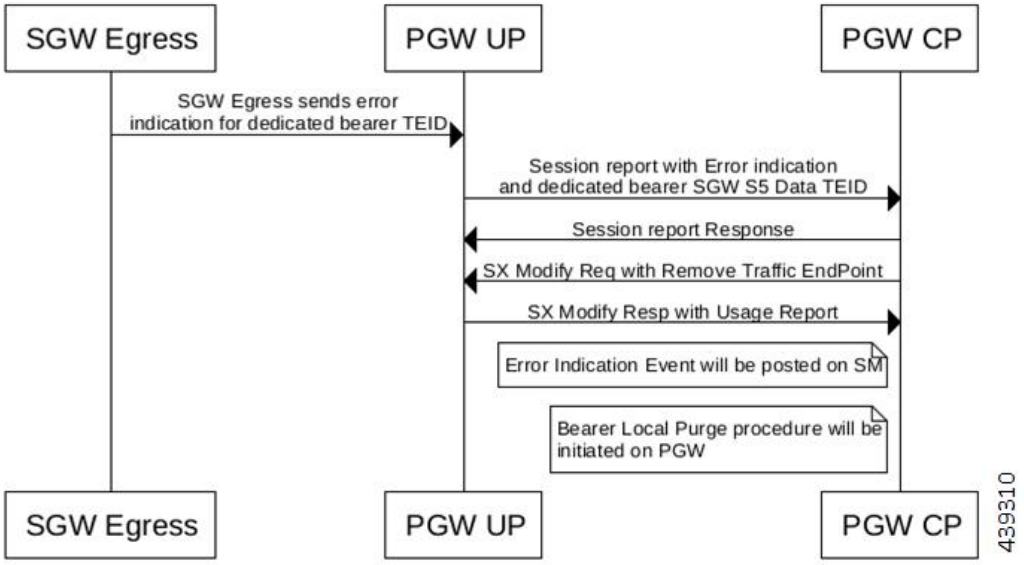
P-GW デフォルトベアラーのエラー通知の処理

次のコールフローは、ローカル消去を伴う P-GW デフォルトベアラーのエラー通知の処理を示しています。



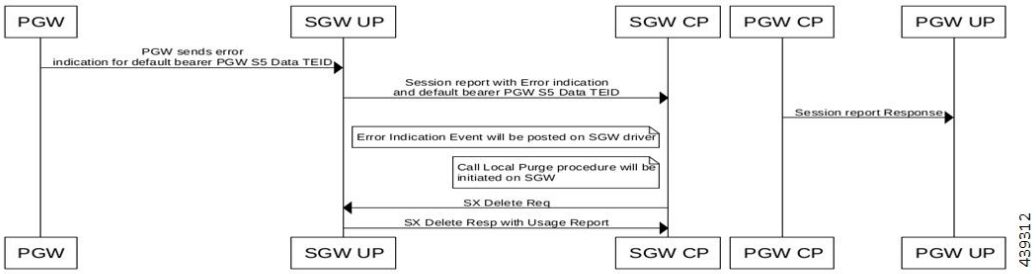
P-GW 専用ベアラーのエラー通知の処理

次のコールフローは、ローカル消去を伴うP-GW専用ベアラーのエラー通知の処理を示しています。



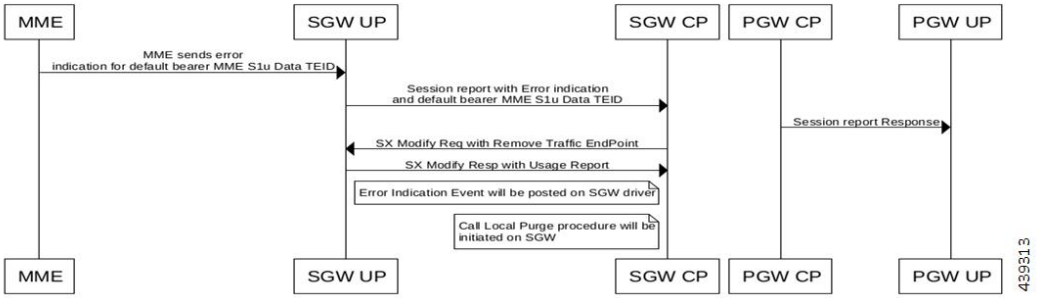
S-GW デフォルトベアラーの通知の処理

次のコールフローは、S5u のローカル消去を伴う S-GW 専用ベアラーのエラー通知の処理を示しています。



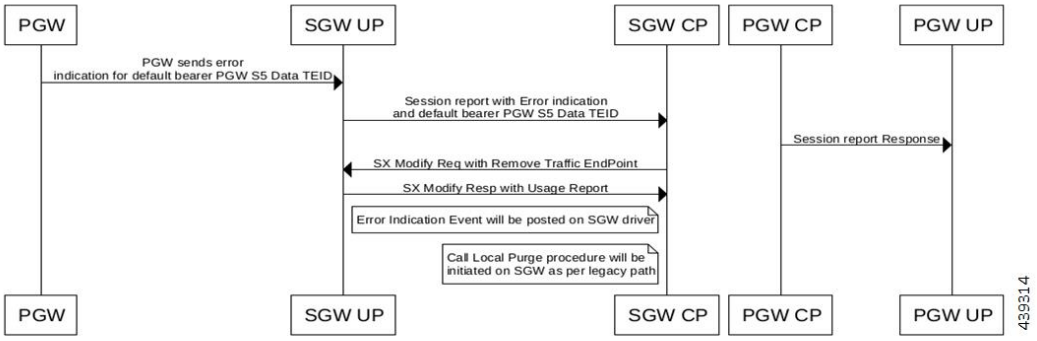
S-GW 専用ベアラーの通知の処理

次のコールフローは、S1u のローカル消去を伴う S-GW 専用ベアラーのエラー通知の処理を示しています。



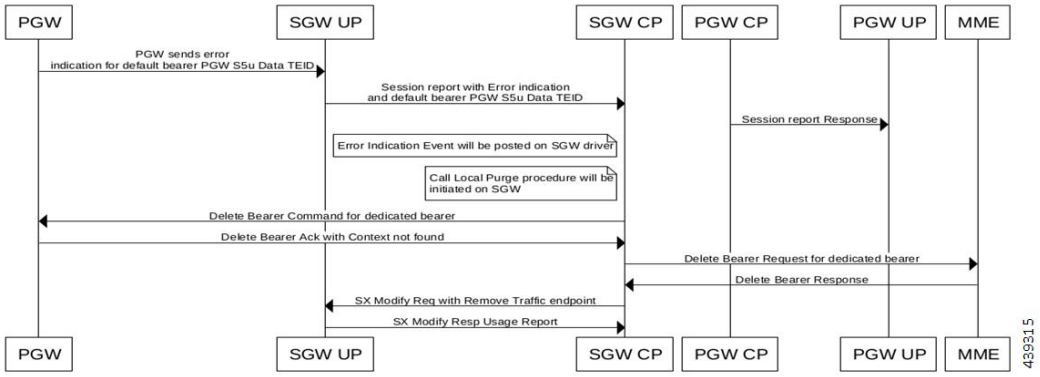
S-GW 専用ベアラーの通知の処理

次のコールフローは、S5u のローカル消去を伴う S-GW 専用ベアラーのエラー通知の処理を示しています。



S-GW 専用ベアラーの通知の処理

次のコールフローは、S5u シグナルピアを使った S-GW 専用ベアラーのエラー通知の処理を示しています。



GTPU パス障害のサポート

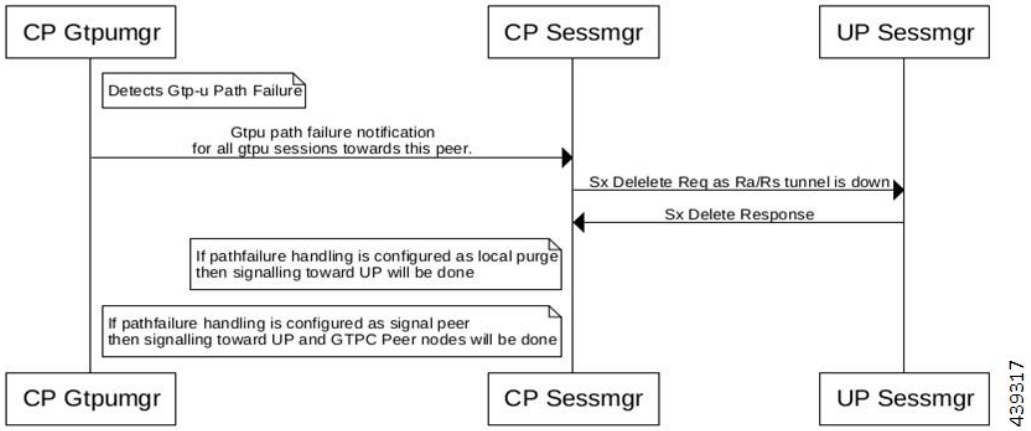
CP での GTPU パス障害のサポート

GTPU エコー要求は、CP で設定された間隔に従って定期的に開始されて送信されます。GTPU エコー応答は、GTPU トンネルを介して UP から受信した GTPU エコー要求に対して送信されます。

GTPU エコー要求に対する応答が受信されない場合、CP は設定された再送信タイムアウトと最大再試行回数に基づいてエコー要求を再試行します。再試行回数が制限を超えると、CP は PFCP セッション削除要求を開始して PFCP セッションを削除します。

CP は UP から PFCP ノードレポート要求を受信すると、 PFCP ノードレポート応答を送信し、UP に対して PFCP セッション削除要求を開始します。PFCP セッション削除応答で使用状況レポートを受信すると、課金レコードが生成されます。

次のコールフローは、CP での GTPU パス障害処理を示しています。



UP での GTPU パス障害のサポート

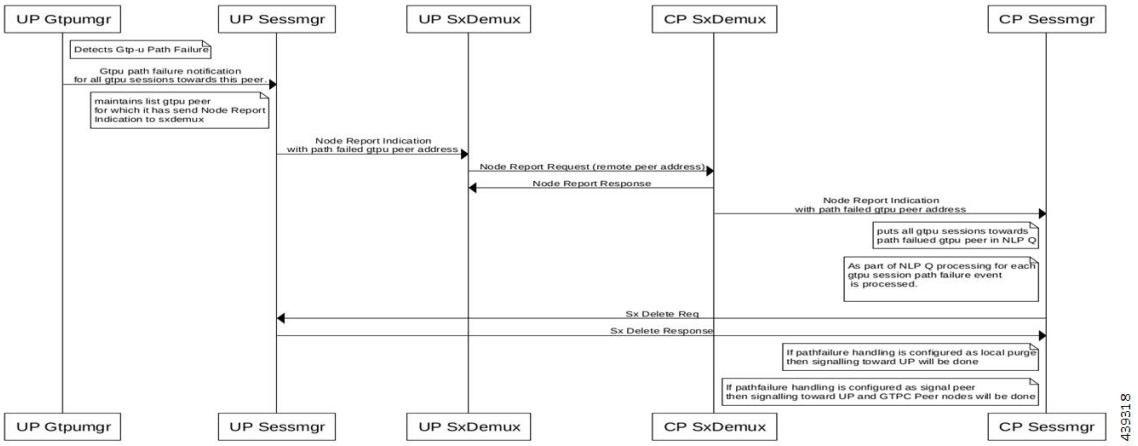
GTPUエコー要求は、UPで設定された間隔に従って定期的に開始されて送信されます。GTPUエコー応答は、GTPU トンネルを介して CP から受信した GTPU エコー要求に対して送信されます。

GTPU エコー要求に対する応答を受信しない場合、UP は設定された再送信タイムアウトと最大再試行回数に基づいてエコー要求を再試行します。再試行が終了すると、UP で PFCP ノードが開始されます。

レポート要求（ノードID、ノードレポートタイプ、リモートGTP-Uピアを含むユーザープレーンパス障害レポート）。

UP は、セッションを削除するための PFCP ノードレポート応答と PFCP セッション削除要求を受信すると、使用状況レポートで削除要求に応答します。

次のコールフローは、UP での GTPU パス障害のサポートを示しています。



制限事項

このリリースでは、エラー表示および GTPU パス障害機能に次の制限事項があります。

- UP が拡張ヘッダーを持つ後続のメッセージやパケットを受信すると、Supported Extension Headers Notification で応答し、拡張ヘッダーがサポートされていないことを隣接する UP に示します。
  - エラー表示
  - GTPU エコー要求
  - GTPU エコー応答
  - GTP-PDU

コントロールプレーンでのエラー表示と GTPU パス障害の設定

CP でのエラー表示の設定

次のコマンドを使用して、GTPUインターフェイス（s1u/s5u）で受信したGTPUエラー通知に基づいて、EGTP ピアに対する CP の動作を制御します。

```
configure
  context context_name
    sgw-service service_name
     gtpu-error-ind { s1u { local-purge | page-ue }| s5u { local-purge
 | signal-peer } }
       end
```

注：

- **gtpu-error-ind**：P-GW から GTP-U エラー通知を受信した場合に実行するアクションを設定します。
- **s1u**：S1u インターフェイス経由で P-GW から GTP-U エラー通知を受信した場合に実行するアクションを指定します。
- **s5u**：S5u インターフェイス経由で P-GW から GTP-U エラー通知を受信した場合に実行するアクションを指定します。
- **local-purge**：S-GW は、ピアに通知せずに、影響を受けるベアラー（またはデフォルトのベアラーでエラー通知が受信された場合は PDN）をクリアします。
- **page-ue**：S-GW は、完全な状態を S1-Idle に移行し、UE のページングを開始します。
- **signal-peer**：影響を受けるベアラーまたは PDN をクリアし、ピア MME および P-GW への制御信号を開始します。

（注） **extension-header source-udp-port** CLI オプションは、ユーザープレーンの GTP-U サービスではサポートされません。

CP での GTPU パス障害の設定

次のコマンドを使用して、GTPUインターフェイス（s1u/s5u）で検出されたGTPUパス障害に基づいて、EGTP ピアに対する CP の動作を制御します。

```
configure
  context context_name
    sgw-service service_name
      path-failure { s1u | s5u }{ local-purge | signal-peer }
      end
```

注：

- **path-failure**：S-GW と MME または P-GW の間でパス障害が発生したときに実行するアクションを設定します。
- **s1u**：S1u インターフェイス経由で P-GW から GTP-U エラー通知を受信した場合に実行するアクションを指定します。
- **s5u**：S5u インターフェイス経由で P-GW から GTP-U エラー通知を受信した場合に実行するアクションを指定します。

- **local-purge**：S-GW は、ピアに通知せずに、影響を受けるベアラー（またはデフォルトのベアラーでエラー通知が受信された場合は PDN）をクリアします。
- **signal-peer**：影響を受けるベアラーまたは PDN をクリアし、ピア MME および P-GW への制御信号を開始します。

制限事項

次の CLI オプションは、このリリースではサポートされません。

- **UP の GTP-U サービス**： **extension-header source-udp-port**
- **CP の SG-W サービス**：

  gtpu-error-ind s4u

  gtpu-error-ind s11u

  gtpu-error-ind s12

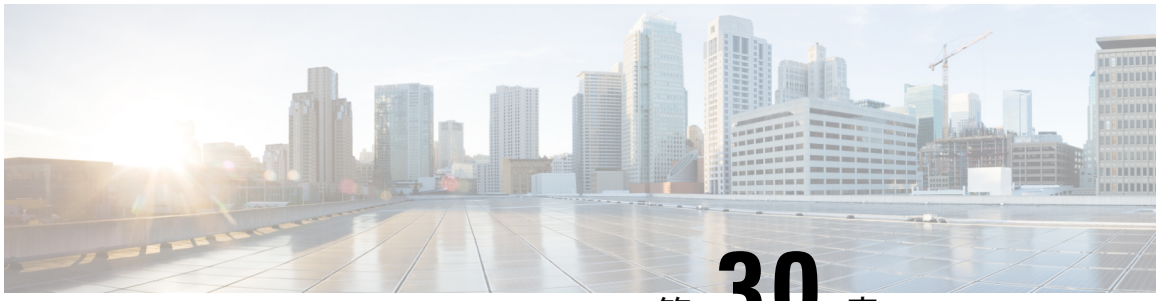
  path-failure s4u

  path-failure s11u

  path-failure s12

エラー通知または GTP-U パス障害に関するユーザープレーンからの Sx セッション変更応答の保留中に、Collapsed から Pure-P へのハンドオーバー要求を受信した場合、遅延していた Sx セッション変更応答の受信後に、ハンドオーバーのためのベアラー変更要求が処理されます。上記のケースでハンドオーバーを正常に完了するため、次の設定が推奨されます。

```
configure
  context egress context_name
    ims-auth-service service_name
      policy-control
        max-outstanding-ccr-u 2
        end
```



第 30 章

CUPS でのファイアウォールのサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

CUPS アーキテクチャのサブスクライバファイアウォール機能を使用すると、ステートレスおよびステートフル パケット インスペクションとパケットフィルタリングを設定して、サブスクライバを悪意のある攻撃から保護できます。ファイアウォールの設定により、システムはサブスクライバ データ セッションの各パケットを検査できます。また、セキュリティ脅威を評価し、アップリンクおよびダウンリンクトラフィックに設定されたポリシーを適用します。

（注） CUPS でのサブスクライバ ファイアウォールの実装は、非 CUPS アーキテクチャでのファイアウォールの実装に似ています。非 CUPS のサブスクライバ ファイアウォールの詳細については、PSF アドミニストレーション ガイド [英語] を参照してください。

概要

ファイアウォール機能は、以下に対応しています。

- DoS 攻撃（DoS attack）
- DDoS 攻撃
- パケットフィルタリング
- ステートレスおよびステートフル パケット インスペクション
- アプリケーション レベル ゲートウェイ
- SNMP のしきい値とロギング

デフォルトのファイアウォール機能の設定

次に、FW ポリシーのデフォルト設定を示します。

```
configure
          active-charging service service_name
            fw-and-nat policy policy_name
            end
```

前述のサービス設定に加えて、サービス内のさまざまな FW 関連 CLI のデフォルトの CLI 動作を次に示します。

```
Dos-Protection:
      Source-Route                          : Disabled
      Win-Nuke                              : Disabled
      Mime-Flood                            : Disabled
      FTP-Bounce                            : Disabled
      IP-Unaligned-Timestamp                : Disabled
      Seq-Number-Prediction                 : Disabled
      TCP-Window-Containment                : Disabled
      Teardrop                              : Disabled
      UDP Flooding                          : Disabled
      ICMP Flooding                         : Disabled
      SYN Flooding                          : Disabled
      Port Scan                             : Disabled
      IPv6 Extension Headers Limit          : Disabled
      IPv6 Hop By Hop Options               : Disabled
      Hop By Hop Router Alert Option        : Disabled
      Hop By Hop Jumbo Payload Option       : Disabled
      Invalid Hop By Hop Options            : Disabled
      Unknown Hop By Hop Options            : Disabled
      IPv6 Destination Options              : Disabled
```

```
  Invalid Destination Options          : Disabled
  Unknown Destination Options          : Disabled
  IPv6 Nested Fragmentation            : Disabled

Max-Packet-Size:
  ICMP                           : 65535
  Non-ICMP                       : 65535
Flooding:
  ICMP limit                     : 1000
  UDP limit                      : 1000
  TCP-SYN limit                  : 1000
  Sampling Interval              : 1

TCP-SYN Flood Intercept:
  Mode                           : None
  Max-Attempts                   : 5
  Retrans-timeout                : 60
  Watch-timeout                  : 30
Mime-Flood Params:
  HTTP Header-Limit              : 16
  HTTP Max-Header-Field-Size     : 4096

No Firewall Ruledef Match Action:
  Uplink Action                  : permit
  Downlink Action                : deny

TCP RST Message Threshold     : Disabled
ICMP Dest-Unreachable Threshold    : Disabled
Action upon receiving TCP SYN packet with ECN/CWR Flag set    : Permit
Action upon receiving a malformed packet  : Deny
Action upon IP Reassembly Failure   : Deny
Action upon receiving an IP packet with invalid Options : Permit
Action upon receiving a TCP packet with invalid Options : Permit
Action upon receiving an ICMP packet with invalid Checksum: Deny
Action upon receiving a TCP packet with invalid Checksum: Deny
Action upon receiving an UDP packet with invalid Checksum: Deny
Action upon receiving an ICMP echo packet with id zero : Permit
TCP Stateful Checks : Enabled
First Packet Non-SYN Action: Drop
ICMP Stateful Checks: Enabled
TCP Partial Connection Timeout: 30
```

IPv4 および IPv6 のファイアウォールの有効化

以下に、IPv4 および IPv6 のファイアウォールを有効にするための設定を示します。

```
configure
         active-charging service service_name
           fw-and-nat policy policy_name
              firewall policy ipv4-and-ipv6
              end
```

サブスクライバ ファイアウォールの設定サポート

コントロールプレーンは、PFD 管理を通じて、サブスクライバ ファイアウォールに必要な設定をユーザープレーンにプッシュします。ファイアウォール設定は、アクティブな課金設定で使用できます。

- Access-Rule-Defs
- Firewall-Nat Policy

ファイアウォール機能を設定すると、ルールベース、APNベース、サブスクライバベースのアクティベーションを使用したファイアウォール機能のアクティベーションがサポートされます。

ここでは、CUPS でサブスクライバファイアウォールを設定する際のさまざまな側面について詳しく説明します。

- config delete コマンドは、設定をただちに削除されます。前述した設定は SCT から削除され、すべてのセッションマネージャからすぐに削除されるため、一括設定タイマーを待つことはありません。
- CP から UP へのファイアウォール設定の追加、削除、変更は、CLI コマンド「push config-to-up all」を使用して伝達します。

モニタリングおよびトラブルシューティング

コントロールプレーンのデフォルトのファイアウォール機能の show コマンド出力を以下に示します。

show config active-charging service name acs verbose

```
fw-and-nat policy SFW_NAT_TEST
      no firewall dos-protection source-router
      no firewall dos-protection winnuke
      no firewall dos-protection mime-flood
      no firewall dos-protection ftp-bounce
      no firewall dos-protection ip-unaligned-timestamp
      no firewall dos-protection tcp-window-containment
      no firewall dos-protection teardrop
      no firewall dos-protection flooding udp
      no firewall dos-protection flooding icmp
      no firewall dos-protection flooding tcp-syn
      no firewall dos-protection port-scan
      no firewall dos-protection ipv6-extension-hdrs
      no firewall dos-protection ipv6-hop-by-hop
      no firewall dos-protection ipv6-hop-by-hop router-alert
      no firewall dos-protection ipv6-hop-by-hop jumbo-payload
      no firewall dos-protection ipv6-hop-by-hop invalid-options
      no firewall dos-protection ipv6-hop-by-hop unknown-options
      no firewall dos-protection ipv6-dst-options
      no firewall dos-protection ipv6-dst-options invalid-options
      no firewall dos-protection ipv6-dst-options unknown-options
      no firewall dos-protection ipv6-frag-hdr nested-fragmentation
      no firewall dos-protection ip-sweep tcp-syn
      no firewall dos-protection ip-sweep udp
      no firewall dos-protection ip-sweep icmp
      firewall max-ip-packet-size 65535 protocol icmp
      firewall max-ip-packet-size 65535 protocol non-icmp
      firewall flooding protocol icmp packet limit 1000
      firewall flooding protocol udp packet limit 1000
      firewall flooding protocol tcp-syn packet limit 1000
      firewall flooding sampling-interval 1
```

```
  firewall tcp-syn-flood-intercept mode none
  firewall tcp-syn-flood-intercept watch-timeout 30
  firewall mime-flood http-headers-limit 16
  firewall mime-flood max-http-header-field-size 4096
  no firewall icmp-destination-unreachable-message-threshold
  access-rule no-ruledef-matches uplink action permit
  access-rule no-ruledef-matches downlink action deny
  firewall tcp-idle-timeout-action reset
  no firewall tcp-reset-message-threshold
  firewall tcp-syn-with-ecn-cwr permit
  firewall malformed-packets drop
  firewall ip-reassembly-failure drop
  no firewall validate-ip-options
  firewall tcp-options-error permit
  firewall icmp-echo-id-zero permit
  firewall icmp-checksum-error drop
  firewall tcp-checksum-error drop
  firewall udp-checksum-error drop
  firewall tcp-fsm first-packet-non-syn drop
  firewall icmp-fsm
  firewall policy ipv4-and-ipv6
  firewall tcp-partial-connection-timeout 30
  no nat policy
  no nat binding-record
  no nat pkts-drop edr-format
  no nat pkts-drop timeout
  default nat suppress-aaa-update
  nat private-ip-flow-timeout 180
  nat check-point-info basic limit-flows 100
  nat check-point-info sip-alg
  nat check-point-info h323-alg
  nat max-chunk-per-realm single-ip
#exit
```

CUPS の show CLI

CUPS の show CLI を次に示します。

ユーザープレーンの場合：

- show subscribers user-plane-only full all
- show subscribers user-plane-only flows
- show user-plane-service inline-services firewall statistics verbose
- show user-plane-service statistics rulebase all
- show alarm outstanding all
- show alarm outstanding all verbose
- show alarm statistics
- show user-plane-service statistics rulebase name <rulebasename>

コントロールプレーンの場合：

- show active-charging fw-and-nat policy all

- show active-charging fw-and-nat policy name "fw_nat_policy_name"
- show active-charging firewall track-list attacking-servers
- show active-charging ruledef name

SNMP トラップ

以下に、CUPS のこの機能をサポートする SNMP トラップを示します。ユーザープレーンでそれぞれの trap CLI を使用して、トラップを有効にします。

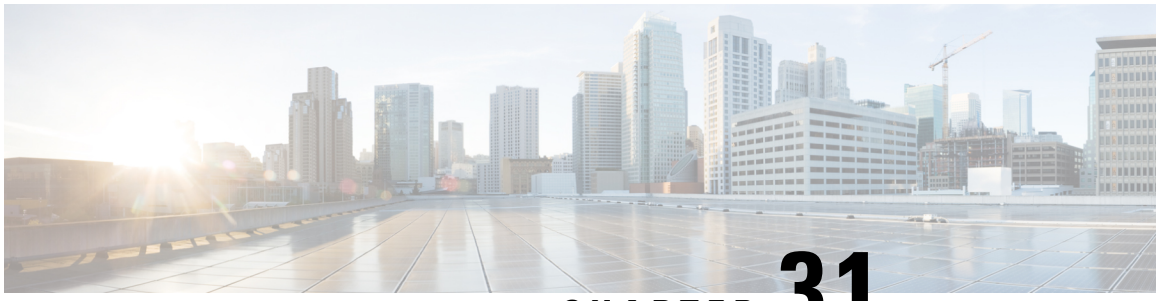
- **Dos-Attacks**：DoS 攻撃の数が設定されたしきい値を超えると SNMP トラップが生成され、設定された時間間隔内に DoS 攻撃の数がしきい値を下回るとトラップがクリアされます。
- **Drop-Packets**：ドロップされたパケットの数がしきい値を超えると SNMP トラップが生成され、設定された時間間隔内にドロップされたパケット数がしきい値を下回るとトラップがクリアされます。
- **Deny-Rule**：拒否ルールの数がしきい値を超えると SNMP トラップが生成され、設定された時間間隔内に拒否ルールの数がしきい値を下回るとトラップがクリアされます。
- **No-Rule**：ルールなしの数がしきい値を超えると SNMP トラップが生成され、設定された時間間隔内にルールなしの数がしきい値を下回るとトラップがクリアされます。

リアセンブル動作の変更

次に、非 CUPS アーキテクチャとは異なる CUPS リアセンブルの詳細を示します。

- 非 CUPS アーキテクチャでは、デフォルトの FW 設定の場合、フラグメントは最大 64K バイトまでバッファリングされます。64K を超えると、バッファリングされたすべてのフラグメントと後続のフラグメントがドロップされます。非 CUPS アーキテクチャでは、この 64K の制限は 30,000 から 65,535 の間で設定可能でした。CUPS では、最大 9K のパケットサイズを最大 6 つのフラグメントにリアセンブルできます。
- 次に、CUPS で廃止された非 CUPS アーキテクチャの 4 つの CLI を示します。
  - firewall dos-protection teardrop
  - firewall dos-protection ipv6-frag-hdr nested-fragmentation
  - firewall max-ip-packet-size <30000-65535> protocol non-icmp
  - o firewall max-ip-packet-size <30000-65535>protocol icmp
- 次に、ティアドロップ攻撃、ネストされたフラグメンテーション、および一般的な ip-reassembly-failure をカバーする単一の CLI を示します。Max-ip-packet-size のサポートは、6 つのフラグメント（最大 9,000 バイト）に制限されます。
  - o Firewall ip-reassembly-failure

- ファイアウォール統計情報のカウンタを次に示します。このカウンタは、リアセンブルに関連するすべての攻撃に対して増分されます。
  - IPv4 リアセンブルの失敗が原因でドロップされたパケット数
  - IPv4 リアセンブル失敗時のダウンリンクドロップバイト数
  - IPv4 リアセンブル失敗時のアップリンクドロップバイト数
  - IPv6 リアセンブルの失敗が原因でドロップされたパケット数
  - IPv6 リアセンブル失敗時のダウンリンクドロップバイト数
  - IPv6 リアセンブル失敗時のアップリンクドロップバイト数



CHAPTER 31

FUI リダイレクト

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
リダイレクト URL の後に元の URL を追加する機能のサポートを追加。	21.28.m10
最初の導入。	21.24 より前

機能説明

CUPS はオンライン課金システム（OCS）で Final Unit Indication（FUI）リダイレクト機能をサポートし、クォータを使い果たしたモバイルサブスクライバに対して自動 URL リダイレクトを設定します。サブスクライバのクォータが使い果たされると、この機能により、事前設定された URL にリダイレクトされます。リダイレクト先でアカウントを再チャージできます。

OCS は Credit Control Answer-Update（CCA-U）メッセージの Diameter 属性値ペア（AVP）のいずれかで FUI リダイレクト情報を送信します。サブスクライバのクォータが使い果たされる前に、これが最後に割り当てられたユニットであることを OCS が UPF に示す必要がある場合に、通常 FUI リダイレクト情報（この機能が OCS で有効になっている場合）が受信されます。

FUI リダイレクト機能は、次の機能をサポートしています。

- HTTP URL を使用した FUI リダイレクト

- HTTP GET 要求の FUI リダイレクト
- FUI リダイレクトの有効期間タイマーの開始を制御するには、**diameter redirect-validity-timer immediate** CLI コマンドを使用します。

  traffic-start キーワード オプションはサポートされていません。
- リダイレクトされた HTTP フローに無料マークを付ける動作を制御するには、**diameter fui-redirected-flow allow** CLI コマンドを使用します。ルールが FUI リダイレクトから実行された場合、リダイレクト対象のトラフィックはリダイレクトされます。
- リダイレクト URL への元の URL の付加

  詳細については、「リダイレクト *URL* への元の *URL* の付加」の項を参照してください。

制限事項

FUI リダイレクション機能には、次の既知の制限事項があります。

- フィルタ ID またはフィルタルールを使用した FUI リダイレクションはサポートされていません。
- トークンベースのメカニズムによるリダイレクションの終了はサポートされていません。
- CUPS では WSP プロトコルはサポートされていません。
- HTTP ヘッダー内のユーザーエージェントの存在を確認するための **redirect-require-user-agent** CLI コマンドはサポートされていません。ユーザーエージェントが設定されていない場合でも、リダイレクションは機能します。

リダイレクト URL への元の URL の付加

UPF は、オンライン課金システム（OCS）によって提供される、URL を使用した動的な課金通知（AoC）のリダイレクトをサポートします。このリダイレクトは、特定のサービス ID/料金設定グループの組み合わせに対して実行されるもので、他のサービス ID/料金設定グループの組み合わせにマッピングされたフローには影響しません。

AoC またはトップアップサーバーへのリダイレクトの場合、UPF はリダイレクトされたセッションに元の HTTP URL を追加します。リダイレクトの元の URL を追加するため、OCS は特殊文字「?」を AoC リダイレクトの末尾に追加します。リダイレクト URL には、**diameter redirect-url-token** コマンドで設定されたトークン名を使用して元の URL 情報が追加されます。AoC サーバーは、AoC 完了時にユーザーを元の場所にリダイレクトします。

機能の仕組み

以下に、リダイレクトの前に元の URL を付け加える手順を示します。

1. リダイレクト URL では、OCS によって提供される AoC ページの末尾の「?」が「&」記号に置き換えられます。
2. 設定可能なパラメータは、この「&」記号の後に追加されます。パラメータ名では大文字と小文字が区別されます。

   パラメータが設定されていない場合は、「&」記号の後にデフォルトの文字列が追加されます。
3. パラメータの後に「=」が追加されます。
4. 「=」記号の後にサブスクライバの元の URL が追加されます。
5. 元の URL はパーセントエンコードされます。

例：

元の URL：

```
http://homepage/
```

OCS が提供する URL：

```
http://test.dev.mms.ag/test/aoc.htm?appName=Return&CODE=UPSELL&OCSCode=FWB&SessionID=4:0001-diamproxy.st40gy2;
130020198;9243;1b02:12000:12000:H:AOC:1299597546:UPSELL:N&transID=AOCPurchasepage?
```

追加後の URL：

```
http://test.dev.mms.ag/test/aoc.htm?appName=Return&CODE=UPSELL&OCSCode=FWB&SessionID=4:0001-diamproxy.st40gy2;
130020198;9243;1b02:12000:12000:H:AOC:1299597546:UPSELL:N&transID=AOCPurchasepage&returnUrl=http%3A%2F%2Fhomepage%2F
```

制限事項

この機能には、次の既知の制限事項があります。

- URL 解析を有効にする既存の設定がない場合、リダイレクト URL は元の URL に追加されません。

リダイレクト URL トークンの設定

リダイレクト URL トークンの設定

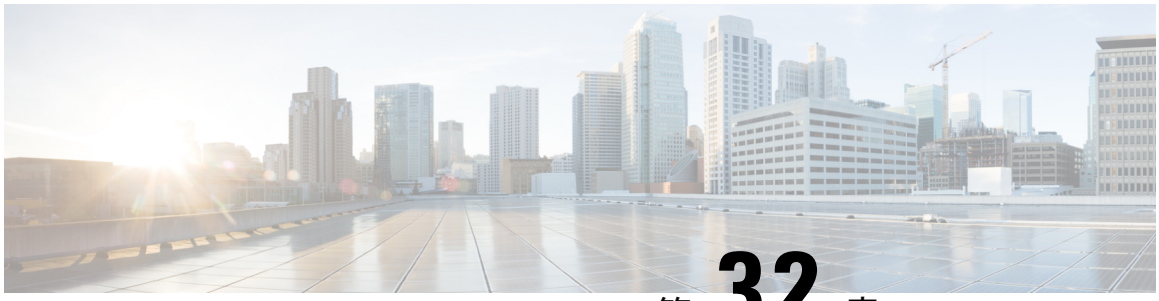
リダイレクトアドレスに元の URL を追加するためのトークンを設定するには、次の設定を使用します。

```
configure
  active-charging service service_name
    credit-control
      diameter redirect-url-token token_string
      exit
```

注：

- **diameter redirect-url-token** *token_string*：リダイレクト URL トークン名を、1 ～ 63 文字の英数字文字列として指定します。

- このコマンドを設定せず、受信した URL の末尾が「?」文字の場合、デフォルトの文字列「returnurl」が「&」文字の後に追加されます。



第 32 章

GTPC ピアレコードと統計の最適化

マニュアルの変更履歴

改訂の詳細	リリース
初版	21.26

機能説明

ゲートウェイがピアから最初のGTPCメッセージを受信すると、新しいピアレコードエントリがセッションマネージャと Demux に追加されます。この新しいピアレコードエントリは、すべてのセッションマネージャにも伝播されます。このプロセスは、特定の GTPC ピアにアクティブなセッションがない場合でも発生します。これにより、非アクティブなピアレコードオブジェクトが蓄積され、セッションマネージャと Demux のメモリが過剰に使用され、影響を受ける Proclet のメモリオーバーランが発生します。この制限に対処するために、コンテキスト コンフィギュレーション モードでは、既存の **gtpc** CLI に新しいキーワード **peer-salvation** が追加されました。

機能の仕組み

peer-salvation キーワードがコンテキストレベルで有効になっている場合、次の動作がサポートされます。

- アクティブセッションの数が「0」でピアが非アクティブになると、そのピアレコードオブジェクトにタイムスタンプが保存され、ピアレコードが非アクティブピアリストに挿入されます。
- 非アクティブピアに新しいセッションが追加されると、タイムスタンプが「0」にリセットされ、ピアレコードエントリが非アクティブピアリストから削除されるため、再アクティブ化されたピアの復旧が回避されます。
- egtpmgr インスタンスレベルで 1 時間のタイムアウトが設定されていても、コンテキストレベルでキーワードが無効になっている場合には、タイムアウトは無効となります。
- egtpinmgr と egtpegmgr に対して個別の復旧タイマーが実行されます。
- デフォルト（キーワードが有効になっていない状態）では、メモリと CPU への影響を最小限に抑えるため復旧タイマーは実行されません。

Demux セッションリカバリシナリオ

Demux proclet がクラッシュまたは再起動すると、すべての非アクティブピアに関連するあらゆる情報が proclet でクリアされ、Demux のセッションリカバリ中に再度追加されることはありません。Demux にサービスを提供するセッションマネージャに蓄積されたこれらの非アクティブピアレコードは、復旧されない可能性があります。ピア復旧機能は、非アクティブピアリストをリカバリ済みの Demux で再構築します。非アクティブピアの最後のアクティビティタイムアウトが Demux リカバリのタイムスタンプに設定されるため、Demux は Demux リカバリ後でも動作できます。

Demux シャーシ間セッションリカバリシナリオ

peer-salvation キーワードは、アクティブシャーシとスタンバイシャーシで設定できます。設定すると、スタンバイシャーシに蓄積された非アクティブピアを復旧することもできます。

セッションマネージャのセッションリカバリ/ICSR シナリオ

peer-salvation キーワードを設定しても、セッションマネージャのリカバリまたは ICSR には影響しません。その逆も同様に影響はありません。

制限事項と制約事項

次に、peer-salvation キーワードを有効にする際の既知の制限事項と制約事項を示します。

- peer-salvation キーワードがコンテキストレベルで有効になっていて、egtp-service レベルで有効になっていない場合、ピアは復旧されません。
- 特定のピアのすべての情報（ピア統計情報やリカバリカウンタなど）は、回収後に失われます。
- コンテキストレベルの設定は、egtpinmgr と egtpegmgr 個別に適用されます。

- min-peers 値は、完全にロードされたシャーシのセッションマネージャが多くのピアレコードで警告/オーバー状態にならないように、慎重に適用する必要があります。セッションマネージャが警告/オーバー状態になった場合は、ピアが確実に復旧されるように、min-peers を小さい値に設定することを推奨します。
- min-peers 設定は、新しいピアの作成時に考慮されません。
- 設定されたタイムアウト値の間、セッション数がゼロのピアのみが復旧されます。セッション数が少なくても、セッション数がゼロ以外の場合は復旧されません。

ピア復旧機能の設定

次の項では、この機能を有効または無効にするための設定コマンドについて説明します。

gtpc peer-salvation（コンテキスト設定モード）

このコマンドを使用して、EGTP サービスの非アクティブな GTPv2 ピアの peer-salvation を有効にします。[Context Configuration] モードに peer-salvation キーワードが導入されました。この CLI により、そのコンテキストで設定されたすべての egtp-services にまたがる egtpmgr ごとの（egtpinmgr と egtpegmgr でそれぞれ別の）最小ピア数とタイムアウト値を指定できます。

[Context Configuration] モードで peer-salvation を設定するには、次のコマンドを入力します。

```
configure
  context  context_name
    [ no ] gtpc peer-salvation min-peers value timeout value
    end
```

注：

- **no**

  ：コンテキストレベルでピア復旧を無効にします。

- **peer-salvation**

  ：このコンテキストで、EGTP サービスの非アクティブな GTPv2 ピアのピア復旧を有効にします。

- **min-peers***value*

  ：すべての EGTP サービスの累積 GTPv2 ピア数が最低いくつに達したら、非アクティブなピアの復旧を開始するかを設定します。値の範囲は 2,000 ～ 12,000 です。

- **timeout***value*

  ：ピア復旧タイムアウトを設定します。復旧期間（時間単位で指定）に非アクティブなピアが復旧されます。値の範囲は 1 ～ 48 時間です。

- このコマンドは、デフォルトで無効になっています。

gtpc peer-salvation（eGTP サービス設定モード）

このコマンドを使用して、EGTP サービスの非アクティブな GTPv2 ピアの peer-salvation を有効にします。peer-salvation キーワードが eGTP サービス コンフィギュレーション モードの既存の gtpc コマンドに追加されました。有効にすると、この機能は特定の egtp-service レベルで有効になります。この機能が egtp-service レベルで有効になっている場合は、コンテキストレベルで有効にする必要があります。設定順序は、この機能を有効にすることには依存しません。

eGTP サービス コンフィギュレーション モードで peer-salvation を設定するには、次のコマンドを入力します。

```
configure
  context context_name
    egtp-service egtp_service_name
    [ no ] gtpc peer-salvation
    end
```

注：

- **no**

  ：コンテキストレベルでピア復旧を無効にします。

- **peer-salvation**

  ：このコンテキストで、EGTP サービスの非アクティブな GTPv2 ピアのピア復旧を有効にします。

- このコマンドは、デフォルトで無効になっています。

モニタリングおよびトラブルシューティング

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show コマンドと出力

この機能をサポートするために、次の CLI コマンドの出力範囲が拡張されています。

gtpc peer-salvation debug-mode debug-min-peers *value1* **debug-timeout** *value2*

show egtp-service all

このコマンドの出力範囲が拡張され、ピア復旧機能をサポートする次の新しいフィールドが追加されました。

- GTPC Peer Salvation

show session subsystem debug-info

このコマンドの出力が拡張され、ピア復旧機能をサポートする次の新しいフィールドが追加されました。

- ピア復旧統計
  - sessmgr で受信したピア復旧要求の数
  - sessmgr で復旧されたピアの数

show demux-mgr statistics egtpinmgr all

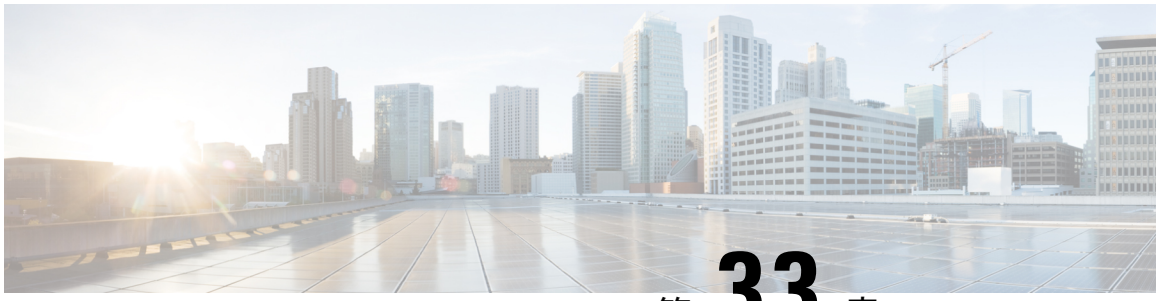
このコマンドの出力が拡張され、ピア復旧機能をサポートする次の新しいフィールドが追加されました。

- ピア復旧統計
  - demux によって送信されたピア復旧要求の数。
  - demux で復旧されたピアの数。

show demux-mgr statistics egtpegmgr all

このコマンドの出力が拡張され、ピア復旧機能をサポートする次の新しいフィールドが追加されました。

- ピア復旧統計
  - demux によって送信されたピア復旧要求の数
  - demux で復旧されたピアの数



第 33 章

Gx エイリアスの機能拡張

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

Gx エイリアス拡張機能は、単一の Gx エイリアスルール名を使用して、事前定義ルールのセットを複数インストールする手法です。このルール名は PCRF から取得され、PCEF に対して透過的です。PCRF は、各ルールに名前を付けることでそのルールをアクティブ化または非アクティブ化します。

この機能は、デフォルトベアラーにのみインストールされるルールに適用されます。多数のルールを正常にインストールするには、[ACS Configuration] モードで **no policy-control update-default-bearer** CLI コマンドを設定するか、[ACS Rulebase Configuration] モードで **no tft-notify-ue-def-bearer** CLI コマンドを設定して、rulebase ごとに実装する必要があります。[Gx-alias Group of Ruledef (GoR)] で定義されているすべての ruledef は、セッションに適用されるように rulebase でも定義する必要があります。

機能の仕組み

CP は Gx エイリアスの GoR を拡張し、PDR ID をこれらのインストール済みのルールに割り当て、ベンダー固有の TLV で情報を伝送します。この情報の一部として、開始 PDR ID と終了 PDR ID を含む Gx エイリアス名が UP に送信されます。UP は、この新しい TLV を受信した後、Gx エイリアスを ruledef に展開し、UP の設定に準拠した順序で対応する PDR ID をマッピングします。

Gx エイリアス拡張機能の機能/動作は次のとおりです。

- CP、UP ともに、Gx エイリアス GoR の内容および順序は、設定の更新の前後でまったく同じです。
- Gx エイリアス GoR への新しい ruledef の追加は、新しいセッションにのみ適用されます。既存のセッションで処理されるのは、Gx エイリアス GoR からの ruledef の削除のみです。
- Gx エイリアスが ruledef にマッピングされている場合、UP の事前定義ルール機能は効果がありません。つまり、URR-ID/課金は、使用されている Gx エイリアスに対して透過的です。

注：

- 設定可能な GoR の上限：64
- GoR あたりのルールの最大数：512
- デフォルトベアラーあたりのルールの最大数：2048

Gx エイリアスの IE フォーマット

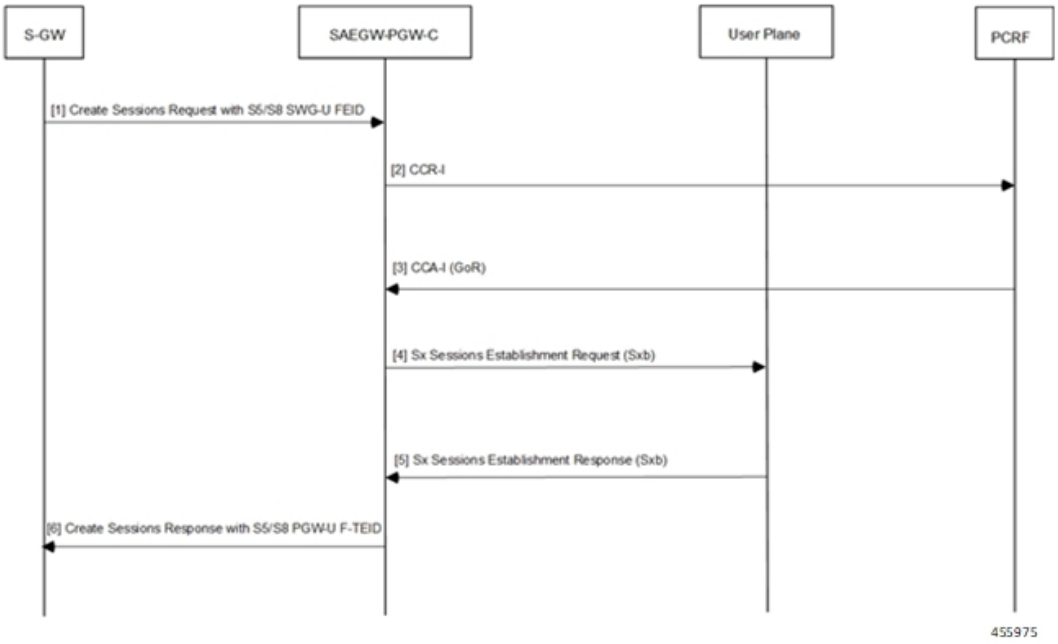
次の表に、Gx エイリアス機能の IE フォーマットとエンコーディングに関する情報を示します。

	ビット								
オクテット	8	7	6	5	4	3	2	1	
1 ～ 2	タイプ = 246（10 進数）								
3 ～ 4	長さ n [最小 = 7、最大 = 69 {5+ACSCTRL_GRP_OF_RDEFS_NAMELEN (64)}]								
5	フラグ（GoR ルールの追加/削除） 例：GoR にルールを追加する場合は「1」、削除する場合は「0」								
6 ～ 7	開始 PDR ID								
8 ～ 9	終了 PDR ID								
10 ～ n+4	Gx エイリアス GoR 名（最小サイズ = 2、最大サイズ = 64）								

PFCP_IE_GX_ALIAS：Gx エイリアス GoR 名、開始および終了 PDR ID、および Sx セッション確立/変更要求メッセージ中にコントロールプレーンからユーザープレーンに実行する操作を伝達する IE。

通話フロー

ここでは、Gx エイリアス拡張コールフローについて説明します。



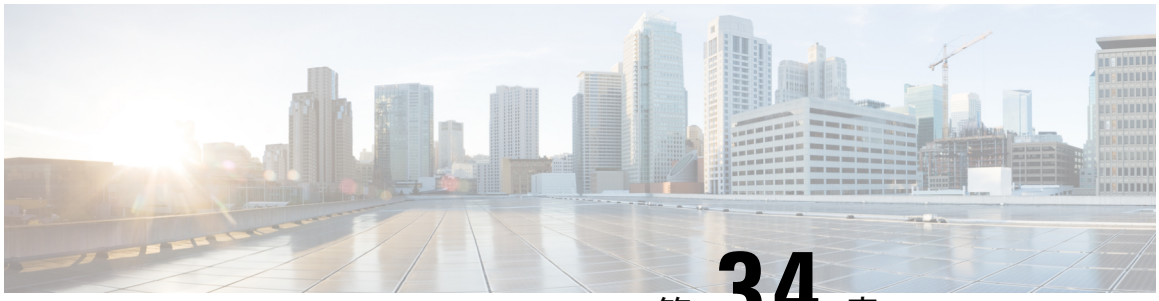
ステップ	説明
1	S-GW が SAEGW-PGW-C に S5/S8 SGW-U FEID を含むセッション作成要求を送信します。
2	SAEGW は、PCRF との Gx 通信 CCR-I を実行します。 CUPS SAEGW の Pure-P コール中に、SAEGW-PGW-C は次の処理を実行します。 • Gx インタラクション後、PCRF との Gx 通信（CCR-I および CCA-I）を実行する。 • IP プール（APN に関連付けられた IP プール）が設定されたユーザー プレーン プロファイルに基づいて、ユーザープレーンの選択を実行する。 • IPv6/IPv4v6 PDN の RA/RS に必要な GTP-U セッションを確立する。 • 選択したユーザープレーンとの Sxab インタラクションを実行する。

ステップ	説明
3	PCRF は、SAEGW との Gx 通信 CCA-I を実行します。 Sx 確立要求セッションには、次の情報が含まれます。 • アップリンクおよびダウンリンクデータパスの GoR/GoR アクション/FAR/URR 情報：ダイナミック/事前定義/静的ルール。 • また、コントロールプレーンは、P-GW 入力（PDR S5/S8 PGW-U F-TEID）に F-TEID を割り当てるようユーザープレーンに要求します。Gx エイリアス GoR では、ruledef は、Day-0 設定の一部であるコントロールプレーンとユーザープレーンで同じ順序内にある必要があります。新しく設定されたルールは、シスコ固有のコントロールプレーンおよびユーザープレーンのノードペアである新しいセッションにのみ適用されます。
4	SAEGW は、ユーザープレーンとの Sx セッション確立要求（Sxb）を確立します。 Gx エイリアスの新しい IE フォーマットである PFCP_IE_GX_ALIAS は、次のアクションを実行します。 • Gx エイリアス GoR（Group-of-Ruledef）名の通信 • 開始/終了 PDR ID • Sx セッションの確立/変更要求メッセージ中の、コントロールプレーンからユーザープレーンに対する操作
5	ユーザープレーンは、Sx セッション確立応答の一部として「P-GW ingress PDR S5/S8-U PGW F-TIED」情報を提供し、SAEGW-PGW-C との Sx セッション確立応答（Sxb）を確立します。
6	Sx セッション確立応答を受信すると、SAEGW-PGW-C は「S5/S8-U PGW F-TEID」を含むセッション作成応答を S-GW に送信します。

制限事項

この機能には次の既知の制限事項があります。

- IE 処理は、シスコがサポートするコントロールプレーンとユーザープレーンのノード間でのみ適用されます。Gx エイリアス GoR で設定された ruledef はすべて、デフォルトのベアラーにのみバインドされます。
- リカバリ時間の超過を回避するために、セッションリカバリ時には 8 つの GoR のみリカバリされます。設定する GoR の推奨最大数は 8 です。
- 2,048 個のルールを使用すると、セッションのスケーリングに影響が出る可能性があります。デフォルトベアラーごとのルールの推奨最大数は 1,000 です。



第 34 章

UP の Gx AVP の識別

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.27

機能説明

重複 IP プールを使用する場合、ポリシー/課金ルール機能（PCRF）でセッションを一意に識別するために、パケットデータネットワーク（PDN）の IP アドレスと UP 機能 ID または ID/識別の両方が必要です。UE にサービスを提供する UP に関する情報は、CP から PCRF によって受信されます。この情報により、PCRF は収集した詳細をもとに新しいマスターキーを作成できます。PCRF は、UE にサービスを提供する UP の ID を取得できます。この情報は、Diameter ダイナミックディクショナリ設定を使用して Gx 経由で送信されます。

パケットデータネットワーク（PDN）セッションの確立中に、System Architecture Evolution Gateway コントロールプレーン（SAEGW-C）は、Gx インターフェイスを介して UP の ID を伝達できます。この新しい AVP は、（該当する場合には）SAEGW-C によって Gx CCR-I および対応する Gx CCR-x メッセージに含まれます。

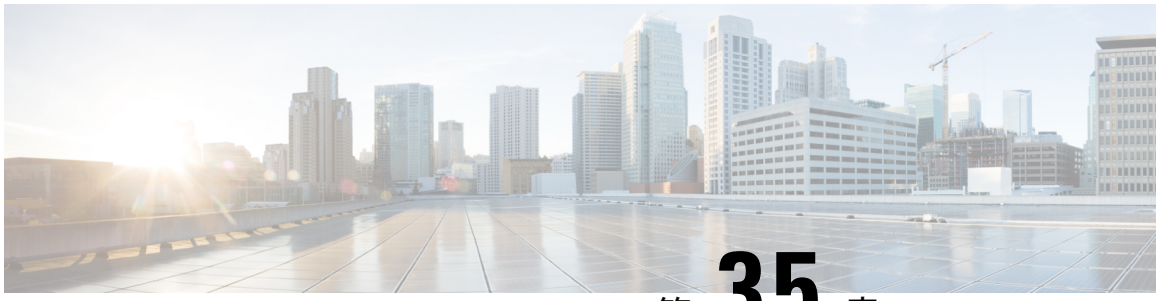
Gx 属性値ペア（AVP）

UP-IP-Address AVP（コード番号 132099）はアドレスタイプであり、UP IP アドレスを含んでいます。IP アドレスタイプには、IPv4 アドレスと IPv6 アドレスの両方が含まれます。AVP は、関連するすべての Gx CCR-x メッセージでサポートされます。

AVP の詳細は次のとおりです。

- AVP 名：**UP-IP-Address**
- AVP コード：132099
- ベンダー ID：9（Cisco）
- 必須フラグ：不要
- ベンダー固有フラグ：必須
- AVP タイプ：アドレス
- 親 AVP：該当なし
- この AVP は、SAEGW-C から PCRF への CCR-I メッセージでエンコードされます。

（注） **UP-IP-Address** AVP で報告されるアドレスは、**show subscribers saegw-only full all** の UP アドレスです。これは、UP の **user-plane-service** に関連付けられた **sx-service** です。



第 35 章

異なる RG を使用した異なる DRA からの同時 Gy RAR の処理

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.28.m1

機能説明

CUPS は複数の Diameter Routing Agent（DRA）をサポートし、Gy インターフェイス上の別のホストやピアを使用した以前の再認証要求（RAR）の保留中のクレジット制御要求更新（CCR-U）要求の中止を防ぎます。

P-GW は、ACS コンフィギュレーション モードで **diameter pending-ccau allow-on-rar-peer-switch** CLI コマンドを設定することで、さまざまなピアの異なる評価グループ（RG）を受け入れます。このコマンドを使用すると、保留中の CCR-U 要求を中止しないように DCCA クライアントを設定できます。

P-GW における複数の DRA サポートの詳細については、P-GW アドミニストレーション ガイド [英語] の「Support for Multiple DRA over Gy Interface」の章を参照してください。

機能の仕組み

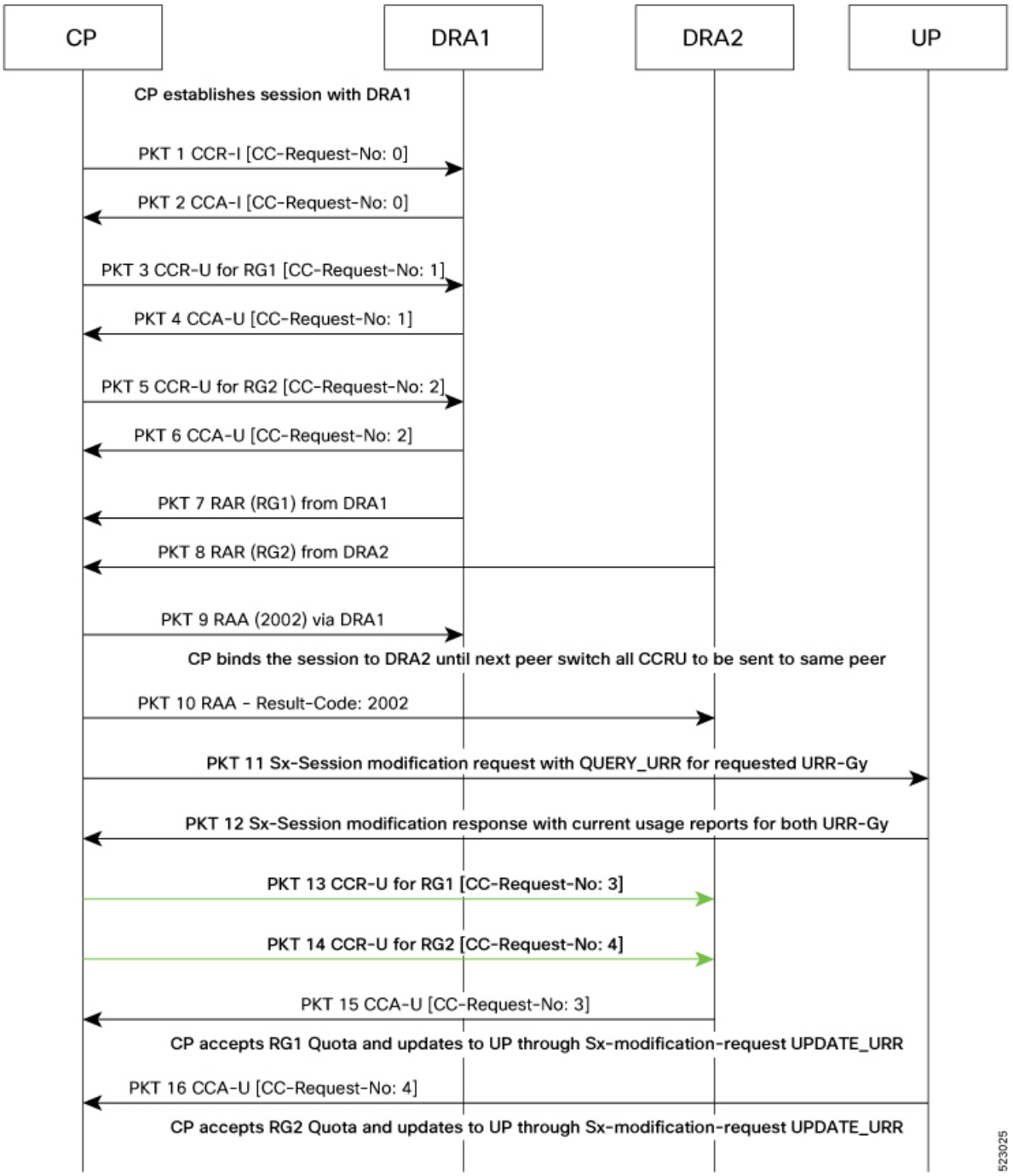
この項では、CUPS での複数 DRA 機能の動作について説明します。

P-GW と CUPS では、コリジョンシナリオの処理方法が異なります。レガシー P-GW では、FORCED REAUTHORIZATION が設定された各 CCR-U が対応する DRA に送信されます。

CUPS では、ユーザープレーンは現在の使用状況レポートとともに送信されるすべての CCR-U を取得します。コリジョン中に、それぞれの評価グループの異なる DRA から複数の特定の RAR を同時に受信した場合、コントロールプレーンが Gy-URR バケットをマークし、Sx セッション変更要求をユーザープレーンに送信します。ユーザープレーンは、要求された Gy-URR バケットの現在の使用状況レポートを Sx セッション変更応答でコントロールプレーンに送り返します。異なる DRA から RAR を受信すると、ピアの切り替えが行われます。CUPS では、要求された評価グループの FORCED REAUTHORIZATION が設定された各 CCR-U が、スイッチされた最新のパスのピア DRA に送信されます。

次のコールフローは、P-GW が異なるピアから両方の RG を受け入れる方法を示しています。

図 *12 : CUPS* での複数の *DRA* コールフロー



機能の設定

複数の DRA を含む複数の RAR 要求に関する処理を設定するには、次の設定を使用します。

```
configure
  context context_name
  active-charging service acs_service_name
    credit-control [ group cc_group_name ]
      diameter dictionary dictionary
        [ no ] diameter pending-ccau allow-on-rar-peer-switch
        end
```

注：

- **diameter dictionary** *dictionary*：さまざまな DRA を処理するように Diameter ディクショナリを設定します。

  例：**diameter dictionary** *dcca-custom-26*

- **diameter pending-ccau allow-on-rar-peer-switch**：DCCA クライアントが保留中の CCAU 要求の中止を防ぐことを許可します。
- **no diameter pending-ccau allow-on-rar-peer-switch**：DCCA クライアントが保留中の CCAU 要求の中止を防ぐことを無効にします。

モニタリングおよびトラブルシューティング

この項では、複数の DRA 機能のモニタリングおよび障害対応情報について説明します。

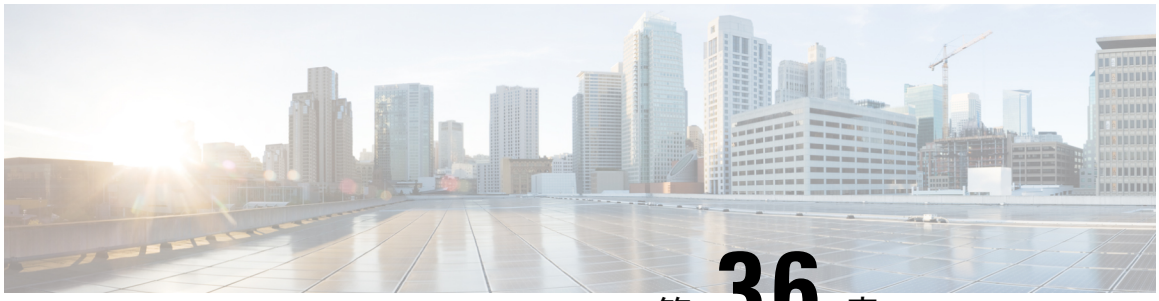
show コマンドと出力

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show active-charging service all

表 *10 : show active-charging service all*

フィールド	説明
保留中の CCA-U:	
allow-on-rar-peer-switch	Gy インターフェイス上の別のホストまたはピアから RAR を受信した場合に、保留中の CCA-U 要求の中止が「Enabled」か「Disabled」かを表示します。この機能が有効になっている場合、この機能は新しい Diameter セッションにのみ適用されます。



第 36 章

ホストルートの明示的なアドバタイズメント

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.27

機能説明

SAEGW-C フェールオーバー中に、UE セッションが確立されると、IP バックボーンにアドバタイズされた IP チャンクサブネットルートが障害のあるサイトからのものである場合、使用できなくなります。

機能の仕組み

IP プールの設定時に IP プールが作成されると、IP プールはチャンクに分割され、チャンクサイズとともにプール構造に保存されます。

UP は、パケット転送制御プロトコル（PFCP）メッセージ **Sx-Association Update** 要求を使用して、CP からチャンクの割り当ての詳細を受信します。UP によってインストールされた IP チャンクサブネットルートは、応答とともにボーダー ゲートウェイ プロトコル（BGP）を介してアドバタイズされます。

セッションの確立中に、IP アドレスの割り当てで **up-id** を使用して、UP に割り当てられていて、空き IP アドレスがあるチャンクを抽出します。この割り当てられた IP アドレスは、**Sx Establishment Req** メッセージを使用して CP から UP に渡されて、UP データベースに保存されます。

リモートサイトでの System Architecture Evolution Gateway for Control Plane（SAEGW-C）のフェールオーバーをサポートするために、UE セッションがセットアップされると、UP チャンクの割り当て中に IP チャンクサブネットのルートインストールの代わりにホストルートがアドバタイズされます。SAEGW-C に障害が発生した場合、リモート UP からのセッション再確立のために、同じホスト IP ルートがリモート SAEGW-C を介してアドバタイズされます。

ホストルートの明示的なアドバタイズメントを設定する前に、次のプロセスが実行されます。

- **explicit-route-advertise** 情報の値は、IP チャンクタイプパラメータに IP プールコンテンツタイプを指定した **Sx-Association Update** 要求を使用して、CP sxmgr から UP sxmgr に伝達されます。最初のビットは、明示的なルートアドバタイズメント機能のサポートを有効にするために設定されます。
- UP vpnmgr は、UP sxmgr から IP チャンクタイプの値を受信します。
- IP チャンクタイプの最初のビットが設定されている場合、UP vpnmgr の BGP を介した IP チャンクサブネットルートのインストールとアドバタイズメントは行われません。
- コールの確立中に、UP の IP チャンク情報で使用可能な IP チャンクタイプ情報に基づいて、ホストルートのアドバタイズメントが行われます。IP チャンクタイプの最初のビットが有効になると、ホストルートのアドバタイズメントが許可されます。
- CP vpnmgr は、UP ごとのホストルートカウントと UP vpnmgr のホストルートカウントの両方をグローバルに維持します。
- ホストルートの上限は 24,000 で、上限に達すると、CP vpnmgr は **Sx Establishment Req** 要求を拒否します。
- セッションのリリース中に、ホストルートが削除され、ホストルートカウントが CP および UP vpnmgr で更新されます。

ICSR

IP チャンクタイプ情報は、UP アクティブモードとスタンバイモードの間で行われる UP IP チャンク詳細の更新中にチェックポイントメッセージを使用して更新されます。

VPNMGR リカバリ

vpnmgr ローカル コンテキスト データベースには、IP チャンクタイプ情報が保存されます。

制限事項

この機能には次の既知の制限事項があります。

- UP ホストルートの上限は 24000 です。

- IPプールの設定は変更できないため、削除してから属性を使用して再度追加する必要があります。
- UPに問題はないが、部分的なサイト障害が発生した場合は、障害が発生したサイトのUPをセカンダリ CP に関連付ける必要があります。プールに十分な容量のチャンクがある場合、すべての UP がそのプールからのコールを処理できます。そうでない場合は、チャンクが割り当てられている UP のみがコールを処理します。
- この機能では IPv6 はサポートされていません。

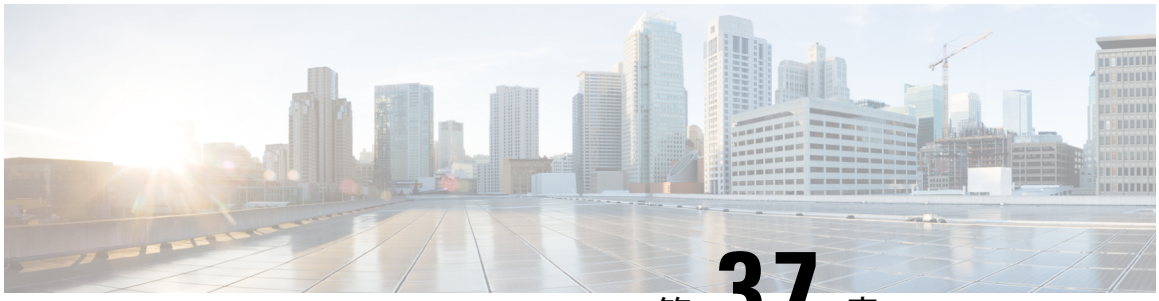
ホストルートの明示的アドバタイズメントの設定

UP グループ固有の IP プールを設定するには、次の CLI コマンドを使用します。

```
configure
  ip pool  pool_name ip_start_range ip_end_range static group-name group_name
chunk-size chunk_size explicit-route-advertisement
  end
```

注：

- *pool_name*：グループ固有の IP プール名。
- *explicit-route-advertisement*：ホストルートの明示的なアドバタイズメントの **host_route_explicit_advertisement** の設定に使用されるパラメータ。



第 37 章

ICSR バルク統計情報

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

この機能により、ユーザープレーンでの ICSR バルク統計スキーマがサポートされます。

ICSR バルク統計スキーマの設定

ユーザープレーンでいくつかの ICSR スキーマを設定するための設定例を以下に示します。

```
configure
   bulkstats collection collection_detail
      bulkstats mode mode_name
         sample interval interval_value
         file file_number
            icsr schema icsr_schema format "ICSR:
switchover-number:%switchover-number% switchover-time:%switchover-time%,
```

```
switchover-reason:%switchover-reason%"
        end
```

show CLI

ICSR スキーマのバルク統計データを取得するための show コマンド CLI を次に示します。

- **Show bulk stats data**：最大 4 つのファイルについて、統計情報の収集スキームに含まれている基準を表示します。「収集されたバルク統計データの表示」を参照してください。
- **bulk force gather**：バルク統計データを表示します。
- **show bulkstats schemas**：収集および送信統計情報を含む統計情報を収集するために使用されるスキームを表示します。「設定の確認」を参照してください。
- **show bulkstats variables**：スキーマ形式に組み込み可能なスキーマタイプ別に、使用可能な bulkstats 変数（%variable%）を表示します。
- **show configuration bulkstats brief**：グローバル範囲でバルク統計設定を表示し、サーバー設定を表示します。スキーマの設定は表示されません。

バルク統計情報

ユーザープレーンで次の CLI を実行して、ICSR スキーマで使用可能なカウンタを確認します。

```
show bulkstats variables icsr
```

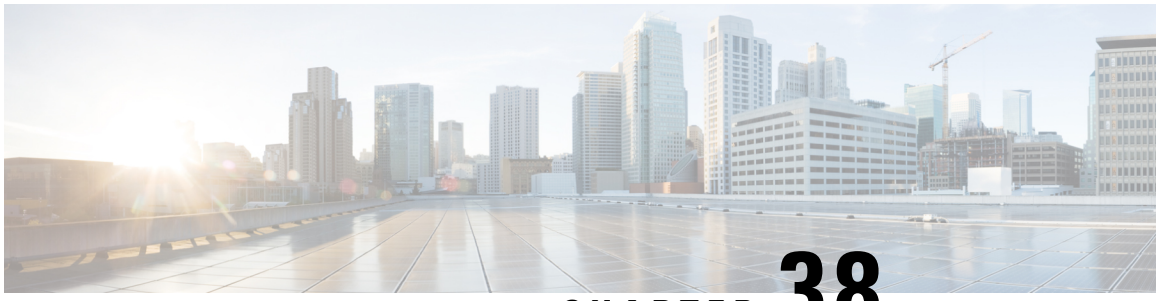
次の表に、ユーザープレーンでサポートされる ICSR カウンタの詳細を示します。

表 *11 : UP* に適用される *ICSR* カウンタ

ICSR カウンタ	説明
switchover-number	前回シャーシがリブートされて以降のスイッチオーバーの識別番号
switchover-time	スイッチオーバー開始時のタイムスタンプ
switchover-reason	スイッチオーバーの理由（手動および BGP の失敗、認証プローブの失敗など）
switchover-duration	スイッチオーバーの完了までにかかった時間
total-num-act-calls-swo-time	スイッチオーバー時のアクティブコールの合計数
total-num-lost-calls-swo-time	スイッチオーバーが原因で失われたデータセッションの合計数
audit_number	前回システムがリブートされて以降に実行された最近の監査の識別番号

ICSR カウンタ	説明
audit_chassis_state	監査が実行されたシャーシの状態（アクティブ/スタンバイ）
audit_start_time	監査開始時のタイムスタンプ
ext-audit-sync-start-time	スタンバイシャーシでの外部監査同期の開始時刻
ready-for-switchover-time	次のスイッチオーバーに向けた準備完了時のスタンバイシャーシのタイムスタンプ
audit_duration	監査の完了までにかかった時間
audit_reason	監査の理由
total_audit_active_sessions	監査中に検出されたアクティブセッションの合計数
total_audit_new_sessions	監査中に検出された新しいセッションの合計数
total_audit_stale_sessions	監査中に検出された古いセッションの合計数
total_audit_inactive_sessions	監査中に検出された非アクティブセッションの合計数
total_sessmgr	シャーシ上のセッション マネージャ インスタンスの合計数
total_sessmgr_active_connected	アクティブ接続状態のセッションマネージャの合計数
total_sessmgr_standby_connected	スタンバイ接続状態のセッション マネージャ インスタンスの合計数
total_sessmgr_pending_connected	保留接続状態のセッション マネージャ インスタンスの合計数
total_sess_crr_count	現在の既存コールリカバリレコード（CRR）の合計数
total_sess_crr_pre_installed	現在プレインストールされている既存の CRR の合計数
total-num-act-sessions-swo-time	スイッチオーバーイベント中に検出された、完全に接続されたセッションの合計数
total-num-lost-sessions-swo-time	スイッチオーバーイベント中に失われた、完全に接続されたセッションの合計数
critical-flush-duration	クリティカルフラッシュの完了までにかかった時間
total-num-checkpoint-fc-flush	スイッチオーバー中にフラッシュされたフルチェックポイントの合計数
total-num-checkpoint-critical-mc-flush	スイッチオーバー中にフラッシュされた重要なマイクロチェックポイントの合計数
total-num-checkpoint-mc-flush	スイッチオーバー中にフラッシュされたマイクロチェックポイントの合計数

ICSR カウンタ	説明
total_first_fc_during_critical_flush	クリティカルフラッシュ中に検出されたフルチェックポイントの合計数
total-num-first-fc-never-sent	スイッチオーバー中に一度も送信されなかった最初のフルチェックポイントの合計数
total-num-critical-fc-not-sent	スイッチオーバー中に送信されなかったクリティカルなフルチェックポイントの合計数
checkpoints-never-sent	送信されなかった SRP チェックポイントの合計数
checkpoints-send-failed	失敗した送信済み SRP チェックポイントの合計数



CHAPTER 38

SAE-GW セッションのアイドルタイマー

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

アイドルタイマーは、SAE-GW で発生するアイドルセッションを識別して削除するためにサポートされています。

セッションが他のネットワークノードから削除されても、セッションがアイドル状態になる場合があります。技術的な不具合により、セッションがSAE-GWに残り、こうしたアイドルセッションによってリソースが保持される可能性があります。

アイドルタイマーを設定すると、設定された時間制限よりも長くアイドル状態のままになっているセッションが削除されるため、システムのキャパシティを効果的に使用できます。

重要 この機能は現在、Pure-P および Collapsed Call に制限されています。

制限事項

アイドルタイマー機能は、冗長性イベントが発生した場合にアイドルタイマーの回復をサポートしていません。

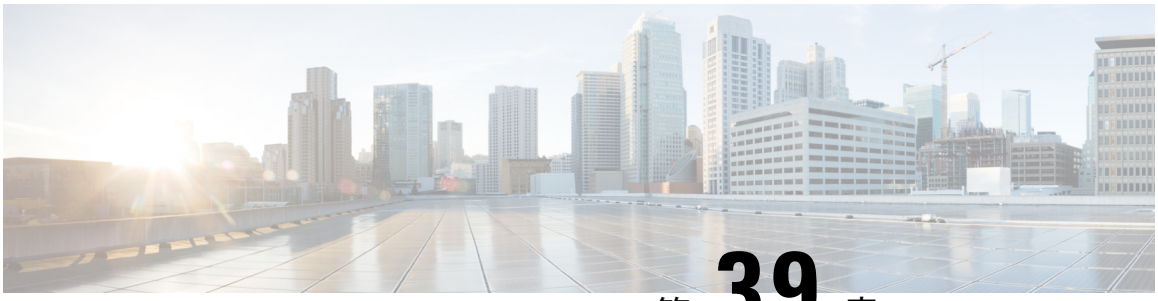
SAE-GW セッションのアイドルタイマーの設定

アイドルタイマーは、APN レベルで設定できます。

SAE-GW セッションのアイドルタイマーを設定するには、次のコマンドを使用します。

```
configure
  context context_name
    apn apn_name
      timeout idle timeout_value
      no timeout idle
      default timeout idle
      end
```

- **no**：アイドルタイマー設定を無効にします。
- **default**：サブスクライバのタイムアウト設定のデフォルト値を設定します。デフォルトのアイドルタイムアウト値は 0 です。
- **idle** *timeout_value*：システムによりセッションが自動的に終了されるまでに、セッションがアイドル状態を維持できる時間の上限を秒単位で指定します。続けて 0 ～ 4294967295 までの秒数を指定する必要があります。「0」は、機能が無効であることを示します。



第 39 章

IFTASK ハイパースレッディング

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.25

機能説明

ハイパースレッディングは、並列コンピューティング技術の活用により、パケット処理におけるシステムパフォーマンスを向上させます。

機能の仕組み

IFTASK ハイパースレッディングは、ポーリングモードドライバ（PMD）/マルチチャネル ダイレクト メモリ アクセス（MCDMA）およびセッション マネージャ スレッドが、ハイパースレッディングが有効になっている物理コアで共存しないようにします。

ハイパースレッディングを有効にすると、1 つのコアが 2 つのコアに分割されます。ハイパースレッディングにより、物理コアとその兄弟のコアで同じ種類のプロセスが実行されます。つまり、両方のコアで PMD/MCDMA スレッドまたはセッションマネージャが実行されます。

Intel Data Plane Development Kit（DPDK）/IFTASK は、PMD および MCDMA スレッドを CPU コア番号 1 からスケジュールし、IFTASK プロセスを処理するためにコア 0（マスターコア）を予約します。

非ハイパースレッドシステムでは、CPU コアで PMD および MCDMA スレッドをスケジュールしても、キャッシュ使用率とシステム全体のパフォーマンスには影響しませんが、ハイパースレッディングが有効になっている場合、コアとその兄弟のコアは PMD/MCDMA またはセッションマネージャを使用してスケジュールされるため、システムパフォーマンスが向上します。パフォーマンスの向上を実現し、CPU ペアを維持するために、コア番号は 1 からではなく、2 からスケジュールされます。IFTASK コアの数は常に偶数である必要があります。

CPU 分離

システムのパフォーマンスを向上させるために、PMD/MCDMA スレッドを実行する CPU はカーネルから分離されています。CPU が分離されると、カーネルは割り込みまたは他のカーネルプロセスのスケジューリングを停止します。

制限事項と制約事項

このリリースでは、この機能には次の制限事項と制約事項があります。

- この機能は現在、VPC-DI シャーシでのみサポートされており、コントロールプレーン（CP）のシングルインスタンス（VPC-SI）ではまだ認定されていません。
- [isolcpu] を有効または無効にすると、変更を反映するため、すべてのサービス機能（SF）カードが 2 回リブートされます。
- [isolcpu] を使用して IFTASK コア設定を変更すると、変更を反映するため、SF カードが 3 回リブートされます。
- ハイパースレッディングを有効にしたら、単一の Non-Uniform Memory Access（NUMA）ノードでは、PMD/MCDMA コア数は偶数である必要があります。
- NUMA が 2 つあるシステムでは、コアが均等に分割されるように、PMD/MCDMA コア数は 4 で割り切れる必要があります。

CPU 分離の設定

CPU 分離を有効にするには、次の設定を使用します。

```
config
   iftask
      isolcpu-enable
      end
```

注：

- **iftask isolcpu-enable**：Virtualized Packet Core - Distributed Instance（VPC-DI）シャーシ上のすべての SF カードの CPU 分離を有効にします。
- **no iftask isolcpu-enable** CLI コマンドを使用して、CPU 分離を無効にします。

第 40 章

間接転送トンネル

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

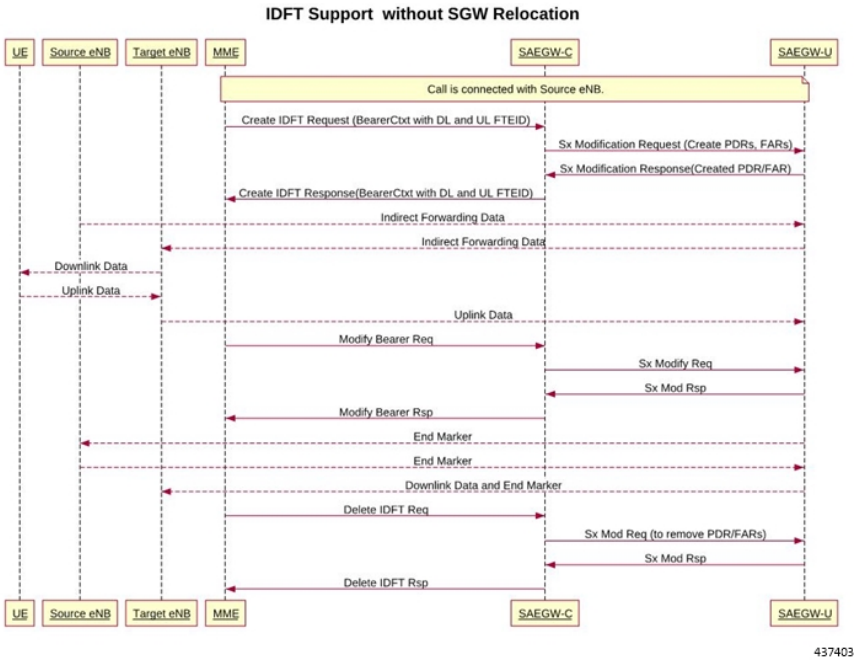
SAEGW は、作成と削除のための間接転送トンネル（IDFT）手順をサポートします。これらの手順の対象は、マルチ PDN とマルチベアラーを使用した Pure-S コールおよび Collapsed コールです。この機能は、S-GW の再配置とコリジョンのシナリオの有無にかかわらず、IDFT サポートの対象です。

（注） CUPS の IDFT は CLI 制御機能です。デフォルトでは、CUPS の IDFT 機能は無効になっています。

機能の仕組み

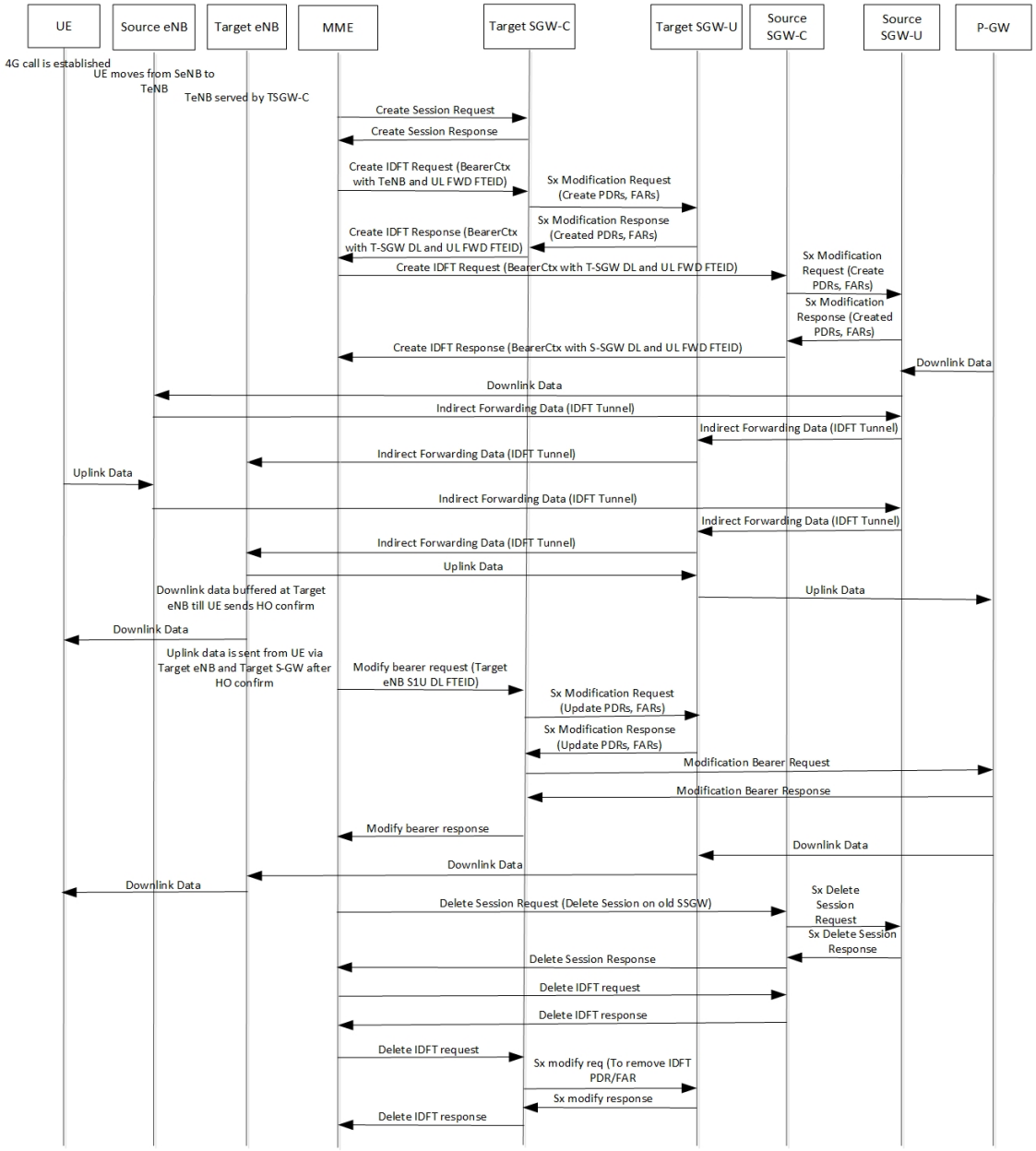
通話フロー

次のコールフローは、S-GW の再配置を伴わない IDFT のサポートの概要を示しています。



次のコールフローは、S-GW 再配置を伴う IDFT のサポートを示しています。

図 *13 : S-GW* 再配置を伴う *IDFT* のサポート



上記のコールフローは、S-GW の再配置を行い、MME の変更を伴わない IDFT トンネルの確立と削除について説明しています。

IDFT トンネルが MME によって削除されない場合、S-GW は IDFT トンネルのローカル削除を開始します。

この機能は、Pure-S コールと Collapse コールの次のシナリオをサポートします。

- 同じ MME を使用した S-GW の再配置
- 同じ MME と異なる eNodeB を使用した S-GW の再配置

- 異なる MME を使用した S-GW の再配置
- S1 ベースの eNodeB ハンドオフ
- EUTRAN から UTRAN へのハンドオフ

（注） S4インターフェイスはCUPSではサポートされていません。したがって、S4 インターフェイスを含む EUTRAN から UTRAN へのハンドオフ（およびその逆）もサポートされません。

- S-GW の再配置を伴う EUTRAN から UTRAN へのハンドオフ
- UTRAN から EUTRAN へのハンドオフ
- S-GW の再配置を伴う UTRAN から EUTRAN へのハンドオフ
- IDFT のセットアップまたは削除中の Sx トランザクションのタイムアウト
- 保留中の Sx トランザクション（PCRF または OCS からのイベント）と IDFT 要求の受信
- IDFT アクティブ時のベアラー作成要求（CBR）
- IDFT アクティブ時のベアラー更新要求（UBR）
- IDFT アクティブ時のベアラー削除要求（DBR）
- IDFT アクティブ時の他の PDN でのベアラー変更要求（MBR）
- 送信元 MME パス障害
- ターゲット MME パス障害
- NTSR 有効時の MME パス障害
- eGTP-C S5 パス障害
- P-GW 再起動通知有効時の eGTP-C S5 パス障害
- Sx パス障害（クリーン IDFT およびコール）
- セッションの中止（clear sub all、local abort など）
- IDFT アクティブ時の他の PDN での CBR、UBR
- IDFT アクティブ時の他の PDN/ベアラーでの DBR
- ターゲット eNodeB の S1-u パス障害
- ターゲット S-GW の S-GW パス障害
- IDFT アクティブ時のデフォルトベアラーでの S1-u エラー通知
- IDFT アクティブ時の専用ベアラーでの S1-u エラー通知

- ターゲット S-GW から送信元 S-GW ベアラーへの S1-u エラー通知
- ターゲット eNodeB からターゲット S-GW ベアラーへの S1-u エラー通知

サポートされる機能

IDFT 機能は、次の機能をサポートしています。

- 複数のベアラーを使用した、Collapsed、Pure-S、Collapsed および Pure-S のマルチ PDN 複合コールの IDFT 作成要求。
- ダウンリンクおよびアップリンク IDFT ベアラーでのデータ転送。
- MME からの IDFT 削除要求。また、MME から IDFT 削除要求が送信されない場合、タイマーベースで、デフォルト値である 100 秒経過後に IDFT ベアラーを削除。
- 通常の PDN がダウンした場合の IDFT PDN の削除（MME/P-GW からのサブスクライバのクリア/削除を含む）。
- Pure-S と Collapsed コールの場合、[IDFT Active]/[IDFT Create Sx-Pending] 状態のときの Sx パス障害処理。
- その他の手順による IDFT PDN の確立時または削除時のメッセージのやり取りとコリジョン。
- IDFT PDN がアクティブな場合、非 IDFT PDN での S11/S5 および Sx パス障害処理がサポートされるようになりました。

重要 GTP-U アドレスのトランスポート機能は、eNodeB および S-GW 間で同じであると想定されます。

間接転送トンネルの設定

この項では、IDFT 機能のサポートで使用可能な CLI コマンドについて説明します。

間接転送トンネル機能の有効化

コントロールプレーンで、次の CLI コマンドを使用して IDFT 機能を有効または無効にします。

```
configure
  context context_name
    sgw-service service_name
      [ default | no ] egtp idft-support
      end
```

注：

- **idft-support**：CUPS の IDFT 機能を有効または無効にします。
- デフォルトでは、IDFT 機能は無効になっており、この CLI コマンドはランタイムの変更に適用できます。

間接転送トンネル機能の確認

show sgw-service name <service_name>

コントロールプレーンでは、この CLI コマンドによる出力範囲が拡張され、IDFT 機能が有効か無効かが表示されるようになりました。

- IDFT-Feature Support for CUPS：Enabled/Disabled

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングと障害対応のサポートに使用できる CLI コマンドに関する情報について説明します。

show コマンドの入力と出力

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show subscribers saegw-only full all

コントロールプレーンで、このコマンドを使用して IDFT ローカルおよびリモート TEID データを表示します。次に、出力例を示します。

```
 Indirect Fwding   : Active
 DL fwd local  addr: 209.165.200.228              DL fwd remote   addr: 209.165.200.226

 DL fwd local  teid: [0x80028004]           DL fwd remote   teid: [0x2002d2e5]
 UL fwd local  addr: 209.165.200.228              UL fwd remote   addr: 209.165.200.226

 UL fwd local  teid: [0x8002a004]           UL fwd remote   teid: [0x20042bca]
```

show subscribers user-plane-only callid <call-id> pdr all

ユーザープレーンでこのコマンドを使用して、IDFT 用に作成された PDR または FAR を表示します。次に、出力例を示します。

重要 IDFT PDR には、送信元および接続先インターフェイスタイプとして ACCESS が設定されます。

```
+-----Source Interface:          (C) - Core            (A) - Access
|-----Type                       (P) - CP-function     (.) - Unknown
|
|+----Destination Interface:     (C) - Core            (A) - Access
||----Type                       (P) - CP-function     (.) - Unknown
||
||
||+---Rule-Type:                 (S) - Static          (P) - Predefined
|||---Type                       (D) - Dynamic         (.) - Unknown
|||
|||
vvv   PDR-ID    Associated FAR-ID    Associated URR-ID(s)    Associated QER-ID(s)
---   ------    -----------------    --------------------    --------------------
ACS   0x0001          0x8001              n/a                  0x80000001
CAS   0x0002          0x8002              n/a                  0x80000001
ACD   0x0003          0x0003           0x00000007              0x00000002
                                          n/a                  0x80000003
CAD   0x0004          0x0004           0x00000007              0x00000002
                                          n/a                  0x80000003
CAD   0x0005          0x0005           0x00000000              n/a
ACD   0x0006          0x0006           0x00000000              n/a
CAD   0x0007          0x0007           0x00000000              n/a
ACD   0x0008          0x0008           0x00000000              n/a
AAD   0x0009          0x0009           0x00000000              n/a
AAD   0x000A          0x000A           0x00000000              n/a
AAD   0x000B          0x000B           0x00000000              n/a
AAD   0x000C          0x000C           0x00000000              n/a

Total subscribers matching specified criteria: 1
```

show subscribers user-plane-only full all

重要 IDFT PDR のデータ統計情報は、既存の PDR 統計情報と同じ方法でキャプチャされますが、制限付きです。DL および UL IDFT の統計情報は、Pkts-Down および Bytes-Down カテゴリで増分されます。

次にサンプル出力を示します。

```
Static & Predef Rule Match stats:
Rule Name           Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  ------------------
catchall                       0          0          3       1368          3
  0          0/0              0/0

Dynamic Rule Match stats:
PDR Id    Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
FP-Down(Pkts/Bytes)    FP-Up(Pkts/Bytes)
-------- ---------- ---------- ---------- ---------- ---------- --------------
-------------------    ------------------
0x0004        2       856          0           0          2              0
 0/0                 0/0
0x000b        2       856          0           0          2              0
 0/0                 0/0
0x000c        2       168          0           0          2              0
 0/0                 0/0
```

show subscribers user-plane-only full all

第 41 章

IP プールの管理

この章では、次の事項について説明します。

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
IPv6 プールのサポートされる最大チャンクサイズ値が 65,536 に増えました。	21.27
IP プールチャンクの可用性に基づく UP の選択のサポート。	21.26
このリリースでは、コンテキストごとに 100 UP という VPN の制限がなくなりました。	21.25
初版	21.24 より前

機能説明

IP プールの大部分が使用されていない場合、それはリソースの効果的な利用方法とは言えません。IP リソースが不足しているユーザープレーン（UP）にとって、使用されていないリソースが動的に使用可能になれば、メリットがあります。

CUPSアーキテクチャには、次の展開において、一元化されたコントロールプレーン（CP）、多数の UP、および UP 全体の IP プールを管理する自動的かつ効率的な方法があります。

- CUPS の共存
- リモート CUPS

この機能により、ダイナミック検出およびUPへのIPプール割り当てのため、最小IPサブネット/48 サイズの IPv6 プールの最大チャンクサイズ値 65536 を設定できます。

機能の仕組み

CUPS アーキテクチャでは、CP の PDN/IP コンテキストにより、複数の登録済み UP 間で IP チャンクリソースが動的に分散されます。以下の項では、ソリューション全体について説明します。

UP 登録解除の処理

UP の登録解除は、次のシナリオでトリガーされます。

- UP からのグレースフル登録解除：このシナリオでは、ユーザープレーンサービス CLI によって、コントロール プレーン グループの関連付けが削除されます。IP アドレスは、CP の sessmgr レベルで解放されます。
- CPからのUP接続障害：このシナリオは、UPからCPへのハートビートが途切れた場合、またはUP が再起動し、それについて CP が通達を受けた場合のいずれかに発生します。UP が再起動するということは、指定された UP の CP が新しい再起動カウンタを受信するということです。

UP の登録解除がトリガーされると、CP の VPNMGR タスクは、VPNMGR データベースで使用可能な情報を使用して UP の ID とアドレスを検証します。一致しない場合、VPNMGR は失敗メッセージを表示します。一致した場合、検証は成功となります。検証に成功すると、VPNMGR は、指定された UP の IPv4 および IPv6 の両方のプールから、すべての割り当て済みおよび未割り当てのチャンクを取得します。

UP の IP の一部が使用されていても、すべて使用されていなくても関係なく、VPNMGR は UP の強制登録解除を実行するまでの2分間のタイマーを開始します。強制登録解除では、すべてのIPアドレスがVPNMGRデータベースからローカルに削除され、セッションエントリが削除され、すべてのチャンクが CP のメインアドレスプールに配置されます。

ホールド タイマー

ホールドタイマーは、IPv4 動的プールのプールごとに設定されます。静的プールと IPv6 プールは考慮されません。ホールドタイマーが設定されていない場合、IPアドレスは割り当てられたときに空き状態から使用済み状態に移行し、セッションが解放されると空き状態に戻ります。プールで設定されたホールドタイマーにより、解放された IP アドレスは保留状態に移行

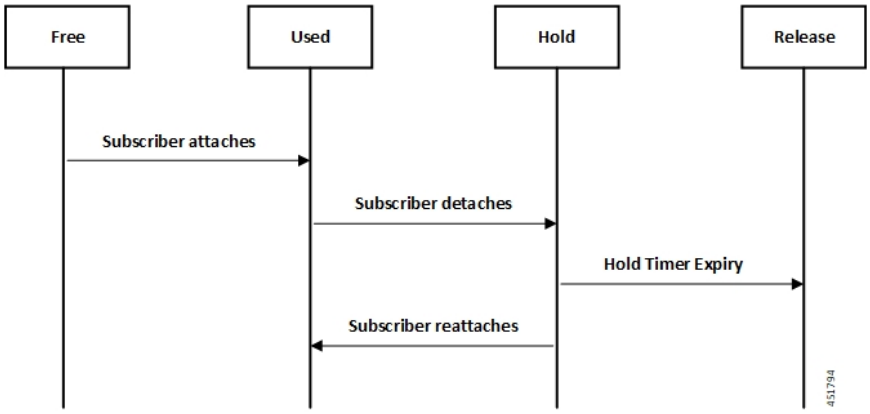
します。設定されたホールドタイマーの期間中、IPアドレスは保留状態のままとなり、同じサブスクライバが再度接続したときに再利用できます。保留状態の間、IPアドレスは他のサブスクライバに割り当てられません。ホールドタイマーの期限が切れると、IPアドレスはリリース状態に移行し、すべての空き IP アドレスが使い果たされると再利用されます。

UP 登録解除の場合、UP の詳細（UP ID と UP の詳細を保持するメモリ）が CP で保持されないため、保留状態のすべての IP アドレスが空き状態に移行します。その結果、IP アドレスが別のサブスクライバに再利用される可能性があります。また、保留アドレスでは、VPNMgr リカバリと ICSR がサポートされています。

アドレス状態の変更

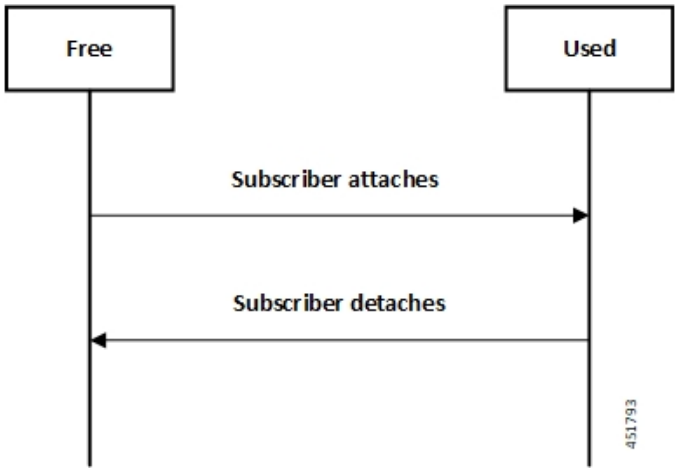
次のコールフローは、ホールドタイマーが設定されている場合のアドレス状態の変更を示しています。

図 *14* : ホールドタイマーを使用したアドレス状態の変更



次のコールフローは、ホールドタイマーを設定しない場合のアドレス状態の変更を示しています。

図 *15* : ホールドタイマーを使用しないアドレス状態の変更



ホールドタイマーの設定

CUPS でホールドタイマー機能を有効にするには、次の設定を使用します。

```
configure
  context context_name
    ip pool pool_name address-hold-timer seconds
    end
```

注：

- *pool_name*：IP アドレスプールの論理名を指定します。*pool_name* は、1 ～ 31 文字の英数字文字列で指定する必要があります。
- この機能が有効な場合に、アクティブなサブスクライバが切断されると、IPアドレスは保持されるか、まだ使用中と見なされ、アドレスホールドタイマーが期限切れになるまで空き状態に戻りません。そのため、指定された時間（秒単位）内に再接続したサブスクライバは、IP プールから同じ IP アドレスを取得できます。*seconds* は秒単位の時間で、0 ～ 31,556,926 の整数で指定する必要があります

プール内のすべての IP アドレスのステータスを確認するには、**show ip pool address pool-name** *pool_name* CLI コマンドを使用します。また、保留されたアドレスの残りのホールド時間も表示されます。

コンテキストごとの IP プール

CP では、1 つのコンテキストで UP グループあたり 600 の IP プールを設定できます。また、CP のコンテキストあたり 2000 の IPv4 プールと 256 の IPv6 プールを設定できます。これを UP あたり 600 プールを上限に、さまざまな UP グループに分散できます。機能は次のとおりです。

- UP グループには、プールタイプの組み合わせとして可能なすべての組み合わせにおいて、最大 600 の IP プールを設定できます。
- プールは、静的、ダイナミック、または静的とダイナミックの混在のいずれかです。
- プールは、すべて IPv4、すべて IPv6、または IPv4 と IPv6 の混在が可能です。
- 600 の IP プールのうち、UP グループあたりの IPv6 プール数は最大 256 です（ASR5500 と同じコンテキストレベルの制限）。600 のプールをすべて IPv4 に設定できます。
- 1 つの UP グループに 600 を超える IP プールが設定された場合、600 のプール/プールチャンクのうち、どのプール/プールチャンクを UP に割り当てるかを決定できません。
- CP は、UP にインストールされたルートの数を保持します。プールのルート数が 6,000（ASR5500 と同じコンテキストレベルの制限）を超えると、使用数超過しきい値に達しても、UP に新しいチャンクが割り当てられません。同様に、新しい IP プールが動的に割り当てられた際に、すでに 6,000 のプールルートがインストールされていた場合、その UP のプール数が 600 未満であっても、そのプールから新しいチャンクは割り当てられません。

この機能の一部として、**show ip user-plane verbose** CLI コマンドでは、IPv4 および IPv6 ダイナミックプール数が IPv4 プールおよび IPv6 プールの合計数に置き換えられます。また、この CLI コマンドの出力が拡張され、[Total Pool Kernel Routes] フィールドと [Max Pool Kernel Routes] フィールドが表示されるようになりました。

IP リソース管理

CUPS アーキテクチャでは、CP には PDN/IP コンテキストのすべての IP プールの設定があります。3GPP 標準に準拠して、UP は Sx 関連付け要求および応答手順によって CP に登録されます。

登録プロセス中に、CP は、特定の UP によって提供されているすべての APN と、各 APN の関連するプール設定を検出します。CP は、IP チャンクリソースの一部を特定の UP に割り当て、Sx 関連付け更新要求および応答手順を介して送信します。この情報は、UP で PDN/IP コンテキストインスタンスに送信されます。

UP の登録が成功すると、PDN/IP インスタンスが、プールから UP への IP チャンクリソース情報の送信を開始します。この IP チャンクリソース情報は、Sx 関連付け更新要求および応答メッセージの独自/カスタム IE で UP に送信されます。UP の PDN/IP インスタンスは、CP から受信した BGP ルートをチャンク単位でアナウンスします。

CP に登録されている各 UP は、「ピア ID」とノード ID を使用して識別されます。

IP リソースの補充および取り消し手順

IP リソースを効率的に使用するために、CP は必要に応じて IP リソースを UP に割り当てるため、IP チャンクリソースの補充および取り消し手順がサポートされています。

CP のしきい値ロジックに基づいて、各 UP の IP リソースの使用状況をプールレベルでモニターします。UP の全体的な IP チャンク使用率が特定のしきい値を超えると、CP は追加の IP チャンクリソースをその UP に送信します。

UP 内の特定の IP チャンクが使用されず、一定期間アイドル状態の場合、CP はそれぞれの UP から未使用の IP チャンクリソースを取り消します。詳細については、「プールごとのチャンクの割合の設定」の項を参照してください。

1 つの UP グループにつき 1 つの UP の No-chunk-pool

機能説明

静的 IP アドレス割り当ての場合、SessMgr は特定の IP アドレスを要求します。VPNMgr は、その特定の IP アドレスを検索します。チャンクがすでに特定の UP に割り当てられている場合、VPNMgr はそのアドレスを割り当てて、コールを処理する UP に応答します。静的 IPv4v6 コールの場合、要求された IPv4 および IPv6 アドレスが異なる UP に属している可能性があるため、UP グループあたりの UP が 1 つのみでない限り、IPv4v6 の成功は保証されません。したがって、静的 IPv4v6 コールの成功のため、UP グループあたり 1 つの UP のみ設定できます。UP グループあたり 1 つの UP を使用する場合、そのプールを使用する UP は 1 つだけです。し

たがって、プールをチャンクに分割するのではなく、プール全体をその UP に割り当てることができるため、プールのチャンク分割は推奨されません。また、一部のユースケースでは、1 つの APN に対して 1 つの UP が含まれる場合もあります。どちらのユースケースもサポートできるように、CUPS アーキテクチャでプールをチャンクに分割しないオプションが導入されました。

no-chunk-pool機能がないと、使用可能なアドレス数がチャンクサイズよりも少ない場合、最低 2 つのチャンクが設定されていました。

no-chunk-pool機能があれば、チャンクに分割することなくプールを設定できます。プール全体が、そのプールを最初に要求した UP に割り当てられます。

（注） no-chunk-pool 機能は、UP グループあたり 1 つの UP を使用するセットアップでのみ推奨されます。UP グループあたり複数の UP を使用するセットアップでは推奨されません。

機能の仕組み

no-chunk-pool 機能には次が含まれます。

- プールが [no-chunk-pool] に設定されている場合、プールそのものがチャンクと見なされ、プールを最初に要求した UP にプール全体が割り当てられます。
- No-chunk-pool は [public]、[private]、または [static] に設定できます。
- No-chunk-pool は VRF 内で設定できます。
- UP グループあたり複数の UP を使用する場合、最初に Sx 関連付けを実行した UP にダイナミック no-chunk-pool 全体が割り当てられます。
- UP グループあたり複数の UP を使用する場合、ラウンドロビンアルゴリズムにより、現在サービスを提供している UP 間で静的 no-chunk-pool が割り当てられます。
- UP グループあたり複数の UP を使用する場合、動的に追加された新しいプールは、UP グループ内のどの UP にも割り当てられる可能性があり、確定的に把握することはできません。

no-chunk-pool の設定

no-chunk-pool 機能を有効にするには、次の設定を使用します。

```
configure
  context context_name
    cups enable
      ip pool pool_name ip_address/subnet_mask no-chunk-pool
      ipv6 pool pool_name prefix ip_address/length no-chunk-pool
  exit
```

次の CLI コマンドの出力で、該当する特定のプールの [total-chunks] フィールドに「1」と表示されていれば、no-chunk-pool であることが分かります。

- **show ip pool-chunks pool-all**
- **show ipv6 pool-chunks pool-all**

静的 IP プール管理

CUPSアーキテクチャでは、静的IPプールの管理方法は、動的プールの管理方法とは異なります。静的 IP プールは、動的プールのチャンク方法と似た方法で「静的チャンク」に分割されますが、それらの静的チャンクはUPに配布されず、セッションの作成中に特定の静的IPチャンクの最初の静的アドレスを UE が要求するまで、CP に残ります。

CPがラウンドロビンアルゴリズムを使用してUPを選択し、要求された静的アドレスが属する静的 IP チャンク全体が選択された UP に割り当てられるため、いずれかの UE がそのチャンクから静的アドレス（IPv4またはIPv6）を要求するたびに、UEにそのUPが割り当てられます。

（注）
- 動的プール内では、「allow static」はサポートされていません。
- IPv4v6 静的 PDP は、1 つの UP グループ内の複数の UP ではサポートされません。
- 静的 IPv4v6 PDN を正常に動作させるには、IPv4 アドレスと IPv6 アドレスの両方が同じ UP 上にある必要があります。確実に動作させる唯一の方法は、UP グループに単一の UP を含めることです。
- 同じ APN 上のマルチ PDN を正常に動作させるには、1 つの PDN を静的、もう 1 つの PDN を動的にし、両方のアドレスが同じ UP 上にある必要があります。確実に動作させる唯一の方法は、UP グループに単一の UP を含めることです。
- 静的 IP プールの場合、アドレスはすでに UE によって決められているため、UP を選択する利点はありません。

UP の選択

CUPS アーキテクチャでは、セッションの確立中に、登録された UP の間で UP が選択されます。UP はさまざまな方法で選択できます。以前のリリースでは、ラウンドロビン アルゴリズム ベースの UP の選択がサポートされていました。現在は、接続が最も少ないユーザープレーン選択アルゴリズムがサポートされています。

IP プールチャンクの可用性に基づく UP の選択

21.26より前のリリースでは、CPは最小セッション使用率またはラウンドロビンアルゴリズムに基づいて UP を選択します。選択した UP でチャンクが使い果たされると、影響を受ける APN に新しい IP プールが追加されるまで、CP によってセッション確立要求が拒否されます。これにより、空き IP アドレスを持つ一部のチャンクが残っている UP で IP リソースが無駄になります。

21.26 以降のリリースでは、この機能が拡張され、IP プールチャンクの可用性に基づいて UP を選択できるようになりました。一部の UP でチャンクが使い果たされ、CP が接続要求を受信すると、CP は使用可能な IP アドレスを持つ UP をランダムに選択します。また、設定されている他の UP 選択アルゴリズムは無視されます。

制限事項

- Pure-S コールの UP 選択はサポートされていません。
- IP アドレスベースの検証では、非 DNS ベースの UP 選択のみが考慮されます。
- 選択した UP にセッションに割り当てる IP アドレスがない場合、UP の選択は上書きされます。
- Sx 関連付けの実行中に、コンテキストの 1 つにすべての UP に対応できるだけの十分な容量のチャンクがない場合、チャンクを取得する UP のみが VPN で維持されます。
- 特定の UP でチャンクが使用できなくなると、VPN は UP の選択を上書きするため、適切な IP プールの計画ガイドラインに従って UP 間の不均等な負荷分散を最小限に抑える必要があります。

  IP プールの計画ガイドラインについては、IP プールプランニングのガイドライン （977 ページ）を参照してください。

サポートされる機能

IP プール管理機能の一部として、次の機能がサポートされます。

- IPv4、IPv6 パブリック、およびプライベートプールベースの IP アドレス割り当て。
- IPv4 静的タイプのアドレス割り当て。
- アクティブコールタイプのセッション マネージャ リカバリおよび VPN マネージャリカバリ。
- CP to CP シャーシ間セッションリカバリ（ICSR）のサポート。
- IPv4 プールの hold-timer。
- IPv4 および IPv6 プールの busy-out（基本機能）。

制限事項

以下に、この機能のこのリリースにおける既知の制限事項と制約事項を示します。

- [allow-static] タイプのプール設定はサポートされません。
- IP コンテキストにプールを追加する前に **cups enabled** CLI を設定して、CUPS モードの IP プール管理機能を有効にします。
- IPv4v6 静的 PDP は、1 つの UP グループ内の複数の UP ではサポートされません。

- 次の CLI コマンドの出力には、すべてのプールと、プールあたり最大 2048 チャンクが表示されます。
  - **show ipv6 pool-chunks up-id** *up_id*
  - **show ipv6 pool-chunks pool-name** *ipv6_pool_name*
  - **show ip pool-chunks up-id** *up_id*
  - **show ip pool-chunks pool-name** *ipv4_pool_name*
- CUPS アーキテクチャでは、次の機能はサポートされません。
  - IPv6：アドレスホールドタイマーはサポートされません。
  - PDN v4v6：アドレスホールドタイマーはサポートされていません。
- UE が再接続すると、CP は同じ UP セッションを選択する必要があります（以前のセッションで IP アドレスがその UP によってすでにアドバタイズされているため）。したがって、UP 負荷ベースの選択またはロケーションベースの UP 選択はできません。
- ホールドタイマー値として「0」はサポートされません。
- ホールドタイマーのリカバリは、セッションマネージャあたり最大 1000 個のアドレスまでサポートされます。
- シャーシをリロードすると、スタンバイシャーシのホールドタイマー情報が失われます。
- ホールドタイマー値を変更すると、他のプール設定の場合と同様に、Sx の再確立も必要になります。

プールシステムの制限

現在、CP DI-Large モデルは、次の表に示すパラメータの拡張数をサポートしています。これらの制限は、使用されるチャンクサイズの値に関係なく一定であり、各パラメータの上限値です。最大値に達したパラメータの制限により、後続のパラメータの上限値が制限されます。

（注） 小規模および中規模モデルでは、他のモデルよりも制限が低くなります。

パラメータ	制限
コンテキストごとの IPv4 プール	2000
コンテキストごとの IPv6 プール	256
シャーシごとの IP プール	5,000（v4 と v6 の両方を含む）

ダイナミックプールアドレス	コンテキストあたり 1,600 万 シャーシあたり 3,200 万
スタティックプールアドレス	コンテキストあたり 3,200 万 シャーシあたり 9,600万
VRF の数	コンテキストあたり 300 シャーシあたり 2,048
最大 IP プールサイズ	512,000
最大 IPv6 プールサイズ	1,000,000

UP グループのチャンクサイズの意味：

プールはチャンク割り当ての基本単位であり、すべての UP に対して関連するプールからチャンクが割り当てられます。チャンクサイズ値が 65,536 のチャンクを取得できる UP の数は最大で、100 万/65,536 = 16 なので、チャンクサイズ値が 65,536 の場合、各 UP グループでサポートされる UP は 16 となります。

APN のチャンクサイズの意味：

APN 設定で使用される単一の UP グループの場合、制限は UP グループ制限値と同じです。

APN 設定で複数の UP グループを使用する場合ついては、「グループ固有の *IP* プールを持つ複数の *UP* グループ」の章を参照してください。16 の UP からなる UP グループの最大数は、コンテキストあたり 1,600 万アドレス、または 100 万アドレスプールなので、16 の UP APN からなる合計 16 の UP グループがサポートされます。

v6 プール内のすべてのプール設定が枯渇したため、同じ VPN コンテキストで動作する残りの APN では同じ IPv6 プールが使用されます。16 の UP からなる 16 の UP グループというのは、IPv4 アドレスがないという前提に基づいています。IPv4 アドレスが含まれる場合には、上限はこの想定より低くなります。システムでは 3,200 万のダイナミックアドレスがサポートされるため、許可される SGI コンテキストは 2 つだけです。

IP プール管理の設定

この項では、この機能をサポートするために使用可能な CLI コマンドについて説明します。

重要

- 以前のリリースでは、S-GW と P-GW に関するユーザー プレーン プロファイルの設定が必要でした。このリリースでは、UP の選択のために S-GW および P-GW でユーザー プレーン プロファイルを設定する必要がなくなり、IP プールの設定に関連付ける必要もありません。
- CP と UP の両方に同じ PDN コンテキストが存在する必要があります。
- APN 設定で指定された IP コンテキスト名は、CP と UP の両方で同じである必要があります。

ネットワークでの IP プールとユーザープレーンのグループ化の計画に関するガイドラインについては、シスコのアカウント担当者にお問い合わせください。

コントロールプレーンでの処理

IP プール管理の IP コンテキストの有効化

IP プール管理の IP コンテキストを有効にするには、次の CLI コマンドを使用します。

```
configure
   context context_name
      cups enable
      end
```

カスタムしきい値タイマーの設定

重要 21.9（7 月中旬）以降のリリースでは、**cups chunk-allocate-timer** *allocate_timer_seconds* **chunk-release-timer** *release_timer_seconds* CLI コマンドは廃止され、**cups chunk-threshold-timer** *threshold_timer_seconds* および **cups min-chunks-threshold-per-pool** *threshold_percent* CLI コマンドに置き換えられています。

UP 間のチャンクの再配布に関するしきい値タイマーがあります。デフォルトでは、過剰に利用されている UP にチャンクを送信する場合は 60 秒ごとにチェックが実行され、十分に活用されていない UP からチャンクを削除する場合は 300 秒ごとにチェックが実行されます。カスタムしきい値タイマーの場合は、次の CLI コマンドを使用します。

```
configure
   context context_name
      cups chunk-allocate-timer allocate_timer_seconds chunk-release-timer
release_timer_seconds
      end
```

注：

- この設定は、オプションです。設定されていない場合、デフォルトの割り当てしきい値は 60 秒、リリースしきい値は 300 秒です。
- **default cups chunk-allocate-timer chunk-release-timer** CLI コマンドを使用して、チャンクの割り当てタイマーとチャンク解放タイマーをそれぞれ 60 と 300 に戻します。
- 設定されている解放タイマーが割り当てタイマーよりも小さい場合、割り当てタイマーと等しい値で上書きされます。

チャンクしきい値タイマーの設定

コンテキストの CUPS IP プールチャンクしきい値タイマーを設定するには、次の CLI コマンドを使用します。

```
configure
  context context_name
    cups chunk-threshold-timer threshold_timer_seconds
    end
```

注：

- *threshold_timer_seconds*：チャンクしきい値タイマー値を秒単位で指定します（30 ～ 300 の整数）。デフォルト：60 秒。
- **default cups chunk-threshold-timer** CLI コマンドを使用して、デフォルト値の 60 秒を設定します。
- 21.9（7月中旬）より前のリリースでは、UP への新しいチャンクの割り当てと、十分に活用されていない UP からのチャンクの解放は、それぞれ割り当てタイマーと解放タイマーに基づいて行われていました。21.9（7 月中旬）以降のリリースでは、チャンクの割り当てと解放が定期的に発生する単一のしきい値タイマーのみが存在します。

プールごとのチャンクの割合の設定

コンテキスト内のプールごとのチャンクの最小割合を設定するには、次の CLI コマンドを使用します。

```
configure
  context context_name
    cups min-chunks-threshold-per-pool threshold_percent
    end
```

注：

- *threshold_percent*：最小チャンクを 0 ～ 50 の割合で指定します。デフォルトは 10 です。
- **default cups min-chunks-threshold-per-pool** CLI コマンドを使用して、デフォルト値の 10% を設定します。
- チャンクは、CP で特定のプールを持つ空きチャンクの割合がこの CLI コマンドで設定された割合よりも少ない場合にのみ、定期的に解放されます。

- 最小チャンクが設定された割合以下になると、使用率が 50% 未満で空きチャンクが 2 つ以上ある UP の存在を確認するためのチェックが実行されます。存在する場合は、その特定のプールにある十分に活用されていない各 UP から 1 つのチャンクが取り消されます。

- CP VPNmgr の最小チャンクが復元されるまで、for: periodicity = chunk-threshold-timer に関する警告ログが生成されます。
- 登録時の UP ロックダウン期間：UP 登録の最初の 5 分間は、他の UP がチャンクを必要としている場合でも、その UP からチャンクが取り消されて別の UP に送信されることはありません。

チャンクサイズ値の設定

この CLI コマンドを使用して、プール作成時に特定の IP プールのチャンクサイズを指定します。

```
configure
  context context_name
    ip pool pool_name prefix mask chunk-size chunk_size_value
    end
```

注：

- chunk-size は、IP プールの初回設定時のみ、プレフィックスまたはマスクと併せて設定します。
- chunk-size 値は 2 の累乗で、16ー65536 の範囲で指定する必要があります。
- デフォルト値：1024

ユーザープレーンでの処理

UP の IP コンテキストの場合、IP プールを設定したり、**cups enabled** CLI コマンドを使用したりする必要はありません。

システムのユーザープレーンの設定

システムで機能することが期待されるユーザープレーンの最大数を設定するには、次の CLI コマンドを使用します。

```
configure
  context context_name
    cups max-user-planes value
    end
```

注：

- 21.25 より前のリリースの場合：

cups max-user-planes *value*：デフォルト値は 10 です。

コンテキストおよび UP グループでサポートされるユーザープレーンの最大数は 100 です。

- 21.25 以降のリリースの場合：

  cups max-user-planes *value*：値の範囲は 1 ～ 1,000 です。デフォルト値は 10 です。

  コンテキストでサポートされるユーザープレーンの最大数が 1,000 に増えました。

  この値は、サポートされるユーザープレーンの実際の数ではなく、VPNMGR の制限数を指します。システムでサポートされるユーザープレーンの実際の数は、Sx によって決定されます。

  Sx 関連付けで最初に割り当てられたチャンクを調整するには、この CLI コマンドを使用します。このコマンドは、システムへの新しい UP の追加を制限するためには使用できません。

- **default cups max-user-planes** CLI コマンドを使用して、ユーザープレーンの最大値を 10 に戻します。

モニタリングおよびトラブルシューティング

ここでは、この機能のモニタリングと障害対応について説明します。

コマンドや出力の表示

ここでは、この機能をサポートする CP の show コマンドとその出力について説明します。

show ip pool-chunks pool-name <pool-name>

このコマンドの出力には、指定した IPv4 プール内のすべてのチャンクが表示されます。

- chunk-id
- pool-id
- up-id
- total-addr
- free-addr
- used-addr
- hold-addr
- release-addr
- busyout-free
- busyout-used

show ip pool-chunks pool all

このコマンド出力には、すべてのユーザープレーンに割り当てられている IPv4 プールチャンクが表示されます。

- chunk-id
- pool-id
- up-id
- total-addr
- free-addr
- used-addr
- hold-addr
- release-addr
- busyout-free
- busyout-used

Note 上記のフィールドは、**show ipv6 pool-chunks pool all** CLI コマンドでも表示されます。ただし、「hold-addr」および「release-addr」フィールドは除きます。

show ip pool-chunks up-id <up_id> user-plane-group name <grp-name>

このコマンドの出力には、特定のユーザープレーンに割り当てられているすべての IPv4 チャンクが表示されます。

- chunk-id
- pool-id
- up-id
- total-addr
- free-addr
- used-addr
- hold-addr
- release-addr
- busyout-free
- busyout-used

show ip user-plane chunks

このコマンドの出力には、各ユーザープレーンに割り当てられた IPv4 チャンクが表示されます。

- up-id
- total-chunks
- free-chunks
- used-chunks
- full-chunks

Note 前述の各フィールドは、**show ipv6 user-plane chunks** CLI コマンドでも表示されます。

show ip user-plane prefixes

このコマンドの出力には、各ユーザープレーンに割り当てられた IPv4 プレフィックスが表示されます。

- up-id
- Total
- Free
- Used
- Hold
- リリース
- Busyout-Free
- Busyout-Used

Note 前述の各フィールドは、**show ipv6 user-plane prefixes** CLI コマンドでも表示されます。

show ip user-plane verbose

このコマンドの出力では、ユーザープレーンに関する詳細がすべて表示されます。

- ユーザープレーンのグループ名
- ユーザープレーン ID
- ユーザープレーンのアドレス
- Sxmgr ID

- IPv4 チャンク
  - 合計
  - 未使用
  - 使用済み
  - フル
- IPv4 アドレス
  - 合計
  - 未使用
  - 使用済み
  - 保留
  - リリース
  - ビジーアウト - 未使用
  - ビジーアウト - 使用済み
- IPv6 チャンク
  - 合計
  - 未使用
  - 使用済み
  - フル
- IPv6 プレフィックス
  - 合計
  - 未使用
  - 使用済み
  - ビジーアウト - 未使用
  - ビジーアウト - 使用済み
- プールの総数
  - IPv4
  - IPv6
- プールカーネルルートの総数

- プールカーネルルートの最大数
- VRF の総数
- apn-without-pool-name-v4
- apn-without-pool-name-v6
- プールグループ

show ip user-plane

このコマンド出力には、VPNマネージャに登録されているすべてのユーザープレーンの詳細が表示されます。

- up-id
- user-plane-address
- user-plane-group-name
- sxmgr-id

注：

- 特定のユーザープレーングループに属する特定のユーザープレーンの詳細を表示するには、**show ip user-plane up-id***up_id***user-plane-group name** *grp-name* を使用します。

show ipv6 pool-chunks pool-name <pool-name>

この CLI コマンドの出力には、IPv6 プール内のすべてのチャンクが表示されます。

- chunk-id
- pool-id
- up-id
- total-addr
- used-addr
- busyout-free
- busyout-used

show ipv6 pool-chunks up-id <up_id> user-plane-group name <grp-name>

このコマンドの出力には、特定のユーザープレーンに割り当てられているすべての IPv6 チャンクが表示されます。

- chunk-id
- pool-id
- up-id

- total-addr
- used-addr
- busyout-free
- busyout-used

show ipv6 pool-chunks up-id <up_id> user-plane-group name <grp-name>

第 42 章

IP ソース違反

この章では、次の事項について説明します。

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

CUPS アーキテクチャは、ユーザープレーンでのパケット送信元の検証をサポートします。送信元の検証は、パケットスプーフィングが疑われる場合や、ネットワーク内でのパケットの回送およびラベル付けの確認に有効です。

ユーザープレーンは、アップリンクデータパケットの送信元 IP アドレスと UE の IP アドレスが一致するかどうかを確認し、さらに設定された値に基づいて、データパケットをドロップするか許可するかを決定します。

この機能には、非 CUPS アーキテクチャの一部である既存の設定が実装されています。**ip source-violation** コマンド（[APN Configuration] モードの一部）は、パケット送信元の検証を実装するために使用されます。

IP ソース違反の設定

特定の APN に対するパケット送信元の検証を有効または無効にするには、次の設定を使用します。

```
configure
  context context_name
    apn apn_name
      ip source-violation { ignore | check [ drop-limit limit ] [
exclude-from-accounting ] }
      default ip source-violation
      end
```

注：

- **default**：サブスクライバから受信した送信元アドレスの違反チェックを有効にします。セッションが削除される前にサブスクライバから受信できる無効パケットのドロップ制限数は 10 です。
- **ignore**：APN の送信元アドレスチェックを無効にします。

  ユーザープレーンでは IP ソース違反カウンタは増分されず、ドロップされたパケットの統計はゼロになります。ユーザープレーンが別のストリームを作成し、VPP が同じストリーム ID を使用し、fastpath を介してそれらのパケットを送信します。
- **check [drop-limit** *limit* **]**：デフォルトは [Enabled] で、limit は 10 です。

  サブスクライバから受信した送信元アドレスの違反チェックを有効にします。drop-limit を設定して、セッションが削除される前にサブスクライバから受信できる無効なパケット数に対する制限を設定できます。

  limit：0 ～ 1,000,000 の任意の整数値に設定できます。値 0 は、すべての無効なパケットが廃棄され、セッションはシステムによって削除されないことを示します。
- **exclude-from-accounting**：アカウンティングレコード用に生成された統計情報から、IP ソース違反で識別されたパケットを除外します。

  exclude-from-accounting が無効になっている場合：
  - ドロップされたパケットは考慮されませんが、VPP から送信されたパケットは課金されます。
  - 使用状況レポートの URR にドロップバイト数が表示されます。
  - パケットドロップカウンタが増加します。

  exclude-from-accounting が有効になっている場合：
  - ドロップされたパケットは考慮されません。
  - 使用状況レポート URR にドロップされたパケットは表示されません。
  - パケットドロップカウンタが増加します。

モニタリングおよびトラブルシューティング

この項では、IP ソース違反機能のモニタリングと障害対応について説明します

コマンドや出力の表示

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show sub user-plane-only full all

上記のコマンドを実行すると、この機能に関する次のフィールドが表示されます。

- ip source violations

第 43 章

CUPS での IPSec

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.25

機能説明

IPSec は、IP ネットワーク全体でセキュアなプライベート通信を提供するために相互にデータをやり取りする一連のプロトコルです。これらのプロトコルにより、システムはピアセキュリティ ゲートウェイとセキュアなトンネルを確立して維持できます。IPSec は、IP データグラムに機密性、データの完全性、アクセス制御、およびデータソース認証を提供します。

IPSec AH および ESP

認証ヘッダー（AH）とカプセル化セキュリティペイロード（ESP）は、IPSec で使用される 2 つの主要なワイヤレベルプロトコルです。IPSec 接続を介して流れるデータを認証（AH）し、暗号化して認証（ESP）します。

- AH は、IP トラフィックの認証に使用されるもので、暗号化には使用されません。認証は、IP パケットのほぼすべてのフィールド（TTL やヘッダーチェックサムなど、転送中に変更される可能性があるフィールドを除く）に対する暗号化ハッシュベースのメッセージ認証コードを計算することによって実行されます。計算されたメッセージ認証コードは、

新たに追加される AH ヘッダーに格納され、相手側に送信されます。AH ヘッダーは、元の IP ヘッダーとペイロードの間に挿入されます。

- ESP は暗号化と、オプションとして認証を提供します。ESP には、暗号化とオプションである認証をサポートするヘッダーフィールドとトレーラフィールドが含まれます。IP ペイロードの暗号化は転送モードでサポートされ、パケット全体の暗号化はトンネルモードでサポートされます。認証は、ESP ヘッダーと暗号化されたデータが対象となります。

IPsec トランスポートモードとトンネルモード

トランスポートモードでは IP ペイロードがカプセル化されるため、2 つのエンドポイント間にセキュアな接続が提供されますが、トンネルモードでは IP パケット全体がカプセル化されて、2 つのゲートウェイ間に仮想「セキュアホップ」が提供されます。

トンネルモードでは、IP パケット全体が別の内部にカプセル化されて、接続先に配信される、より一般的な VPN 機能が形成されます。完全な IP ヘッダーとペイロードがカプセル化されます。

（注） IPSec を介した UP:UP ICSR は、トンネルモードでのみ機能します。トランスポートモードはサポートされていません。

IPSec 用語

暗号アクセス制御リスト

アクセス制御リストでは、特定の条件を満たすサブスクライバ データ パケットを処理するためのルール（通常は権限）を定義します。ただし、暗号 ACL では、IPSec トンネルを介してルーティングされるサブスクライバ データ パケットに対応するために必要な条件を定義します。

インターフェイス、コンテキスト、または 1 つ以上のサブスクライバに適用される他の ACL とは異なり、暗号 ACL はクリプトマップと照合されます。また、暗号 ACL には 1 つのルールのみが含まれますが、他の ACL タイプは複数のルールで構成できます。

ルーティングの前に、システムは各サブスクライバデータ パケットのプロパティを調べます。パケットのプロパティが暗号 ACL で指定された条件と一致する場合に、システムはクリプトマップで指定された IPSec ポリシーを開始します。

トランスフォームセット

トランスフォームセットは、IPSec セキュリティ アソシエーション（SA）を定義するために使用されます。IPSec SA では、パケットを保護するために使用する IPSec プロトコルを指定します。

トランスフォームセットは、IPSec 確立のフェーズ 2 で使用されます。このフェーズでは、システムとピア セキュリティ ゲートウェイが、パケットを保護するためのルールを含む 1 つ以上のトランスフォームセット（IPSec SA）をネゴシエートします。このネゴシエーションにより、両方のピアがパケットを適切に保護および処理できるようになります。

ISAKMP ポリシー

Internet Security Association Key Management Protocol（ISAKMP）ポリシーを使用すると、インターネット キー エクスチェンジ（IKE）SA を定義できます。IKE SA は、システムとピア セキュリティ ゲートウェイ間の共有セキュリティパラメータ（使用する暗号化パラメータ、リモート ピアの認証方法など）を指定します。

IPSec 確立のフェーズ 1 では、システムとピア セキュリティ ゲートウェイが IKE SA をネゴシエートします。これらの SA は、IPSec SA ネゴシエーション プロセスを含むピア間の後続の通信を保護するために使用されます。

クリプト マップ

クリプトマップは、サブスクライバ データ パケットに IPSec を実装する方法を決定するトンネルポリシーを定義します。

CUPS では、いくつかのタイプのクリプトマップがサポートされています。その内容は次のとおりです。

- 手動クリプトマップ
- IKEv2 クリプトマップ
- ダイナミッククリプトマップ

暗号テンプレート

暗号テンプレートは、IKEv2 IPSec ポリシーを設定します。これには、暗号化および認証アルゴリズムのほとんどの IPSec パラメータと IKEv2 ダイナミックパラメータが含まれます。セキュリティ ゲートウェイ サービスは、暗号化テンプレートが設定されていなければ機能しません。

サービスごとに設定できる暗号テンプレートは 1 つのみです。ただし、1 つの StarOS インスタンスで、同じサービスの複数のインスタンスを実行することは可能で、これらのインスタンスそれぞれが該当する暗号テンプレートに関連付けられます。

ESP パケットの DSCP マーキング

SRP、SX、RCM、LI、TACACS などのアプリケーションは、異なるネットワークに展開されたノード間で動作します。これらすべてのアプリケーションでは、リモートシステムとの通信中に迅速なターンアラウンドが要求されます。Differentiated Services Code Point（DSCP）などの Quality of Service（QoS）を使用したカプセル化セキュリティペイロード（ESP）パケットのマーキングは、各タイプのパケットのトラフィック分類を決定するのに役立ちます。この機能

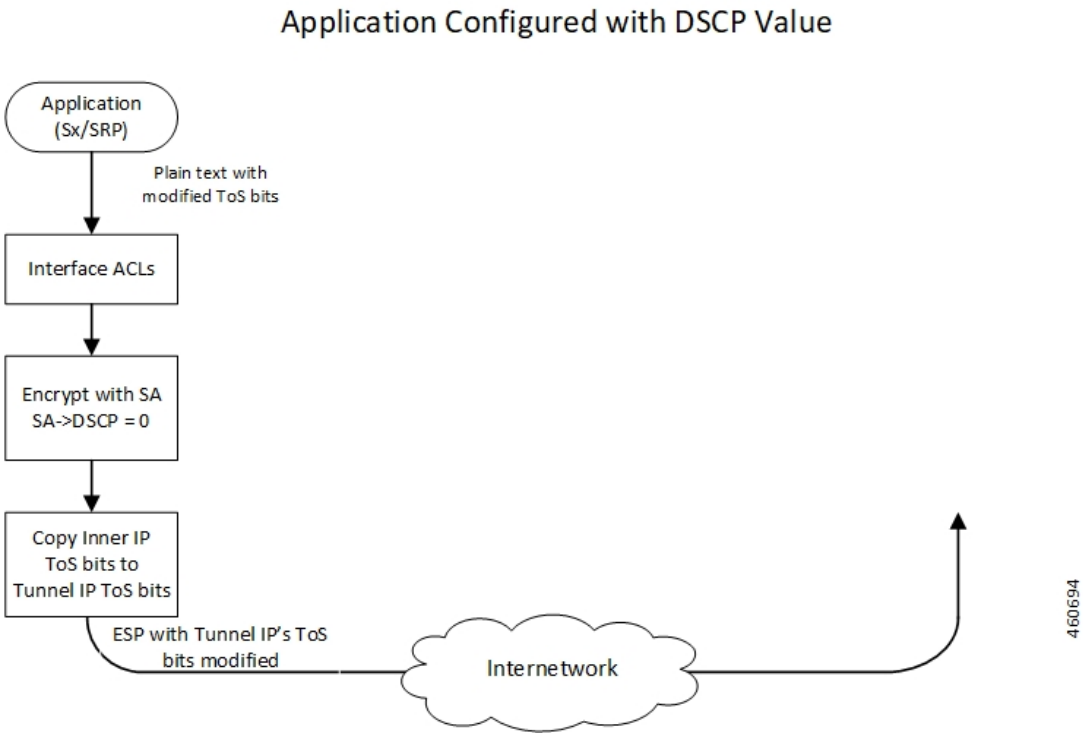
により、IP コアネットワーク内の IPsec パケットの優先順位付けが可能になり、IPsec を使用した Sx や SRP などのインターフェイスの拡張性が向上します。

ESP パケットに DSCP 値を適用する方法には、次の 2 つがあります。

- DSCP 値が設定されたアプリケーション経由
- DSCP 値が設定された暗号マップ経由

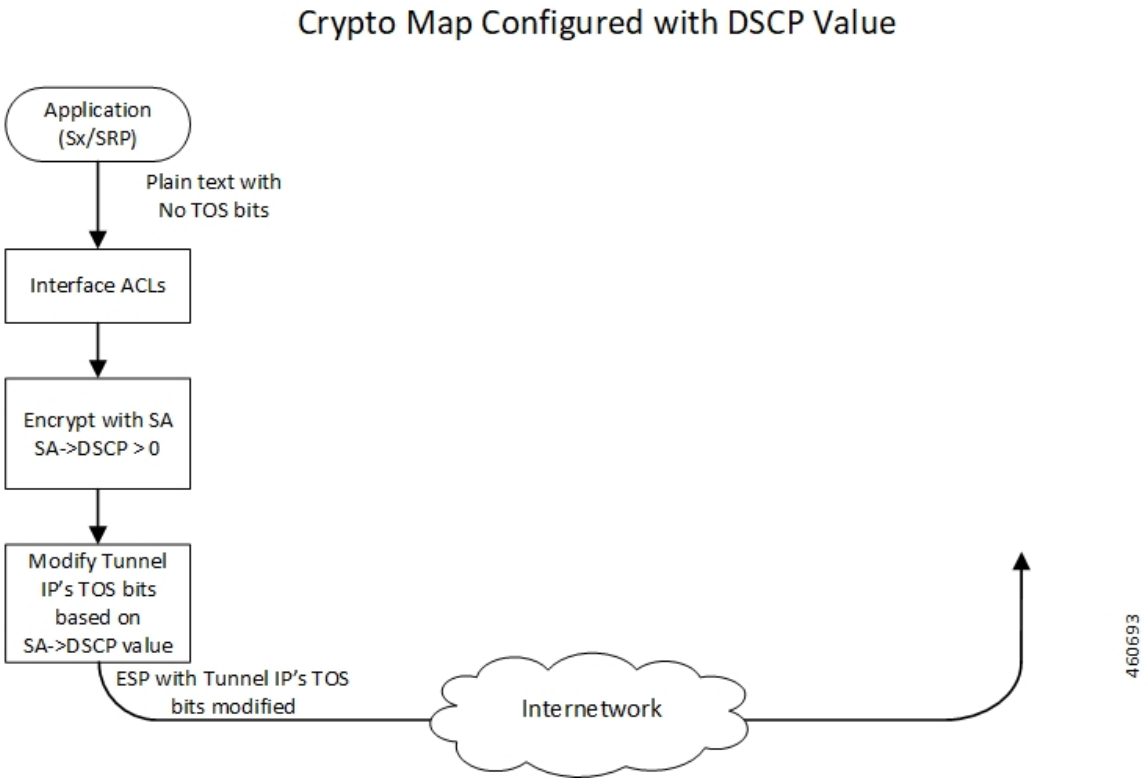
DSCP 値で設定されたアプリケーション

SRP、SX、LI などのアプリケーションが DSCP 設定をサポートしている場合、暗号化後の ESP パケットは、タイプオブサービス（ToS）ビットがアプリケーションの IP ヘッダーに設定されているかどうかを確認します。アプリケーションの IP ヘッダーの ToS ビットがゼロ以外の場合、内部 ToS ビットをトンネルの IP ヘッダーの ToS ビットにコピーしてから、パケットを出力します。次の図は、この処理の流れを示しています。



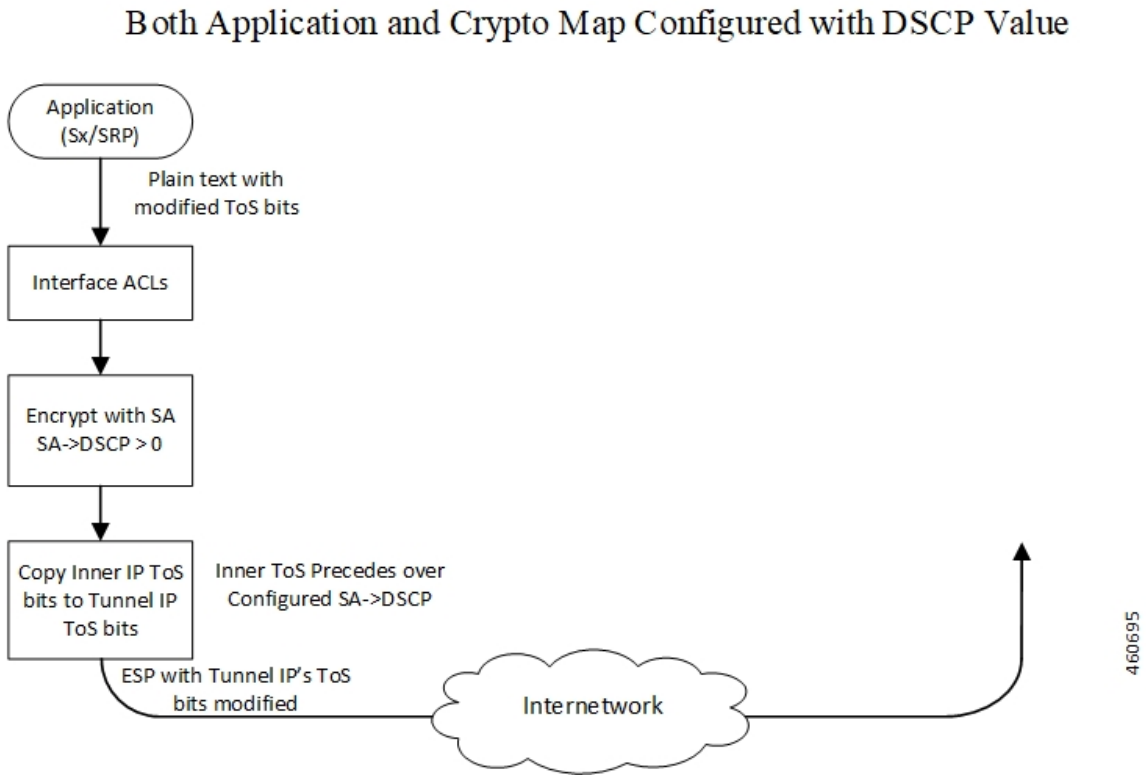
DSCP 値で設定されたクリプトマップ

暗号化が必要なすべてのアプリケーションには、ユーザーが設定できるクリプトマップが関連付けられています。特定のインターフェイスでクリプトマップを有効にすると、このクリプトマップのセキュリティ アソシエーション（SA）データベースで DSCP 値が更新されます。DSCP 値を保持するための新しいフィールドが SA データベース構造に定義されています。パケットが暗号化されると、SA データベースに有効な DSCP 値があるかどうかがチェックされます。有効な DSCP 値が見つかった場合、この DSCP 値はトンネル IP ヘッダーの ToS ビットにコピーされ、パケットは出力されます。次の図は、この処理の流れを示しています。



DSCP 値で設定されたアプリケーションとクリプトマップ

DSCP 値がクリプトマップとアプリケーション IP ヘッダーの両方で設定されている場合、アプリケーション ToS ビットが優先され、この値はトンネル IP ヘッダーの ToS ビットにコピーされます。次の図は、この処理の流れを示しています。



サポートされるアルゴリズム

CUPS の IPSec は、RFC 5996 で指定されている次の表のプロトコルをサポートします。

プロトコル	タイプ	サポートされるオプション（VPP なし）	サポートされるオプション（VPP あり）
インターネットキー	IKEv2 暗号化	DES-CBC、3DES-CBC、AES-CBC-128、AES-CBC-256	

プロトコル	タイプ	サポートされるオプション（VPP なし）	サポートされるオプション（VPP あり）
Exchange バージョン 2	IKEv2 疑似ランダム関数	PRF-HMAC-SHA1、PRF-HMAC-MD5、AES-XCBC-PRF-128	PRF-HMAC-SHA1、PRF-HMAC-MD5、AES-XCBC-PRF-128
	IKEv2 整合性	HMAC-SHA1-96、HMAC-SHA2-256-128、HMAC-SHA2-384-192 HMAC-SHA2-512-256、HMAC-MD5-96、AES-XCBC-96	HMAC-SHA1-96、HMAC-SHA2-256-128、HMAC-SHA2-384-192 HMAC-SHA2-512-256、HMAC-MD5-96、AES-XCBC-96
	IKEv2 Diffie-Hellman グループ	グループ 1（768 ビット）、グループ 2（1,024 ビット）、グループ 5（1,536 ビット）、グループ 14（2,048 ビット）	グループ 1（768 ビット）、グループ 2（1,024 ビット）、グループ 5（1,536 ビット）、グループ 14（2,048 ビット）
IP Security	IPSec カプセル化セキュリティペイロード暗号化	NULL、DES-CBC、3DES-CBC、AES-CBC-128、AES-CBC-256、AES-128-GCM-128、AES-128-GCM-64、AES-128-GCM-96、AES-256-GCM-128、AES-256-GCM-64、AES-256-GCM-96	NULL、DES-CBC、3DES-CBC、AES-CBC-192、AES-CBC-128、AES-CBC-256、AES-128-GCM-128、AES-128-GCM-64、AES-128-GCM- 96、AES-192-GCM、AES-256-GCM-128、AES-256-GCM-64、AES-256-GCM-96
	拡張シーケンス番号	0 またはオフの値がサポートされます（ESN 自体はサポートされません）。	0 またはオフの値がサポートされます（ESN 自体はサポートされません）。
	IPSec 整合性	NULL、HMAC-SHA1-96、HMAC-MD5-96、AES-XCBC-96、HMAC-SHA2-256-128、HMAC-SHA2-384-192、HMAC-SHA2-512-256 **重要** HMAC-SHA2-384-192 および HMAC-SHA2-512-256 は、ハードウェアに暗号化ハードウェアがない場合、VPC-DI および VPC-SI プラットフォームではサポートされません。	NULL、HMAC-SHA1-96、HMAC-MD5-96、HMAC-SHA2-256-128、HMAC-SHA2-384-192、HMAC-SHA2-512-256 **重要** HMAC-SHA2-384-192 および HMAC-SHA2-512-256 は、ハードウェアに暗号化ハードウェアがない場合、VPC-DI および VPC-SI プラットフォームではサポートされません。

（注） IPSec の詳細については、StarOS IPSec リファレンス [英語] を参照してください。すべての機能が CUPS に適用されるわけではないことに注意してください。

IPSec for Sx、LI、SRP などの詳細については、CUPS CP ガイド [英語]、CUPS UP ガイド [英語]、Sx インターフェイスガイド [英語]、および CUPS LI ガイド [英語] の関連する章を参照してください。

制限事項と制約事項

この機能には次の既知の制限事項と制約事項があります。

- この機能は、アプリケーション ToS の変更をサポートしていません。
- 暗号マップ CLI コマンドの DSCP 値の設定は、アプリケーションが UP の **Day-1** 設定として設定されているコンテキストと同じコンテキストに追加する必要があります。
- トンネルの作成後に DSCP 設定を適用する場合は、関連付けられた暗号マップをインターフェイスに再適用する必要があります。
- SA でパケットの順序変更が発生すると、アンチリプレイメカニズムが原因で、レシーバでパケットが廃棄される可能性があります。

暗号マップでの DSCP の設定

特定のトランスフォームセットの DSCP 値を適用するには、次の CLI コマンドを使用します。

```
configure
   context context_name
     ipsec transform-set set_name
       dscp dscp_value
       exit
     exit
   end
```

設定例

以下に設定例を示します。

```
context ipsec-d
    ip access-list foo0
      permit tcp 209.165.200.225 209.165.200.250 209.165.200.245 209.165.200.250

    #exit

    ip access-list foo1
      permit tcp 209.165.200.225 209.165.200.250 209.165.200.247 209.165.200.250
```

```
    #exit
    ipsec transform-set A-foo
    dscp 0x28
    #exit
    ikev2-ikesa transform-set ikesa-foo
    #exit
crypto map foo0 ikev2-ipv4
      match address foo0
      authentication local pre-shared-key encrypted key encrypted_key
      authentication remote pre-shared-key encrypted key encrypted_key
      ikev2-ikesa max-retransmission 3

      ikev2-ikesa retransmission-timeout 15000

      ikev2-ikesa setup-timer 60

      ikev2-ikesa transform-set list ikesa-foo

      ikev2-ikesa rekey

      payload foo-sa0 match ipv4
        ipsec transform-set list A-foo
        lifetime 9000
        rekey keepalive
      #exit
      peer 209.165.201.1

      ikev2-ikesa policy error-notification

    #exit
    crypto map foo1 ikev2-ipv4

      match address foo1

      authentication local pre-shared-key encrypted key encrypted_key
      authentication remote pre-shared-key encrypted key encrypted_key
      ikev2-ikesa max-retransmission 3

      ikev2-ikesa retransmission-timeout 15000

      ikev2-ikesa transform-set list ikesa-foo

      ikev2-ikesa rekey

      payload foo-sa0 match ipv4

        ipsec transform-set list A-foo

        lifetime 9000

        rekey keepalive

      #exit

      peer 209.165.201.2

      ikev2-ikesa policy error-notification

    #exit
```

QoS の設定

DSCP でマーキングされた ESP パケットは、基盤となる L2 マーキング インフラストラクチャに従います。

DSCP に基づく QoS 設定により、シャーシからの出力前に ESP パケットの L2 マーキングがトリガーされます。

以下に設定例を示します。

```
Config
  qos ip-dscp-iphb-mapping dscp 0x28 internal-priority cos 0x1
  qos l2-mapping-table name l2Marktable
    internal-priority cos 0x1 color 0x0 802.1p-value 0x4 mpls-tc 0x6
   exit
end
```

注：

- **qos ip-dscp-iphb-mapping**：QoS プロファイルを作成します。
- **dscp***dscp_value*：IP DSCP 値を内部 QoS にマッピングします。
- **internal-priority cos** *class_of_service_value* **color** *color_value* **802.1p-value** *mpls_tc_value*：内部 QoS の優先順位を COS 値にマッピングします。

IPSec コンテキストで L2 マッピングテーブルを関連付けるための設定例を以下に示します。

```
config
   context ipsec-s
      associate l2-mapping-table name l2Marktable
end
```

注：

- **associate l2-mapping-table**：QoS を内部 QoS から l2 値にマッピングします。
- **name** *table_name*：QoS を内部 QoS から l2 値にマッピングするテーブルの名前を指定します。*table_name* は、1 ～ 80 文字の英数字にする必要があります。

モニタリングおよびトラブルシューティング

ここでは、ESP パケット機能の DSCP マーキングのモニタリングや障害対応に使用できる CLI コマンドについて説明します。

show コマンドと出力

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show crypto map tag *tag_name*：このコマンドを使用して、設定された DSCP 値を表示します。

```
Map Name: foo0
=======================================

  IPSec Manager: 54
  Map status: Complete
  Payload:
 ACLs:
   foo0
 Rules:
   permit tcp 209.165.200.225 209.165.200.250 209.165.200.245 209.165.200.250 eq 6002
  Crypto Map Type: IPSEC IKEv2 over IPv4
  IKE SA Transform 1/1
    Transform Set:
      Encryption Cipher: aes-cbc-128
      Encryption Accel: None
      Pseudo Random Function: sha1
      Hashed Message Authentication Code: sha1-96
      HMAC Accel: None
      Diffie-Hellman Group: 2
  IKE SA DSCP Value:  0x28

  IKE SA IDi [Peer]: Disabled

  IKE SA DH Exponentials reuse groups : None

  IKEv2 IKESA DDOS Mitigation Params:
    Half Open Timer: Disabled
    Decrypt Fail Count: Disabled
    Max IKEv2 requests Allowed : Disabled
    Message Queue Size: Disabled
    Rekey Rate: Disabled
    Max Certificate Size: Disabled

  IKEv2 Notify Payload:
    Device Identity: Enabled[Default]
  Notify Payload Error Message Type:
    UE: 0
    Network Transient Minor: 0
    Network Transient Major: 0
    Network Permanent: 0

  Blacklist/Whitelist : None

  OCSP Status         : Disabled
  OCSP Nonce Status  : Enabled
  OCSP Responder Address :None
  OCSP HTTP version : 1.0


  Remote-secret-list: <not-configured>

  Authentication Local:
   Phase 1 - Pre-Shared Key (Size = 7)

  Authentication Remote:
   Phase 1 - Pre-Shared Key (Size = 7)


  Self-Certificate Validation: Disabled
  Certificate Server Timeout: 20 Sec
  Minimum Certificate Key Size Validation: Disabled
```

```
Max Dhost Connections: 40

IPSec SA Payload 1/1
  Name : foo-sa0
  Payload Maximum Child SA: 1 [Default]
  Payload Ignore Ikesa Rekey: Disabled
  Payload Lifetime Params:
    Seconds: 90
    Sequence Number: 4293918720 [Default]
  Payload TSI Start Address: Address Endpoint
  Payload TSI End Address: Address Endpoint

  IPSec SA Transform 1/1
    Transform Set:
      Protocol: esp
      Encryption Cipher: aes-cbc-128
      Encryption Accel: None
      Hashed Message Authentication Code: sha1-96
      HMAC Accel: None
      Diffie-Hellman Group: none
      ESN: Disabled
      Dscp: 0x28
Dont Fragment: Copy bit from inner header
IPv4 Payload fragment type: outer
MTU: 1438 [Default]

NATT: Disabled


IKEv2 Fragmentation: Enabled
IKEv2 MTU Size IPv4/IPv6: 1384/1364

CERT Enc Type URL Allowed: Disabled
Custom FQDN Allowed: Disabled
DNS Handling: Normal [Default]

interface using this crypto-map: saegw-li1-loopback-ipv4

Local Gateway: 209.165.202.129
Remote Gateway: 209.165.201.1
```

show qos ip-dscp-iphb-mapping：このコマンドを使用して、パケット内の QoS 情報から internal-qos マーキングへのマッピングを表示します。

```
--------------+-----------------
    DSCP      |     Internal Qos
--------------+-----------------
   0x00       |          0
   0x01       |          0
   0x02       |          0
   0x03       |          0
   0x04       |          0
   0x05       |          0
   0x06       |          0
   0x07       |          0
--------------+-----------------
   0x08       |          0
   0x09       |          0
   0x0a       |          0
   0x0b       |          0
   0x0c       |          0
   0x0d       |          0
```

```
   0x0e       |         0
   0x0f       |         0
--------------+-----------------
   0x10       |         0
   0x11       |         0
   0x12       |         0
   0x13       |         0
   0x14       |         0
   0x15       |         0
   0x16       |         0
   0x17       |         0
--------------+-----------------
   0x18       |         0
   0x19       |         0
   0x1a       |         0
   0x1b       |         0
   0x1c       |         0
   0x1d       |         0
   0x1e       |         0
   0x1f       |         0
--------------+-----------------
   0x20       |         0
   0x21       |         0
   0x22       |         0
   0x23       |         0
   0x24       |         0
   0x25       |         0
   0x26       |         0
   0x27       |         0
--------------+-----------------
  0x28        |         1
   0x29       |         0
   0x2a       |         0
   0x2b       |         0
   0x2c       |         0
   0x2d       |         0
   0x2e       |         0
   0x2f       |         0
--------------+-----------------
   0x30       |         0
   0x31       |         0
   0x32       |         0
   0x33       |         0
   0x34       |         0
   0x35       |         0
   0x36       |         0
   0x37       |         0
--------------+-----------------
   0x38       |         0
   0x39       |         0
   0x3a       |         0
   0x3b       |         0
   0x3c       |         0
   0x3d       |         0
   0x3e       |         0
   0x3f       |         0
--------------+-----------------
```

show qos l2-mapping-table name *table_name* ：このコマンドを使用して、L2 マッピング値への内部の名前付きテーブルを表示します。

```
Table: l2Marktable
------------------------+-------+-------
    Internal Priority    |802.1p | MPLS
```

Class-of-service	Color		
0	0	0x0	0
0	1	0x0	0
0	2	0x0	0
0	3	0x0	0
1	**0**	**0x4**	**6**
1	1	0x2	1
1	2	0x2	1
1	3	0x2	1
2	0	0x4	2
2	1	0x4	2
2	2	0x4	2
2	3	0x4	2
3	0	0x6	3
3	1	0x6	3
3	2	0x6	3
3	3	0x6	3
4	0	0x8	4
4	1	0x8	4
4	2	0x8	4
4	3	0x8	4
5	0	0xa	5
5	1	0xa	5
5	2	0xa	5
5	3	0xa	5
6	0	0xc	6
6	1	0xc	6
6	2	0xc	6
6	3	0xc	6
7	0	0xe	7
7	1	0xe	7
7	2	0xe	7
7	3	0xe	7

第 44 章

L2 マーキングのサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

CUPS の L2 マーキングのサポートにより、CUPS の QoS クラス識別子（QCI）のマーキングおよび Differentiated Services Code Point（DSCP）から派生した L2 マーキングが可能になります。QoS マーキングのサポートは、非 CUPS プラットフォームでサポートされる QoS マーキングのサポートに似ており、パケットが L2 ルータを通過するときに QoS 処理が維持されます。

機能の仕組み

ここでは、L2 マーキングの仕組みについて簡単に説明します。

基本的機能

- L2 マーキングのタイプは、サービス設定に従ってコントロールプレーン（CP）で決定されます。サポートされる L2 マーキングのタイプは、[DSCP-based]、[QCI-based]、および [None] です。
- ユーザープレーン（UP）で QCI 値が決まると、サービスに関連付けられた QCI テーブルでルックアップが実行されます。ルックアップの結果に基づき、対応する QCI 値の優先順位が選択または決定されます。
- 選択されたレイヤ 2 マーキングのタイプと優先順位は、Sx メッセージで UP に通知されます。
- UP への新しい情報の受け渡しをサポートするため、新しいカスタム IE が FAR IE に追加されます。
  - レイヤ 2 マーキング：
    - タイプと優先順位：<type> <priority-value>

      新しいカスタム IE は type-number「228」と定義されます。
- L2 マーキング（タイプまたは優先順位）が変更されると、ベアラーの更新が発生した場合と同じ内容が UP に通知されます。

Sx インターフェイスの変更

FAR 内の Layer 2 Marking IE

ベアラーの L2 マーキング情報を UP に渡すため、新しいカスタム IE が定義され、これを含む FAR が次のように変更されます。

表 *12 :* レイヤ *2* マーキング情報要素

情報要素	条件/コメント	アプリケーション				IE ID
		Sxa	Sxb	Sxc	N4	
レイヤ 2 マーキング	この IE は、レイヤ 2 マーキングのタイプ（存在する場合）を示します。	X	X			

Layer 2 Marking IE は次のようにエンコードされます。

表 *13 : PFCP FAR* 内の *Layer 2 Marking IE*

オクテット 1 および 2		Layer 2 Marking IE タイプ = 228（10 進数）			
オクテット 3 および 4		長さ = n			
情報要素	条件/コメント	アプリケーション			
		Sxa	Sxb	Sxc	N4
レイヤ 2 マーキング	この IE は、この FAR に一致するパケットに適用されるレイヤ 2 マーキングを特定します。 IE の長さは「0」または「1」です。この 1 バイトの中には、次の情報が含まれます。 • タイプと優先順位：<type> <priority-value> • タイプ：（1-DSCP、2-QCI、3-None）：最初の 2 ビット Priority-Value：最後の 6 ビット • タイプが [QCI] / [None] の場合は内部プライオリティ • タイプが [DSCP] の場合は DCSP 値	X	X	Sxc	N4

制限事項

このリリースにおけるこの機能の制限事項は次のとおりです。

QCI テーブルの変更は、サブスクライバにすぐには適用されず、ベアラーの更新後にのみ適用されます。

L2 マーキングの設定のサポート

ここでは、機能を有効または無効にするために使用できる CLI コマンドについて説明します。

内部優先順位の設定

GGSN、GTPv1 P-GW、および SAEGW コールの QCI マッピングテーブルで内部優先順位を設定するには、次のサービス固有の設定を使用します。GGSN サービス コンフィギュレーションのこのコマンドは、データパケット専用の QCI - QoS マッピングの動作をオーバーライドします。

```
configure
     context context_name
        ggsn-service service_name
           internal-qos data { dscp-derived | none | qci-derived }
           { no | default } internal-qos data { dscp-derived | none |
qci-derived }
           end
```

注：

- **no:** ：指定された機能を無効にします。
- **default:** ：機能を無効にします。
- **dscp-derived:** ：データパケットは、QCI - QoS マッピングテーブルで設定された DSCP に基づいてレイヤ 2 でマーキングされます。DSCP が QCI - QoS マッピングテーブルで設定されていない場合、データパケットはマーキングされません。
- **none:** ：データパケットは、レイヤ 2（MPLS EXP/802.1P）マーキングでマーキングされません。
- **qci-derived:** ：データパケットは、QCI - QoS マッピングテーブルで設定された internal-qos-priority に基づいてレイヤ 2 でマーキングされます。internal-qos-priority が QCI - QoS マッピングテーブルで設定されていない場合、データパケットはマーキングされません。

QCI-QoS マッピングテーブルの関連付け

CP で QCI-QoS マッピングテーブルを関連付けるには、次のコマンドを使用します。

```
configure
  context context_name
    associate qci-qos-mapping { map_table_name map_table_name }
    exit
```

注：

- **map_table_name** *map_table_name*：QoS を L2 値にマッピングする内部テーブルの名前を指定します。

  map_table_name は、0 ～ 80 文字の文字列である必要があります。

- このコマンドは、デフォルトで無効になっています。

QCI 派生 L2 マーキングの設定

下記のコマンドを使用すると、次のことを行えます。

- レイヤ 2 マッピングテーブルを作成または変更する。
- QoS L2 マッピング コンフィギュレーション モードを開始して、内部 QoS の優先順位をユーザープレーン（UP）のレイヤ 2 QoS 値にマッピングする。

```
configure
  qos l2-mapping-table { name map_table_name| system-default }
  exit
```

注：

- **name** *map_table_name*：QoS を L2 値にマッピングする QoS マッピングテーブルの名前を指定します。802.1p、mpls などの L2 値への内部マッピングを有効にします。

  map_table_name は、0 ～ 80 文字の英数字文字列である必要があります。

- **system-default**：システムのデフォルトマッピングを設定します。システムデフォルトは、すべての VRF またはコンテキストのデフォルトとして常に関連付けられます。
- このコマンドは、デフォルトでイネーブルになっています。

L2 マッピングテーブルの関連付け

設定された L2 マッピングテーブルを特定の VRF やコンテキストに関連付けるには、次のコマンドを使用します。

```
configure
  context context_name
    associate l2-mapping-table name table_name
    exit
```

注：

- **l2-mapping-table name** *table_name*：QoS を L2 値にマッピングする内部テーブルの名前を指定します。

  map_table_name は、0 ～ 80 文字の英数字文字列で指定する必要があります。

- このコマンドは、デフォルトでイネーブルになっています。

DSCP 派生 L2 マーキングの設定

次のコマンドを使用して、ユーザープレーン（UP）で Differentiated Services Code Point（DSCP; DiffServ コードポイント）からサービスクラス（CoS）へのマッピングを変更します。

```
configure
  qos ip-dscp-iphb-mapping dscp dscp_value internal-priority cos
```

```
class_of_service_value
  exit
```

注：

- **ip-dscp-iphb-mapping**：パケット内の DSCP 情報の内部 QoS マーキングへのマッピングを管理します。

  「ip-dscp-iphb-mapping」は、UP ごとのグローバルテーブルです。

- **dscp** *dscp_value*：IP DSCP 値を内部 QoS にマッピングします。

  dscp_value は、0x0 ～ 0x3F の 16 進数である必要があります。

- **internal-priority cos** *class_of_service_value*：内部 QoS 優先順位または CoS にマッピングします。

  class_of_service_value は、0x0 ～ 0x7 の 16 進数である必要があります。

- このコマンドは、デフォルトでイネーブルになっています。

第 45 章

Ruledef での L3、L4、および L7 ルールの組み合わせ

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
拡張 ACS 機能の一部として CLI コマンドのサポートが追加されました。	21.27
最初の導入。	21.24 より前

機能説明

Ruledef 機能の L3、L4、および L7 ルールの組み合わせを使用すると、トラフィックを次の特定の評価グループ（RG）に分類できます。

- 特定の IP アドレス
- ポート
- Uniform Resource Locator（URL）

ホストプールの拡張性が向上し、256 から 512 に増えました。この機能を使用すると、1 つのプールに 256 エントリがある **url-sni-pool** の設定を許可および定義できます。エントリは、URL 値と Server Name Indication（SNI）値を組み合わせて指定できます。URL-SNI プールのシステム全体の制限は 384 エントリです。

機能の仕組み

この機能を使用すると、**url-sni-pool** 設定の URL または SNI のリストを定義できます。システムは、ruledef 内の L7 フィルタとして URL または SNI のプールを使用します。ruledef には、ホストプール、ポートマップ、および URL SNI プール一致の組み合わせを指定できます。システムは、既存の 32 のルール行を占有することなく、他のルール行の基準と合わせて url-sni-pool の設定を照合します。

拡張 ACS 機能

この機能は、Config Manager における次の ECS 構造をサポートします。

- Ruledef
- ホストプール
- ポートマップ
- IMSI プール
- Ruledef のグループ
- 課金アクション
- URL-SNI プール
- ルールベース
- アクション優先回線
- ルーティングの ruledef
- 帯域幅ポリシー
- モニタリングキー
- XHeader
- ACS レベルの設定

ECSv2 構造に関する新しい制限事項は次のとおりです。

構造	制限
Ruledef	5000
Ruledef ごとのルール行	32

構造	制限
Group-of-Ruledef	512
Group-of-Ruledef 内の Ruledef	512
ホストプール	1200
ホストプールごとの IP/IP 範囲	256
ポートマップ	800
ポートマップごとのポート/ポート範囲	20
URL-SNI-Pool	1200
URL-SNI-Pool プールごとの URL/SNI	256
GW ノードごとの IP/IP 範囲	30,000
GW ノードごとの URL/SNI	30,000
GW ノードごとのポート/ポート範囲	3000
ルールベースごとのアクション優先回線	3000
GW ノードごとのアクション優先回線	50,000
GW ノードごとのルーティング優先回線	5000

拡張 ACS 機能の有効化

拡張 ACS モードを有効にするには、次の設定を使用します。

CP の場合：

```
configure
  require enhanced-acs-config control-plane
```

UP の場合：

```
configure
  require enhanced-acs-config user-plane
```

（注） これら 2 つの設定は、リブート後にのみ有効になります。したがって、Day-0 設定に追加する必要があります。

Ruledef 機能での L3、L4、および L7 ルールの組み合わせの設定

新しい [URL-SNI Pool Configuration] モードは、[ACS Configuration] モード内で使用できます。この機能を有効にするには、次の設定を使用します。

```
configure
  active-charging service service_name
    url-sni-pool pool_name
      http url { contains | starts-with | ends-with | = | !contains
| !starts-with | !ends-with | != } url_name
      tls sni { contains | starts-with | ends-with | = | !contains |
 !starts-with | !ends-with | != } sni_identity
    ruledef ruledef_name
      ip server-ip-address host_poolname
      tcp either-port port-map port_mapname
      http-tls url-sni-pool pool_name
      end
```

（注）

- システムは、デフォルトの [all-lines AND] オプションまたは [multi-line-or-all-lines] オプションを使用して ruledef を設定します。
- [url-sni-pool] ルール行が設定されている場合、URL または SNI 値は、AND 一致または OR 一致のいずれの演算かに関係なく常に照合されます。
- AND 演算が設定されている場合、プール内の URL または SNI 値に加えて、他のすべてのルール行が照合されます。
  - AND 演算がデフォルト設定です。
- OR 演算を設定すると、システムはルールアクションを有効にするために次の値を照合します。
  - 他のルール行のいずれか
  - URL または SNI

Ruledef 機能設定での L3、L4、および L7 ルールの組み合わせの確認

次の show CLI コマンドを使用して、url-sni-pool 設定を確認します。

- コントロールプレーンの場合：**show configuration active-charging service name** *service_name*

例として、この show CLI コマンドの出力の一部を示します。

```
url-sni-pool url_pool1
         http url contains google.com
         tls sni contains gmail.com
```

- ユーザープレーンの場合：**show user-plane-service url-sni-pool name** *pool_name*

  例として、この show CLI コマンドの出力の一部を示します。

```
url-sni-pool url_pool1
         http url contains google.com
         tls sni contains gmail.com

Total url-pool(s) found: 1
```

モニタリングおよびトラブルシューティング

show コマンドと出力

ここでは、この機能をサポートするために使用可能な show CLI コマンドについて説明します。

show configuration active-charging service name <service_name>

ルール定義への url-sni-pool 付加情報を表示するには、コントロールプレーンでこの CLI コマンドを使用します。

コマンドの出力例の一部を以下に示します。

```
ruledef special_charging_group1
      ip server-ip-address range host-pool IP_FREE_MUSIC
      tcp either-port range port-map PORT_FREE_MUSIC
      http-tls url-sni-pool url_pool1
```

show user-plane-service ruledef name <ruledef_name>

ルール定義への url-sni-pool 付加情報を表示するには、ユーザープレーンでこの show CLI コマンドを使用します。

コマンドの出力例の一部を以下に示します。

```
Ruledef Name: special_charging_group1
    ip server-ip-address range host-pool IP_FREE_MUSIC
    tcp either-port range port-map PORT_FREE_MUSIC
    Rule Application Type: Charging
    Copy Packet to Log: Disabled
    Tethered Flow Check: Disabled
    Attached Url-Sni-Pool: url_pool1
    Multi-line OR: Disabled
```

第 46 章

L7 PCC ルール

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

この機能により、L7 アナライザ機能が CUPS アーキテクチャでサポートされます。

次の L7 アナライザがサポートされています。

- HTTP
- HTTPS
- RTP/RTSP
- FTP
- DNS
- コンテンツ フィルタリング
- DNS スヌーピング

次の課金アクションがサポートされています。

- 廃棄
- 終了フロー
- リダイレクト（該当する場合）

機能の仕組み

この項では、この機能の一部としてサポートされている L7 アナライザ機能の概要について説明します。

コンテンツ フィルタリング

コンテンツフィルタリングは、3GPP および 3GPP2 ネットワークで使用可能なインラインサービスです。HTTP リクエスト内の URL に基づいてモバイルサブスクライバからの HTTP リクエストをフィルタ処理します。これにより、オペレータは個々のサブスクライバがアクセスできるコンテンツをフィルタ処理して制御できるため、サブスクライバが常識的に容認されないコンテンツや望まないコンテンツに思いがけずさらされることはありません。

コンテンツフィルタリング機能は、非 CUPS アーキテクチャで実装されているものと同じです。詳細については、『 *CF Administration Guide*』 の「 *Content Filtering Support Overview*」の章 [英語] を参照してください。

コンテンツフィルタリングの設定

コンテンツフィルタリングを有効にするには、次の追加設定を使用します。

```
configure
  require user-plane content-filtering
    content-filtering category database directory path path_address
    content-filtering category database max-version version_number
    end
```

（注） コンテンツフィルタリングを有効にするには、ブート時に上記の設定をユーザープレーンで設定する必要があります。ユーザープレーン設定後に上記の設定を定義すると、エラーや不整合が発生します。

（注） この機能を有効にするには、ユーザープレーンのライセンスと既存のコンテンツ フィルタリング ライセンスがユーザープレーンで必要です。

（注） ICSR ユーザープレーン 1:1 の場合、データベースは両方の UP に個別にロードされます。コントロールプレーンの残りのコンテンツフィルタリング設定はそのままです。コンテンツフィルタリングの設定は、コントロールプレーンからアクティブユーザープレーンにプッシュされ、次にスタンバイユーザープレーンにプッシュされます。

コントロールプレーンでの設定

次の設定例は、コンテンツフィルタリング機能に対応するためにコントロールプレーンで必要な変更を示しています。

```
config
            active-charging-service ACS
               content-filtering category policy-id 1
               analyze priority 1 category ABOR
               analyze priority 2 category ADVERT action allow
               analyze priority 2 category ADVERT action allow action content-insert
"Content Restricted : The Web Guard feature has been enabled on your line. Web Guard has
 restricted your access to this content. The person on your Wireless account who is
designated as the Primary Account Holder can disable this restriction through the account
 management website"
                exit
           rulebase cisco
              content-filtering mode category static-only
              content-filtering flow-any-error permit
              content-filtering category policy-id 5
```

コントロールプレーンの設定は、PFD メカニズムを使用してユーザープレーンにプッシュされます。

ユーザープレーンのコンテンツフィルタリング設定を検証するには、次の show コマンドを使用します。

- show user-plane-service rulebase name cisco
- show user-plane-service content-filtering category policy-id

ユーザープレーンでの CFDB の生成を確認するには、次の show コマンドを使用します。

- show content-filtering category database facility srdbmgr
- show content-filtering category database verbose debug-only
- show content-filtering category database verbose
- show content-filtering category database url
- show content-filtering category url

特定のサブスクライバの PCRF から受信したコンテンツ フィルタリング ポリシー ID は、コールの確立時にユーザープレーンに送信されます。PFCP メッセージの Sx 確立要求や Sx 変更要求には、CF ポリシー ID が含まれています。

ユーザープレーンの CF ポリシー ID を確認するには、次のコマンドを使用します。

show subscribers user-plane-only callid full all

CUPS のコンテンツフィルタリングをサポートするために、次のフィールドが表示されます。

- Content Filtering Policy ID

SRDB 要求/応答/CF ポリシーアクションをモニターするには、次の show コマンドを使用します。

- show user-plane-service inline-services content-filtering category statistics
- show user-plane-service inline-services content-filtering category statistics rulebase name
- show content-filtering category statistics
- show content-filtering category statistics facility srdbmgr instance 1
- show content-filtering category statistics volume all

（注） 非CUPSアーキテクチャでコンテンツフィルタリング用に定義された既存のすべてのバルク統計情報は、CUPS にも適用できます。

制限事項

- ダイナミック コンテンツ フィルタリング モードはサポートされていません。
- ルールベースコマンド **content-filtering flow-any-error [permit | deny]** はサポートされていません。

DNS

SM-P へのオフロード

DNS パケットは SM-P にオフロードされません。

課金

DNS パケットは SM-P で課金されます。

ルールの照合

この機能は、非 CUPS アーキテクチャと同じです。

統計

DNSに関連する統計情報を取得するには、CLI コマンド**show user-plane-service statistics analyzer name dns** を使用します。

DNS スヌーピング

充電中

DNS スヌーピングの課金は SM-P で実行されます。

ルール定義

ルール定義のホスト名（domain-names）とホスト名の一部を指定するには、次の CLI コマンドを使用します。

```
ruledef <ruledef_name>
        ip [server-domain-name {contains|=|ends-with|starts-with}
<url_string>]
        ip [server-domain-name {contains|=|ends-with|starts-with}
<url_string>]
        multi-line-OR enabled
```

ip server-domain-name のルールラインを削除するには、この CLI の no バージョンを使用します。

```
ruledef <ruledef_name>
   no ip [server-domain-name {contains|=|ends-with|starts-with}
<url_string>]
   exit
```

ECS レベルで DNS エントリについて設定可能なタイマーには、次の CLI を使用します。

```
configure
        active-charging service service_name
           ip dns-resolved-entries timeout <value_secs>
           end
```

ip server-domain-name キーワードを含む ruledef が定義され、ルールベースで使用されるたびに、インスタンス単位でルールベースごとに ip-table が作成されます。

ルールの照合

この機能は、非 CUPS アーキテクチャの機能と同じです。

show CLI

次の CLI を使用して、DNS IP エントリ：**show user-plane-service [statistics dns-learnt-ip-addresses {summary | sessmgr instance <id> |all [verbose] }]** のテーブルを確認します。

バルク統計情報

DNS スヌーピング機能をサポートするために、次のバルク統計情報を使用できます。

- ecs-dns-learnt-ipv4-entries
- ecs-dns-flushed-ipv4-entries
- ecs-dns-replaced-ipv4-entries

- ecs-dns-overflown-ipv4-entries
- ecs-dns-learnt-ipv6-entries
- ecs-dns-flushed-ipv6-entries
- ecs-dns-replaced-ipv6-entries
- ecs-dns-overflown-ipv6-entries

前述のバルク統計情報は、非 CUPS アーキテクチャと同様に ECS スキーマに追加されます。

（注） SNMP トラップ生成コマンドは、CUPS DNS スヌーピング機能ではサポートされていません。

FTP

SM-P へのオフロード

FTP データの場合のみ、TRM エンゲージメントが実行されます。FTP データフローは、SM-P へのオフロードに適しています。

制御 FTP フローに対する TRM エンゲージメントはありません。

課金

FTP パケットは SM-P で課金されます。

ルールの照合

この機能は、非 CUPS アーキテクチャと同じです。

統計

FTP に関連する統計情報を取得するには、CLI コマンド **show user-plane-service statistics analyzer name ftp** を使用します。

HTTP

SM-P への HTTP オフロード

HTTP リクエスト/応答ヘッダーが完了すると、次の場合にアップリンク/ダウンリンクのデータパケットが VPP にオフロードされます。

- Content-Length：ボリュームベースのオフロードは、GET や POST などのメソッドでサポートされます。チャンクエンコーディングによるデータ転送メカニズムを使用した HTTP フローは、HTTP で定義されているメソッドに関係なくオフロードされません。ストリームがコンテンツ長に基づいてオフロードされた場合、もう一方のストリームも、前者がオンロードされなくなるまでオフロードされます。

- CONNECT メソッド：フローが CONNECT にアップグレードされると、アップリンクとダウンリンクの両方のストリームがオフロードされるメソッド。
- WebSocket メソッド：フローが WebSocket プロトコルとして分類されると、アップリンクとダウンリンクの両方のストリームがオフロードされます。
- ストリームは、次のいずれかの場合に SM-U アプリケーションにオンロードされます。
  - FIN パケットを受信した場合
  - コンテンツ長に違反している場合
  - PDN の更新

ヘッダー解析

非 CUPS 実装と同様に、rulebase に含まれる ruledef で定義されているヘッダーフィールドのみが解析されます。または、X-Header などの機能の場合は、一部の HTTP ヘッダーフィールドに応じたリダイレクトが設定されます。

ルール照合

CUPS で行われるルール照合の方法に機能的な変更はありません。唯一の変更は、アップリンクとダウンリンクの両方に独自の TRM がある場合の TRM に特有なものです。

HTTP 課金

- 完全なパケットは SM-P で課金されます。
- 部分的パケットは、完成時に SM-U で課金されます。部分的パケットを完成させるパケットも SM-U で課金されます。
- 連結パケットは SM-U で課金されます。
- 遅延課金が有効になっている場合：未課金のバイトがあると、パケットと合わせて未課金のバイトも SM-U で課金されます。
- 応答ベースの課金が有効になっている場合：応答を受信すると、アップリンクとダウンリンクの両方のパケットが SM-U で課金されます。後続のアップリンクおよびダウンリンクパケットは、部分的パケットまたは連結パケットでない限り、SM-P で課金されます。

X-Header の解析とルール照合

x-header ルール行が含まれる ruledef が解析され、照合されます。

WebSocket

機能は、非 CUPS アーキテクチャと同じです。

TRM および応答ベースの課金

トランザクションルール照合では、フローが完全に分類されてはじめて、パケットごとのルール照合が回避されます。

方向ベースの TRM が CUPS で導入されました。1 つのフローに対して、アップリンク方向とダウンリンク方向の 2 つの TRM があます。1 つのパケットが TRM を有効にすると、後続の（TRM 対応）パケットも続けて同じルールに一致するため、効率的なルール照合が行われます。つまり、アップリンクパケットはアップリンク TRM キャッシュルールに一致し、ダウンリンクパケットはダウンリンク TRM キャッシュルールに一致します。

URL ベースのリダイレクト

機能は、非 CUPS アーキテクチャと同じです。

フローアクションの redirect-url で [encrypt] はサポートされません。現在、次のダイナミックフィールドがサポートされています。

- #HTTP.URI#
- #HTTP.HOST#
- #HTTP.URL#
- #ACSMGR_BEARER_CALLED_STATION_ID#
- #RULEBASE#
- #RTSP.URI#

X-Header の挿入

HTTP リクエストへの X-Header の挿入がサポートされます。動作は、非 CUPS アーキテクチャでの動作と同じです。SM-P へのオフロードに関しては、次のとおりです。

- パケットに X-Header が挿入されているフローはオフロードされません。
- X-Header 設定では、送信順序 CLI に関係なく、すべての TCP OOO パケットがバッファされ、順序変更後に送信されます。

X-Header 挿入統計 CLI

show user-plane-service statistics charging-action name *charging_action_name*

X-Header の挿入をサポートする次のフィールドが追加されました。

- 要求の場合：
  - 挿入された XHeader のバイト数
  - 挿入された XHeader のパケット数
  - 削除された XHeader のバイト数
  - 削除された XHeader のパケット数

• XHeader によって消費される IP フラグメント数

制限事項

- X-Header スプーフィングはサポートされません。
- 応答パケットへの X-Header への挿入はサポートされません。
- X-Header の暗号化では、RSA および RC4MD5 はサポートされますが、AES はサポートされません。
- X-Header のモニタープロトコルはサポートされません。
- パケットへの次の X-Header フィールドの挿入はサポートされません：QoS、UIDH、Customer ID、Hash Value、Time of the Day、Radius String、Session-Id、Congestion Level、User-Profile

HTTP アナライザ統計

HTTP アナライザに関連する統計を取得するには、**show user-plane-service statistics analyzer name http** CLI コマンドを使用します。

HTTPS

SM-P への HTTPS オフロード

HTTPS フローは、アプリケーションパケットの受信後に SM-P にオフロードされます。P2P アナライザの場合、P2P アナライザが L7 プロトコルを検出するとオフロードが機能します。

HTTPS 課金

HTTPS パケットの課金は SM-P で行われます。

統計

HTTPS に関連する統計情報を取得するには、次の CLI コマンドを使用します。**show user-plane-service statistics analyzer name secure-http**

HTTP URL フィルタリング機能

HTTP URL フィルタリング機能は、URL 検出に使用されるルール定義を簡素化します。

HTTP リクエストパケットには、プロキシ（プレフィックス付き）URL と実際の URL を含めることができます。プロキシ URL が HTTP リクエストパケットで見つかった場合、HTTP URL フィルタリング機能は解析された情報からこの URL を切り捨て、実際の URL のみがルール照合とイベントデータレコード（EDR）の生成に使用されます。

HTTP URL フィルタリング機能の設定

ここでは、HTTP URL フィルタリング機能の設定方法について説明します。

プレフィックス付き URL のグループの設定

プレフィックス付き URL のグループを設定するには、次の CLI コマンドを使用します。

```
configure
  active-charging service ecs_service_name
    group-of-prefixed-urls prefixed_urls_group_name
    end
```

プレフィックス付き URL のグループ内 URL の設定

プレフィックス付き URL のグループでフィルタリング対象の URL を設定するには、次の CLI コマンドを使用します。

```
configure
  active-charging service ecs_service_name
    group-of-prefixed-urls prefixed_urls_group_name
      prefixed-url url_1
      ...
      prefixed-url url_10
      end
```

ルールベースでのプレフィックス付き URL のグループの有効化

プレフィックス付き URL を処理するためにルールベースでプレフィックス付き URL のグループを有効にするには、次の CLI コマンドを使用します。

```
configure
  active-charging service ecs_service_name
    rulebase rulebase_name
      url-preprocessing bypass group-of-prefixed-urls
prefixed_urls_group_name_1
      ...
      url-preprocessing bypass group-of-prefixed-urls
prefixed_urls_group_name_64
      end
```

コントロール プレーン シャーシのこの設定は、「group-of-prefixed-urls」と「rulebase-url-preprocessing」の PFD メッセージを使用してユーザープレーンにプッシュされます。

プレフィックス付き URL のグループにはプロキシ URL のリストがあり、このリストは削除する必要があります。rulebase には、プレフィックス付き URL の複数のグループが含まれており、フィルタリングする必要があります。課金 ruledef には、プレフィックス付き URL グループ内の URL を削除してから検索する必要がある実際の URL のルールが含まれています。

（注）
- プレフィックス付き URL の 1 グループあたり、最大 10 個のプレフィックス付き URL を追加できます。
- 最大 64 のプレフィックス付き URL グループを作成および設定できます。

コマンドの表示

show user-plane-service group-of-prefixed-urls all | name *group_name*

この show コマンドをユーザープレーンで使用すると、プレフィックス付き URL のグループがプッシュされているかどうかを確認できます。このコマンドの出力は次のとおりです。

- Name of the group of prefixed URLs
- Prefixed URLs
- Total number of prefixed URLs found

show user-plane-service rulebase name *rbase_name*

この show コマンドをユーザープレーンで使用すると、プレフィックス付き URL のグループが rulebase で設定されているかどうかを確認できます。このコマンドの出力は次のとおりです。

- Name of rulebase
- Name of the groups of prefixed Urls for URL pre-processing

show user-plane-service statistics analyzer name http

このコマンドの出力は次のとおりです。

- Total HTTP Sessions
- Current HTTP Sessions
- Total Uplink Bytes
- Total Downlink Bytes
- Total Uplink Pkts
- Total Downlink Pkts
- Uplink Bytes Retrans
- Downlink Bytes Retrans
- Uplink Pkts Retrans
- Downlink Pkts Retrans
- Total Request Succeed
- Total Request Failed
- GET Requests

- POST Requests
- CONNECT Requests
- PUT requests
- HEAD requests
- Websocket Flows
- Invalid packets
- Wrong FSM packets
- Unknown request method
- Pipeline overflow requests
- Corrupt request packets
- Corrupt response packets
- Unhandled request packets
- Unhandled response packets
- Partial HTTP Header Anomaly prevented
- New requests on closed connection
- Memory allocation failures
- Packets after permanent failure
- Prefixed Urls Bypassed
- FastPath Statistics
- Total FP Flows
- Uplink (Total FP Pkts)
- Downlink (Total FP Pkts)
- Uplink (Total FP Bytes)
- Downlink (Total FP Bytes)

（注） パフォーマンス測定指標として、[Prefixed URLs Bypassed] カウンタが http アナライザ統計に追加されました。削除済みのプレフィックス付き URL 数を表示します。

RTP/RTSP

SM-P へのオフロード

UDP プロトコル上にある RTP はすぐにオフロードされます。

RTSP フローはオフロードされません。RTSP フローの TRM エンゲージメントはありません。

課金

RTP パケットは SM-P で課金されます。 RTSP パケットは、パケットが部分的でない場合、または遅延課金が有効になっている場合に SM-P で課金されます。

ルールの照合

この機能は、非 CUPS アーキテクチャと同じです。

統計

RTP に関連する統計情報を取得するには、CLI コマンド **show user-plane-service statistics analyzer name rtp** を使用します。

RTSP に関連する統計情報を取得するには、次の CLI コマンドを使用します。

- **show user-plane-service statistics analyzer name rtsp**
- **show user-plane-service statistics analyzer name rtsp verbose**

RTP ダイナミックフローの検出

rtp dynamic-flow-detection CLI コマンドは、[ACS Rulebase Configuration] モードで、Real Time Streaming Protocol（RTSP）および Session Description Protocol（SDP）アナライザが子 RTP および RTCP フローを検出できるようにします。RTSP/SIP および SDP アナライザを設定し、**rtp dynamic-flow-detection** CLI が存在していれば、RTP/RTCP の明示的な設定は必要ありません。**rtp dynamic-flow-detection** CLI コマンドを使用すると、子 RTP または RTCP フローが親 RTSP/SIP-SDP フローと相互に関連付けられます。

親フロー（RTSP/SIP-SDP）がクリアされると、子 RTP/RTCP フローもクリアされます。この CLI がない場合、RTP および RTCP の L7 レイヤ分析には、別途アナライザの設定が必要です。RTP/RTCP フローと RTSP/SIP-SDP フローとの相関関係はありません。

ベアラー固有フィルタのルール照合

ルール照合

機能は、非 CUPS アーキテクチャと同じです。

IMSI ベースのルールは、サブスクライバの IMSI に従って照合されます。

APN ベースのルールを使用すると、ベアラーフローのアクセスポイント名（APN）と一致するルール式を定義できます。

RAT タイプを使用すると、ベアラーフロー内の無線アクセス技術（RAT）に一致するルール式を定義できます。

ルール定義

IMSI プールを設定するには、次の CLI コマンドを使用します。

```
configure
  active-charging service service_name
    imsi-pool pool_name
      imsi { imsi_number | range start_imsi to end_imsi }
```

imsi-pool には、IMSI 値または IMSI の範囲を含めることができます。

次の CLI コマンドを使用して、ruledef でルール行を設定します。

```
configure
  active-charging service service_name
    ruledef ruledef_name
      bearer 3gpp imsi { = imsi_value } | { range imsi-pool pool_name }
      bearer 3gpp apn operator apn_name
      bearer 3gpp rat-type operator rat_type
```

IMSI 範囲は、IMSI プールを使用してルール内で設定できます。

上記の CLI コマンドの詳細については、StarOS の『*Command Line Interface Reference*』[英語] の「*ACS Ruledef Configuration Mode Commands*」を参照してください。

show CLI

サービスで設定されている IMSI プールに関する情報を表示するには、ユーザープレーンで次の CLI を使用します：**show user-plane-service imsipool name** *pool_name*

SIP

SM-P へのオフロード

SIP フローはオフロードされません。

充電中

SIP パケットは SM-P で課金されます。

ルールの照合

この機能は、非 CUPS アーキテクチャの機能と同じです。

統計

SIP に関連する統計情報を取得するには、次の CLI コマンドを使用します。**show user-plane-service statistics analyzer name sip**

第 47 章

CUPS のローカルポリシー

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

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、サーバー使用率など、セッションのさまざまな側面をローカルに定義されたポリシーに従って制御するために使用されます。これは、PCRF ベースのポリシー制御の代替や拡張を目的としています。ローカルポリシーは、特定のイベントや関連する条件の発生時にトリガーされます。

ローカルポリシー機能には、次の利点があります。

- 再利用性：ルールエンジンが PCRF ベースのポリシーの共通インフラストラクチャとして再利用可能です。
- リソース消費：メモリ使用率、CPU 使用率、および応答時間が低下します。
- 拡張性：最小限の労力で新しいイベントと属性を処理するための拡張性を備えています。
- 実行速度：ネットワークイベントの反応時間が短縮されます。

- 統合：既存のサービスへの影響を最小限に抑えながら、既存のポリシーインフラストラクチャ（IMSA および PCEF）とシームレスに統合します。到達不能イベントの場合、PCRF にフォールバックするメカニズムが実装されています。

ローカルポリシーは、さまざまなシナリオで役立ちます。次に例を示します。

- PCRF が使用できない場合、またはオペレータがインフラストラクチャに PCRF を展開していない場合、ローカルポリシーはフォールバックメカニズムとして動作します。
- PCRF トリガーのエンハンサーとして、特定のトリガーをローカルで処理するか、3GPP 標準または PCRF でサポートされていないトリガーを処理します。
- サブスクリプションポリシーが静的で階層化されている展開、または明確に定義されたサブスクライバグループがある展開。
- 応答時間の短縮が求められている場合。

（注） CUPS 環境でのローカルポリシー機能の動作は、非 CUPS P-GW および SAEGW ノードと同様です。

機能の仕組み

ローカルポリシー機能は、次の概念に基づいて実装されます。

- イベント駆動型ルールエンジン。例：RAT 変更イベント。
- 登録されたイベントトリガーが発生すると、イベントのタイプと現在の状態に基づいて一連の登録済みのルールが評価されます。
- ルールが一致すると、一連のアクションが実行されます。

CUPS でのローカルポリシーの設定

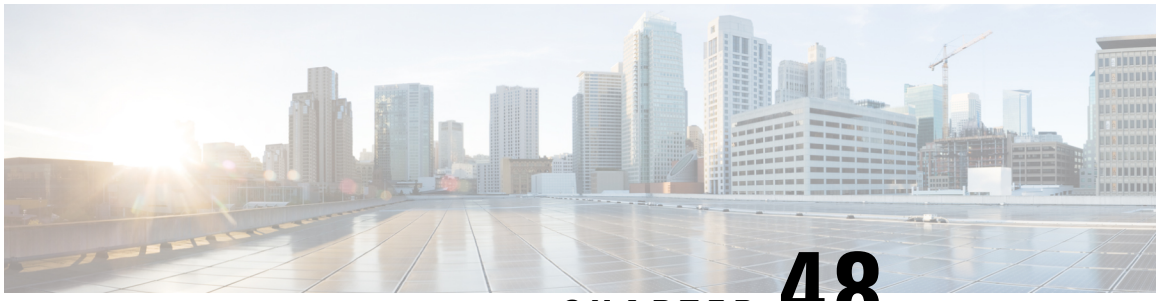
（注） 非 CUPS ローカルポリシー機能で使用可能な CLI コマンドは、CUPS 環境にも適用できます。

コントロールプレーンノードのローカルポリシーの設定例を以下に示します。

```
configure
  local-policy-service service_name
    ruledef ruledef_name
      condition priority priority radio-access-technology eq eutran
    ruledef ruledef_name
      condition priority priority apn eqcompare_string
```

```
      actiondef actiondef_name
        action priority priority default-qos qci qci_value arp arp_value
      actiondef actiondef_name
        action priority priority activate-rulebase name rulebase_name
eventbase eventbase_name
       rule priority priority event new-call ruledef ruledef_name actiondef
 actiondef_name
       rule priority priority event location-change ruledef ruledef_name
actiondef actiondef_name
       end
```

（注） ユーザープレーンノードでの設定は必要ありません。



CHAPTER 48

Sxでの負荷/過負荷およびUPデータスロットリングのサポート

機能説明

負荷/過負荷のサポートが PC CUPS アーキテクチャに実装されています。このサポートは、制御プレーン（CP）とユーザープレーン（UP）の間で処理されます。

負荷制御機能により、UP は負荷情報を CP に送信し、有効負荷に応じて UP 機能全体で PFCP セッション負荷を調整して分散できます。一方、過負荷制御機能では、特定の UP に対する新しいセッション要求をスロットリングできます。

機能の仕組み

ユーザープレーンの選択

負荷/過負荷のサポートが有効になっている場合、UP グループを使用して、以下のように UP の選択が実装されます。

- 過負荷状態の UP がない場合は、負荷制御情報（LCI）が UP の選択に使用されます。この場合、最も負荷が少ない UP が選択されます。
- すべての UP が過負荷状態の場合、過負荷制御情報（OCI）に基づいて UP が選択されます。この場合、最も過負荷が少ない UP が選択されます。
  - 特定の UP が選択された後も、スロットリングのために削減メトリックがこの UP に適用されます。

- スロットリングをドロップする必要がある場合、そのPDN接続に対するUPの選択要求は拒否されます。

- 一部の UP が過負荷状態で、一部の UP が過負荷状態ではないシナリオでは、OCI 値に基づいて選択が行われます。
- ピアノードの LCI または OCI 値が同じ場合、セッションカウント情報が UP の選択に使用されます。

ノードレベルの負荷/過負荷のサポート

CP は、有効になっている負荷/過負荷のサポートについて UP に通知します。この情報に基づいて、UP は負荷/過負荷情報を CP ピアに送信するかどうかを決定します。

CPでの負荷/過負荷のサポートは、Sxサービスノード設定の一部として設定されます。この情報は、dynamix 設定によって情報が変更された場合、Sx 関連付け応答または Sx 関連付け更新要求時に UP に送信されます。

（注） CPがサポートされているCLIを使った負荷/過負荷機能をサポートしていない場合、UPによって報告された負荷/過負荷は無視されます。その場合、引き続きセッションカウント情報に基づく UP の選択が行われます。

過負荷状態の CP での Sx 確立要求スロットリング

UP が過負荷状態になると、CP は UP に向けて Sx 確立要求メッセージのスロットリングを開始します。その結果、過負荷のUPへの新しいコール（低優先順位/非緊急）が回避されます。

スロットリングは、報告されたOCI値（過負荷削減メトリック値）に基づいて行われます。値は割合で計算され、当該 UP ピアに対する Sx 確立要求の必要な割合がランダムにドロップされます。結果として、切断理由「sx-no-resource」によって CP でコールがドロップされます。また、それぞれの統計が同じ数だけ増加します。

（注） eMPS（高優先順位）サブスクライバのセッションや緊急サブスクライバのセッションはスロットリングされません。

自己保護モードの UP での Sx 確立要求スロットリング

UP は自己保護状態になると、すべての新しいセッション（非 eMPS セッションのみ）、既存のセッションの Sx 確立要求、および Sx 変更要求（非 eMPS セッションのみ）を拒否し始めます。

自己保護モードの UP からのセッション終了トリガー

自己保護モードでは、UP の負荷状態が改善されない場合、UP が自己保護状態にあることを示す Sx レポート要求メッセージを介して、CP に対して段階的なセッション終了要求のトリガーを開始します。これに基づいて、CP は該当するセッションの Sx 終了要求の発出を開始します。

Self Protection Termination Request (SPTER)：このビットは、自己保護に基づく終了を開始するために、UP から CP に対して設定されます。CP は、「graceful-term-up-self-protectn」という切断理由でコールを解放します。

（注） [Actual Load] 値が [Session-Termination-Start-Threshold] 値より大きくなると、CP に対してセッション終了がトリガーされます。

制限事項

この機能には、次の既知の制限事項があります。

- UP でサポートされている負荷/過負荷プロファイルの最大数は 8 です。
- 負荷/過負荷プロファイルが UP グループ内のすべての UP で設定されていない場合、セッションの分散が不均一になる可能性があります。単一の UP グループで負荷/過負荷サポートを使用してすべての UP を設定することを推奨します。
- セッションリカバリ後、SessMgr インスタンスは SxDemux から負荷/過負荷値を再学習します。SxDemux では、負荷/過負荷の値が変更された場合にのみ、各値が伝達されます。
- オンザフライでの負荷制御設定の切り替え（有効から無効、または無効から有効）はサポートされていません。
- 1 つの UP グループ内の UP はすべて、有効または無効にする必要があります。CP の負荷/過負荷値が不適切な値になる可能性があるため、UP グループ内で 1 つの UP を有効にし、もう 1 つの UP を無効にすることはできません。
- すべての IMS UP の負荷制御を無効にすることを推奨します。

負荷および過負荷サポートの設定

負荷および過負荷のサポートは、次を使用して設定します。

- ユーザープレーン負荷制御プロファイルの設定
- ユーザープレーン過負荷制御プロファイルの設定
- ユーザープレーンサービスへの負荷プロファイルの関連付け

- コントロールプレーンでの Sx プロトコルの設定

ユーザープレーン負荷制御プロファイルの設定

負荷制御プロファイルを設定するには、次のコマンドを使用します。

```
configure
  userplane-load-control-profile profile_name
  end
```

ユーザープレーン負荷制御プロファイルのパラメータの設定

UP 負荷プロファイルのパラメータを設定するには、次の設定を使用します。

```
configure
  userplane-load-control-profile profile_name
     system-weightage system-cpu-utilization utilization_value
system-memory-utilization utilization_value license-session-utilization
utilization_value
     sessmgr-weightage sessmgr-cpu-utilization utilization_value
system-memory-utilization utilization_value
    inclusion-frequency advertisement-interval interval_value change-factor
 changefactor_value
     end
```

注：

- **inclusion-frequency**：負荷制御情報 IE の包含頻度を決定するパラメータを設定します。
- **advertisement-interval**：アドバタイズメント間隔は、負荷値がアドバタイズされる定期的な間隔です。負荷制御のアドバタイズメント間隔を設定します。デフォルト値は 300 です。該当するすべてのメッセージに LCI IE を含めるには、値を 0（ゼロ）に設定します。
- **change-factor**：Change-factor は、負荷アドバタイズメントの発生に基づく負荷値の差分増減です。負荷制御の変更要因を設定します。デフォルト値は 5 です。
- **sessmgr-weightage**：さまざまな負荷制御パラメータの sessmgr の重みを設定します。全パラメータの重みの合計は 100 である必要があります。デフォルトの比率は、sessmgr-cpu-utilization に対する重みが 65%、sessmgr-memory-utilization に対する重みが 35% です。
- **sessmgr-cpu-utilization**：セッションマネージャの CPU 使用率の重みを割合で設定します。負荷率のデフォルトの重みは 35% です。
- **sessmgr-memory-utilization**：セッションマネージャのメモリ使用率の重みを割合で設定します。負荷率のデフォルトの重みは 65% です。
- **system-weightage**：さまざまな負荷制御パラメータに対するシステムの重みを設定します。全パラメータの重みの合計は 100 である必要があります。デフォルト値は、system-cpu-utilization に対して 40% の重み、system-memory-utilization に対して 30% の重み、および license-session-utilization に対して 30% の重みです。

- **system-cpu-utilization**：システム CPU 使用率の重みを割合で設定します。負荷率のデフォルトの重みは 40% です。

（注） **show cpu table** CLI コマンドで表示される値は、5 分、10 分、および 15 分の平均値に基づいています。システム CPU 使用率の平均値の結果を使用して、使用率を手動で確認します。

- **system-memory-utilization**：システムメモリ使用率の重みを割合で設定します。負荷率のデフォルトの重みは 30% です。

（注） **show cpu table** CLI コマンドで表示される値は、5 分、10 分、および 15 分の平均値に基づいています。システムメモリ使用率の平均値の結果を使用して、使用率を手動で確認します。

- **license-session-utilization**：ユーザープレーンサービスのライセンスセッション使用率の重みを割合で設定します。負荷率のデフォルトの重みは 30% です。ライセンス使用率は、最大の UP セッションのうち、現在の UP セッションの使用率と同じです。

ユーザープレーン過負荷制御プロファイルの設定

過負荷制御プロファイルを設定するには、次のコマンドを使用します。

```
configure
  userplane-overload-control-profile profile_name
  end
```

ユーザープレーン過負荷制御プロファイルのパラメータの設定

UP 過負荷プロファイルのパラメータを設定するには、次の設定を使用します。

```
configure
  userplane-overload-control-profile profile_name
    overload-threshold system lower-limit limit_value upper-limit
limit_value sessmgr lower-limit limit_value upper-limit limit_value vpp-cpu
lower-limit limit_value upper-limit limit_value
    system-weightage system-cpu-utilization utilization_value
system-memory-utilization utilization_value license-session-utilization
utilization_value
    sessmgr-weightage sessmgr-cpu-utilization utilization_value
system-memory-utilization utilization_value
   inclusion-frequency advertisement-interval interval_value change-factor
 changefactor_value
    tolerance tolerance_value
    validity-period validity_period
    end
```

注：

- **inclusion-frequency**：過負荷制御情報 IE の包含頻度を決定するパラメータを設定します。
- **advertisement-interval**：アドバタイズメント間隔は、過負荷値がアドバタイズされる定期的な間隔です。過負荷制御のアドバタイズメント間隔を設定します。デフォルト値は 300 です。該当するすべてのメッセージに LCI IE を含めるには、値を 0（ゼロ）に設定します。
- **change-factor**：Change-factor は、過負荷アドバタイズメントの発生に基づく過負荷値の差分増減です。過負荷制御の変動係数を設定します。デフォルト値は 5 です。
- **tolerance**：過負荷の許容限度を設定します。
- **validity-period**：過負荷制御情報の妥当性を設定します。デフォルト値は 600 です。
- **overload-threshold**：システム、セッションマネージャ、および VPP CPU の過負荷しきい値制限を設定します。
- **system**：ノードが自己保護モードに移行するまでの過負荷システムしきい値を設定します。
- **vpp-cpu**：ノードが自己保護モードに移行するまでの過負荷 VPP CPU しきい値を設定します。
- **sessmgr**：ノードが自己保護モードに移行するまでのセッションマネージャの過負荷しきい値を設定します。
- **upper-limit** *limit_value*：さまざまな上限値を設定します。次に示すとおり、さまざまな上限値があります。
  - システムしきい値の上限：ノードが自己保護モードに移行するまでのシステムの過負荷しきい値を設定します。デフォルトの制限値は 80% です。
  - セッションマネージャしきい値の上限：ノードが自己保護モードに移行するまでのセッションマネージャの過負荷しきい値を設定します。デフォルトの制限値は 60% です。
  - VPP CPU.しきい値の上限：ノードが自己保護モードに移行するまでの VPP CPU 過負荷しきい値 L2 を設定します。デフォルトの制限値は 60% です。
- **lower-limit** *limit_value*：さまざまな下限値を設定します。次に示すとおり、さまざまな下限値があります。
  - システムしきい値の下限：ノードが自己保護モードに移行するまでのシステムの過負荷しきい値を設定します。デフォルトの制限値は 60% です。
  - セッションマネージャしきい値の下限：ノードが自己保護モードに移行するまでのセッションマネージャの過負荷しきい値を設定します。デフォルトの制限値は 50% です。
  - VPP CPU.しきい値の下限：ノードが自己保護モードに移行するまでの VPP CPU 過負荷しきい値 L1 を設定します。デフォルトの制限値は 50% です。

- **sessmgr-weightage**：さまざまな負荷制御パラメータに対するセッションマネージャの重みを設定します。全パラメータの重みの合計は 100 である必要があります。デフォルトの比率は、sessmgr-cpu-utilization に対する重みが 65%、sessmgr-memory-utilization に対する重みが 35% です。
- **sessmgr-cpu-utilization**：セッションマネージャの CPU 使用率の重みをパーセンテージで設定します。過負荷係数のデフォルトの重みは 35% です。
- **sessmgr-memory-utilization**：セッションマネージャのメモリ使用率の重みをパーセンテージで設定します。過負荷係数のデフォルトの重みは 65% です。
- **system-weightage**：さまざまな過負荷制御パラメータのシステムの重みを設定します。全パラメータの重みの合計は 100 である必要があります。デフォルト値は、system-cpu-utilization に対する重みが 40%、system-memory-utilization に対する重みが 30%、license-session-utilization に対する重みが 30% です。
- **system-cpu-utilization**：システムの CPU 使用率の重みをパーセンテージで設定します。過負荷係数のデフォルトの重みは 40% です。

（注） **show cpu table** CLI コマンドで表示される値は、5 分、10 分、および 15 分の平均値に基づいています。システム CPU 使用率の平均値の結果を使用して、使用率を手動で確認します。

- **system-memory-utilization**：システムメモリ使用率の重みをパーセンテージで設定します。過負荷係数のデフォルトの重みは 30% です。

（注） **show cpu table** CLI コマンドで表示される値は、5 分、10 分、および 15 分の平均値に基づいています。システムメモリ使用率の平均値の結果を使用して、使用率を手動で確認します。

- **license-session-utilization**：ユーザープレーンサービスのライセンスセッション使用率の重みをパーセンテージで設定します。過負荷係数のデフォルトの重みは 30% です。ライセンス使用率は、最大 UP セッションのうちの現在の UP セッションの使用率と同じです。

負荷制御プロファイルとユーザープレーンサービスの関連付け

次のコマンドを使用して、過負荷制御プロファイルをユーザープレーンサービスに関連付けます。

```
configure
  context context_name
    user-plane-service service_name
    [ no ] associate userplane-load-control-profile profile_name
```

注：

- **associate**：このコマンドは、ユーザープレーン過負荷制御プロファイルをユーザープレーンサービスに関連付けます。

コントロールプレーンでの Sx プロトコルの設定

CP Function Features IE は、CP でサポートされている機能を示します。この IE によって通知されるのは、（システム全体の）UP 機能の動作に影響を与える機能のみです。

CP では次の機能がサポートされます。

- LOAD（負荷制御）
- OVRL（過負荷制御）

Sx プロトコルを介して CP でサポートされる機能を設定するには、次の設定を使用します。

```
configure
   context context_name
      sx-service service_name
       sx-protocol supported-features { load-control | overload-control
 }
        no sx-protocol supported-features [ load-control |
overload-control ]
        end
```

注：

- **supported-features**：CP によりサポートされる Sx インターフェイスの機能を設定します。デフォルト値は [無効（Disabled）] です。
- **load-control**：CP 機能による負荷制御機能のサポートを有効または無効にします。
- **overload-control**：CP 機能による過負荷制御機能を有効または無効にします。

モニタリングおよびトラブルシューティング

show コマンドの入力と出力

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show userplane-load-control-profile name *name*

この機能をサポートするために、次のフィールドが表示されます。

- ユーザープレーン負荷制御プロファイル
- ユーザープレーン負荷制御プロファイル名

- システムの重みとしきい値：
  - CPU Utilization Weightage
  - Memory Utilization Weightage
  - License Session Utilization Weightage
  - System Threshold Lower Limit
  - System Threshold Upper Limit
- Sessmgr の重みとしきい値：
  - CPU Utilization Weightage
  - Memory Utilization Weightage
  - Sessmgr Threshold Lower Limit
  - Sessmgr Threshold Upper Limit
- VPP の重みとしきい値：
  - VPP Utilization Weightage
  - vpp-cpu Threshold Lower Limit
  - vpp-cpu Threshold Upper Limit
- 包含頻度：
  - 変更要因
  - アドバタイズメント間隔

show userplane-overload-control-profile name *name*

この機能をサポートするために、次のフィールドが表示されます。

- ユーザープレーン過負荷制御プロファイル
- ユーザープレーン過負荷制御プロファイル名
- システムの重みとしきい値：
  - CPU 使用率の重み
  - メモリ使用率の重み
  - ライセンスセッション使用率の重み
  - システムしきい値の下限
  - システムしきい値の上限
- Sessmgr の重みとしきい値：

- CPU 使用率の重み
- メモリ使用率の重み
- Sessmgr しきい値の下限
- Sessmgr しきい値の上限

- VPP の重みとしきい値：
  - VPP 使用率の重み
  - vpp-cpu しきい値の下限
  - vpp-cpu しきい値の上限

- 包含頻度
  - 変更要因
  - アドバタイズメント間隔

- 有効期間

show user-plane-service statistics all

この機能をサポートするために、次のフィールドが表示されます。

- 過負荷統計情報
  - 現在の状態：正常
  - ユーザープレーンで自己保護状態に達した回数：0
  - 自己保護モード中に拒否されたセッション確立要求の数：0
  - 自己保護モード中に拒否されたセッション変更要求の数：0
  - 自己保護モード中に許可された eMPS セッション確立要求の数：0
  - 自己保護モード中に許可された eMPS セッション変更要求の数：0
  - 過負荷削減メトリック：0
  - 現在の過負荷率（system）：0
  - 現在の過負荷率（sessmgr）：0
  - 現在の過負荷率（vpp cpu）：0

- 過負荷データの統計情報：
  - 過負荷が原因でドロップされたパケットの総数：0
  - 過負荷が原因でドロップされたバイトの総数：0

- 自己保護モードでドロップされたパケットの総数：0
- 自己保護モードでドロップされたバイトの総数：0

- 負荷統計情報：
  - 負荷メトリック：0
  - 現在の負荷率（system）：0
  - 現在の負荷率（sessmgr）：0
  - 現在の負荷率（vpp cpu）：0

- eMPS PDN の合計
  - アクティブ
  - 設定
  - リリース日
  - Rejected

show sx service statistics all

この機能をサポートするために、次のフィールドが表示されます。

- スロットル

バルク統計情報

Sx機能でサポートされる負荷および過負荷をサポートする、次のバルク統計を使用できます。

表 *14*：サポートされるバルク統計

バルク統計情報	説明
num-self-protection-reached	UP が自己保護状態に達した時間の合計。
num-session-estab-rejected-on-self-protection	自己保護モード中に拒否されたセッション確立要求の合計数。
num-session-modif-rejected-on-self-protection	自己保護モード中に拒否されたセッション変更要求の合計数。
num-emps-session-estab-allowed-on-self-protection	自己保護モード中に許可されたeMPSセッション確立要求の合計数。
num-emps-session-modif-allowed-on-self-protection	自己保護モード中に許可されたeMPSセッション変更要求の合計数。

バルク統計情報	説明
overload-reduction-metric	過負荷低減メトリックは、設定された過負荷条件の下限と上限に基づいて計算されます。
overload-factor-system	システムの過負荷係数は、システム CPU、メモリ、VPP CPU、およびリソースマネージャ（RM）からポーリングされたその他の情報に基づいて計算されます。
overload-factor-session	UP は、自己保護モード中に新しいセッションとデータスロットリングの拒否を開始します。
overload-factor-vpp-cpu	過負荷時のコアあたりの VPP CPU 合計値の平均。
load-metric	現在の負荷メトリックの合計値。
load-factor-system	現在のシステム負荷係数の合計値。
load-factor-session	現在のセッション負荷係数の合計値。
load-factor-vpp-cpu	現在の VPP CPU 負荷係数の合計値。
num-packets-dropped-on-overload	過負荷時に破棄されたパケットの総数。
num-bytes-dropped-on-overload	自己保護モード中にドロップされたバイト数の合計。
num-packets-dropped-on-self-protection	自己保護モード中にドロップされたパケット数の合計。
num-bytes-dropped-on-self-protection	自己保護モード中にドロップされたバイト数の合計。

SNMP トラップ

この機能をサポートするために、次の SNMP トラップが追加されました。

- UPlaneSelfOverload：システムが自己保護モードに切り替わったとき。
- UPlaneSelfOverloadClear：システムの自己保護モードが解除されたとき。

第 49 章

LTE-M RAT タイプのサポート

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.27

機能説明

LTE-M（LTE-MTC low-power-wide area（LPWA））は、3GPP が規定する、低消費電力広域接続ソリューション対応のセルラー無線アクセス技術です。具体的には、IoT LTE-M に適した LTE UE のカテゴリを指します。IoT LTE-M は、デバイスの複雑さを軽減して IoT をサポートし、カバレッジを拡大すると同時に、LTE のインストールベースの再利用を可能にします。

RAT Type 情報要素（IE）は、多くのインターフェイス間のさまざまなコールフローに含まれます。不明な RAT タイプを含むセッション作成要求を受信した場合、[RAT Type] はこのメッセージの必須 IE であるため、S-GW または P-GW がセッション作成要求を拒否する場合があります。この機能により、CUPS の LTE-M RAT（無線アクセス技術）タイプがサポートされます。

RAT タイプは、IE（GTPv2-C、GTPP など）、AVP（Diameter ベースのインターフェイスなど）として、または多くのインターフェイスにまたがる属性（EDR など）として存在します。

CUPS の LTE-M ソリューションは、以下のインターフェイスプロトコルおよびディクショナリで次の新しい [LTE-M RAT Type] 属性値をサポートします。

- Gx インターフェイス：Diameter Protocol

- Gy インターフェイス：Diameter Protocol
- Gz/Rf インターフェイス：GTPP/Diameter/RADIUS
- S6b インターフェイス：Diameter Protocol
- S11/S5/S8 インターフェイス：GTPv2-C
- RADIUS APV およびディクショナリ
- CDR 生成用の Rf インターフェイス
- EDR の属性

既存機能の拡張

LTE-M RAT タイプをサポートするために、次の既存の機能が拡張されます。

- **RAT タイプに基づく仮想 APN の選択**：仮想 APN は、単一の APN 内におけるサービスの差別化を可能にします。仮想 APN 機能により、キャリアは単一の APN を使用してサービスの差別化を設定できます。MME によって提供される APN は、複数の設定可能パラメータを使用して P-GW により評価されます。次に、P-GW は、指定された APN とそれらの設定可能パラメータに基づいて APN 設定を選択します。APN 設定は、APN ごとにポリシーが異なる P-GW において、セッションのあらゆる側面を決定します。

  ベース APN 下に直接設定することで、仮想APNを選択できます。このAPNの選択は、RAT タイプに基づいて行われます。このリリースでは、CLI を使った LTE-M RAT タイプに応じた仮想 APN の選択がサポートされるようになりました。

- **QCI および QoS マッピング**：P-GW は、RAT タイプ [LTE-M] に基づく APN との QCI および QoS マッピングの関連付けをサポートします。QCI および QoS マッピングを使用すると、[QoS Class Index (QCI) to QoS Mapping Configuration] モードでクイックアクションを実行できます。このモードは、QoS クラス指標を適用可能な QoS パラメータにマッピングするために使用されます。マッピングは、LTE ネットワークの S-GW あるいは P-GW、またはその両方で発生する可能性があります。

- **PCRF ベースの処理**：P-GW は Credit Control Request -Initial and Updated（CCR-I および CCR-U）メッセージを介して RAT タイプの変更を PCRF に通知し、PCRF は新しい PCC ルールを提供します。ポリシー/課金ルール機能（PCRF）から新しいポリシーおよび課金制御（PCC）ルールを適用することで、ベアラーを作成できます。

機能の仕組み

この機能の一部として、多くのインターフェイスの RAT タイプが変更され、LTE-M RAT タイプを示す追加の値が含まれるようになりました。標準およびお客様固有のディクショナリのみが変更されます。

次の表に、LTE-M RAT タイプをサポートするさまざまなインターフェイスのフィールドとその値を示します。

表 *15*：

ウィールドインタフェース	PMA メッセージ属性	
P-GW		
Gx	RAT タイプ（1032） 直径	MEL • クレジット制御要求：初期 • クレジット制御要求：更新済み
Gy	3GPP RAT タイプ（21） 直径	MEL • クレジット制御要求：初期 • クレジット制御要求：更新済み
SWx	3GPP RAT タイプ（21）	MEL • アカウンティング要求：開始 • アカウンティング要求：停止 • アカウント要求：中間
Rf	3GPP RAT タイプ（21） 直径	MEL • アカウンティング要求：開始 • アカウンティング要求：停止 • アカウント要求：中間
SGi	3GPP RAT タイプ（1032） 直径	MEL • 認証 • 承認 • 要求
ROE	RAT タイプ	MEL—
RTP	RAT タイプ（30） GTPP	MEL • GTPP データレコード • 転送要求
S-GW		
RTS	RAT タイプ（30）	MEL • GTPP データレコード • 転送要求

制限事項

LTE-M 関連の変更は、次の機能には実装されていません。

- ECS でのルール照合
- ローカルポリシーでの ruledef 照合

サポートされる標準

シスコの LTE RAT タイプの実装は、次の標準に準拠しています。

- 3GPP 23.401 リリース 15.4.0：3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 3GPP 29.274 リリース 15.4.0：3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
- 3GPP 32.299 リリース 15.4.0：3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC)。
- 3GPP 29.060：3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface。
- 3GPP 29.061：3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)
- 3GPP 32.298：3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP 29.212 リリース 15.4.0：3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC)。

LTE-M RAT タイプの設定

LTE-M RAT タイプに基づく仮想 APN 選択の設定

次の設定を使用して、LTE-M RAT タイプに基づいて仮想 APN を選択します。

```
configure
  context context_name
    apn apn_name
```

```
virtual-apn preference value apn  apn_name rat-type lte-m
end
```

注：

- **rat-type lte-m**：仮想 APN の [RAT Type] として「LTE-M」を有効にします。

QCI - QoS マッピングの設定

APN に対する QCI - QoS マッピングを設定するには、次の設定を使用します。

```
configure
  qci-qos-mapping mapping_name
  end
```

QCI - QoS マッピングと LTE-M RAT タイプの関連付け

次の設定を使用して、セッションのセットアップ時に QCI - QoS マッピングの LTE-M RAT タイプを選択します。

```
configure
  context context_name
    apn apn_name
      associate qci-qos-mapping mapping_name rat-type lte-m
      end
```

LTE-M RAT タイプの設定を使用した QCI - QoS マッピングの確認

次の show CLI コマンドの出力をチェックして、QCI - QoS マッピング設定が LTE-M RAT タイプに関連付けられているか確認します。

- **show configuration**
- **show apn name** *apn_name*
- **show apn name** *apn_name* **all**

モニタリングおよびトラブルシューティング

ここでは、SAEGW、P-GW、および S-GW サービスにおける LTE-M RAT タイプのサポートのモニタリングおよび障害対応に使用できるコマンドについて説明します。

show コマンドと出力

ここでは、LTE-M RAT タイプの機能の show コマンドとコマンド出力について説明します。

show apn statistics { all | name }

show apn statistics { all | name } CLI コマンドの出力が拡張され、[Initiated Sessions per RAT Type] および [Active Sessions per RAT Type] セクションに [LTE-M] フィールドが表示されるようになりました。

show subscribers { full | full all | call-id <call_id> }

これらの show CLI コマンドの出力は、サブスクライバコールのモニタリングに使用されます。これらのコマンドの出力が拡張され、この機能の一部として [Access Tech] に [(R) - LTE-M] が加わりました。

show subs { pgw-only | sgw-only | saegw-only }{ full | full all }

次の show CLI コマンドの出力は、コールのアクセス技術を LTE-M として表示するように拡張されています。

- アクセス技術：LTE-M

show session subsystem [full | verbose]

これらの CLI は、セッション関連の統計情報のモニタリングに使用されます。これらのコマンドの出力は、この機能の一部として拡張されており、[User Data Statistics] の下に次のフィールドが表示されます。

- LTE データ統計
  - ユーザーに送信したパケット数
  - ユーザーに送信したオクテット数
  - ユーザーから受信したパケット数
  - ユーザーから受信したオクテット数
- LTE-M 接続統計情報
  - Total Sessions
  - 着信コールの総数
  - 接続されたコールの総数
  - 切断されたコールの総数

show session summary

この show CLI コマンドの出力が拡張され、[LTE-M] フィールドが表示されるようになりました。

show subscribers { subscription full | activity all }

これらの show CLI コマンドの出力が拡張され、コールの RAT タイプとして [LTE-M] フィールドが表示されるようになりました。

show { pgw-service | sgw-service | saegw-service } statistics { all | name }

次の show CLI コマンドの出力は、RAT タイプとして「LTE-M」フィールドが含まれるように拡張されています。

show pgw-service statistics { all | name }

この CLI は、P-GW サービスごとの統計情報を表示するために使用されます。この CLI の出力は、P-GW サービスごとの LTE-M RAT タイプで「Initiated PDNs By RAT-Type」と「Current PDNs By RAT-Type」の数を表示するように拡張されています。

show sgw-service statistics { all | name }

この CLI は、S-GW サービスごとの統計情報を表示するために使用されます。この CLI の出力は、S-GW サービスごとの LTE-M RAT タイプを使用した「Current Subscribers By RAT-Type」と「Current PDNs By RAT-Type」の数を表示するように拡張されています。

show saegw-service statistics { all | name }

この CLI は、SAEGW サービスごとの統計情報を表示するために使用されます。この CLI の出力は、LTE-M RAT タイプの「Colocated PDNs」、「PGW-Anchor PDNs」、「SGW-Anchor PDNs」、および「GGSN-Anchor PDNs」の数を表示するように拡張されています。

バルク統計情報

LTE-M RAT タイプ機能をサポートするために、次の統計情報が追加されました。

APN スキーマ

APN スキーマでは、次の LTE-M RAT タイプ機能関連のバルク統計を使用できます。

バルク統計情報	説明
active-lte-m-sessions	APN ごとのアクティブ LTE-M セッション（RAT タイプは [LTE-M]）の合計数。
initiated-lte-m-sessions	開始された LTE-M セッションの合計数。

P-GW スキーマ

P-GW スキーマでは、次の LTE-M RAT タイプ機能関連のバルク統計を使用できます。

バルク統計情報	説明
sesstat-pdn-rat-lte-m	LTE-M の PDN タイプセッション統計の合計数。
sessstat-rat-init-lte-m	開始された LTE-M PDN（RAT タイプは [LTE-M]）の合計数。

P-GW スキーマ

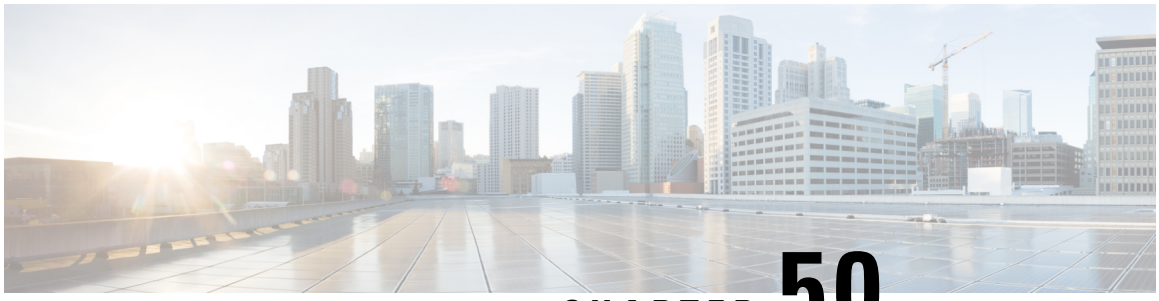
次の LTE-M RAT タイプの機能関連のバルク統計情報は、S-GW スキーマで使用できます。

バルク統計情報	説明
sessstat-totcur-ue-lte-m	RAT タイプが LTE-M のアクティブ UE の総数。
sessstat-totcur-pdn-lte-m	RAT タイプが LTE-M のアクティブ PDN の総数。

SAEGW スキーマ

SAEGW スキーマでは、次の LTE-M RAT タイプ機能関連のバルク統計を使用できます。

バルク統計情報	説明
sgw-sessstat-totcur-ue-lte-m	RAT タイプが [LTE-M] のアクティブ UE の合計数。
sgw-sessstat-totcur-pdn-lte-m	RAT タイプが [LTE-M] の LTE-M PDN（P-GW アンカー/Collapsed PDN）の合計数。
pgw-sesstat-pdn-rat-lte-m	RAT タイプが [LTE-M] の LTE-M PDN（P-GW アンカー/Collapsed PDN）の合計数。
pgw-sessstat-pdn-rat-init-lte-m	開始された LTE-M PDN の合計数。
saegw-sgw-anchor-pdn-rat-lte-m	RAT タイプが [LTE-M] の LTE-M PDN（S-GW アンカー）の合計数。
saegw-pgw-anchor-pdn-rat-lte-sm	RAT タイプが [LTE-M] の LTE-M PDN（P-GW アンカー）の合計数。
saegw-collapsed-pdn-rat-lte-m	RAT タイプが [LTE-M] の LTE-M PDN（SAEGW Collapsed PDN）の合計数。



CHAPTER 50

CUPS における LTE - Wi-Fi 間のシームレスハンドオーバー

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

進行中のデータセッションを継続する必要がある UE での LTE と Wi-Fi（S2a/S2b）間のシームレスなハンドオーバーは、CUPS アーキテクチャでサポートされています。

LTE から Wi-Fi へのハンドオーバーが開始され、セッション作成応答（CSR）が Wi-Fi トンネルで送信されるとすぐに、ベアラー削除要求（DBR）が LTE トンネルを介して送信されます。このとき、ePDG での IPSec トンネル確立の遅延により、パケット損失が発生します。パケット損失の問題に対処するために、設定されたハンドオーバータイマーの期限が切れたときにのみ、ベアラー削除要求が LTE トンネルで送信されます。LTE トンネルがアクティブな場合、アップリンクとダウンリンクのデータは LTE トンネルで交換されます。ハンドオーバーが完了すると、アップリンクとダウンリンクのデータが Wi-Fi トンネルで交換されます。これによ

り、パケット損失を防げます。Wi-Fi から LTE へのハンドオーバー中に、ベアラー変更要求が HI=1 で受信されると、仕様に従って Wi-Fi から LTE へのトンネル切り替えが開始されます。

この機能には次の利点があります。

- LTE から Wi-Fi（S2bGTP）へのハンドオーバー中のパケット損失を最小限に抑え、ハンドオーバーをシームレスにします（つまり、メイクビフォアブレーク）。
- P-GW で両方のトンネルが確立されている場合、LTE 手順は LTE トンネルを介して正常に処理されます。
- P-GW で両方のトンネルが確立されている場合、Wi-Fi 手順は Wi-Fi トンネルを介して正常に処理されます。

重要

- LTE から Wi-Fi または Wi-Fi から LTE へのハンドオーバーでは、シームレスなハンドオーバーを実行するために、新しいアクセストラフィックタイプにトンネル識別子が割り当てられます。

機能の仕組み

LTE - Wi-Fi ハンドオーバー

- HO の開始前：
  - 複数の未処理の CCR-U がサポートされている場合、ハンドオフ要求前のすべての要求はドロップされます。
  - LTE アクセスで保留中のトランザクションはすべて破棄されます。たとえば、CBR または UBR が LTE アクセス用に送信され、CBR または UBR トランザクションが完了する前にハンドオフが開始された場合、CBR または UBR は P-GW で無視されます。PCRF には障害が通知されません。
- 移行期間中：
  - ポリシー変更のために PCRF が RAR を送信する場合、ハンドオーバーの完了後に処理されます。
  - ASR が受信されると、コールドロップが発生して、両方のトンネルがダウンします。
  - PCRF からセッション解放が発生した場合、コールはドロップされ、CSR が「リソースなし」という理由で送信されます。
  - HO-Ind が 1 に設定された状態で（ガードタイマー後）、ユーザーが LTE に戻る（つまり、LTE から Wi-Fi、LTE へのハンドオフが繰り返される）場合、HO は正常に処理され、ユーザーセッションは再び LTE に移行されます。

- ユーザーが HO-Ind を 0 に設定した状態で LTE に戻る（つまり、LTE から Wi-Fi、LTE へのハンドオフを繰り返す）場合、コンテキストの置換が発生します。古いコールは「コンテキスト置換」という理由で Wi-Fi アクセスでクリアされ、LTE を介した新しいコールのように処理されます。
- ベアラー変更コマンド（MBC）が LTE（新規アクセス）で受信された場合、サービス拒否メッセージを付けて拒否されます。
- ベアラー変更コマンド（MBC）が Wi-Fi（旧アクセス）で受信された場合、そのコマンドは破棄されます。
- HO の進行中に LTE（新規アクセス）でベアラー削除コマンド（DBC）が受信されると、セッションが終了します。
- 進行中のハンドオーバー中に Sx パス障害が発生した場合、進行中のトランザクションは中止され、コールはローカルで切断されます。
- GTPC S5/S11 パス障害
  - LTE から Wi-Fi への HO 中に、古いトンネルでパス障害が発生すると、コールがクリアされます。新しいトンネルでパス障害が発生すると、コールが切断されます。
  - Wi-Fi から LTE への HO 中に、古いトンネルでパス障害が発生すると、古いトンネルがクリアされ、新しいトンネルコールが続行されます。これは、MBReq が MME から保留中の場合にのみ可能です。他のすべての状態では、コールはローカルで切断されます。
  - WIFI から LTE（Collapsed コール）の HO、コールは継続できません。古いトンネルでパス障害が発生した場合、コールはローカルで切断されるだけです。
  - HO 中に、新しいトンネルでパス障害が発生すると、コールが切断されます。

ICSR とセッションのリカバリ

- コントロールプレーンでは、遷移時に直近の状態が安定した状態と見なされ、LTE から Wi-Fi（S2BGTP）またはその逆のハンドオーバーが完了すると、フルチェックポイントがトリガーされます。これは、セッションリカバリと ICSR に適用されます。ユーザープレーンには、受信したすべてのメッセージに個別のセッションリカバリと ICSR チェックポインティングがあります。
- ハンドオーバーが失敗した場合、つまり CP と UP が同期していない場合には、CP セッションは直近のアクセス時の状態で回復され、UP は新たな遷移状態で回復されます。この動作は、UP 障害発生時に適用されます。

制限事項

LTE - Wi-Fi 間のシームレスハンドオーバー機能では、LTE から eHRPD および Wi-Fi から eHRPD へのハンドオーバーとハンドバックはサポートされません。

標準準拠

LTE - Wi-Fi シームレスハンドオーバー機能は、次の標準規格に準拠しています。

- 3GPP TS 23.214
- 3GPP TS 29.244
- 3GPP TS 23.401
- 3GPP TS 23.402

LTE と Wi-Fi 間のシームレスハンドオーバーの設定

ここでは、機能を有効または無効にするために使用できる CLI コマンドについて説明します。

次の CLI コマンドを使用して、LTE から Wi-Fi へのハンドオーバータイマーを設定します。

```
configure
  context context_name
    apn apn_name
      lte-s2bgtp-first-uplink timeout_value
      { default | no } lte-s2bgtp-first-uplink
      end
```

注：

- **default**：Wi-Fi トンネルでセッション作成応答が送信された時点での、LTE から Wi-Fi へのハンドオーバーの完了を有効にします。
- **no**：機能を無効にし、セッション作成応答時点でハンドオーバーが完了します。
- **lte-s2bgtp-first-uplink** *timeout_value*：LTE から S2bGTP へのハンドオーバー完了タイムアウトを 100 ミリ秒の倍数で設定します。有効な範囲は 100 ～ 3000 です。推奨設定は 1000 ミリ秒です。
- デフォルトでは、Wi-Fi トンネルでセッション作成応答が送信された時点で、LTE から Wi-Fi へのハンドオーバーが完了します。ただし、ハンドオーバータイムアウトの設定後は、ハンドオーバーはタイムアウトまで遅延されます。
- CUPS アーキテクチャではユーザープレーンノードとコントロールプレーンノードが分離されているため、最初のアップリンクデータパケットによるハンドオーバーのトリガーはサポートされていません。

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングとトラブルシューティングのサポートで使用できるCLIコマンドについて説明します。

コマンドや出力の表示

この項では、この機能のサポートにおけるshowコマンドまたはその出力について説明します。

show apn statistics name <*name*>

この CLI コマンドの出力が拡張され、APN に関する次のフィールドが表示されるようになりました。

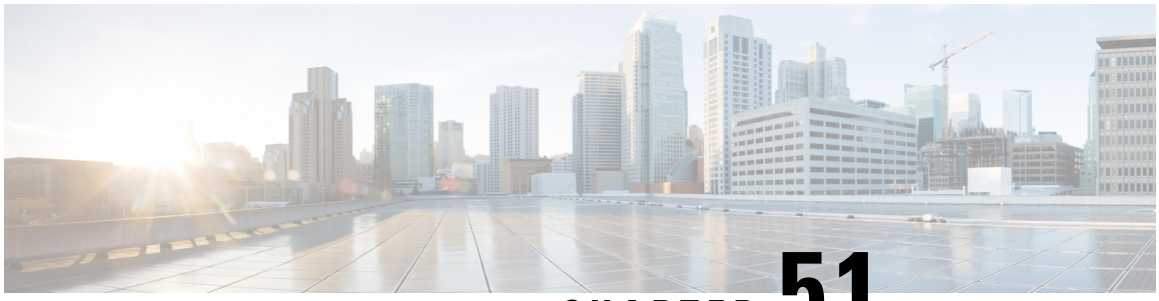
- LTE-to-S2bGTP handover Succeeded on Timer Expiry：タイマー時間の終了によるハンドオーバーの回数を指定します。

注：

この機能の一部として導入された新しいフィールドは、次のCLIコマンドでも表示されます。

- **show pgw-service statistics name** *service_name* **verbose**
- **show pgw-service statistics name all verbose**
- **show saegw-service statistics all function pgw verbose**

show apn statistics name <name>



CHAPTER 51

CUPS のモニターサブスクライバ

マニュアルの変更履歴

表 *16 :* マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.24 より前

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

機能説明

サブスクライバモニター（MonSub）機能を使用すると、サブスクライバ関連情報のトレースが可能になります。これには、ユーザートラフィックと制御トラフィック、およびデバッグに役立つ課金イベントや内部イベントなどのイベントが含まれます。デフォルトでは、この情報

はコントロールプレーン コンソールに表示されます。このコンソールでMonSub トレース CLI コマンドを実行すると、この情報はユーザープレーンのパケットキャプチャ（PCAP）ファイルにキャプチャされます。

ユーザートラフィックは、パケットがアプリケーションを横断する slowpath、またはパケットがアプリケーションを横断する必要はないが fastpath 処理（VPP）にオフロードされる fastpath で伝送されます。fastpath オフロード（VPP）が SAEGW に導入されるまでは、slowpath モードがデフォルトモードでした。

サブスクライバモニターには、次の機能があります。

- ユーザープレーン上の PCAP ファイルの fastpath からユーザートラフィックを継続的にキャプチャします。
- 非ユーザートラフィック情報、つまり、制御イベントトラフィックおよびその他の関連情報は、コントロール プレーン コンソールに表示されます。これらの情報は、ユーザープレーン上の個別の PCAP ファイルにキャプチャされます。
- 新しいオプション UP PCAP トレース [W - UP PCAP Trace (ON)] が、MonSub CLI のコントロールプレーンおよびユーザープレーンの CUPS に導入されました。新しいオプションは、ICUPS の D オプションに似ています。slowpath および fastpath PCAP は、このオプションがオンの場合にのみ生成されます。
- NPUMGR インスタンスごとに最大 4 つのサブスクライバ トレース セッションがあります。NPUMGR（ユーザー プレーン インスタンスごと）は、最大トレースセッション制限を適用します。slowpath キャプチャの命名規則には、SMGR インスタンスの MonSub トレースセッション ID が含まれますが、fastpath トレースセッションにはセッション ID として PSN が含まれます。SESSMGR インスタンスですでに 4 つのトレースセッションが実行されている場合、slowpath キャプチャは「S4」という名前で実行されます。これは、最大トレース制限に達したために NPUMGR がトレースセッションを拒否するまで継続します。

この機能に関連する重要な定義の一部を以下に示します。

- **シャーシトラフィック量**：シャーシのパケットスループットの合計量。
- **モニター対象トラフィック量**：すべての MonSub セッションにおける、MonSub を介したすべてのサブスクライバの合計スループットのモニタリング。
- [**PCAP 成功** ：PCAP ファイルでの MonSub トラフィックキャプチャ要求と成功したキャプチャの割合。

パケット処理スループット

パケット処理スループットに影響を与えるシナリオを以下に示します。

- VPP 使用率が 80% を超えると、MonSub がパケット処理スループットに影響を与える可能性があります。影響の度合いは、モニター対象のトラフィック量に比例します。

- 具体的には、モニター対象のトラフィック量がシャーシのトラフィック量の 10% に近づくと、VPP スループットに影響を与えて、サブスクライバのパケット損失が発生する可能性があります。
- モニターの優先順位を 0（ゼロ）より大きくすると、パケット処理スループットへの影響が大きくなります。

注意 パケット処理中は注意が必要です。VPP が 80% の使用率で実行され、約 10 Gbps のシャーシトラフィック量を処理している場合、一連の MonSub セッションがサブスクライバを一元的にモニターし、モニター対象のトラフィック量が合計 1 Gbps を超えると、パケット処理に影響があります。

PCAP の成功

PCAP の成功は次の要因によって決まります。

- PCAP の成功レベルは、モニター対象のトラフィック量、VPP 使用率、MonSub のモニター優先順位、バックグラウンドディスク I/O など、いくつかの要因によって決まります。
- 一般に、PCAP の成功率は次の場合に高くなります。
  - VPP 使用率が低く、MonSub のモニター優先順位がベストエフォートを超えている場合。
  - モニター対象のトラフィック量がシャーシのトラフィック量の 10% 未満である場合。

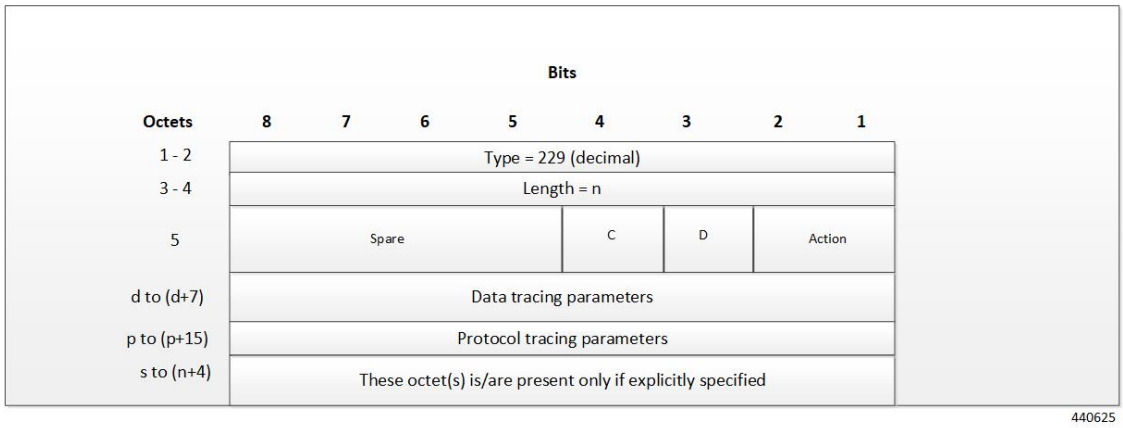
  例：VPP が 80% の使用率で実行され、約 10 Gbps のシャーシトラフィック量を処理している場合、モニター対象のトラフィック量が 1 Gbps 以下であれば、PCAP 成功率が高くなると考えられます。

モニターサブスクライバ Sx プライベート IE

サブスクライバトレース

モニターサブスクライバ Sx プライベート IE は、Sx セッション確立要求および Sx セッション変更要求の条件付き IE です。この IE は、Sxa、Sxb、および Saxb コールタイプでのみ有効です。

図 *16 :* サブスクライバトレース



アクション：サブスクライバトレースを STOP / START でモニターします。STOP = 1、START = 2。

（注） D：D = 1 の場合、データイベントのトレースは [ON] です。8 オクテット（d ～ d + 7）には、D = 1 の場合にのみ存在する必要があるデータイベントのトレース情報が含まれています。

C：C = 1 の場合、制御イベントのトレース [ON] です。

データトレース情報（8 オクテット）：パケットキャプチャ、パケットキャプチャサイズ、MEH ヘッダーなどのデータフィルタパラメータが含まれます。

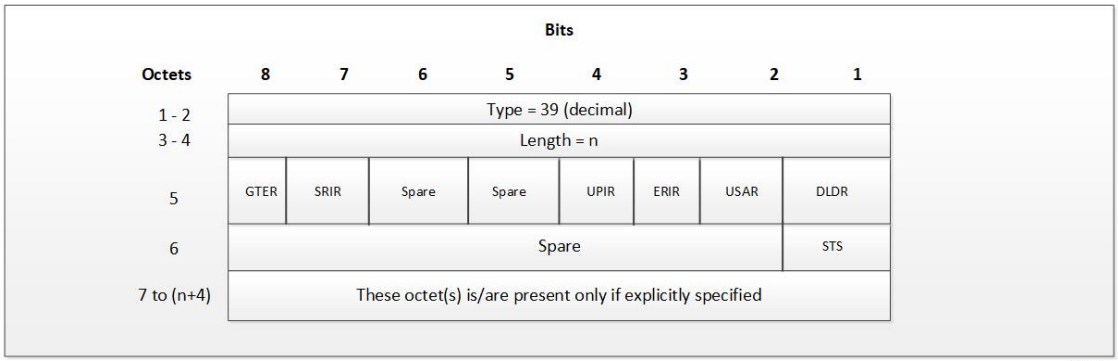
- オクテット 1：
  - ビット 1：VPP の有効化/無効化
  - ビット 2：FCAP：パケットキャプチャ
  - ビット 3：MEH あり
  - ビット 4 ～ 6：優先順位
- オクテット 2 ～ 3：パケットサイズ
- オクテット 4 ～ 8：将来の使用のために予約済み。現在、すべて 0 に設定されています。

プロトコルトレース情報（16 オクテット/128 ビット）：16 オクテット（p ～ p + 15）にはプロトコルトレース情報が含まれ、制御フラグ（C）またはデータフラグ（D）が有効な場合にのみ存在します。各ビットは、モニターする一意のプロトコルを表します。たとえば、49 番目のビットが 1 の場合、PFCP イベントトレースは [ON] です。プロトコルトレースルール一致イベント（オプション 34）、L3 データ（オプション 19）、EDR（オプション 77）、およびコール切断後のサブスクライバサマリーは、制御イベントフラグによって制御されます。

サブスクライバ トレース ステータス レポート（UP to CP のみ）

PFCP セッションに対してサブスクライバトレースが有効になっている場合、レポートタイプ IE には 1 つの追加オクテット（オクテット 6）が含まれます。このオクテットの有無は長さで示されます。

図 *17* : レポートタイプ *IE*



440626

オクテット 5 は次のようにエンコードされます。

- ビット 1：DLDR（ダウンリンクデータレポート）：1 に設定されている場合、ダウンリンクデータレポートを表します。
- ビット 2：USAR（使用状況レポート）：1 に設定されている場合、使用状況レポートを表します。
- ビット 3：ERIR（Error Indication レポート）：1 に設定されている場合、Error Indication レポートを表します。
- ビット 4：UPIR（ユーザープレーン非アクティブレポート）：1 に設定されている場合、ユーザープレーン非アクティブレポートを表します。
- ビット 5 ～ 6：予備。
- ビット 7：SRIR（セッション置換）：1 に設定されている場合、UP からのセッション置換要求を表します。
- ビット 8：GTER（グレースフル終了）：1 に設定されている場合、UP からのグレースフル終了要求を表します。

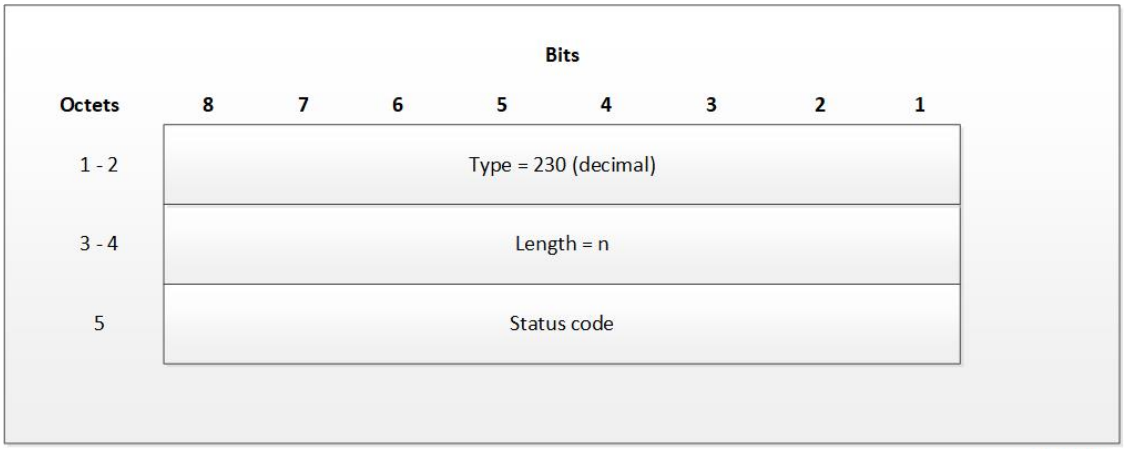
オクテット 6（長さ > 1 の場合に存在）は次のようにエンコードされます。

- ビット 1：STS（サブスクライバ トレース ステータス レポート）：1 に設定されている場合、サブスクライバ トレース ステータス レポートを表します。
- ビット 2 ～ 8：予備。

サブスクライバ トレース ステータス レポート IE（プライベート IE）

サブスクライバ トレース ステータス レポート IE は、Sxa、Sxb、および Sxab コールタイプ専用の条件付き IE です。N4 コールタイプの場合、この IE は存在しません。

図 *18 :* サブスクライバ トレース ステータス レポート



ステータスコードは、UP でのサブスクライバトレースの受け入れまたは拒否を表します。ステータスコード = 0 は、成功を意味します。1 ～ 255 の値で、特定のエラーコードや通知を一意に指定します。エラーコードのリストは、開発後に定義されます。

表 *17 :* エラーコードと通知テーブル

ステータス コード	ステータスの説明
MONSUB_SM_SUCCESS（0）	
MONSUB_SM_ERROR_FAILURE（1）	MonSub：一般的な障害ステータスを受信しました。
MONSUB_SM_ERROR_UNSUPPORTED（2）	MonSub：サポートされていない障害です。
MONSUB_SM_ERROR_SESSION_EXIST_NONE（3）	MonSub：セッションが見つかりません。);
MONSUB_SM_ERROR_SESSION_LIMIT_EXCEED（4）	MonSub：最大接続数に達しました。
MONSUB_SM_ERROR_SESSION_INVALID_PARAM（5）	MonSub：メッセージの接続に失敗しました。
MONSUB_SM_ERROR_SESSION_ALLOC_FAIL（6）	MonSub：NPU で MonSub セッションを割り当てられませんでした。

ステータス コード	ステータスの説明
MONSUB_SM_ERROR_CONFIG_INVALID_PARAM（7）	MonSub：設定メッセージが失敗しました。
MONSUB_SM_ERROR_MONITOR_LIMIT_EXCEED（8）	MonSub：最大ストリーム制限に達しました。
MONSUB_SM_ERROR_MONITOR_INVALID_PARAM（9）	MonSub：モニターメッセージが失敗しました。
MONSUB_SM_ERROR_MAX（10）	MonSub：最大エラー。
MONSUB_COPROCDATA_CORRUPTED（11）	MonSub：ファイル処理プロセスが失敗しました。
MONSUB_MAX_TRACING_SESSIONS_REACHED（12）	MonSub：トレースセッションの最大数に達しました。
MONSUB_STOP_RECVD_WAIT_POLL_TIMEOUT（13）	MonSub：STOP 通知が成功しました。次のトレースを開始するには、ポーリングタイムアウトの設定時間まで待機してください。
MONSUB_FILECOPY_SOURCE_DIR_NOT_EXIST（14）	MonSub：ソースディレクトリが存在しません。
MONSUB_FILECOPY_DEST_DIR_NOT_EXIST（15）	MonSub：宛先ディレクトリが存在しません。
MONSUB_FILECOPY_SOURCE_DIR_OPEN_FAILURE（16）	MonSub：ソースディレクトリを開けません。
MONSUB_FILECOPY_DEST_DIR_OPEN_FAILURE（17）	MonSub：宛先ディレクトリを開けません。
MONSUB_FILECOPY_SOURCE_OPEN_FAILED（18）	MonSub：ソースファイルを開けません。
MONSUB_FILECOPY_DESTINATION_OPEN_FAILED（19）	MonSub：宛先ファイルを開けません。
MONSUB_FILECOPY_DONE_FILE_DELETION_FAILED（20）	MonSub: ソースパスの .done ファイルを削除できません。
MONSUB_FILECOPY_PCAP_FILE_DELETION_FAILED（21）	MonSub: 宛先パスの .pcap ファイルを削除できません。
MONSUB_RESPONSE_NPUMGR_MONSUB_SESS_FAILED（22）	MonSub：NPUMGR へのセッション通知中に Messenger に障害が発生しました。

ステータス コード	ステータスの説明
MONSUB_RESPONSE_NPUMGR_MONSUB_CFG_FAILED（23）	MonSub-Config を NPUMGR にプッシュします。
MONSUB_RESPONSE_NPUMGR_MONSUB_MONITOR_FAILED（24）	NPUMGR への MonSub-Monitor 通知。
MONSUB_RESPONSE_COPROC_FAILED（26）	MonSub：ファイル処理プロセスが失敗しました。
MONSUB_RESPONSE_FILE_TRANSFER_SUCCESS（27）	MonSub：ファイル転送が成功しました。
MONSUB_RESPONSE_FILE_TRANSFER_FAILED（28）	MonSub：ファイル転送が失敗しました。
MONSUB_ADMINISTRATIVE_DISCONNECT（29）	MonSub：管理上の接続解除。
MONSUB_FILECOPY_DESTINATION_DISK_FULL（30）	MonSub：宛先パスにスペースがありません。
MONSUB_FILECOPY_COPROC_ABRUPTLY_KILLED（31）	MonSub：File copy co-proc が突然終了しました。
MONSUB_LOGGING_COPROC_ABRUPTLY_KILLED（32）	MonSub：Logging co-proc が突然終了しました。
MONSUB_SM_DISCONNECT（33）	
MONSUB_FILECOPY_STATUS_MAX（34）	
その他	プロトコルモニタートレースの追加中に内部エラーが発生しました。中止しています…

コントロールプレーン SMGR 機能

この機能をサポートするための CP SMGR における変更は次のとおりです。

- MonSub トレースを有効または無効にするためのサービスを CLI に提供しています。
- コントロールプレーンでサブスクライバの MonSub を有効にすると、CP CLI の指示に従って、Sx インターフェイスを介して対応する U プレーンに変更が伝達されます。
- UP でのトレース障害は、UP から CP への Sx セッションレポート要求メッセージ内の「Private IE Subscriber Trace Status Report」で CP に報告されます（CP コンソールを介して MonSub が有効になっている場合）。

- この機能は、ユーザープレーンインスタンスごとにCPからfastpathおよびslowpath PCAPを作成するための4つの同時サブスクライバ トレース セッションのトレースをサポートします。
- CP インスタンスは、CP から MonSub を有効にするときに CLI インスタンス ID を送信するため、UP が正しい CP CLI インスタンス ID に通知を送信するようにします。

（注） 新規またはcamp-onコールのトレースを有効にすると、競合状態のシナリオが発生します。UE接続が進行中の場合、プライベート IE は Sx 確立要求または Sx 変更（接続フローを妨げないために、既存の接続シーケンス）で送信されます。既存のコールの場合、プライベート IE は Sx 変更要求で送信されます。

ユーザープレーン SMGR 機能

この機能をサポートするために UP SMGR は次のように変更されました。

- MonSub トレースを有効または無効にするためのサービスを CLI に提供します。
- コントロールプレーンの Sx インターフェイスを介した MonSub プライベート IEに基づきます、MonSubトレースを有効または無効にし、「Subscriber Trace Status Report」を生成して、トレースが有効かどうかをコントロールプレーンに通知します。
- NPUMGR を制御して、ストリームや TEP ベアラーを接続、開始、停止、追加、削除、切断します。
- SMGR は NPUMGR（CONNECT API の一部として）およびサブセッション ID から PSN を維持します。セッションIDはSMGR（ローカルSMGRインスタンス）固有です。SMGR はモニター サブスクライバ トレース セッションの NPUMGR に対して、PSN とサブセッション ID を含む要求をすべて送信します。
- CLIからの指示に基づいて、パケットサイズや優先順位などを変更するために（NPUMGRを介して）パノプティコンを設定します。
- 「16進ダンプモジュール」設定を読み取り、ローカルに保存します。関連するパラメータ（ファイル名など）をセッションマネージャ Co-Proc に渡します。
- セッションマネージャ Co-Proc をインスタンス化し、パノプティコンが生成した PCAP ファイルをハードディスクにコピーするように指示します。また、MonSub セッションが終了したときのセッションマネージャ Co-Proc の終了を処理します。
- セッションマネージャCo-Procからのファイルコピー メッセージを処理し、コピーされたバンドルについてパノプティコンに通知します。
- ファイルのコピーが失敗した場合、またはセッションマネージャ Co-Proc のインスタンス化に問題がある場合は、SNMP アラームを生成します。

- パノプティコンから通知されたバッファフルの兆候を処理し、RAM ディスクから設定された宛先ディレクトリに PCAP をコピーします。
- 制御/slow-path パケットをキャプチャします。それらをセッションマネージャ Co-Proc に渡して、個別の PCAP としてパブリッシュします。
- この機能は、ユーザープレーンインスタンスの最大4つのモニターサブスクライバ トレース セッションをサポートします。NPUMGR はトレース制限を適用します。
- ハードディスクに空き領域がない場合、またはハードディスクがない場合、MonSub トレースセッションは終了します。
- UP-SMGR インスタンスごとに co-proc（ファイルコピーとロギング）があり、その SMGR インスタンスに対してモニター サブスクライバ トレースが開始されます。
- 最終的なポーリングタイマーと co-proc/NPUMGR からの応答の切断によっては、MonSub セッションの切断に時間がかかります。

（注） 新規/camp-on コールに対してトレースが有効になっている場合、競合状態のシナリオが発生します。UE 接続が進行中の場合、プライベート IE は Sx/N4 確立要求または Sx/N4 変更要求（接続フローが妨げられないように既存の接続シーケンス）で送信されます。既存のコールの場合、プライベート IE は Sx/N4 変更要求で送信されます。

マルチ PDN マルチトレース

マルチ PDN コールの場合、Multi-trace=OFF で MonSub を開始すると、その MonSub セッションの一部として 1 つの PDN のみがトレースされます。新しい PDN が開始されると、既存の PDN トレースが停止し、新しい PDN トレースが開始します。この場合、最初に新しい PDN トレースが開始されてから、既存の PDN トレースが停止されるため、新しい PSN および SMGR サブセッション ID が割り当てられます。

マルチ PDN コールの場合、Multi-trace=ON で MonSub を開始すると、新しい FASTPATH トレースセッション（MonSub セッション）の一部として新しい PDN がトレースされるため、4 つの PDN をトレースすると、最大トレースセッションに到達したことが MonSub CLI に示されます。各 PDN のトレースは、個別の MonSub セッションとして実行されます。

（注） Pure-S コールの場合、CP から MonSub を開始すると、マルチ PDN のトレースは、MT=ON または OFF に関係なく、別の FASTPATH トレースセッション（別の MonSub セッション）として実行されます。

MonSub 統計

fastpath PCAP キャプチャの品質に関する統計情報をパブリッシュするための新しいメカニズムが MonSub CLI に追加されました。新しいメカニズムは、5 秒ごとにスロットリングされたバッファフル MEH 指示を SESSMGR で受信するたびに統計情報をパブリッシュします。この機能は、MonSub セッションに対応する fastpath PCAP に対して最大 4 つのバッファをサポートします。この機能はデフォルトでは統計情報をパブリッシュしないため、UP でデバッグ CLI を使用して有効にする必要があります。

- **debug uplane monsub-stats disabled**
- **debug uplane monsub-stats enabled**

統計情報には、次の情報が含まれます。

```
Packet accepted: 14250000                          Packet rejected: 62297
Congestion Short Term: 0                            Congestion Longer Term: 0
Throttled: 0                                                  PCAP File Transfer Rate:
9.91 mbps
```

PCAP ファイルの転送速度は、copy co-proc が RAM-FS から HD-RAID に PCAP を書き込む速度です。

X-Header

この機能は、slowpath PCAP における X-Header のキャプチャをサポートします。PGW-U は、アップリンクパケットの X-HEADER を挿入します。PGW-U は、入口インターフェイスと出口インターフェイスでパケットをキャプチャします。したがって、SGi に送信される出口パケットには、挿入済みの x-header が含まれます。

PGW-U は、ダウンリンクパケットの X-HEADER を挿入します。PGW-U は、入口インターフェイスと出口インターフェイスでパケットをキャプチャします。したがって、S5-U または S1-U に送信される出口パケットには、挿入済みの x-header が含まれます。

機能の仕組み

サブスクライバのモニター機能については、次項で詳しく説明します。

UPF におけるサブスクライバのモニターの設定手順

プロトコルモニターは、現在処理中の特定のサブスクライバセッションの情報を表示するために使用できます。モニター対象のプロトコルの数と進行中のセッション数に応じて、大量のデータが生成されます。生成されたすべての情報をキャプチャするには、端末クライアントでロギングを有効にすることを強くお勧めします。

MonSub は、UPF コンソールから開始することもできます。特定の IMSI のモニタリングは、SMF および UP コンソールのいずれからも有効にしないでください。

特定のサブスクライバセッションのプロトコルモニタリングツールを起動して設定するには、この項の手順に従います。

手順

ステップ 1 **monitor subscriber** CLI コマンドを入力して、Exec モードから monitor subscriber コマンドを呼び出します。

```
[local]host_name# monitor subscriber { callid | imei | imsi | ipaddr | ipv6addr |
msid | msisdn | next-call | pcf | peer-fa | peer-lac | sgsn-address | type |
username }
```

現在使用可能なすべてのプロトコル（それぞれに割り当てられた番号を持つ）が一覧表示された出力が表示されます。適切なキーワードを入力して、モニターが使用するメソッドを指定します。

ステップ 2 適切なキーワードを入力して、モニターが使用するメソッドを指定します。

その他のオプションを選択したり、選択したキーワードに適切な情報を入力したりします。

ステップ 3 その他のオプションを選択したり、選択したキーワードに適切な情報を入力したりします。

モニターの起動時に、指定された基準に一致するセッションが処理されなかった場合は、使用可能なモニタリングオプションの画面が表示されます。

ステップ 4 モニターによって表示される情報の量を設定します。オプションを有効または無効にするには、そのオプションに関連付けられている文字または 2 桁の数字（C、D、E、11、12 など）を入力します。冗長性を向上または低下させるには、プラス（+）またはマイナス（-）キーを使用します。

各オプションの右側には、[ON (enabled)] または [OFF (disabled)] の現在の状態が表示されます。

マルチコールトレースを実行するためのオプション **Y** は、GGSN での使用に対してのみサポートされています。

```
WARNING!!! You have selected options that can DISRUPT USER SERVICE
Existing CALLS MAY BE DROPPED and/or new CALLS MAY FAIL!!!
(Under heavy call load, some debugging output may not be displayed)
Proceed? - Select (Y)es or (N)o
```

ステップ 5 必要に応じてステップ 6 を繰り返して、複数のプロトコルを有効または無効にします。

ステップ 6 **[Enter]** キーを押して画面を更新し、モニタリングを開始します。

モニターは、無効になるまでアクティブのままになります。プロトコルモニターを終了してプロンプトに戻るには、**q** を押します。

Monsub CLI オプション

次のオプションがデフォルト値で既存の **monitor subscriber** コマンドに追加されました。

UPF Monitor Subscriber CLI

オプションは次のとおりです。

- **W** - UP PCAP Trace (ON)：このパラメータは、slowpath と fastpath の PCAP トレースを作成するために使用されます。
- **U** - Mon Display (ON)：非プロトコルイベント（ECS からの統計情報や課金情報など）も slowpath PCAP ファイルにキャプチャされ、UPF モニターコンソールに表示されます。
- **V** - PCAP Hexdump (ON)：UPF で 16 進ダンプ形式のテキストファイルにプロトコルパケットをキャプチャするには、このフラグを ON に設定する必要があります。

（注） 現在、fastpath および slowpath PCAP ファイルをキャプチャするには、UP PCAP トレースフラグを ON に設定する必要があります。

- **F - Packet Capture (Full Pkt)**：fastpath からすべてのパケットをキャプチャします。

  オペレータはこのオプションを使用して、完全なパケットキャプチャと部分的なパケットキャプチャを選択できます。**F** を入力すると、パケットキャプチャタイプを完全なキャプチャまたは部分的なキャプチャに変更できます。部分的なパケットキャプチャでは、1 ～ 16384 バイトのパケットサイズを入力できます。たとえば、20 と入力すると、fastpath パケットの最初の 20 バイトだけがキャプチャされ、残りのパケットはドロップされます。

（注） PCAP ファイルを開くと、概要ビューにはパケットのフルレングスが表示されますが、詳細ビューには切り捨てられたパケットのみが表示されます。

- **/ - Priority (0)**：値は「0（ベストエフォート）」～「7（保証）」の範囲です。
  - 0：ベストエフォート
  - 1：低
  - 2：低～中
  - 3：中
  - 4：中～高
  - 5：高
  - 6：クリティカル
  - 7：保証

⚠

注意 デフォルト値を変更しないことを強く推奨します。システム パフォーマンスに悪影響を及ぼす可能性があります。

- **N - MEH Header (OFF)**：このオプションが設定されている場合、IP パケットから MEH ヘッダーが削除されます。

Monitor Subscriber セッションの表示

進行中の MonSub セッションを表示する新しい CLI を以下に示します。

show monitor subscriber fastpath session all CLI コマンドは、SMF と UPF の両方からトリガーできます。**show monitor subscriber fastpath session up-ip-address** CLI コマンドは SMF からトリガーできます。

- **SessId**：UPF Sessmgr の MonSub セッションのローカルセッション ID です。
- **CallID**：UPF のコール ID。
- **PSN**：これはパノプティコンのシーケンス番号です。1 つの UPF には、0 ～ 3 の範囲の PSN を持つ最大 4 つの MonSub fastpath トレースセッションがあります。
- **Start time**：MonSub トレースセッションの開始時刻。
- **Interface Type**：開始された MonSub fastpath トレースセッションのコールタイプ（Sxa、Sxb、Sxab）を識別します。

Monitor Subscriber セッションの解除

進行中の MonSub セッションを切断する新しい CLI を以下に示します。CP と UP の両方から CLI をトリガーできます。

monitor subscriber fastpath disconnect sessmgr-instance *upf_sessmgr_instance_id* **session-id** *local_monsub_sessid_sessmgr_level*

MonSub セッションの切断に成功すると、次のメッセージがコンソールに表示されます。

```
Session Disconnected Successfully
```

MonSub セッションの切断に失敗すると、次のメッセージがコンソールに表示されます。

```
Monitor Subscriber session does not exist
```

（注） モニター切断 CLI を実行できるのは、セキュリティ管理者だけです。

モニターサブスクライバのコンテキスト、CDRMOD、および16進ダンプのインタラクション

16進ダンプモジュールは、オペレータがファイル名とポーリングタイマーを設定するためのプロビジョニングを提供するように設定する必要があります。16進ダンプモジュールは、CDRMOD機能の一部である EDR、UDR などのモジュールの 1 つです。ECS コンテキストなどの非ローカルコンテキストで16進ダンプを設定します。ローカルコンテキストでは16進ダンプモジュールはサポートされていません。

16 進ダンプモジュールとその設定の詳細については、「UPF での MonSub の 16 進ダンプモジュールの設定」の項を参照してください。

PCAP ファイル名の表記法

ここでは、PCAP ファイルの命名規則について説明します。

（注） PCAP ファイルの命名では、**monitor-subscriber-file-name** および **rotation** オプションのみを使用します。

slowpath ファイル名の規則

slowpath ファイル名は次のフォーマットになります。

```
curr_slowpath_{SMGR Mon Sub Session
Id}_{monsub_file_name_option_val}_{Timestamp}_{RotationCount}.pcap
```

、または

```
slowpath_{SMGR Mon Sub Session
Id}_{monsub_file_name_option_val}_{Timestamp}_{RotationCount}.pcap
```

プレフィックス「curr_」が付いているファイルは、現在書き込み中で、まだ閉じられていないファイルです。ファイルをローテーションする場合（ファイル ローテーション パラメータに応じて）、プレフィックス「curr_」が付いていないファイルがハードディスクにコピーされます。

SMGR MonSub Session Id：これは、この PCAP を作成した Uplane SMGR インスタンス ID で作成された MonSub セッションのセッション ID です。この ID は SMGR インスタンスに対してローカルであるため、同じ ID でキャプチャされた slowpath PCAP が 2 つ存在する可能性があります。

ファイルをハードディスクにコピーする場合、monsub_file_name_option_val は次のように置き換えられます。

- **monitor-subscriber-file-name** が「imsi」に設定されている場合は IMSI 値
- **monitor-subscriber-file-name** が「call-id」に設定されている場合はコール ID 値
- **monitor-subscriber-file-name** が「username」に設定されている場合はユーザー名の値

タイムスタンプのフォーマットは「MMDDYYYYHHMMSS」です。

- MM：月、DD：日、YYYY：年
- HH：時間、MM：分、SS：秒

RotationCountは9桁の値で、古いファイルがローテーションされ、新しいファイルが生成されるたびに1増加します。

最初のファイルは00000000、2番目のファイルは00000001というように増えていきます。

slowpathファイルのローテーションは、**hexdump-module file**設定の次のオプションによって規定されます。

rotation { num-records *number* **| time** *seconds*| **volume** *bytes* **}**

- **num-records**：[num-records]はパケット数を指定します。パケット数がこの数を超えると、新しいファイルが生成され、ファイル名の[RotationCount]が1増加します。[number]の範囲は100 ～ 10240で、デフォルト値は1024です。
- **time**：[time]は新しいファイルが生成され、ファイル名の[RotationCount]が1増加するまでの待機時間を秒単位で指定します。[seconds]は30 ～ 86400までの整数である必要があります。デフォルト値は3600です。
- **volume**：[volume]はバイト数を指定します。バイト数がこの数を超えると、ファイル名の[RotationCount]が1増加します。[bytes]は51200 ～ 62914560までの整数である必要があります。デフォルト値は102400です。

（注） ローテーション中の**tarriff-time**パラメータは、PCAPファイルのキャプチャには適していないため、無視されます。

以下に、slowpath PCAP ファイルのファイル命名規則の例を示します。

- [imsi]オプションが設定されていて、IMSIが「112233445566778」である場合、slowpathファイルは次のように命名されます。

```
slowpath_S0_112233445566778_07152019050907_000000000.pcap
```

- [call_id]オプションが設定されていて、コールIDが「01317b22」である場合、slowpathファイルは次のように命名されます。

```
slowpath_S0_01317b22_07152019050907_000000000.pcap
```

（注） **tarrif-time** パラメータは、PCAP ファイルキャプチャには適用されません。

fastpath ファイル名の規則

fastpath ファイル名は次のフォーマットになります。

```
vpp_{S}_{B}_{encap}_{monsub_file_name_option}_{Timestamp}_{FileCount}.pcap
```

- S は、「S1」、「S2」、「S3」、「S4」のいずれかに置き換えられます。
- Bは、Panopticonによって生成されたバンドルに応じて、「B0」、「B1」、「B2」、「B3」のいずれかに置き換えられます。
- monsub_file_name_option は次のように置き換えられます。
  - **monitor-subscriber-file-name** が「imsi」に設定されている場合は IMSI 値
  - **monitor-subscriber-file-name** が「call-id」に設定されている場合はコール ID 値
  - **monitor-subscriber-file-name** が「username」に設定されている場合はユーザー名の値

タイムスタンプのフォーマットは「MMDDYYYYHHMMSS」です。

- MM：月、DD：日、YYYY：年
- HH：時間、MM：分、SS：秒

RotationCountは9桁の値で、古いファイルがローテーションされ、新しいファイルが生成されるたびに 1 増加します。

最初のファイルは00000000、2番目のファイルは00000001というように増えていきます。

fastpath の [FileCount] は、slowpathの [RotationCount] パラメータと同じではないため、fastpathファイルの命名時には [hexdump-module file Rotation] パラメータは無視されます。

この機能のフェーズ 1 では、fastpath で生成されたファイル名は「vpp_S1_B0_ip.pcap」または「vpp_S1_B1_ip.pcap」などであり、不揮発性ストレージにコピーされるときに次のように名前が変更されます。

- `vpp_S1_B0_ip_01317b22_07152019050907_000000000.pcap`
- `vpp_S1_B1_ip_01317b22_07152019050908_000000001.pcap`
- `vpp_S1_B0_ip_01317b22_07152019050908_000000002.pcap`

MonSub フェーズ 3 では、PCAP「バンドル」は、イーサネットカプセル化を使用する単一の PCAP ファイルに置き換えられます。

フェーズ3では、各 fastpathセッションファイルは「vpp_S0_B0_eth.pcap」というイーサネット PCAP ファイルにキャプチャされ、不揮発性ストレージにコピーされるときに次のように名前が変更されます。

```
vpp_S0_B0_eth_01317b22_07152019050907_000000000.pcap
```

[call_id] オプションが設定されていて、コール ID が「12345678ef」である場合：

- `slowpath_S0_12345678ef _07152019050907_000000000.pcap`

- vpp_S1_B0_eth_12345678ef _07152019050907_000000000.pcap

[username] オプションが設定されていて、ユーザー名が「9890098900」である場合：

- slowpath_S0_07152019050907_000000000_9890098900.pcap
- vpp_S1_B0_eth_07152019050907_000000000_9890098900.pcap

PCAP ファイルの場所

fastpath PCAP ファイルは、セッションマネージャがサブスクライバセッションを所有しているのと同じカードおよび CPU コンプレックス内の /records/pcap ディレクトリに書き込まれます。

/records ディレクトリは「tmpfs」ファイルシステムにマッピングされ、このファイルシステムは RAM にマッピングされます。この状態で、ファイルには「.pending」の拡張子が付けられます。次に例を示します。

```
-rw-rw-r-- 1 root root 268599296 Sep 23 14:04 vpp_S1_B0_eth.pending
```

（注） この段階のファイルサイズは、永続ストレージに書き込まれるときの実際のファイルサイズではありません。

fastpath トレースメカニズムによってファイルが書き込まれると、「.pcap」ファイルに変換され、次のように名前が変更されます。「.done」の拡張子で終わるファイルもあります。

```
-rw-rw-r--    1 root     root       8689188 Oct 16 22:06 vpp_S0_B0_eth.pcap
```

PCAP ファイルが fastpath トレースメカニズムによって書き込まれた後、Co-Proc 機能によってファイルがインスタンス化され、ハードディスクまたは永続ストレージにコピーされます。

前述の fastpath のファイル格納プロセスは、slowpath にも当てはまります。

すべてのケースでターゲットファイルの場所は /hd_raid/records/hexdump になります。ただし、16 進ダンプモジュールの設定では **use-harddisk** が有効になっており、**hexdump file** では **directory** オプションはカスタム値になります。たとえば、**directory** オプションの値が「abc」に設定されている場合、PCAP ファイルのターゲットの場所は /hd_raid/records/hexdump/abc/ になります。

この機能を実装すると、事前定義した場所が PCAP ファイルに設定されます。

- **use-harddisk** および **hexdump module** の設定を使用して問題が発生した場合に、/records/pcap ディレクトリにデータが入力されないようにするため。
- /hd_raid/records/hexdump ディレクトリを定期的にクリーンアップするため。

外部ロケーションへのファイル転送

ファイルがハードディスクにコピーされたら、**hexdump-module** コンフィギュレーションの **hexdump** コマンドで **transfer-mode** オプションを使用すると、外部サーバーにコピーできます。

transfer-mode 以外にも、**hexdump** では他の関連オプションを外部へのファイル転送に使用できます。オペレータはこれらのコマンドを使用して、fastpath 処理中のストレージ不足を回避できます。

制限事項

制限事項は次のとおりです。

- 終了直後にトレースを再開すると、`/records/pcap` ディレクトリ内の fastpath ファイルが上書きされる可能性があります。短時間（数秒）待ってからセッションを再開することを推奨します。
- MonSub トレースが停止すると、切断プロセスに数秒かかることがあるため、数秒待つことを推奨します。最大 5 秒（秒単位の 16 進ダンプのポーリングタイマー値）待ってから切り替えて、MonSub トレースを開始します。そうしないと、MAX TRACING SESSIONS REACHED が一時的にオペレータに表示されることがあります。
- show monitor subscriber fastpath sessions CLI では、停止中の MonSub セッションは表示されないため、最大セッション数に達したことで、新しい MonSub セッションが一時的に拒否される期間があり、show CLI ではセッション数が少なく表示されます。オペレータは、しばらく待機してから、新しい MonSub トレースセッションを開始することを推奨します。
- fastpath 設定オプションの変更は、**UP Pcap トレース**が [OFF] に設定されている場合にのみ可能です。
- マルチ PDN で MT=ON になっている場合、MT=OFF になると、MAX TRACING REACHED が原因で新しい PDN トレースは開始されず、他のすべてのトレースが停止します。これは、最初の新しい PDN トレースが開始されてから MT=OFF になり、以前の PDN がすべて停止されたためです。
- 異なる CLI から同じ UE MonSub セッションを起動しないことを推奨します。
- slowpath PCAP では、GTP-U を追加する機能が fastpath にあり、出力 DL パケットに GTPU-U ヘッダーが表示されないため、入力パケットに適用された HTTP X-Header などのパケット変更がない限り、入力および出力 DL パケットは重複して表示されます。
- C オプションと D オプションを切り替えても、PCAP キャプチャには影響しません。
- マルチ PDN の場合、fastpath ファイル名にコール ID は使用されません。これは、定義上、マルチ PDN のケースには複数のコール ID があり、IMSI などの上位レベルの設定がファイルの命名に適しているためです。
- このドキュメントで明示的に言及されている名前付きオプションのみが、hexdump-module ファイルの設定でサポートされます。

- fastpath でトレースできるストリームの数は 5,000 に制限されています。ストリームは、送信元 IP アドレス、宛先 IP アドレス、送信元ポート、および宛先ポート、トランスポートプロトコル（TCP または UDP）で構成される TCP または UDP フローとして定義されます。
- fastpath パケットは外部サーバーにストリーミングできないため、ハードディスクに保存され、手動で、または **transfer-mode** オプションを使用して転送されます。
- fastpath および slowpath PCAP ファイルをキャプチャするには、UP PCAP トレースを [ON] に設定する必要があります。
- MonSub CLI オプション <SPACE> [Pause] は、コンソールイベントを一時停止するだけです。このオプションは、他のトレースイベント（slowpath PCAP、fastpath PCAP、および 16 進ダンプ形式のテキストファイルのプロトコルパケットトレース）には影響しません。
- UP トレース PCAP ファイルには、競合状態が原因で、最初の PFCP Sx 要求/応答は含まれていません。
- ICMP パケットと TCP および UDP ストリームの最初のパケットは、slowpath と fastpath の両方を通過します。GTPU（オプション 26）およびユーザー L3（オプション 19）のデフォルト値は [OFF] に設定されているため、それらのパケットは slowpath キャプチャでキャプチャされません。オプション 26 が [ON] に設定されている場合、それらのパケットは slowpath PCAP キャプチャでキャプチャされます。前のポイントで説明したように、オプション 19 は slowpath PCAP キャプチャには影響を及ぼしません。
- fastpath および slowpath PCAP ファイルをキャプチャするには、データイベントフラグを [ON] に設定する必要があります。
- Pure-S コールでは最初の PDN トレースのみがサポートされます。この制限は、複数のサブスクライバトレースのサポートで修正されます。
- MoSub トレースは、UP 時の **Next-SAEGW Call** オプションではサポートされていません。
- MonSub トレースは、Pure-S コールタイプの **Next call by APN** オプションではサポートされていません。
- デフォルト値の poll-timer を使用した ASR 5500 セットアップでは、既知の問題が原因ですべてのパケットがキャプチャされない可能性があります。多数のパケットが拒否されないようにするには、poll-timer 値を可能な限り低い値（10 ミリ秒）に変更することを推奨します。
- コンテキストの置換が発生した場合（同じサブスクライバが切断されずに再接続した場合）、新しいコールの slowpath キャプチャは古い slowpath ファイルに残り続けます。

UPF での MonSub の 16 進ダンプモジュールの設定

MonSub ポールタイマーの設定

この設定を使用して、PCAP ファイルキャプチャチェックの頻度を設定します。

```
configure
  context context_name
    hexdump-module
      hexdump monitor-subscriber-poll-timeout poll_timer_value
      end
```

注：

- **hexdump monitor-subscriber-poll-timeout** ：このオプションは、揮発性ストレージ内の新たにキャプチャされたPCAPファイルを、永続ストレージにコピーする前に実行する必要があるチェックの頻度を指定します。
- *poll_timer_value*：ポーリングタイマー値をミリ秒単位で指定します。10 ミリ秒～ 60 秒までの整数で指定する必要があります。デフォルト：30 秒。

（注） このタイマーに 5 秒未満の値は設定しないでください。

- このオプションは、fastpath 機能を備えた製品（PGW、ASR-5500 上の SAEGW、および VPC-SI）で MonSub が有効になっている場合にのみ適用されます。

MonSub ファイル名の設定

次の設定を使用して、IMSI、コール ID、またはユーザー名を含む PCAP ファイルのファイル名を指定します。

```
configure
  context context_name
    hexdump-module
      file rotation { num-records number | tariff-time minute minutes
hour hours | time seconds| volume bytes | monitor-subscriber-file-name {
imsi | username | call-id }
      end
```

注：

- **monitor-subscriber-file-name { imsi | username | call-id }**：このオプションは、キャプチャされた PCAP ファイルの名前に IMSI、コール ID、またはユーザー名を含むかどうかを指定します。このオプションは、fastpath 機能を備えた製品（PGW、ASR 5500 上の SAEGW、および VPC-SI）で、かつサブスクライバのモニター機能が有効になっている場合にのみ適用されます。デフォルトは IMSI です。

- **rotation { num-records** *number* **| tariff-time minute** *minutes* **hour** *hours* **| time** *seconds* **| volume** *bytes* **}**：16 進ダンプファイルを閉じて新しいファイルを作成するタイミングを指定します。
  - **num-records** *number*：16進ダンプファイルに追加する必要があるレコードの最大数を指定します。ファイル内のレコード数がこの値に達すると、ファイルが完成します。

    number は 100 ～ 10240 の整数である必要があります。デフォルト：1024
  - **tariff-time minute** *minutes* **hour** *hours*：現在の 16 進ダンプファイルを閉じて、タリフ時間（時分単位）に基づいて新しいファイルを作成します。

    minutes は 0 ～ 59 までの整数である必要があります。

    hours は 0 ～ 23 までの整数である必要があります。
  - **time** *seconds*：現在の 16 進ダンプファイルを閉じて新しいファイルを作成するまでの待機時間（秒単位）を指定します。

    seconds は 30 ～ 86400 の整数である必要があります。デフォルト：3600

重要 ローテンション時間は 30 秒に設定します。

  - **volume** *bytes*：16 進ダンプファイルを閉じて、新しいファイルを作成するまでのファイルの最大サイズを指定します（バイト単位）。

    bytes は 51200 ～ 62914560 の整数である必要があります。compression キーワードが gzip に設定されている場合、設定が大きいほど圧縮率が向上する場合があることに注意してください。デフォルト：102400

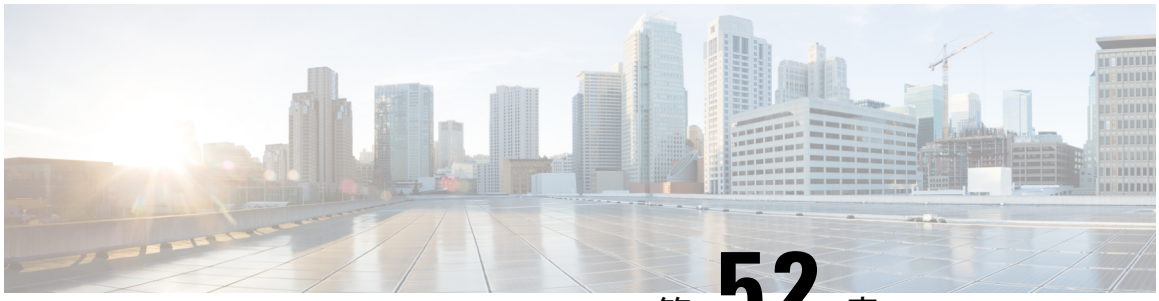
モニタリングおよびトラブルシューティング

この項では、モニターサブスクライバ機能のモニタリングと障害対応について説明します。

SNMP トラップ

モニターサブスクライバ機能をサポートするために、次の SNMP トラップが追加されました。

- **MonSubProcessInitFailure**：このトラップは、MonSub ハンドラプロセスが特定のプロセスやサービスで失敗した場合にトリガーされます。



第 52 章

CUPS の VPC-SI での MPLS のサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

既存のプラットフォーム（VPC-DI、ASR 5500）では、Boxer が MPLS をサポートしており、MPLS が基盤となるデータプレーンフォワーダを使用して MPLS トラフィックを切り替えます。ASR 5500 では、NP4c ネットワークプロセッサが MPLS トラフィックを生成および処理し、VPC-DI では、IFTask が MPLS トラフィックを生成および処理します。

CUPS の VPC-SI における MPLS サポート機能により、データプレーンフォワーダとして VPP を使用する VPC-SI（SI-CUPS）での MPLS サポートが有効になります。

VPP は、個別のグラフノードとして MPLS スタックを含む複数のデータプレーン機能をサポートし、提供します。また、ラベル付きパケットを生成し、着信ラベル付きパケットを同時に処理するため、さまざまな顧客 VRF を区別して、アドレッシングモデルと要件が異なる多数の企業 APN をサポートできます。

CUPS の VPC-SI における MPLS サポート機能は、次の機能をサポートしています。

- VPP MPLS スタックを使用した、MPLS ラベル付きパケットの送信。
- VPP MPLS スタックを使用した、着信ラベル付き MPLS パケットの処理。
- 既存のすべての MPLS 設定（VPC-DI、ASR 5500）のサポート、および VPC-SI CUPS を使用した新しい展開と同等の機能の提供。
- VPP 内にある NHLFE および ILM テーブルを表示して、値をデバッグしたり、Boxer 設定と比較したりするための VPPCTL CLI コマンドのサポート。

機能の仕組み

ここでは、CUPS の VPC-SI での MPLS サポートの仕組みについて簡単に説明します。

現在の CUP アーキテクチャでは、VPP フォワーダが独自の MPLS スタックを提供し、MPLS パケット処理に関する既存の機能をすべてサポートします。VPP MPLS スタックは、適切なネクストホップラベル転送エントリ（NHLFE）および着信ラベルマップ（ILM）テーブルで設定されます。これは、正しい MPLS ヘッダーを使用して出力時に MPLS パケットを生成するのに役立ちます。また、着信 MPLS パケットを処理し、着信ラベルに基づいてこのパケットを適切なネクストホップテーブル ID（サブスクライバの VRF コンテキスト）に切り替えます。

MPLS ソリューションでは、次のシナリオがサポートされています。

- PE に接続された MPLS-CE
- PE としての VPC-SI

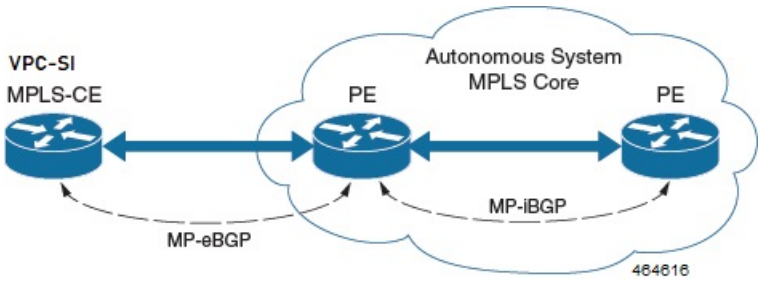
また、VPC-SI は RFC 4659（*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*）で説明されているとおり、VPNv6 をサポートします。

PE に接続された MPLS-CE

VPC-SIは、プロバイダーエッジ（PE）ラベルエッジルータ（LER）に接続されているMPLS-CE（カスタマーエッジ）ネットワーク要素として機能し、その結果、RFC 4364 に従い MPLS コアに接続されます。

次の図は、MPLS-CE から PE への接続を示しています。

図 *19 : VPC-SI MPLS-CE* から *PE*



MPLS-CE は、独自の自律システム（AS）内の PE ルータのように機能します。MPLS-CE では、Virtual Routing and Forwarding（VRF）ルートが維持され、MP-eBGP（マルチプロトコル外部 BGP）セッションを介して、VPN ルート情報が PE と交換されます。

PE も VRF を使用して設定され、MP-iBGP（マルチプロトコル内部 BGP）接続を介して AS 内の他の PE と VPN ルートを交換し、MP-eBGP 接続を介して MPLS-CE を交換します。

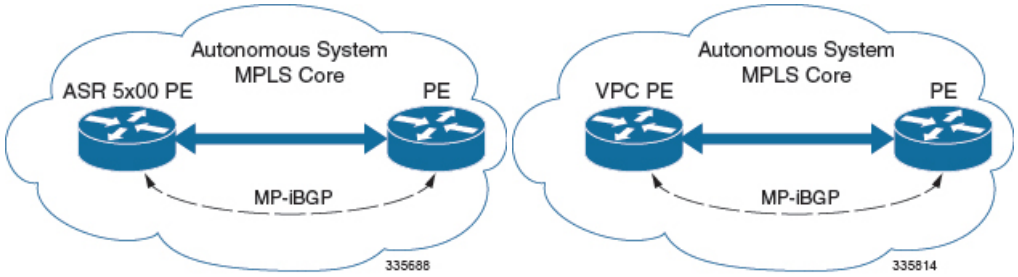
EBGP 接続を使用すると、PE は、IBGP ピアから学習したルート内のネクストホップ IP アドレスとラベルを変更してから、MPLS-CE にアドバタイズできます。MPLS-CE は、ルートをアドバタイズして学習するために MP-eBGP だけを使用します。直接接続 EBGP ピアリングのため、Label Distribution Protocol（LDP）および Resource Reservation Protocol（RSVP）は必要ありません。MPLS-CE は、PE との間で（MP-eBGP 接続を介して学習された）単一のラベルをプッシュまたはポップします。

PE としての VPC-SI

概要

このシナリオでは、VPC-SI は MPLS コアのエッジにある PE ルータとして機能します。以下の図を参照してください。

図 *20 : PE* としての *VPC-SI*



VPC-SI では、 最初の 2 つのシナリオに示されているように、ASBR や PE は不要です。このシナリオでは、IBGP 機能と MPLS ラベル配布プロトコルという 2 つの主要な要件が導入されています。

VPC-SI は、次の 2 つのラベルを追加するように設定できます。

- LDP または RSVP TE から学習した外部ラベル（RSVP トラフィックエンジニアリング）
- MP-iBGP から学習した内部ラベル

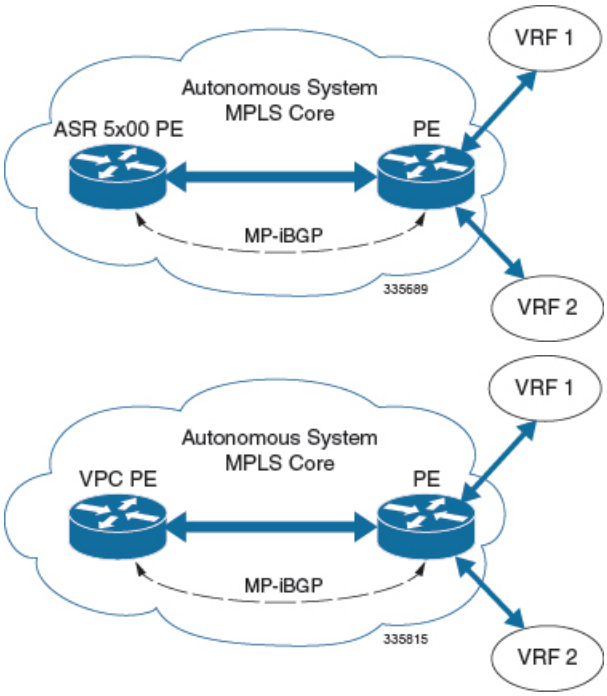
このソリューションは、VPC-SI を介して開始されたトラフィック エンジニアリングと QoS をサポートします。

設定例

この例では、VRF は ASR 5500 PE で設定され、プールは VRF に関連付けられています。VPC-SI は、VPN ルートを IBGP ピア（PE ルータ）と交換し、LDP 経由で PE に到達するための MPLS

パスを学習します。VPC-SI は、2 つのラベル（PE から学習した内部ラベルとネクストホップ IBGP ネイバーから学習した外部ラベル）を持つネクストホップにパケットを転送します。

図 *21* : 設定例




```
mpls ip
  protocol ldp
    enable
  exit
exit

ip vrf vrf1
  mpls traffic-class copy
exit
ip vrf vrf2
  mpls traffic-class value 5
exit

router bgp 300
  ip vrf vrf1
    route-target export 300 1
      route-target import 300 1
      route-distinguisher 300 1
  exit
    ip vrf vrf2
      route-target export 300 2
        route-target import 300 2
        route-distinguisher 300 2
  exit

  router-id 209.165.201.1
  neighbor 209.165.200.225 remote-as 300
  neighbor 209.165.200.225 update-source node1_loopback

  address-family vpnv4
    neighbor 209.165.200.225 activate
```

```
      neighbor 209.165.200.225 send-community both
      neighbor 209.165.200.225 next-hop-self
  exit

  address-family ipv4 vrf vrf1
    redistribute connected
  exit

  address-family ipv4 vrf vrf2
    redistribute connected
exit

interface interface_to_internet
  ip address 209.165.200.224/27
  mpls ip
exit
router ospf
  network 209.165.201.0/27 area 209.165.201.5
exit
```

BGP MPLS VPN の IPv6 サポート

概要

VPC-SI は RFC 4659（*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*）で説明されているとおり、VPNv6 をサポートします。

IPv6 VPN は、PE ルータを通じ、IPv6 インターフェイスまたはサブインターフェイスを介してサービスプロバイダー（SP）のバックボーンに接続されます。このサイトは IPv4 と IPv6 の両方に対応できます。各 VPNv6 には独自のアドレス空間があります。つまり、特定のアドレスが異なる VPN 内の異なるシステムを示すことになります。これは、ルート識別子（RD）を IP アドレスに付加する VPNv6 アドレスファミリによって実現します。

VPNv6 アドレスのバイト数は 24 で、8 バイトの RD から始まり、16 バイトの IPv6 アドレスで終わります。サイトが IPv4 と IPv6 対応の場合、同じ RD を IPv4 と IPv6 の両方のアドレスのアドバタイズメントに使用できます。

システムは、IPv6 ルートに RD を追加し、VPNv6 アドレスファミリを使用してラベル付けされた IPv6 を交換します。VPNv6 ルートのアドレスファミリ識別子（AFI）と後続のアドレスファミリ識別子（SAFI）の フィールドは、2 と 128 にれぞれ設定されます。

IPv6 VPN トラフィックは、IPv4 トンネリングを介して BGP スピーカーに転送されます。BGP スピーカーは、8 オクテットの RD がゼロに設定され、16 オクテットの IPv6 アドレスがアドバタイズルータの IPv4 アドレスを含む IPv4 マッピング IPv6 アドレス（RFC 4291）としてエンコードされている VPN-IPv6 アドレスを含むネクスト ホップ ネットワーク アドレス フィールドをピアにアドバタイズします。これは、VPNv6 ルートを交換するために EBGP ピアリングのみが使用されることを前提としています。

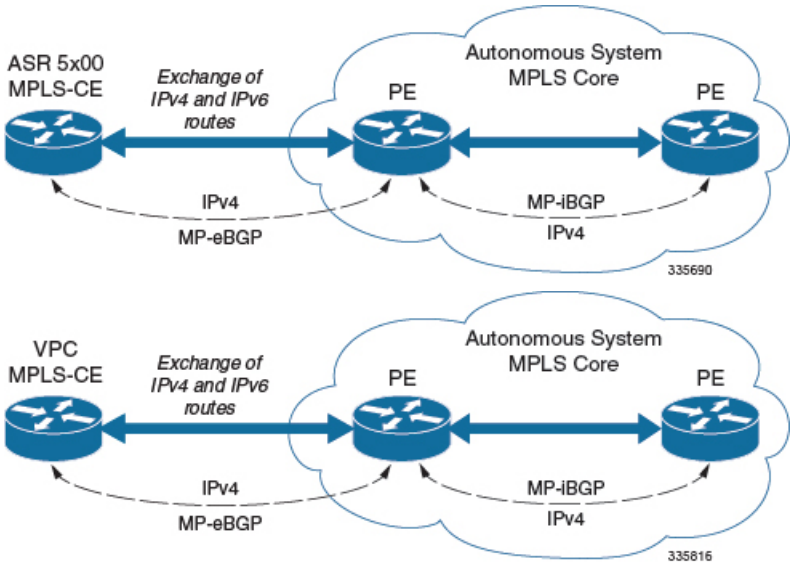
VPN IPv6 のサポートは、次を前提としています。

- デュアルスタック（IPv4/IPv6）ルーティング
- VRF の IPv6 プール

- 直接接続された IPv4 インターフェイスを介した BGP ピアリング

以下の図を参照してください。

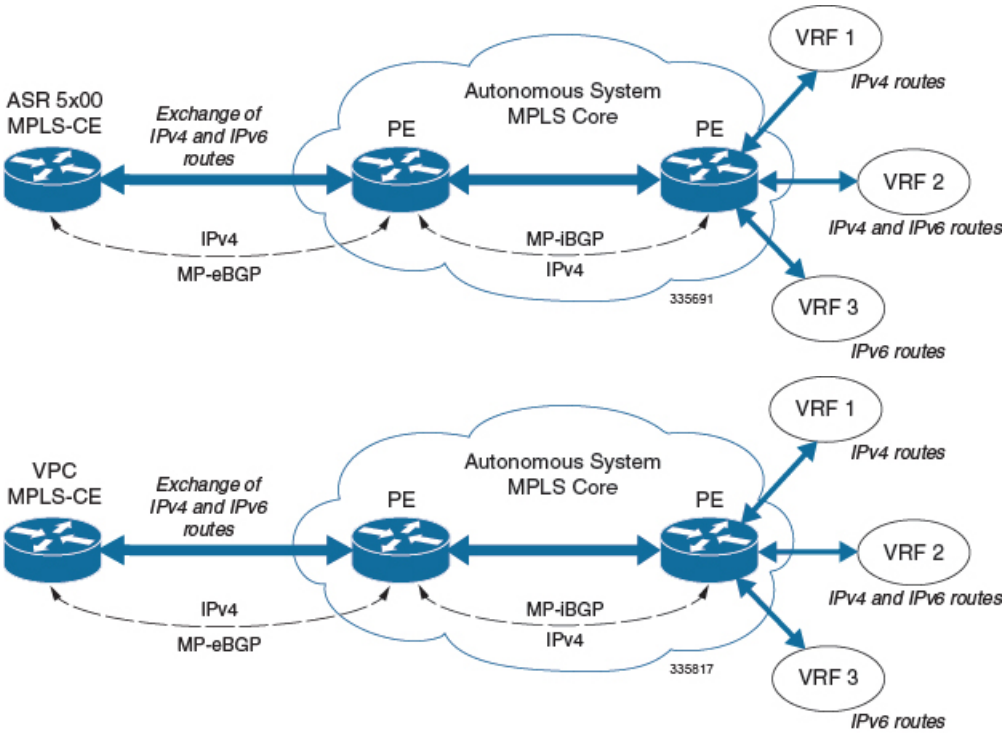
図 *22 : VPNv6* に対する *IPv6-RD* サポート



設定例

この例では、3 つの VRF を想定しています。VRF 1 には IPv4 ルートのみがあり、VRF 2 には IPv4 と IPv6 の両方のルートがあり、VRF 3 には IPv6 ルートのみがあります。

図 *23 : VPNv6* の設定例



VRF を設定します。

```
ip vrf vrf1
exit
ip vrf vrf2
exit
ip vrf vrf3
exit
```

MPLS bgp forwarding を有効にします。

```
mpls bgp forwarding
```

プールを設定します。

```
ip pool vrf1-pool 209.165.200.230 255.255.255.224 private 0 vrf vrf1
exit
ip pool vrf2-pool 209.165.200.230 255.255.255.224 private 0 vrf vrf2

exit
ipv6 pool vrf2-v6pool prefix 2005:0101::/32 private 0 vrf vrf2
exit
ipv6 pool vrf3-v6pool prefix 2005:0101::/32 private 0 vrf vrf3
exit
```

インターフェイスを設定します。

```
interface ce_interface_to_rtr
  ip address 209.165.200.226 255.255.255.224
exit
interface ce_v6_interface
  ip address 2009:0101:0101:0101::1/96
exit
interface ce_loopback loopback
```

```
  ip address 209.165.200.227 255.255.255.255
exit
interface vrf1-loop loopback
  ip vrf forwarding vrf1
  ip address 209.165.200.228 255.255.255.255
exit
interface vrf2-loop loopback
  ip vrf forwarding vrf2
  ip address 209.165.200.229 255.255.255.255
exit
interface vrf2-v6loop loopback
  ip vrf forwarding vrf2
  ip address 2005:0202:0101::1/128
exit
interface vrf3-v6loop loopback
  ip vrf forwarding vrf3
  ip address 2005:0303:0101::1/128
exit
```

アドレスファミリおよび再配布ルールとともに BGP を設定します。

```
router bgp 800
  router-id 209.165.200.225
neighbor 209.165.200.240 remote-as 1003
  neighbor 209.165.200.240 activate
address-family vpnv4
  neighbor 209.165.200.240 activate
  neighbor 209.165.200.240 send-community both
exit
address-family vpnv6
  neighbor 209.165.200.240 activate
  neighbor 209.165.200.240 send-community both
exit
ip vrf vrf1
  route-distinguisher 800 1
  route-target export 800 1
  route-target import 800 1
exit
address-family ipv4 vrf vrf1
  redistribute connected
  redistribute static
exit
ip vrf vrf2
  route-distinguisher 800 2
  route-target export 800 2
  route-target import 800 2
exit
address-family ipv4 vrf vrf2
  redistribute connected
  redistribute static
exit
address-family ipv6 vrf vrf2
  redistribute connected
  redistribute static
exit
ip vrf vrf3
  route-distinguisher 800 3
  route-target export 800 3
  route-target import 800 3
exit
address-family ipv6 vrf   vrf3
  redistribute connected
  redistribute static
exit
```

APN を設定します。

```
apn walmart51.com
  selection-mode sent-by-ms
  accounting-mode none
  aaa group walmart-group
  authentication pap 1 chap 2 allow-noauth
  ip context-name Gi_ce
  ip address pool name vrf1-pool
exit
apn amazon51.com
  selection-mode sent-by-ms
  accounting-mode none
  aaa group amazon-group
  authentication pap 1 chap 2 allow-noauth
  ip context-name Gi_ce
  ip address pool name vrf2-pool
  ipv6 address prefix-pool vrf2-v6pool
exit
apn apple51.com
  selection-mode sent-by-ms
  accounting-mode none
  aaa group apple-group
  authentication pap 1 chap 2 allow-noauthip context-name Gi_ce
  ipv6 address prefix-pool vrf3-v6pool
exit
aaa-group amazon-group
  radius ip vrf vrf2
aaa group default
exit
gtpp group default
exit
ip igmp profile default
exit
```

物理インターフェイスをポートにバインドします。

VPN 関連の CLI コマンド

VPN 関連の機能は、いくつかの CLI コマンドモードでサポートされています。次の表は、VPN 関連の機能の設定とモニタリングに関連するコマンドを示しています。

表 *18 : VPN* 関連の設定コマンド

CLI モード	コマンド	説明
BGP アドレスファミリ（IPv4/IPv6）コンフィギュレーション モード	**neighbor** *ip_address* **activate**	ピアルータとのルーティング情報の交換を有効にします。
BGP アドレスファミリ（IPv4/IPv6）コンフィギュレーション モード	**neighbor** *ip_address* **send community { both | extended | standard }**	ピアルータ（ネイバー）にコミュニティ属性を送信します。
BGP アドレスファミリ（IPv4/IPv6）コンフィギュレーション モード	**redistribute connected**	別のプロトコルから BGP へのルートを BGP ネイバーとして再配布します。

CLI モード	コマンド	説明
BGP アドレスファミリ（VPNv4）コンフィギュレーション モード	**neighbor** *ip_address* **activate**	ピアルータとのルーティング情報の交換を有効にします。
BGP アドレスファミリ（VPNv4）コンフィギュレーション モード	**neighbor** *ip_address* **send community { both | extended | standard }**	ピアルータに拡張コミュニティ属性を送信します。VPN では、ルート識別子とルートターゲットは BGP 拡張コミュニティでエンコードされます。このコマンドは、拡張コミュニティを持つ BGP ルートをネイバーに送信できるようにします。
BGP アドレスファミリ（VRF）コンフィギュレーション モード	**neighbor** *ip_address* **activate**	ピアルータとのルーティング情報の交換を有効にします。
BGP アドレスファミリ（VRF）コンフィギュレーション モード	**neighbor** *ip_address* **send community { both | extended | standard }**	ピアルータに拡張コミュニティ属性を送信します。VPN では、ルート識別子とルートターゲットは BGP 拡張コミュニティでエンコードされます。このコマンドは、拡張コミュニティを持つ BGP ルートをネイバーに送信できるようにします。
BGP アドレスファミリ（VRF）コンフィギュレーション モード	**redistribute connected**	別のプロトコルから BGP へのルートを BGP ネイバーとして再配布します。
BGP コンフィギュレーション モード	**address-family { ipv4 vrf** *vrf_name* **| vpnv4 }**	IPv4 VRF のルーティング情報の交換を有効にします。アドレスファミリごとに異なるモードがあります。
BGP コンフィギュレーション モード	**address-family { ipv6 vrf** *vrf_name* **| vpnv6 }**	BGP で VPNv6 アドレスファミリと IPv6 VRF ルーティングを設定します。
BGP コンフィギュレーション モード	**ip vrf** *vrf_name*	BGP に VRF を追加し、VRF コンフィギュレーション モードにスイッチして、VRF の BGP 属性を設定できるようにします。
BGP IP VRF コンフィギュレーション モード	**route-distinguisher {** *as_value* **|** *ip_address* **}** *rd_value*	VRF の ルート識別子（RD）を割り当てます。RD 値は、VRF ごとにルータ上の一意の値にする必要があります。

CLI モード	コマンド	説明
BGP IP VRF コンフィギュレーション モード	**route-target { both | import | export } { *as_value* | *ip_address* } *rt_value***	インポートおよびエクスポートのルートターゲット拡張コミュニティのリストを VRF に追加します。
コンテキスト コンフィギュレーション モード	**ip pool** *pool_name addr_range* **vrf** *vrf_name* **[mpls-label input** *inlabel1* **output** *outlabel1 outlabel2* **]**	指定された VRF にプールを設定します。このパラメータは、ネクストホップパラメータで指定する必要があります。*inlabel1* は、このプールを宛ての着信トラフィックを識別する MPLS ラベルです。*outlabel1* および *outlabel2* は、このプールからサブスクライバに対して送信されるパケットに追加する MPLS ラベルを指定します。
コンテキスト コンフィギュレーション モード	**ip vrf** *vrf_name*	VRF を作成し、VRF-ID を割り当てます。VRF がルータに作成されます。
コンテキスト コンフィギュレーション モード	**ipv6 pool** *pool_name* **vrf** *vrf_name*	プールを VRF に関連付けます。 **注**：デフォルトでは、設定された ipv6 プールはグローバル ルーティング ドメインに関連付けられます。
コンテキスト コンフィギュレーション モード	**mpls bgp forwarding**	MPLS のボーダー ゲートウェイ プロトコル（BGP）転送をグローバルに有効化します。

CLI モード	コマンド	説明
コンテキスト コンフィギュレーション モード	**mpls exp** *value*	3 ビット MPLS EXP ヘッダーのゼロ値を使用して、デフォルトの動作をベストエフォートとして設定します。この値は、コンテキスト内のすべての VRF に適用されます。デフォルトの動作では、DSCP から EXP への明示的な設定がない場合に、モバイルサブスクライバのトラフィックの DSCP 値が EXP ヘッダーにコピーされます (**mpls map-dscp-exp dscp** *n* **exp** *m*コマンドを使用)。 **mpls exp** はデフォルトの動作を無効にし、EXP 値を設定された値に設定します。
コンテキスト コンフィギュレーション モード	**mpls ip**	通常ルーティングされるパスに沿って IPv4 パケットの MPLS 転送がグローバルに行われるようにします。
コンテキスト コンフィギュレーション モード	**radius change-authorize-nas-ip ip_address** *ip_address* **{ encrypted | key }** *value* **port** *port_num* **mpls input** *inlabel* **output** *outlabel1 outlabel2*	指定された MPLS ラベルを使用するように COA トラフィックを設定します。 *inlabel* は着信 COA トラフィックを識別します。 *outlabel1* および *outlabel2* は、COA 応答に追加する MPLS ラベルを指定します。*outlabel1* は内部出力ラベル、*outlabel2* は外部出力ラベルです。
イーサネット インターフェイス コンフィギュレーション モード	**mpls ip**	このインターフェイスで IP パケットのダイナミック MPLS 転送を有効にします。
Exec モード	**clear ip bgp peer**	BGP セッションをクリアします。
Exec モード	**lsp-ping** *ip_prefix_FEC*	指定された転送等価クラス（FEC）の MPLS ラベルスイッチドパス（LSP）接続を確認します。その後に IPv4 または IPv6 の FEC プレフィックスが続く必要があります。

CLI モード	コマンド	説明
Exec モード	**lsp-traceroute** *ip_prefix_FEC*	パケットが宛先に転送されるとき に実際にたどる MPLS LSP ルー を検出します。その後に IPv4 ま は IPv6 の FEC プレフィックスが 続く必要があります。
IP VRF コンテキスト コンフィギュレーション モード	**mpls map-dscp-to-exp dscp** *dscp_bit_value* **exp** *exp_bit_value*	IP パケットヘッダーにおける最 の Differentiated Services Code Poi （DSCP; DiffServ コードポイン ト）ビット値を、着信トラフィ クの MPLS ヘッダーにおける最 の Experimental（EXP）ビット値 にマッピングします。
IP VRF コンテキスト コンフィギュレーション モード	**mpls map-exp-to-dscp exp** *exp_bit_value* **dscp** *dscp_bit_value*	MPLS ヘッダーの着信 EXP ビッ 値を発信トラフィックの IP パケ トヘッダーの内部 DSCP ビット値 にマッピングします。
MPLS-IP コンフィギュレーション モード	**protocol ldp**	MPLS プロトコルファミリのコン フィギュレーションモードを作成 するか、または既存のプロトコル を設定して、現在のコンテキスト で MPLS-LDP コンフィギュレー ションモードを開始します。この コマンドは、MPLS プロトコル ファミリのプロトコルパラメータ を設定します。
MPLS-LDP コンフィギュレーション モード	**advertise-labels { explicit-null | implicit-null }**	このコンテキストでシステムに よってアドバタイズされたすべて のプレフィックスについて、暗黙 的ヌルまたは明示的ヌルラベルの アドバタイズメントを設定しま す。
MPLS-LDP コンフィギュレーション モード	**discovery { hello { hello-interval** *seconds* **| hold-interval** *seconds* **} | transport-address** *ip_address* **}**	Label Distribution Protocol（LDP; ラ ベル配布プロトコル）のネイバー 探索パラメータの設定
MPLS-LDP コンフィギュレーション モード	**enable**	ラベル配布プロトコル（LDP）を 有効にします。
MPLS-LDP コンフィギュレーション モード	**router-id** *ip_address*	LDP ルータ ID を設定します。

CLI モード	コマンド	説明
MPLS-LDP コンフィギュレーション モード	**session timers { hold-interval** *seconds* **| keepalive-interval** *seconds* **}**	LDP セッションパラメータを設定します。

表 *19 : VPN* 関連のモニタリングコマンド

CLI モード	コマンド	説明
Exec モードの show コマンド	**show ip bgp neighbors**	BGP ネイバーに関する情報を表示します。
Exec モードの show コマンド	**show ip bgp vpnv4 { all | route-distinguisher | vrf }**	すべての VPNv4 ルーティングデータ、VRF またはルート識別子のルーティングデータを表示します。
Exec モードの show コマンド	**show ip bgp vpnv6**	VPNv6 ルーティングテーブルの内容を表示します。
Exec モードの show コマンド	**show ip bgp vpnv6 { all | route-distinguisher | vrf }**	すべての VPNv6 ルーティングデータ、VRF またはルート識別子のルーティングデータを表示します。
Exec モードの show コマンド	**show ip pool**	設定された VRF を含むプールの詳細を表示します。
Exec モードの show コマンド	**show mpls cross-connect**	MPLS 相互接続情報を表示します。インターフェイスとラベルスイッチドパス（LSP）間で相互接続する MPLS トンネルは、LSP をコンジットとして使用する MPLS トンネルを介して、同じタイプの 2 つの遠隔インターフェイス回線を接続します。
Exec モードの show コマンド	**show mpls ftn [vrf** *vrf_name*	MPLS FEC-to-NHLFE（FTN）テーブルの情報を表示します。
Exec モードの show コマンド	**show mpls ftn [vrf** *vrf_name* **]**	指定された VRF の MPLS FTN テーブルの内容を表示します。
Exec モードの show コマンド	**show mpls ilm**	MPLS の着信ラベルマップ（ILM）テーブルの情報を表示します。
Exec モードの show コマンド	**show mpls ldp**	MPLS LDP 情報を表示します。

CLI モード	コマンド	説明
Exec モードの show コマンド	**show mpls nexthop-label-forwarding-entry**	MPLS のネクストホップラベル転送エントリ（NHLFE）テーブルの情報を表示します。

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングと障害対応に使用できるCLIコマンドに関する情報について説明します。

show コマンドと出力

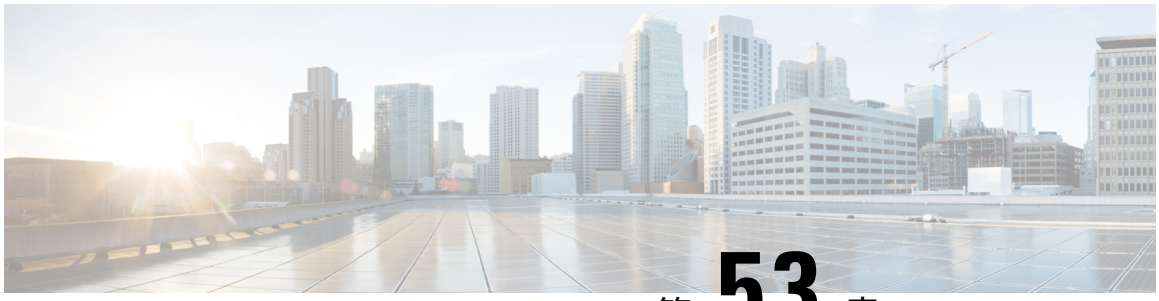
ここでは、この機能をサポートする show コマンドとその出力について説明します。

show mpls fn vpp

この CLI コマンドの出力には、CUPS の VPC-SI 機能で MPLS をサポートするため、次の新しいフィールドが含まれています。

- vpp
  - all-vrf
  - summary
  - vrf

（注） この新しいフィールドにより、VPP データプレーンフォワーダで設定されている VPP データプレーン値を表示できます。この show コマンドは、既存の debug コマンドと併せてデバッグに使用されます。



第 53 章

ユーザープレーンでの複数のコントロールプレーンのサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
このリリースでは、1 つの UP で最大 8 つの CP の接続をサポートするように機能が拡張されています。	21.26
このリリースでは、1 つの UP で最大 5 つの CP の接続をサポートするように機能が拡張されています。	21.25
最初の導入。	21.24 より前

機能説明

21.19.1 より前のリリースでは、CUPS アーキテクチャはユーザープレーン（UP）とコントロールプレーン（CP）間の単一の Sx インターフェイスのみをサポートしていました。21.19.1 以降のリリースでは、この機能により、1 つの UP で複数の CP に対する複数の Sx インターフェイ

スを確立できます。1 つの UP と複数の CP 間で複数の Sx 関連付けを確立するために、CP グループ内の複数の Sx ピアが UP で設定されます。

複数の CP が 1つの UP に接続されている場合、サブスクライバは使用可能な CP のいずれかを使用して UP に接続できます。マルチ Sx 機能の主なユースケースの 1 つは、アクティブ-アクティブ冗長性です。コールが回復されないため、冗長性は提供されませんが、マルチ Sx 機能により、CP に障害が発生した場合でも 1 つの CP に接続された UP は引き続きアクセス可能になります。CPに障害が発生した場合、そのCPによって処理されたコールは失われます。再接続すると、コールは同じUPプールを再利用する他の使用可能なCPにルーティングされます。

21.20 以降のリリースでは、この機能は複数の CP で同じ APN の設定、および関連するすべての設定をサポートしているため、サブスクライバは使用可能な CP のいずれかを使用して接続できます。

Sx IP プール更新メッセージには、UP VPNMgr がさまざまな CP からインストールされたルートを区別できるようにするための CP アドレスが含まれています。

（注）
- CP と UP は、ともに個別に設定されます。
- PFD プッシュの代わりに、Redundancy and Configuration Management（RCM）が UP で設定をプッシュします。
- 1 つの CP グループに 5 つ以上の CP ピア IP アドレスを設定しないことを推奨します。

機能の仕組み

さまざまなアクティブ課金システム（ACS）サービスを使用する複数のCPを設定するために、この機能は冗長性および設定管理（RCM）機能を活用して、設定のスーパーセットを UP にプッシュします。

前提条件

複数の CP を設定するには、次の前提条件を満たす必要があります。

- **Ruledef**:

  UP は、同じ ACS（ECS）サービス下にある複数の CP で異なるルール定義（Ruledef）設定を UE サービスに提供します。ただし、異なる CP にある同じ名前の Ruledef は共通している必要があります。複数の CP における Ruledef の設定例を次の表に示します。

CP1	CP2	CP3	CP4
Rule_def 1	Rule_def 1	Rule_def 2	Rule_def 2
Rule_def 3	Rule_def 4	Rule_def 5	Rule_def 6

- **Group-of-Ruledefs（GoR）**：

UPは、同じACS（ECS）サービス下にある複数のCPで異なるGroup-of-Ruledef（Ruledef）設定をUEサービスに提供します。ただし、異なるCPにある同じ名前のGoRは共通している必要があります。複数のCPにおけるGoRの設定例を次の表に示します。

CP1	CP2	CP3	CP4
GoR 1	GoR 1	GoR 2	GoR 2
GoR 3	GoR 4	GoR 5	GoR 6

- **Rulebase**:

  UP は、同じ ACS（ECS）サービス下にある複数の CP で異なるルールベース（RB）設定を UE サービスに提供します。ただし、異なる CP にある同じ名前の Rulebase は共通している必要があります。複数の CP における Rulebase の設定例を次の表に示します。

CP1	CP2	CP3	CP4
RB 1	RB 1	RB 2	RB 2
RB 3	RB 4	RB 5	RB 6

- **IP プール**：

  各 CP は、相互に排他的な IP プールで設定する必要があります。これは、同じ APN が設定されたサブスクライバが異なる CP によってサービスを提供されている場合に、一意の IP アドレスがサブスクライバに割り当てられるようにするためです。複数の CP における IP プールの設定例を次の表に示します。

CP1	CP2	CP3	CP4
Pool 1	Pool 2	Pool 3	Pool 4

  各 CP は、Sx 関連付け手順中に IP プール設定を UP にプッシュします。

UP1	UP2
Pool 1	Pool 1
Pool 2	Pool 2
Pool 3	Pool 3
Pool 4	Pool 4

- **APN**:

  UP は、複数の CP で異なる APN 定義設定を UE サービスに提供します。ただし、異なる CP で同じ名前の APN 定義は共通している必要があり、同じ出力コンテキストを指す必要があります。複数の CP における APN の設定例を次の表に示します。

CP1	CP2	CP3	CP4
APN 1	APN 1	APN 2	APN 2
APN 3	APN 4	APN 5	APN 6

- 出力コンテキスト

  各 CP の設定で使用するコンテキスト名は、その CP で設定されている APN の出力コンテキスト名と同じにする必要があります。IP プールを CP から UP の特定の出力コンテキストにプッシュするには、異なる CP に存在するすべての出力コンテキストを使用して UP を設定する必要があります。複数の CP における出力コンテキストの設定例を次の表に示します。

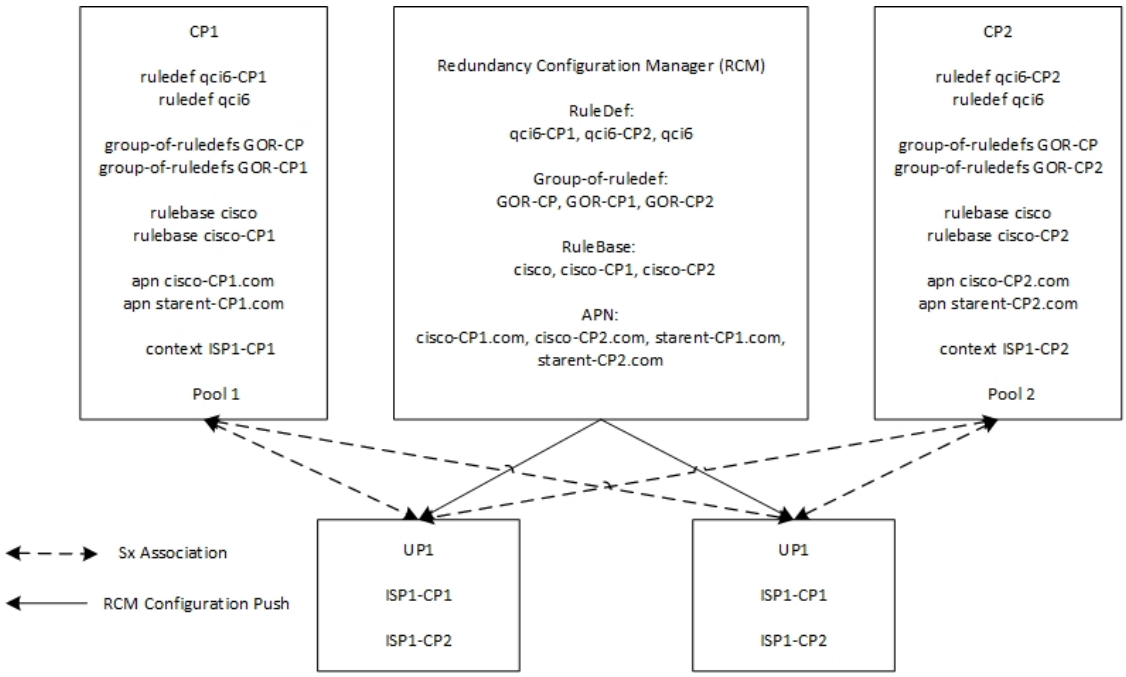
CP1	CP2	CP3	CP4
ISP1	ISP1	ISP1	ISP1

  複数の UP における出力コンテキストの設定例を次の表に示します。

UP1	UP2
ISP1	ISP1

次の図は、2 つの UP と通信する 2 つの CP の RCM 設定例を示しています。

図 *24 : 2* つの *UP* と通信する *2* つの *CP* の *RCM* 設定例



ユーザープレーンにおける複数コントロールプレーンのサポートの設定

ここでは、この機能をサポートするために使用可能な CLI コマンドについて説明します。

CP からの PFD 設定プッシュの無効化

UP への設定のプッシュは RCM を介して実行されるため、次の CLI コマンドを使用して CP からの PFD 設定のプッシュを無効にします。

```
configure
  user-plane-group group_name
    sx-pfd-push disabled
    end
```

UP での複数の CP の設定

次の CLI コマンドを使用して、[Control Plane Group Configuration] モードで複数のピアノードを追加することで、UP に複数の CP を設定します。

```
configure
  control-plane-group group_name
    peer-node-id ipv4-address ipv4_address
    peer-node-id ipv4-address ipv4_address
    end
```

モニタリングおよびトラブルシューティング

ここでは、UP 障害時のマルチ CP サポートのモニタリングと障害対応について説明します。

show コマンドと出力

この項では、この機能をサポートするために使用可能な show コマンドについて説明します。

show sx-service statistics address <ip_address>

CP ノードの Sx 統計情報を表示するには、このコマンドを使用します。次に、出力例を示します。

```
Session Management Messages:
Session Establishment Request:
 Total TX:                          0   Total RX:                          2
 Initial TX:                        0   Initial RX:                        2
 Retrans TX:                        0   Retrans RX:                        0
 Discarded:                         0
 No Rsp RX:                         0
 Throttled:                         0

Session Establishment Response:
 Total TX:                          2   Total RX:                          0
 Initial TX:                        2   Initial RX:                        0
 Accepted:                          2   Accepted:                          0
 Denied:                            0   Denied:                            0
 Retrans TX:                        0   Discarded:                         0

Session Modification Request:
 Total TX:                          0   Total RX:                         10
```

```
 Initial TX:                          0   Initial RX:                         10
 Retrans TX:                          0   Retrans RX:                          0
 Discarded:                           0   Intf Type Mismatch:                  0
 No Rsp RX:                           0

Session Modification Response:
 Total TX:                           10   Total RX:                            0
 Initial TX:                         10   Initial RX:                          0
 Accepted:                           10   Accepted:                            0
 Denied:                              0   Denied:                              0
 Retrans TX:                          0   Discarded:                           0

Session Deletion Request:
 Total TX:                            0   Total RX:                            2
 Initial TX:                          0   Initial RX:                          2
 Retrans TX:                          0   Retrans RX:                          0
 Discarded:                           0
 No Rsp RX:                           0

Session Deletion Response:
 Total TX:                            2   Total RX:                            0
 Accepted:                            2   Accepted:                            0
 Denied:                              0   Denied:                              0
 Discarded:                           0

Session Report Request:
 Total TX:                            3   Total RX:                            0
 Initial TX:                          3   Initial RX:                          0
 Retrans TX:                          0   Retrans RX:                          0
 Discarded:                           0
 No Rsp RX:                           0

Session Report Response:
 Total TX:                            0   Total RX:                            3
 Initial TX:                          0   Initial RX:                          3
 Accepted:                            0   Accepted:                            3
 Denied:                              0   Denied:                              0
 Retrans TX:                          0   Discarded:                           0

Node Management Messages:
Prime PFD Management Request:
 Total TX:                            0   Total RX:                            0
 Initial TX:                          0   Initial RX:                          0
 Retrans TX:                          0   Retrans RX:                          0
 No Rsp received TX:                  0   Discarded:                           0

Prime PFD Management Response:
 Total TX:                            0   Total RX:                            0
 Initial TX:                          0   Initial RX:                          0
 Accepted:                            0   Accepted:                            0
 Denied:                              0   Denied:                              0
 Retrans TX:                          0   Discarded:                           0

Association Setup Request:
 Total TX:                            1   Total RX:                            0
 Initial TX:                          1   Initial RX:                          0
 Retrans TX:                          0   Retrans RX:                          0
 No Rsp received TX:                  0   Discarded:                           0

Association Setup Response:
 Total TX:                            0   Total RX:                            1
 Initial TX:                          0   Initial RX:                          1
 Accepted:                            0   Accepted:                            1
 Denied:                              0   Denied:                              0
```

```
 Retrans TX:                          0   Discarded:                          0

Association Update Request:
 Total TX:                            0   Total RX:                           3
 Initial TX:                          0   Initial RX:                         3
 Retrans TX:                          0   Retrans RX:                         0
 No Rsp received TX:                  0   Discarded:                          0

Association Update Response:
 Total TX:                            3   Total RX:                           0
 Initial TX:                          3   Initial RX:                         0
 Accepted:                            3   Accepted:                           0
 Denied:                              0   Denied:                             0
 Retrans TX:                          0   Discarded:                          0

Association Release Request:
 Total TX:                            0   Total RX:                           0
 Initial TX:                          0   Initial RX:                         0
 Retrans TX:                          0   Retrans RX:                         0
 No Rsp received TX:                  0   Discarded:                          0

Association Release Response:
 Total TX:                            0   Total RX:                           0
 Initial TX:                          0   Initial RX:                         0
 Accepted:                            0   Accepted:                           0
 Denied:                              0   Denied:                             0
 Retrans TX:                          0   Discarded:                          0

Node Report Request:
 Total TX:                            0   Total RX:                           0
 Initial TX:                          0   Initial RX:                         0
 Retrans TX:                          0   Retrans RX:                         0
 No Rsp received TX:                  0   Discarded:                          0

Node Report Response:
 Total TX:                            0   Total RX:                           0
 Initial TX:                          0   Initial RX:                         0
 Accepted:                            0   Accepted:                           0
 Denied:                              0   Denied:                             0
 Retrans TX:                          0   Discarded:                          0

Heartbeat Request:
 Total TX:                         1398   Total RX:                        1398
 Initial TX:                       1398   Initial RX:                      1398
 Retrans TX:                          0

Heartbeat Response:
 Total TX:                         1398   Total RX:                        1398

Stats framework related messages:
Stats Query Request:
 Total TX:                            0   Total RX:                           0
 Initial TX:                          0   Initial RX:                         0
 Retrans TX:                          0   Retrans RX:                         0
 No Rsp received TX:                  0   Discarded:                          0

Stats Query Response:
 Total TX:                            0   Total RX:                           0
 Initial TX:                          0   Initial RX:                         0
 Accepted:                            0   Accepted:                           0
 Denied:                              0   Denied:                             0
 Retrans TX:                          0   Discarded:                          0

Stats Query Acknowledgement:
```

```
 Total TX:                              0   Total RX:                              0
 Initial TX:                            0   Initial RX:                            0
 Retrans TX:                            0   Retrans RX:                            0
 Discarded:                             0

Total Signalling Packets:
         TX:                           21           RX:                           21

Total Signalling Bytes:
         TX:                         2092           RX:                         5381
```

CP ノードの Sx 統計情報をクリアするには、**clear sx-service statistics address** *ip_address* CLI コマンドを使用します。

show user-plane-service statistics peer-address <ip_address>

UP のノードレベルのサービス統計情報を表示するには、このコマンドを使用します。次に、出力例を示します。

```
Peer IP                     : 209.165.200.225

Subscribers Total:
PDNs Total:
Active:                             1        Setup:                             1
Released:                           0        Rejected:                          0

PDNs By PDN-Type:
IPv4 PDNs:
Active:                             1        Setup:                             1
Released:                           0

IPv6 PDNs:
Active:                             0        Setup:                             0
Released:                           0

IPv4v6 PDNs:
Active:                             0        Setup:                             0
Released:                           0

eMPS PDNs Total:
Active:                             0        Setup:                             0
Released:                           0        Rejected:                          1

PDNs By interface-Type:
Sxa interface-type PDNs:
Active:                             0        Setup:                             0
Released:                           0

Sxb interface-type PDNs:
Active:                             1        Setup:                             1
Released:                           0

Sxab interface-type PDNs:
Active:                             0        Setup:                             0
Released:                           0

N4 interface-type PDNs:
Active:                             0        Setup:                             0
Released:                           0

PDNs Rejected By Reason:
No Resource:                        0        Missing or unknown APN:            0
Addr not alloc:                     0        Addr not present:                  0
```

```
No memory available:                0        System Failure:                  0
Rule install failed:                0        SFW policy mismatch:             0

PDNs Released By Reason:
Network initiated release:          0        Admin disconnect:                0

Total Data Statistics:
Uplink :                                     Downlink :
Total Pkts:                         0        Total Pkts:                      0
Total Bytes:                        0        Total Bytes:                     0
Total Dropped Pkts:                 0        Total Dropped Pkts:              0
Total Dropped Bytes:                0        Total Dropped Bytes:             0

Data Statistics Per PDN-Type:
IPv4 PDNs:
Uplink :                                     Downlink :
Total Pkts:                         0        Total Pkts:                      0
Total Bytes:                        0        Total Bytes:                     0

IPv6 PDN Data Statistics:
Uplink :                                     Downlink :
Total Pkts:                         0        Total Pkts:                      0
Total Bytes:                        0        Total Bytes:                     0

IPv4v6 PDN Data Statistics:
Uplink :                                     Downlink :
Total Pkts v4:                      0        Total Pkts v4:                   0
Total Bytes v4:                     0        Total Bytes v4:                  0
Total Pkts v6:                      0        Total Pkts v6:                   0
Total Bytes v6:                     0        Total Bytes v6:                  0
```

clear user-plane-service statistics peer-address *ip_address* CLI コマンドを使用して、UP のノードレベルのサービス統計情報をクリアします。

show ip chunks peer <ip_address>

このコマンドを使用して、UP で CP ごとの IPv4 プールチャンクを表示します。次に、出力例を示します。

```
==========================================================================================
Peer Address: 1.0.0.1
==========================================================================================
|----------|------------|------------------------------|--------------|--------------|------------|
| chunk-id | chunk-size |              vrf-name        |   start-addr  |    end-addr
  | used-addrs |
|----------|------------|------------------------------|--------------|--------------|------------|
|   1048576|        1024|                              |      192.0.2.1|      192.0.2.2|
           0|
|   1048577|        1024|                              |      192.0.2.3|      192.0.2.4|
           0|
|   1048578|        1024|                              |      192.0.2.5|      192.0.2.6|
           0|
|   3145728|        1024|                         vrf1|      192.0.2.7|      192.0.2.8|
           0|
|   3145729|        1024|                         vrf1|      192.0.2.9|     192.0.2.10|
           0|
|   3145730|        1024|                         vrf1|     192.0.2.11|     192.0.2.12|
           0|
|   4194304|        1024|                              |     192.0.2.13|     192.0.2.14|
           0|
|   4194305|        1024|                              |     192.0.2.15|     192.0.2.16|
           0|
|   4194306|        1024|                              |     192.0.2.17|     192.0.2.18|
```

```
           0|
|----------|-----------|------------------------------|--------------|--------------|-----------|
```

show ipv6 chunks peer <ip_address>

このコマンドを使用して、UP で CP ごとの IPv6 プールチャンクを表示します。次に、出力例を示します。

```
==============================================================================================
Peer Address: 1.0.0.101
==============================================================================================
|----------|-----------|-----------------|-------------------|-------------------|--------------|
| chunk-id | chunk-size |     vrf-name     | start-prefix       |   end-prefix       |
used-prefixes |
|----------|-----------|-----------------|-------------------|-------------------|--------------|
|2098200576|        1024|                 |              3001::|      3001:0:0:3ff::|
             0|
|2098200577|        1024|                 |      3001:0:0:400::|      3001:0:0:7ff::|
             0|
|2098200578|        1024|                 |      3001:0:0:800::|      3001:0:0:bff::|
             0|
|2099249152|        1024|              vrf1|              4001::|      4001:0:0:3ff::|
             0|
|2099249153|        1024|              vrf1|      4001:0:0:400::|      4001:0:0:7ff::|
             0|
|2099249154|        1024|              vrf1|      4001:0:0:800::|      4001:0:0:bff::|
             0|
|----------|-----------|-----------------|-------------------|-------------------|--------------|
```

RCM の設定例

以下に、この機能を設定するための RCM の設定例を示します。

```
configure
etcd replicas 1
endpoint rcm-chkptmgr
 replicas 7
 vip-ip 209.165.200.225
exit
endpoint rcm-configmgr
 vip-ip 209.165.200.225
exit
endpoint rcm-bfdmgr
 vip-ip 209.165.200.226
exit
endpoint rcm-controller
 vip-ip 209.165.200.225
exit
logging level application trace
logging level transaction trace
logging level tracing off
logging name infra.config.core level application trace
logging name infra.config.core level transaction trace
logging name infra.resource_monitor.core level application debug
logging name infra.resource_monitor.core level transaction debug
k8 smf profile rcm-config-ep disable-cm apn gtpp creditCtrl packetFilter urrList ruledef
 rulebase miscacs global chargingAction upfCpg upSvcs sxService gtpuService upfIfc
```

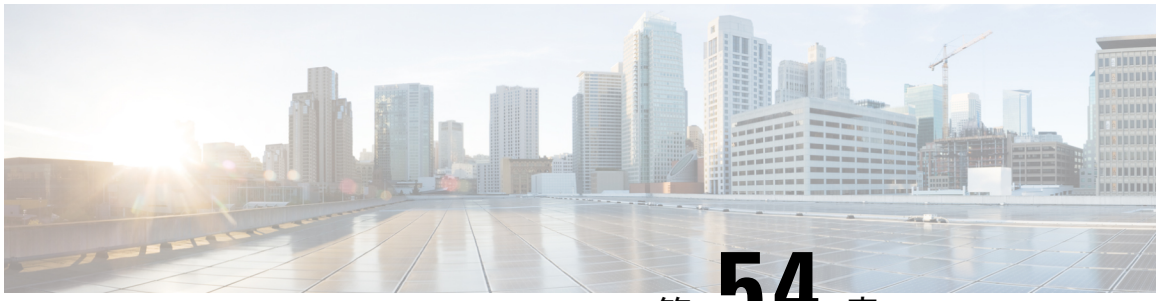
```
lawfulIntercept apnprofile
k8 smf profile rcm-bfd-ep bfd-monitor group 1
 endpoint ipv4 209.165.200.227
 endpoint ipv4 209.165.200.228
 endpoint ipv4 209.165.200.229
 standby 1
exit
system mode running
helm default-repository smf
helm repository smf
 access-token
dev-deployer.gen:AKCp5ekcXA7TknM9DbLASNBw4jwVEsx9Z9WpQwEvCvCQ2mJhLymcz6BfbH38YJiWC6fn1cKmw

 url http://example.com
exit
k8s name          unknown
k8s namespace     rcm
k8s nf-name       rcm
k8s registry      dockerhub.xxx.com/smi-fuse-docker-internal
k8s single-node   false
k8s use-volume-claims false
k8s ingress-host-name 209.165.200.225.nip.io
profile smf rcm
 node-id 123456
exit
svc-type upinterface
svc-type sxsvc
svc-type upsvc
svc-type gtpusvc
svc-type cpgrp
 redundancy-group 1
  host 209.165.200.225:22
host 295 "config "
host 296 "control-plane-group CPGROUP21 "
host 297 "peer-node-id ipv4-address 209.165.200.230 "
host 298 "peer-node-id ipv4-address 209.165.200.231 "
host 299 "exit "
host 300 "end "
exit
exit
svc-type sxsvc
svc-type upsvc
svc-type gtpusvc
svc-type cpgrp
 redundancy-group 1
  host 209.165.200.225:22
host 393 " config "
host 394 "control-plane-group CPGROUP21 "
host 395 "peer-node-id ipv4-address 209.165.200.230 "
host 396 "peer-node-id ipv4-address 209.165.200.231 "
host 397 "48 exit "
host 398 "49 end "
exit
exit
exit
redundancy-group 1
common 1 " sleep 5  "
common 2 " config "
common 3 "   active-charging service ACS "
common 4 "     #exit "
common 5 "     ruledef ipv6 "
common 6 "       icmpv6 any-match = TRUE "
common 7 "     #exit "
common 8 "     ruledef qci1 "
```

```
common 9 "       tcp src-port = 1001 "
common 10 "     #exit "
common 11 "     ruledef qci2 "
common 12 "       tcp src-port = 1002 "
common 13 "     #exit "
common 14 "     ruledef qci6 "
common 15 "       tcp src-port = 1006 "
common 16 "     #exit "
common 17 "     ruledef qci6-CP1 "
common 18 "       udp src-port = 1010 "
common 19 "     #exit "
common 20 "     ruledef qci6-CP2 "
common 21 "       udp src-port = 1020 "
common 22 "     #exit "
common 23 "     group-of-ruledefs GOR "
common 24 "       add-ruledef priority 11 ruledef qci1 "
common 25 "       add-ruledef priority 22 ruledef qci2 "
common 26 "       add-ruledef priority 33 ruledef ipv6 "
common 27 "     #exit "
common 28 "     group-of-ruledefs GOR-CP1 "
common 29 "       add-ruledef priority 11 ruledef qci1 "
common 30 "       add-ruledef priority 33 ruledef ipv6 "
common 31 "     #exit "
common 32 "     group-of-ruledefs GOR-CP2 "
common 33 "       add-ruledef priority 11 ruledef qci2 "
common 34 "       add-ruledef priority 33 ruledef ipv6 "
common 35 "     #exit "
common 36 "     packet-filter ipv6 "
common 37 "       ip protocol = 58 "
common 38 "       priority 22 "
common 39 "     #exit "
common 40 "     packet-filter qci1 "
common 41 "       ip protocol = 6 "
common 42 "       ip remote-port = 1001 "
common 43 "       priority 1 "
common 44 "     #exit "
common 45 "     packet-filter qci2 "
common 46 "       ip protocol = 6 "
common 47 "       ip remote-port = 1002 "
common 48 "       priority 2 "
common 49 "     #exit "
common 50 "     packet-filter qci6 "
common 51 "       ip protocol = 6 "
common 52 "       ip remote-port = 1006 "
common 53 "       priority 6 "
common 54 "     #exit "
common 55 "     packet-filter qci6-CP1 "
common 56 "       ip protocol = 17 "
common 57 "       ip remote-port = 1010 "
common 58 "       priority 1 "
common 59 "     #exit "
common 60 "     packet-filter qci6-CP2 "
common 61 "       ip protocol = 17 "
common 62 "       ip remote-port = 1020 "
common 63 "       priority 1 "
common 64 "     #exit "
common 65 "     urr-list URR_ID_LIST "
common 66 "       rating-group 1 urr-id 1 "
common 67 "       rating-group 2 urr-id 2 "
common 68 "       rating-group 3 urr-id 3 "
common 69 "       rating-group 4 urr-id 4 "
common 70 "       rating-group 5 urr-id 5 "
common 71 "       rating-group 6 urr-id 6 "
common 72 "       rating-group 7 urr-id 7 "
```

```
common 73 "       rating-group 8 urr-id 8 "
common 74 "       rating-group 9 urr-id 9 "
common 75 "       rating-group 10 urr-id 10 "
common 76 "       rating-group 11 urr-id 11 "
common 77 "       rating-group 12 urr-id 12 "
common 78 "       rating-group 13 urr-id 13 "
common 79 "       rating-group 14 urr-id 14 "
common 80 "     #exit "
common 81 "     charging-action ipv6 "
common 82 "       content-id 11 "
common 83 "       billing-action egcdr "
common 84 "       billing-action rf "
common 85 "       cca charging credit rating-group 11 "
common 86 "       qos-class-identifier 5 "
common 87 "       flow limit-for-bandwidth id 2 "
common 88 "       tft packet-filter ipv6 "
common 89 "     #exit "
common 90 "     charging-action qci1 "
common 91 "       content-id 1 "
common 92 "       billing-action egcdr "
common 93 "       billing-action rf "
common 94 "       cca charging credit rating-group 1 "
common 95 "       qos-class-identifier 1 "
common 96 "       flow limit-for-bandwidth id 1 "
common 97 "       allocation-retention-priority 1 pvi 0 pci 1 "
common 98 "       tft packet-filter qci1 "
common 99 "     #exit "
common 100 "     charging-action qci1-GOR "
common 101 "       content-id 1 "
common 102 "       billing-action egcdr "
common 103 "       billing-action rf "
common 104 "       cca charging credit rating-group 1 "
common 105 "       qos-class-identifier 1 "
common 106 "       flow limit-for-bandwidth id 1 "
common 107 "       allocation-retention-priority 1 pvi 0 pci 1 "
common 108 "       tft packet-filter ipv6 "
common 109 "       tft packet-filter qci1 "
common 110 "       tft packet-filter qci2 "
common 111 "     #exit "
common 112 "     charging-action qci1-GOR-CP1 "
common 113 "       content-id 1 "
common 114 "       billing-action egcdr "
common 115 "       billing-action rf "
common 116 "       cca charging credit rating-group 1 "
common 117 "       qos-class-identifier 1 "
common 118 "       flow limit-for-bandwidth id 1 "
common 119 "       allocation-retention-priority 1 pvi 0 pci 1 "
common 120 "       tft packet-filter ipv6 "
common 121 "       tft packet-filter qci1 "
common 122 "     #exit "
common 123 "     charging-action qci1-GOR-CP2 "
common 124 "       content-id 1 "
common 125 "       billing-action egcdr "
common 126 "       billing-action rf "
common 127 "       cca charging credit rating-group 1 "
common 128 "       qos-class-identifier 1 "
common 129 "       flow limit-for-bandwidth id 1 "
common 130 "       allocation-retention-priority 1 pvi 0 pci 1 "
common 131 "       tft packet-filter ipv6 "
common 132 "       tft packet-filter qci2 "
common 133 "     #exit "
common 134 "     charging-action qci2 "
common 135 "       content-id 2 "
common 136 "       billing-action egcdr "
```

```
common 137 "       billing-action rf "
common 138 "       cca charging credit rating-group 2 "
common 139 "       qos-class-identifier 2 "
common 140 "       flow limit-for-bandwidth id 1 "
common 141 "       allocation-retention-priority 2 pvi 0 pci 1 "
common 142 "       tft packet-filter qci2 "
common 143 "     #exit "
common 144 "     charging-action qci6 "
common 145 "       content-id 6 "
common 146 "       billing-action egcdr "
common 147 "       billing-action rf "
common 148 "       cca charging credit rating-group 6 "
common 149 "       qos-class-identifier 6 "
common 150 "       flow limit-for-bandwidth id 2 "
common 151 "       allocation-retention-priority 6 pvi 0 pci 1 "
common 152 "       tft packet-filter qci6 "
common 153 "     #exit "
common 154 "     charging-action qci6-CP1 "
common 155 "       content-id 12 "
common 156 "       billing-action egcdr "
common 157 "       billing-action rf "
common 158 "       cca charging credit rating-group 12 "
common 159 "       qos-class-identifier 6 "
common 160 "       flow limit-for-bandwidth id 2 "
common 161 "       allocation-retention-priority 6 pvi 0 pci 1 "
common 162 "       tft packet-filter qci6-CP1 "
common 163 "     #exit "
common 164 "     charging-action qci6-CP2 "
common 165 "       content-id 13 "
common 166 "       billing-action egcdr "
common 167 "       billing-action rf "
common 168 "       cca charging credit rating-group 13 "
common 169 "       qos-class-identifier 6 "
common 170 "       flow limit-for-bandwidth id 2 "
common 171 "       allocation-retention-priority 6 pvi 0 pci 1 "
common 172 "       tft packet-filter qci6-CP2 "
common 173 "     #exit "
common 174 "     bandwidth-policy bw_policy1 "
common 175 "       flow limit-for-bandwidth id 1 group-id 1 "
common 176 "       flow limit-for-bandwidth id 2 group-id 2 "
common 177 "       group-id 1 direction downlink peak-data-rate 256000 peak-burst-size
768000 violate-action discard committed-data-rate 128000 committed-burst-size 384000 "
common 178 "       group-id 1 direction uplink peak-data-rate 256000 peak-burst-size
768000 violate-action discard committed-data-rate 128000 committed-burst-size 384000 "
common 179 "       group-id 2 direction downlink peak-data-rate 256000 peak-burst-size
768000 violate-action discard "
common 180 "       group-id 2 direction uplink peak-data-rate 256000 peak-burst-size
768000 violate-action discard "
common 181 "     #exit "
common 182 "     rulebase cisco "
common 183 "       billing-records egcdr "
common 184 "       action priority 1 dynamic-only group-of-ruledefs GOR charging-action
 qci1-GOR "
common 185 "       action priority 11 dynamic-only ruledef qci1 charging-action qci1 "
common 186 "       action priority 22 dynamic-only ruledef qci2 charging-action qci2 "
common 187 "       action priority 66 dynamic-only ruledef qci6 charging-action qci6 "
common 188 "       action priority 666 dynamic-only ruledef ipv6 charging-action ipv6 "
common 189 "       egcdr threshold interval 3600 "
common 190 "       egcdr threshold volume total 100000 "
common 191 "       bandwidth default-policy bw_policy1 "
common 192 "     #exit "
common 193 "     rulebase cisco-CP1 "
common 194 "       billing-records egcdr "
common 195 "      action priority 1 dynamic-only group-of-ruledefs GOR-CP1 charging-action
```

```
 qci1-GOR-CP1 "
common 196 "       action priority 11 dynamic-only ruledef qci1 charging-action qci1 "
common 197 "       action priority 22 dynamic-only ruledef qci2 charging-action qci2 "
common 198 "       action priority 66 dynamic-only ruledef qci6-CP1 charging-action
qci6-CP1 "
common 199 "       action priority 666 dynamic-only ruledef ipv6 charging-action ipv6 "
common 200 "       egcdr threshold interval 1000 "
common 201 "       egcdr threshold volume total 100000 "
common 202 "       bandwidth default-policy bw_policy1 "
common 203 "     #exit "
common 204 "     rulebase cisco-CP2 "
common 205 "       billing-records egcdr "
common 206 "      action priority 1 dynamic-only group-of-ruledefs GOR-CP2 charging-action
 qci1-GOR-CP2 "
common 207 "       action priority 11 dynamic-only ruledef qci1 charging-action qci1 "
common 208 "       action priority 22 dynamic-only ruledef qci2 charging-action qci2 "
common 209 "       action priority 66 dynamic-only ruledef qci6-CP2 charging-action
qci6-CP2 "
common 210 "       action priority 666 dynamic-only ruledef ipv6 charging-action ipv6 "
common 211 "       egcdr threshold interval 1000 "
common 212 "       egcdr threshold volume total 100000 "
common 213 "       bandwidth default-policy bw_policy1 "
common 214 "     #exit "
common 215 "     rulebase default "
common 216 "     #exit "
common 217 "     credit-control group default "
common 218 "       diameter origin endpoint PGW-Gy "
common 219 "       diameter peer-select peer PGW-Gy-server "
common 220 "       quota time-threshold 10 "
common 221 "       diameter pending-timeout 150 deciseconds msg-type any "
common 222 "       diameter session failover "
common 223 "       trigger type rat qos sgsn serving-node "
common 224 "       pending-traffic-treatment noquota pass "
common 225 "       pending-traffic-treatment quota-exhausted buffer "
common 226 "       timestamp-rounding floor "
common 227 "     #exit "
common 228 "     traffic-optimization-policy default "
common 229 "     #exit "
common 230 "   #exit "
common 231 " end "
common 232 " config  "
common 233 " context ISP1-CP1  "
common 234 "    apn xxx-CP1.com  "
common 235 "      ip context-name ISP1-CP1  "
common 236 "    exit  "
common 237 "    apn yyy-CP1.com  "
common 238 "      ip context-name ISP1-CP1  "
common 239 "    exit  "
common 240 " end  "
common 241 " config  "
common 242 " context ISP1-CP2  "
common 243 "    apn xxx-CP2.com  "
common 244 "      ip context-name ISP1-CP2  "
common 245 "    exit  "
common 246 "    apn yyy-CP2.com  "
common 247 "      ip context-name ISP1-CP2  "
common 248 "    exit  "
common 249 " end  "
  exit
```



第 54 章

MOCN による CRA および CNR の特別な処理

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

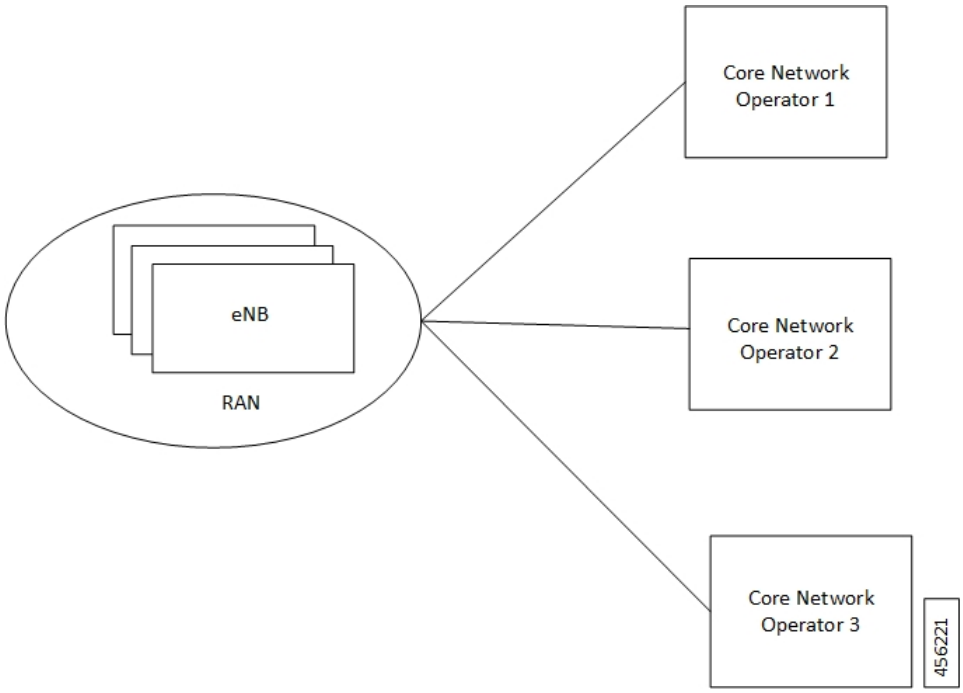
機能説明

ここでは、Multi Operator Core Network（MOCN）を有効または無効にする SAE-GW のサポートについて説明します。また、MOCN が有効になっているときに PCRF によって要求されたトラッキングエリア ID（TAI）変更イベントの処理についても説明します。

SAE-GW は PCRF の要求に応じて、TAI 変更イベントの報告を開始/停止するように MME に指示します。SAE-GW は MME から TAI 変更を受信すると、次を報告します。

- PCRF への TAI 変更イベント
- OCS へのロケーションの更新

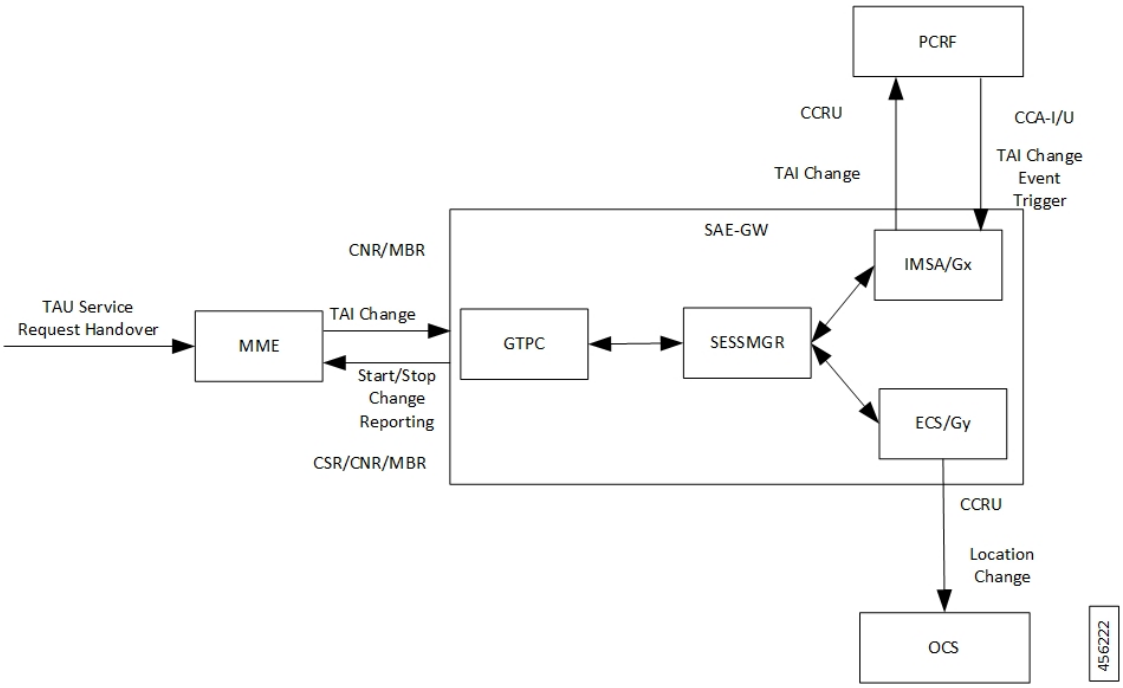
次の図は、さまざまなコアネットワークオペレータが共有無線アクセスネットワークに接続できるようにする MOCN 機能について説明しています。



TAI 変更イベントの処理

次の図は、TAI 変更イベント処理のアーキテクチャの概要を示しています。

図 *25 : TAI* 変更イベント処理：プロセスフロー



SAE-GW で MOCN 機能を有効にし、Credit Control Answer-Initial/Update（CCA-I/U）のイベントトリガー AVP で PCRF から TAI 変更トリガーを受信すると、SAE-GW はセッション作成応答/ベアラー変更要求/変更通知応答の変更レポートアクション（CRA）で、MME に TAI のレポート開始指示を送信します。

MME は、トラッキングエリア更新（TAU）、サービスリクエスト、S1AP/X2 ハンドオーバーなどのさまざまな手順において TAI が変更された場合、変更通知要求/ベアラー変更要求のユーザーロケーション情報で、TAI の変更を SAE-GW に送信します。

続いて SAE-GW は、Event Trigger AVP とクレジット制御要求更新（CCR-U）の 3GPP-User-Location-Info AVP の値によって PCRF に TAI の変更を指示し、ロケーション依存ポリシーを受信します。

また、SAE-GW は、Trigger Type AVP、PS-Information AVP および Multiple Services Credit Control（MSCC）のユーザーロケーション情報によって OCS にロケーションの変更を指示し、ロケーション依存の課金関連手順を有効にします。

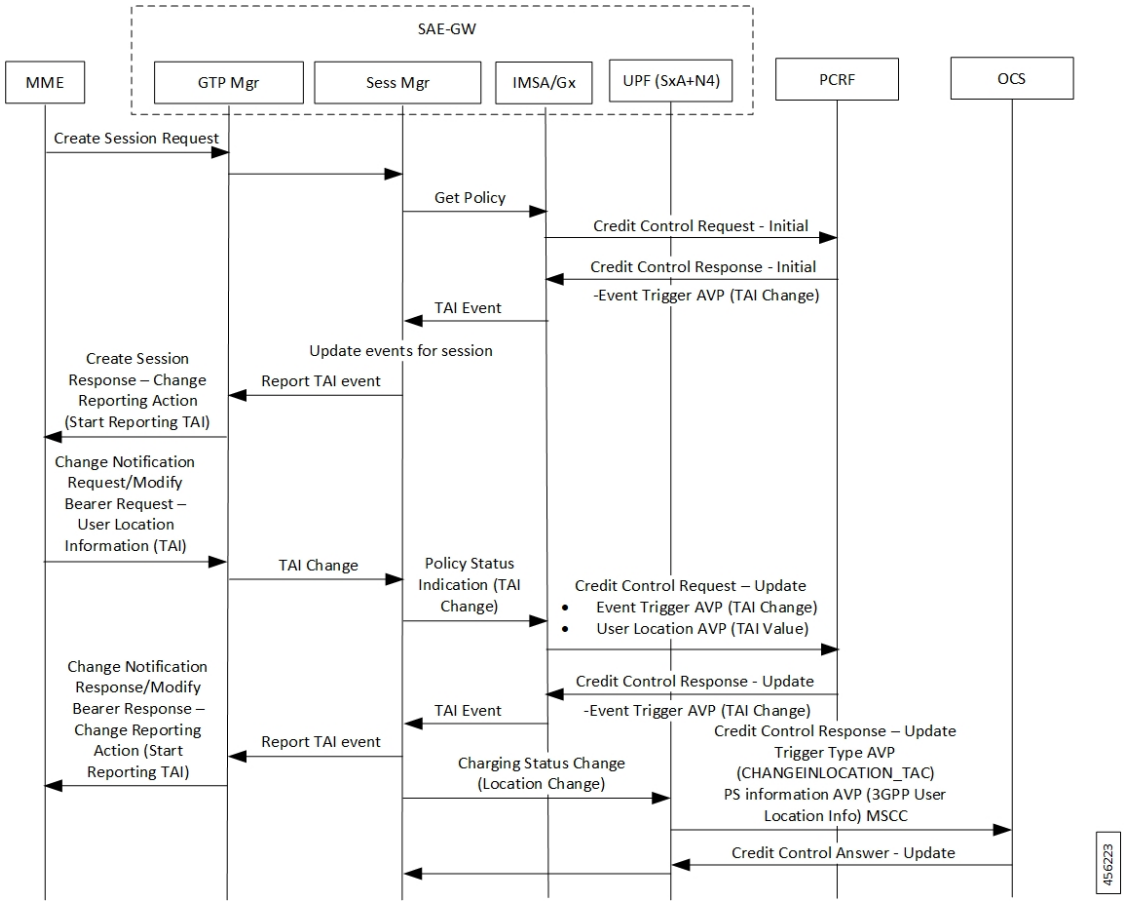
SAE-GW で MOCN 機能を有効にし、Credit Control Answer-Initial/Update（CCA-I/U）のイベントトリガー AVP で PCRF から [No Event] トリガーを受信すると、SAE-GW はセッション作成応答/ベアラー変更要求/変更通知応答の変更レポートアクション（CRA）で、MME に TAI のレポート終了指示を送信します。

機能の仕組み

次のコールフローは、TAI 変更レポートの開始と停止について説明したものです。

TAI 変更のレポートの開始

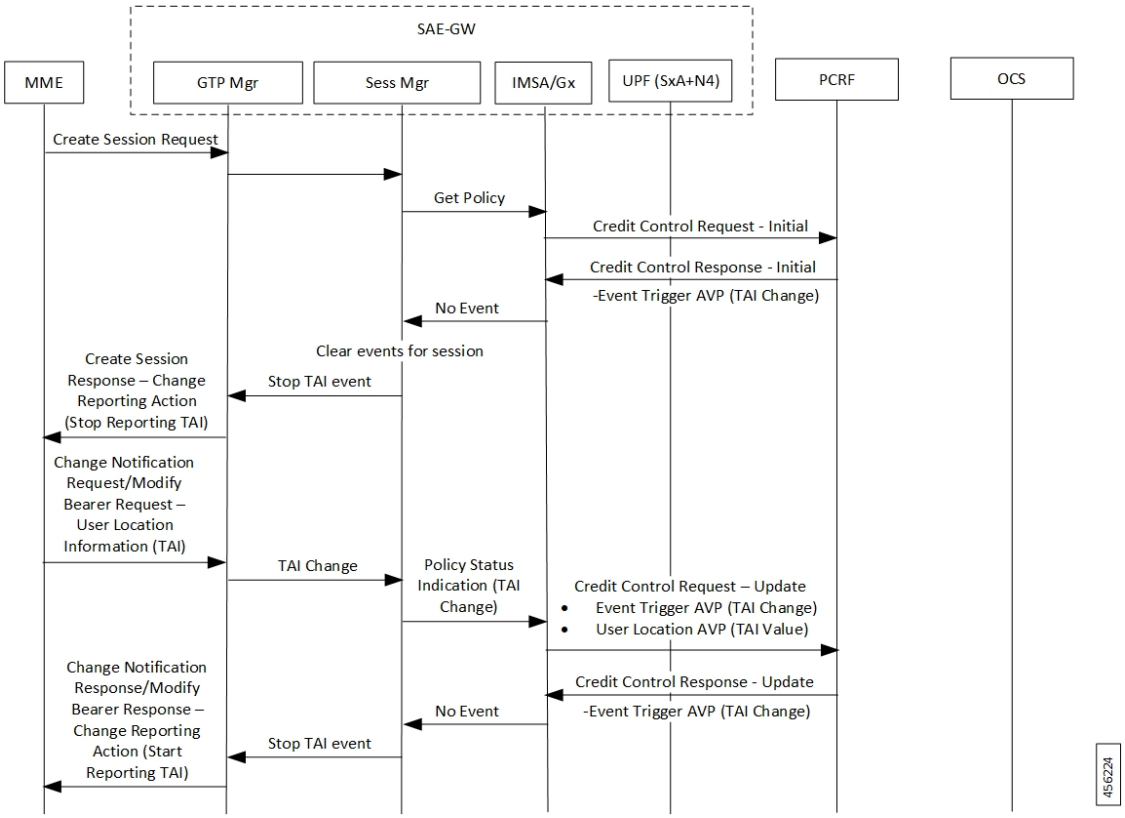
次のコールフローでは、TAI 変更のレポートについて説明します。



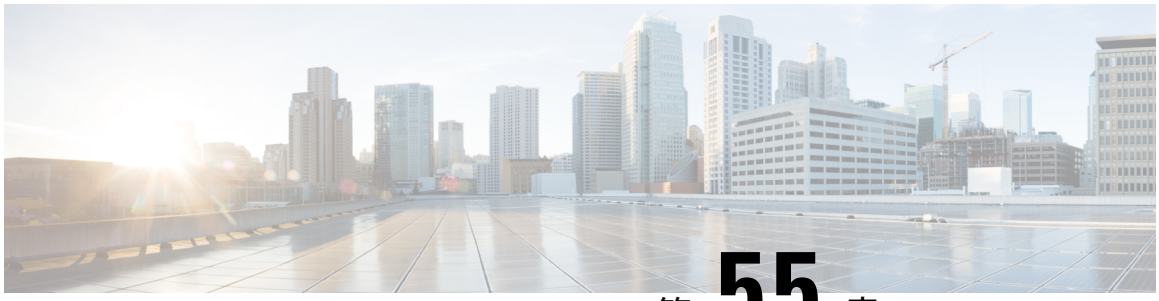
手順	説明
1.	セッション確立手順において、CCA-I のイベントトリガーを [TAI_CHANGE (26)] に設定することで PCRF が SAE-GW に TAI 変更レポートを要求した場合、SAE-GW は、変更レポートアクション（CRA）値を [Start Reporting TAI] に設定したセッション作成応答を MME に送信します。
2 に送信します。	MME は、UE の TAI の変更を検出すると、新しい TAI を含む ULI を使用して変更通知要求またはベアラー変更要求を送信します。SAE-GW は、PCRF に送信されるイベントトリガーが [TAI_CHANGE (26)] に設定された CCR-U と、User Location AVP を加えます。イベントトリガーが [TAI_CHANGE (26)] に設定された CCA-U を PCRF から受信すると、SAE-GW は、CRA 値を [Start Reporting TAI] に設定した変更通知応答または変更ベアラー応答を送信します。
3.	次に、SAE-GW は、[CHANGEINLOCATION_TAC (35)] に設定された Trigger-Type AVP、PS-Information AVP（3GPP-User-Location：新しい TAI）、および OCS に送信された CCR-U の MSCC を加え、OCS から CCA-U を受信します。

TAI 変更のレポートの停止

次のコールフローでは、TAI 変更のレポートについて説明します。



セッション確立手順において、PCRF が SAE-GW にイベントレポートなしを要求した場合（CCA-I のイベントトリガーを [NO_EVENT_TRIGGERS] に設定）、SAE-GW は、変更レポートアクション（CRA）値を [Stop Reporting TAI] に設定したセッション作成応答を MME に送信します。



第 55 章

N+2 UP リカバリ

変更履歴

マニュアルの変更履歴

Note リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

3GPP に従い、CP は UP からの Sx キープアライブメッセージ応答に依存する Sx ベースの障害検出を使用します。

このアプローチでは、CP は UP からの応答が受信されない場合、その UP をダウン状態と宣言してセッションの切断を開始する前に、一定の回数（設定可能） Sx メッセージを再送信します。信頼性の高い方法で UP のダウン状態を判別するため、再試行の回数と再試行の間隔によっては、障害検出期間が 10 秒以上になる場合があります。Sx パス障害が CP で検出されるまで、CP は引き続き失敗した UP を選択し、失敗した UP に UE からの新しい PDN 接続を配置します。

CP による UP のダウン状態の検出にかかる時間を短縮するため、Cisco CP は Bidirectional Forwarding Detection（BFD）プロトコル（RFC 5883 - Bidirectional Forwarding Protocol Detection (BFD) for Multihop Paths）を使用するように設定できます。

BFD は大幅に短い再試行期間（約 200 ミリ秒）を使用するため、より迅速な UP ダウン検出が可能です。他の展開シナリオ（UP の 1:1 冗長性など）の Sx キープアライブメカニズムに加えて、これを使用できます。

注：PFD は共通する Day-N 設定を UP 全体にプッシュするため、この機能はパケットフローの記述（PFD）に依存しません。

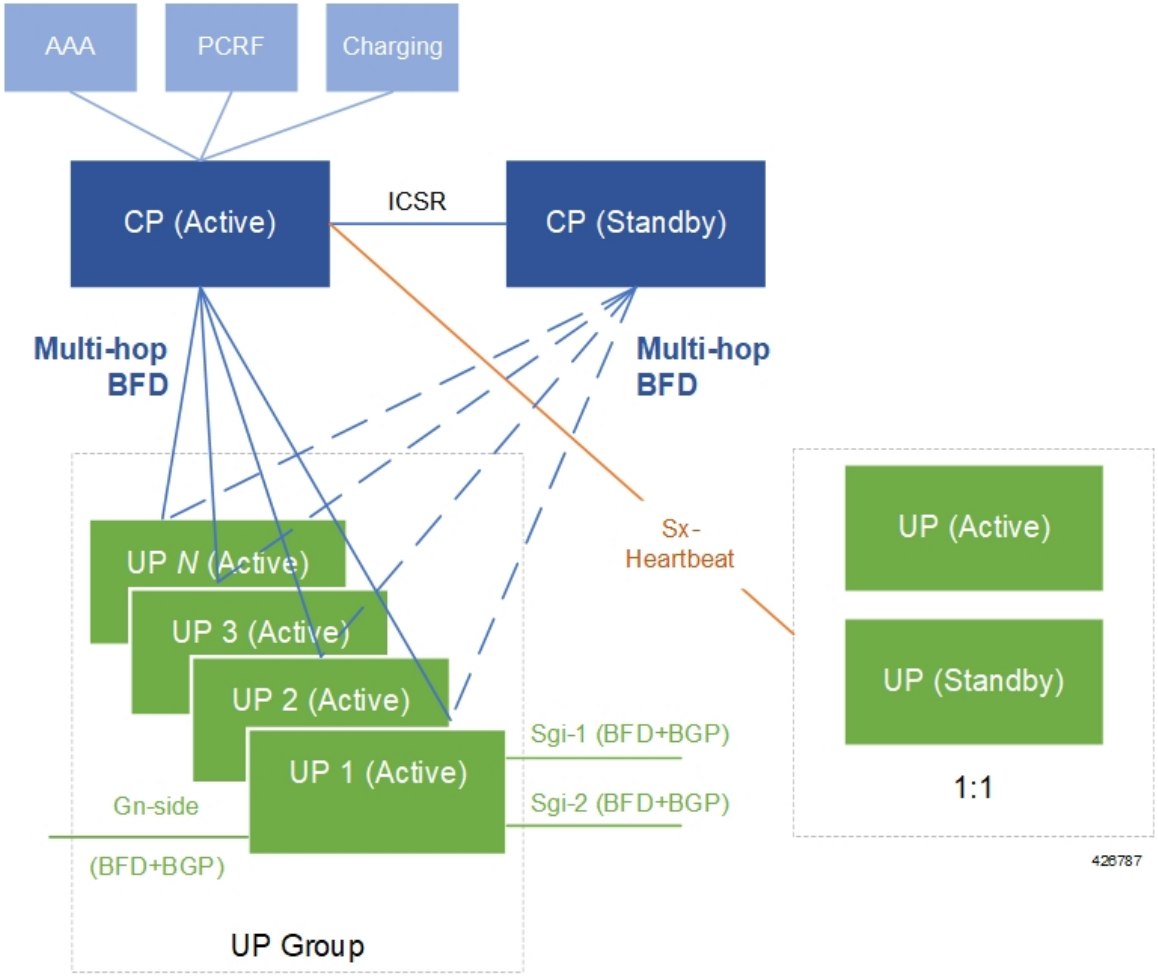
導入アーキテクチャ

この機能は、データセッションを処理する UP の「N+2」展開シナリオでのみ有効にできます。このシナリオでは、CP はアクティブ/スタンバイペアとして展開されます。「N」個のアクティブな UP を展開して CP と通信できます。展開した UP はすべて、デフォルト以外の特定の UP グループに含まれている必要があります。

注：N+2 では、すべての UP がアクティブなため、この機能はデータの UP リカバリ時間を短縮するためにのみ機能し、冗長性モデルではありません。IMS トラフィックを処理する UP は、1:1 冗長性モデルでのみ展開することを強く推奨します。

CP と UP 間の BFD 通信には、CP/UP ごとに 1 つの追加のループバック IP アドレスを設定する必要があります。

Figure 26: N+2 展開での *BFD* モニタリング



制限事項

- BFD ベースの CP 障害検出は、このリリースではサポートされていません。CP 障害は、Sx パス障害検出の既存のメカニズムを UP で使用して引き続き検出できます。

  注：古い UP セッションをより迅速に防ぐために、Sx パス障害タイマーをより積極的に設定することを推奨します。

- UP の Gi/Gn インターフェイスでの BGP モニタリングはサポートされていません。
- マルチ BFD はサポートされていません。
- BFD は、CP と UP の両方で Sx が設定されているのと同じコンテキスト（Gn 側）で設定する必要があります。

機能の仕組み

次の図と表に、UP がダウンと検出された場合のセッションの切断および再接続プロセスの概要を示します。

***Figure 27: N+2 UP* リカバリフロー**

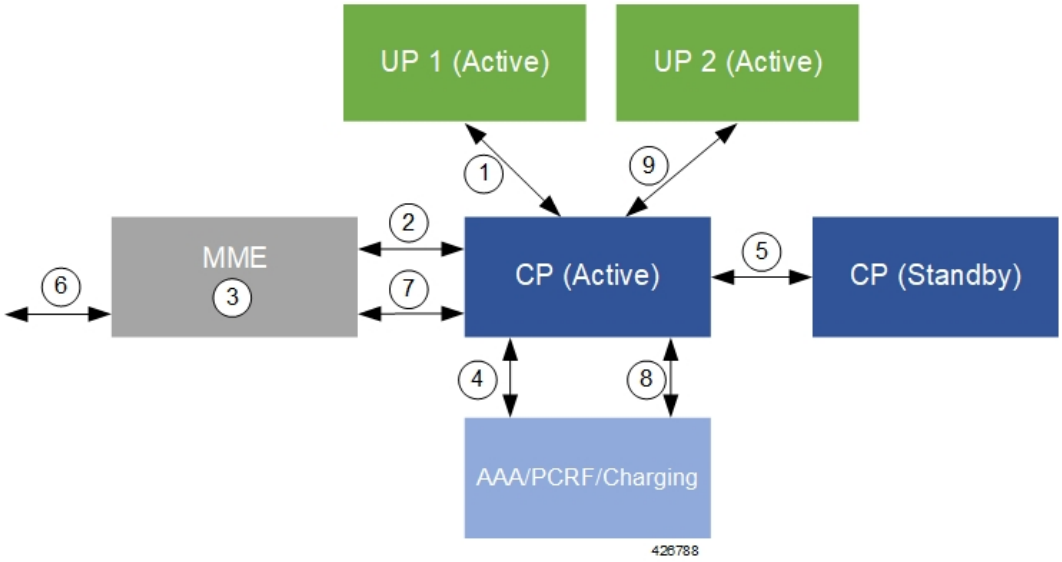


***Table 20: N+2 UP* リカバリフロー**

ケース	説明
1	CP が UP 障害を検出します。
2	CP は、原因コードが Local-Detach の UP 切断セッションメッセージを MME に送信します。
3	MME は要求を処理し、セッションを切断します。
4	CP は、AAA/PCRF/課金インフラストラクチャと通信して、セッションを切断します。
5	CP（アクティブ）はスタンバイ CP と通信して、UP 切断のチェックポイント処理を実行します。
6	以前にセッションが切断された UE は、MME に再接続します。
7	MME は CP と通信して、UE セッションを再接続します。
8	CP は、AAA/PCRF/課金インフラストラクチャと通信して、セッションを再接続します。
9	CP は、代替アクティブ UP を使用して Sx インターフェイスを介してセッション再接続プロセスを完了します。

SAEGW CP/UP、P-GW CP/UP、S-GW CP/UP、および GnGp GGSN CP/UP のパス障害フローの切り離しと再アタッチの詳細については、次の項を参照してください。

コール フロー

パス障害発生時の SAEGW の接続解除および再接続

次の図と表で、SAEGW CP および UP のパス障害発生時の接続解除および再接続プロセスについて説明します。

Figure 28: パス障害発生時の ***SAEGW CP/UP*** 接続解除および再接続プロセス

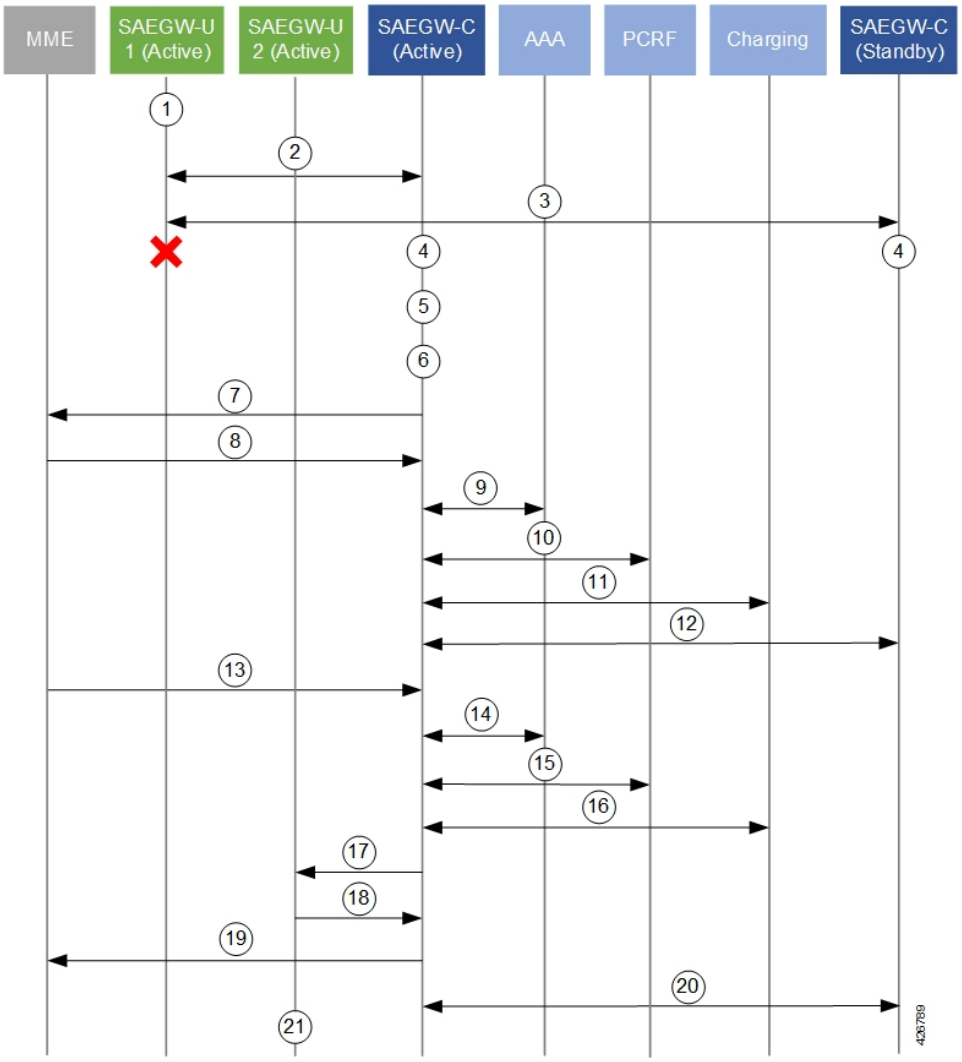


Table 21: パス障害発生時の *SAEGW CP/UP* 接続解除および再接続プロセス

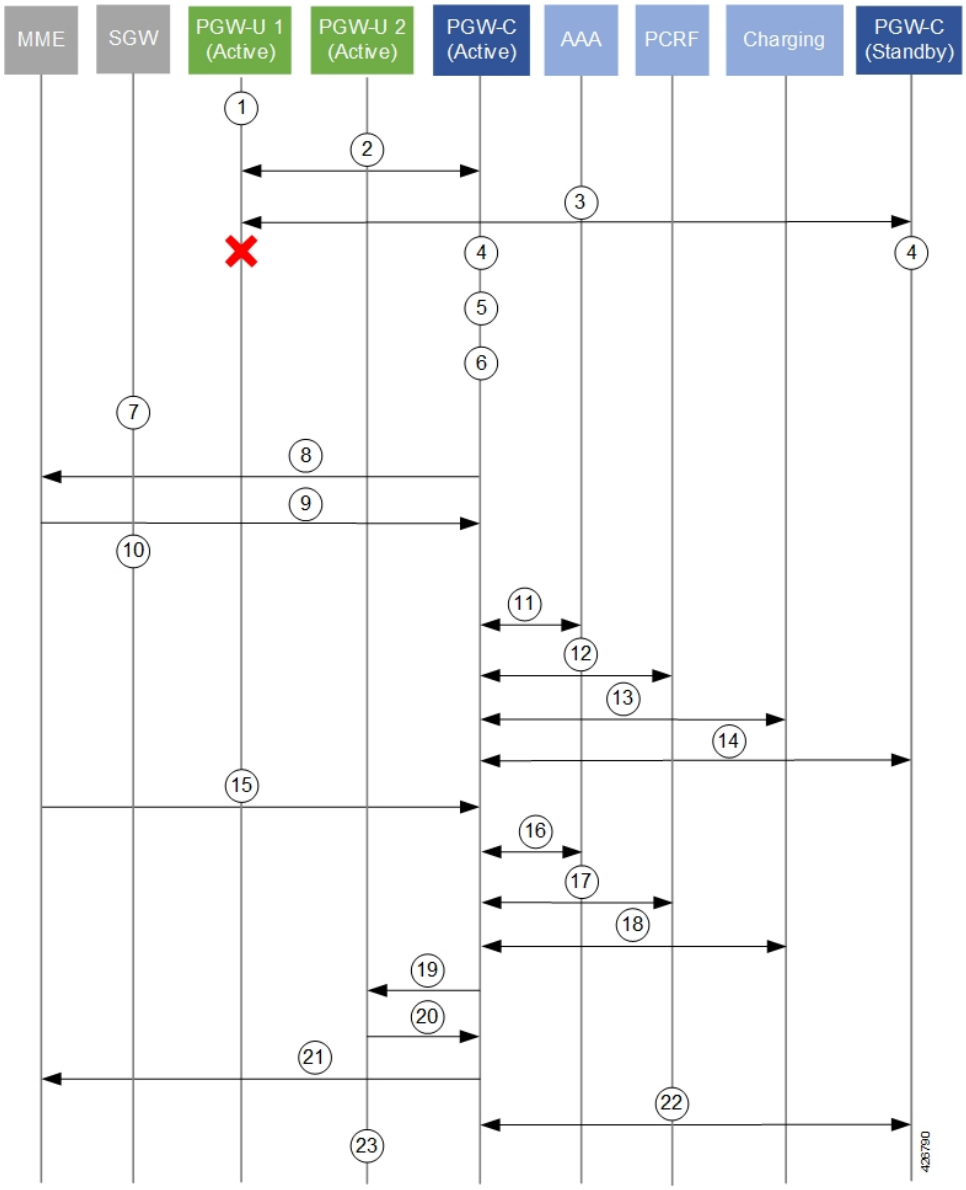
ケース	説明
1	UE データセッションは、アクティブな SAEGW UP によって処理されます。
2	アクティブ SAEGW CP は、BFD および Sx-Heartbeat メッセージを介して SAEGW UP をモニターします。
3	セカンダリ CP も、BFD を介して SAEGW UP をモニターします。
4	アクティブ CP とスタンバイ CP が、eNB 検出（Sx タイマー（間隔、再送信、タイムアウト）のリレー）の前に、UP で BFD 障害を検出します。
5	アクティブ CP の BFD/VPNMGR が、Sx-demux プロセスに BFDDown イベントを通知します。
6	アクティブ CP 上の Sx-demux プロセスが、CP 上のすべてのセッションマネージャに対するパス障害通知を開始します。
7	すべてのセッションマネージャは、MME に Local-Detach の原因を含む Delete-bearer-req メッセージを送信することで、セッションの接続解除プロセスを開始します。事前定義されたレートで接続解除が開始されます。
8	MME が Delete-bearer-resp メッセージを CP に送り返します。 MME はセッションが切断されているアイドル状態の UE をページングしません。 また、セッションが切断されているアクティブな UE に E-RAB リリースメッセージを送信します。
9	アクティブ CP が、AAA サーバーとのセッションを解放します。
10	アクティブ CP が、PCRF とのセッションを解放します。
11	アクティブ CP が、課金インフラストラクチャとのセッションを解放します。
12	アクティブ CP が、セッション切断情報をセカンダリ CP と同期します。
13	UE がセッションを再開する場合、MME がアクティブ CP に Create-session-request メッセージを送信します。 MME が負荷アルゴリズム（DNS、ローカル設定など）に基づいて CP を選択します。
14	アクティブ CP が、AAA サーバーとのセッション接続要求を処理します。
15	アクティブ CP が、PCRF を使用してセッション接続要求を処理します。
16	アクティブ CP が、課金インフラストラクチャとのセッション接続要求を処理します。
17	アクティブ CP が、代替アクティブ UP に Sx セッション確立要求メッセージを送信します。 CP が負荷アルゴリズムに基づいて UP を選択します。

ケース	説明
18	UP が Sx セッション確立応答メッセージを CP に送り返します。
19	CP が Create-session-response メッセージを MME に送信します。
20	アクティブ CP が、新しく接続されたセッションの情報をセカンダリ CP と同期します。
21	これで、UE データセッションがアクティブな SAEGW UP によって処理されます。

パス障害時の P-GW の切断と再接続

次の図と表は、P-GW CP および UP のパス障害時の切断および再接続プロセスを示しています。

Figure 29: パス障害時の *P-GW CP/UP* 切断および再接続プロセス



パス障害時の P-GW CP/UP 切断および再接続プロセス

Table 22: パス障害時の *P-GW CP/UP* 切断および再接続プロセス

ケース	説明
1	UE データセッションが、アクティブな P-GW UP によって処理されます。
2	アクティブな P-GW CP が、BFD および Sx ハートビートメッセージを介して P-GW UP をモニターします。
3	セカンダリ CP が、BFD を介して P-GW UP もモニターします。

ケース	説明
4	アクティブ CP とスタンバイ CP が、eNB 検出（Sx タイマー（間隔、再送信、タイムアウト）のリレー）の前に、UP で BFD 障害を検出します。
5	アクティブ CP の BFD/VPNMGR が、Sx-demux プロセスに BFDDown イベントを通知します。
6	アクティブ CP 上の Sx-demux プロセスが、CP 上のすべてのセッションマネージャへのパス障害通知を開始します。
7	S-GW が MME に対して db-req を開始します。
8	すべてのセッションマネージャが、MME に Local-Detach の原因を含む Delete-bearer-req メッセージを送信することで、セッションの切断プロセスを開始します。事前定義されたレートで切断が開始されます。
9	MME が Delete-bearer-resp メッセージを CP に送り返します。 MME はセッションが切断されているアイドル状態の UE をページングしません。 また、セッションが切断されているアクティブな UE に E-RAB リリースメッセージを送信します。
10	S-GW が db-resp を PGW-C に転送し、その PDN セッションを削除します。
11	アクティブ CP が、AAA サーバーとのセッションを解放します。
12	アクティブ CP が、PCRF とのセッションを解放します。
13	アクティブ CP が、課金インフラストラクチャとのセッションを解放します。
14	アクティブ CP が、セッション切断情報をセカンダリ CP と同期します。
15	セッションを再開する UE の場合、MME がアクティブ CP に Create-session-request メッセージを送信します。 MME が負荷アルゴリズム（DNS、ローカル設定など）に基づいて CP を選択します。
16	アクティブ CP が、AAA サーバーとのセッション接続要求を処理します。
17	アクティブ CP が、PCRF を使用してセッション接続要求を処理します。
18	アクティブ CP が、課金インフラストラクチャとのセッション接続要求を処理します。
19	アクティブ CP が、代替アクティブ UP に Sx セッション確立要求メッセージを送信します。 CP が負荷アルゴリズムに基づいて UP を選択します。
20	UP が Sx セッション確立応答メッセージを CP に送り返します。
21	CP が Create-session-response メッセージを MME に送信します。

ケース	説明
22	アクティブ CP が、新しく接続されたセッションの情報をセカンダリ CP と同期します。
23	これで、UE データセッションがアクティブな SAEGW UP によって処理されます。

パス障害時の S-GW の切断と再接続

次の図と表は、S-GW CP および UP のパス障害時の切断および再接続のプロセスフローを示しています。

Figure 30: パス障害時の ***S-GW CP/UP*** の切断と再接続プロセス

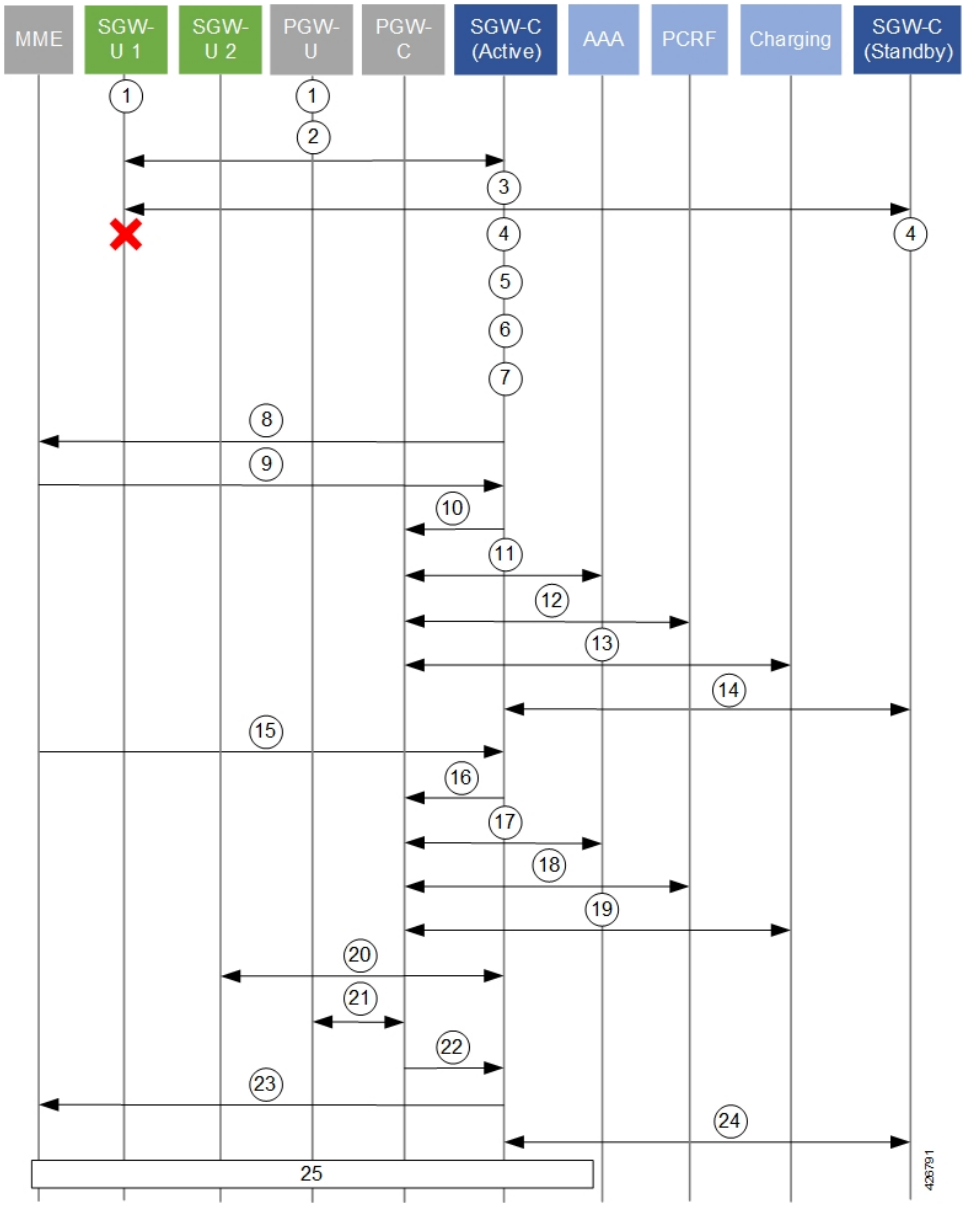


Table 23: パス障害時の *S-GW CP/UP* の切断と再接続プロセス

ケース	説明
1	アクティブ S-GW UP およびアクティブ PGW UP は、UE データセッションを処理します。
2	アクティブ S-GW CP は、BFD および Sx ハートビートメッセージを介して S-GW UP をモニターします。
3	セカンダリ S-GW CP も BFD を介して S-GW UP をモニターします。
4	アクティブ S-GW CP とスタンバイ S-GW CP は、eNB 検出（Sx タイマー（間隔、再送信、タイムアウト）のリレー）の前に、S-GW UP で BFD 障害を検出します。
5	アクティブ S-GW CP 上の BFD/VPNMGR は、Sx-demux プロセスに BFDDown イベントを通知します。
6	アクティブ CP 上の Sx-demux プロセスは、CP 上のすべてのセッションマネージャへのパス障害通知を開始します。
7	S-GW CP は MME に対して db-req を開始します。
8	すべてのセッションマネージャは、MME にローカル切断の原因を含む ベアラー削除要求メッセージを送信することで、セッションの切断プロセスを開始します。事前定義されたレートで切断が開始されます。
9	MME はベアラー削除応答メッセージを S-GW CP に送り返します。 MME はセッションが切断されているアイドル状態の UE をページングしません。 また、セッションが切断されているアクティブな UE に E-RAB リリースメッセージを送信します。
10	アクティブ S-GW CP は、PGW UP を使用してセッションを解放します。
11	PGW CP は AAA サーバーとのセッションを解放します。
12	PGW CP は PCRF とのセッションを解放します。
13	PGW CP は、課金インフラストラクチャとのセッションを解放します。
14	アクティブ S-GW CP は、セッション切断情報をセカンダリ S-GW CP と同期します。
15	セッションを再開する UE の場合、MME がアクティブな S-GW CP にセッション作成要求メッセージを送信します。 MME は負荷アルゴリズム（DNS、ローカル設定など）に基づいて CP を選択します。
16	アクティブ S-GW CP は、 セッション作成要求メッセージを PGW CP にリレーします。
17	PGW CP は、AAA サーバーとのセッション接続要求を処理します。
18	PGW CP は、PCRF を使用してセッション接続要求を処理します。

ケース	説明
19	PGW CP は、課金インフラストラクチャとのセッション接続要求を処理します。
20	アクティブ S-GW CP は、代替のアクティブ S-GW UP と Sx セッション確立要求および応答メッセージを交換します。
21	アクティブ PGW CP は、アクティブ PGW UP と Sx セッション確立要求および応答メッセージを交換します。
22	PGW CP は、セッション作成応答メッセージを S-GW CP に送信します。
23	S-GW CP は、セッション作成応答メッセージを MME に送信します。
24	アクティブ S-GW CP は、新しく接続されたセッションの情報をセカンダリ S-GW CP と同期します。
25	UE データがアクティブ UP を通過する前に、S-GW CP と は、MME と連携してベアラー変更要求手順を完了します。

パス障害時の GnGp GGSN の切断と再接続

次の図と表は、GnGp GGSN CP および UP のパス障害時の切断および再接続プロセスフローを示しています。

Figure 31: パス障害時の *GnGp GGSN CP/UP* 切断および再接続プロセス

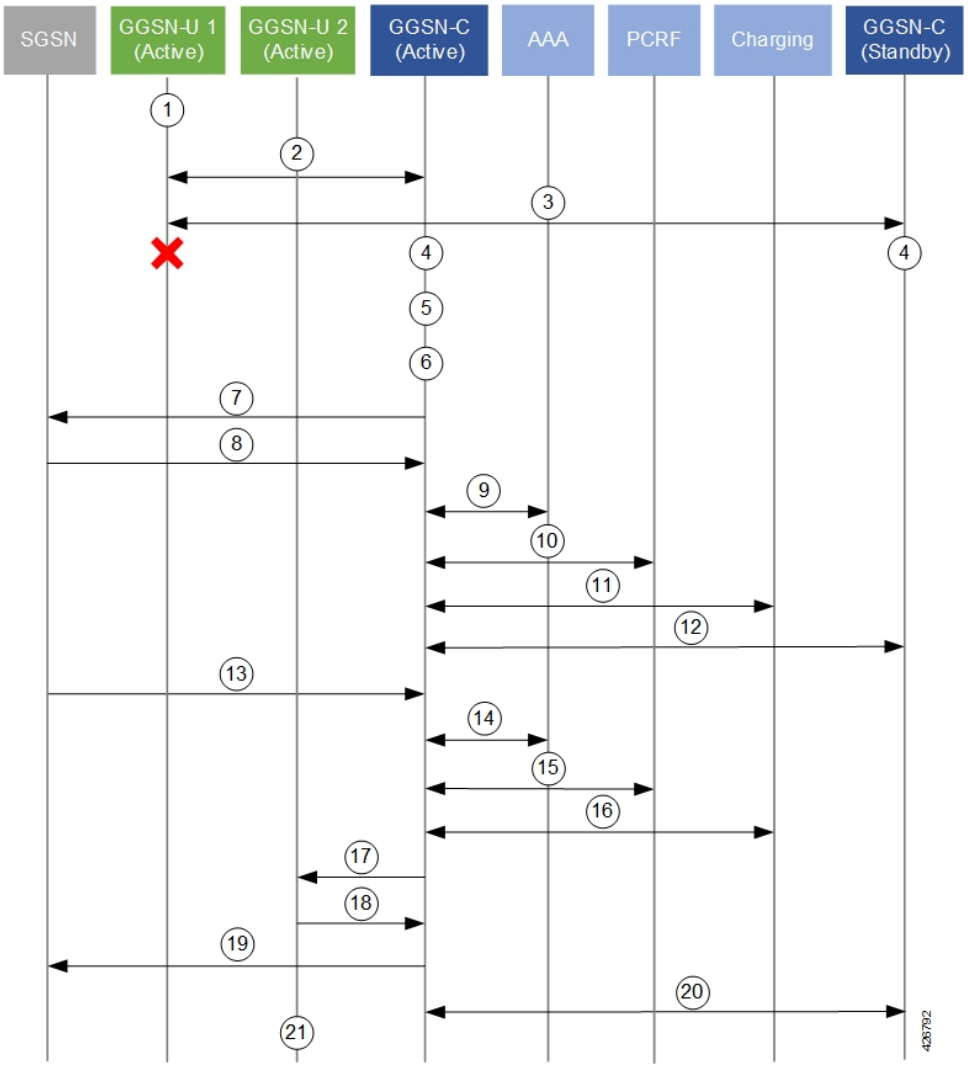


Table 24: パス障害時の *GnGp GGSN CP/UP* 切断および再接続プロセス

ケース	説明
1	アクティブ GGSN UP は、UE データセッションを処理します。
2	アクティブ GGSN CP は、BFD および Sx ハートビートメッセージを介して GGSN UP をモニターします。
3	セカンダリ CP も BFD を介して GGSN UP をモニターします。
4	アクティブ CP とスタンバイ CP は、eNB 検出（Sx タイマー（間隔、再送信、タイムアウト）のリレー）の前に、UP で BFD 障害を検出します。
5	アクティブ CP 上の BFD/VPNMGR は、Sx-demux プロセスに BFDDown イベントを通知します。

ケース	説明
6	アクティブ CP 上の Sx-demux プロセスは、CP 上のすべてのセッションマネージャへのパス障害通知を開始します。
7	すべてのセッションマネージャは、原因コードを含まない Delete-pdp-context-req メッセージを SGSN に送信することによって、セッションの切断プロセスを開始します。事前定義されたレートで切断が開始されます。
8	SGSN は Delete-pdp-context-resp メッセージを CP に送り返します。 SGSN はセッションが切断されているアイドル状態の UE をページングしません。 また、セッションが切断されているアクティブな UE に E-RAB 解放メッセージを送信します。
9	アクティブ CP は AAA サーバーとのセッションを解放します。
10	アクティブ CP は PCRF とのセッションを解放します。
11	アクティブ CP は課金インフラストラクチャとのセッションを解放します。
12	アクティブ CP はセッション切断情報をセカンダリ CP と同期します。
13	セッションを再開する UE の場合、SGSN はアクティブ CP に Create-pdp-request メッセージを送信します。 SGSN はロードアルゴリズム（DNS、ローカル設定など）に基づいて CP を選択します。
14	アクティブ CP は、AAA サーバーとのセッション接続要求を処理します。
15	アクティブ CP は、PCRF を使用してセッション接続要求を処理します。
16	アクティブ CP は、課金インフラストラクチャとのセッション接続要求を処理します。
17	アクティブ CP は、代替アクティブ UP に Sx セッション確立要求メッセージを送信します。 CP は負荷アルゴリズムに基づいて UP を選択します。
18	UP は Sx セッション確立応答メッセージを CP に送り返します。
19	CP は Create-pdp-context 応答メッセージを SGSN に送信します。
20	アクティブ CP は、新しく接続されたセッションの情報をセカンダリ CP と同期します。
21	これで、UE データセッションがアクティブな GGSN UP によって処理されます。

追加の N+2 処理シナリオ

前の項で説明したフロー以外に、N+2 が設定されたさまざまな条件下でのネットワーク機能（NF）やシステムの動作について次の表で説明します。

***Table 25: N+2* 処理シナリオ**

ID	シナリオ	ハンドル	注意
1	アクティブ UP がクラッシュ	アクティブ CP が UP で BFD 障害を検出すると、その UP に属するセッションを切断します。 アクティブ CP は、SRP を介してスタンバイ CP に切断を伝達します。 UP がアクティブに戻ると、アクティブ CP に再度関連付けられます。	検出は BFD タイムアウト間隔内で実行されます。 CP Sx は BFD をモニターします。
2	アクティブ CP がクラッシュ	アクティブ CP がスタンバイ CP に切り替わります。 アクティブ UP は、アクティブ CP とスタンバイ CP の両方の Sx ハートビートセッションをモニターします。 アクティブ UP は、ICSR フェールオーバー時間に達するまでセッションを消去しません。	スタンバイ CP はフェールオーバー時に Sx ハートビートの送信を開始します。アクティブ UP によってセッションが消去されることはありません。
3	スタンバイ CP がクラッシュ	スタンバイ CP が起動し、アクティブ CP でチェックポイント処理を実行してセッションを回復します。	アクティブ CP とアクティブ UP のセッションはそのまま残ります。

ID	シナリオ	ハンドル	注意
4	アクティブ CP とアクティブ UP 間でネットワークフラップが発生し。スタンバイ CP とアクティブ UP 間のネットワークは稼働中	アクティブ CP は、UP の BFD-Down を検出すると、セッション切断プロセスを開始し、UP の関連付けを解除します。 アクティブ CP は、SRP を介してスタンバイ CP に切断を伝達します。 アクティブ UP は、アクティブ CP を使用して Sx ハートビートをモニターします。 アクティブ UP は、設定された Sx ハートビート/パス障害検出タイムアウトが発生する（SRP スイッチオーバー時間を超える）まで待機してから、セッションをクリアします。	
5	スタンバイ CP とアクティブ UP 間でネットワークフラップが発生し。アクティブ CP とアクティブ UP Sx ハートビートもダウン	アクティブ UP が Sx パス障害を検出します。 アクティブ UP は、設定された Sx ハートビート/パス障害検出タイムアウトが発生する（SRP スイッチオーバー時間を超える）まで待機してから、セッションをクリアします。 アクティブ CP は、UP の BFD-Down を検出すると、セッション切断プロセスを開始し、UP の関連付けを解除します。	UP は、Sx ハートビートのタイムアウトによりセッションを削除します。

ID	シナリオ	ハンドル	注意
6	スタンバイ CP とアクティブ UP 間でネットワークフラップが発生し、アクティブ CP とアクティブ UP 間のネットワークは稼働中	スタンバイ CP は正常に動作します。 アクティブ CP-active は動作中で、ハートビートに応答します。 アクティブ UP は正常に動作します。	
7	Sx は到達不能だが、BFD は到達可能	アクティブ UP が Sx パス障害を検出します。 アクティブ UP は、設定された Sx ハートビート/パス障害検出タイムアウトが発生する（SRP スイッチオーバー時間を超える）まで待機してから、セッションをクリアします。 アクティブ CP は、UP の Sx パス障害を検出すると、セッション切断プロセスを開始し、UP の関連付けを解除します。	現在の動作ごとに Sx パス障害として扱われるコーナーケース（N+2 の前）。
8	アクティブ CP とスタンバイ CP 間で ICSR リンクがダウンし、スタンバイ CP もアクティブになる（デュアルアクティブの場合）	デュアルアクティブになると、スタンバイ CP はより高いメトリックでアクティブ UP にメッセージを送信します。	デュアルアクティブ構成のスタンバイ CP によってアドバタイズされるすべてのサービスで、IP のメトリックが高くなります。
9	アクティブ UP の BGP 障害の Gn 側	N+2 に関連するアクションは実行されません。	
10	アクティブ UP の BGP 障害の SGI 側	N+2 に関連するアクションは実行されません。	
11	アクティブ UP で SessMgr がクラッシュ	セッション回復プロセスがアクティブ UP で発生します。	

ID	シナリオ	ハンドル	注意
12	アクティブ UP で Sx-demux がクラッシュ	Sx-demux 回復プロセスがアクティブ UP で発生します。	
13	アクティブ UP で VPP がクラッシュ	NPUMgr が UP を再起動すると、BFD 損失が発生し、UP 障害検出がトリガーされます。 この表の ID 1 および 5 の処理に関する情報を参照してください。	
14	アクティブ UP で VPNMgr がクラッシュ	VPNMgr 回復プロセスがアクティブ UP で発生します。	
15	アクティブ UP で BFD がクラッシュ	BFD 回復プロセスがアクティブ UP で発生します。	
16	アクティブ CP で Sx-demux がクラッシュ	Sx-demux 回復プロセスがアクティブ CP で発生します。 Sx-demux は、リカバリの一環として CP とすべての UP 間の BFD を再登録し、各 UP の状態を再検出します。 Sx-demux は SessMgr から再起動タイムスタンプを回復します。	アクティブ CP での Sx-demux リカバリ中に UP 状態の遷移が発生する可能性があります（たとえば、UP は再起動しますが、リカバリ後に CP に対してアクティブと示されます）。 次の状態が検出されます。 • Sx-demux が回復し、CP が Sx ハートビートまたは UP 障害から UP 再起動タイムスタンプを検出します。 • アクティブ CP はこの情報に基づいて、セッションの消去を開始します。

ID	シナリオ	ハンドル	注意
17	アクティブ CP で VPNMgr がクラッシュ	VPNMgr 回復プロセスがアクティブ CP で発生します。 アクティブ CP の SCT から BFD 登録情報が回復されます。 アクティブ CP は UP で BFD を再起動します。	
18	アクティブ CP で BFD がクラッシュ	BFD 回復プロセスがアクティブ CP で発生します。	
19	アクティブ CP で SessMgr がクラッシュ	SessMgr 回復プロセスがアクティブ CP で発生します。	

二重障害処理シナリオ

N+2 二重障害シナリオは、BFD 障害の後に別のイベント/障害が発生した場合に発生します。このようなシナリオの処理については、次の表で説明します。

***Table 26: N+2* 二重障害シナリオの処理**

ID	シナリオ	ハンドル	注意
1	セッションの接続解除中にアクティブ CP に障害が発生する	CP 間で ICSR スイッチオーバーが発生します。 スタンバイ CP がアクティブ CP になります。 アクティブ CP が BFD を介して UP 障害を検出します。 アクティブ CP が Sx ハートビートを介して UP の再起動を検出します。	影響： 二重障害で UP が再起動した場合、スタンバイ CP によるセッションの回復が完了していても、UP にはセッションがありません。 これらのセッションは、セッションの置換時または UE からのセッション接続解除時に消去されます。 UP が再起動しない場合、CP-new-active は障害が発生した UP のセッションをクリアします。

ID	シナリオ	ハンドル	注意
2	セッションの接続解除中にスタンバイ CP に障害が発生する	スタンバイ CP は、アクティブ CP の状態情報のチェックポイントを生成します。 削除されたセッションに関する情報は、アクティブ CP から無効化されます。	
3	アクティブ CP がルータフラップによる UP 障害と判断する。アクティブ CP がセッションの接続解除を開始した後に UP BFD を受信する	まず UP BFD のダウン状態が検出され、すべてのセッションが接続解除されます。	

BFD フラッピングと VPC

N+2 は BFD を使用して、セッションエンドポイント間のネットワークパスの存在や実行可能性をモニターします。ループバックエンドポイントでマルチホップ BFD を使用することで、BFD セッション状態は、接続先のシステム状態のプロキシとして機能します。

ただし、相手側のシステム障害以外の理由（ARP ストームやルータの設定不備など）で、BFD セッションがダウンしたり、バウンス/フラップしたりする可能性があります。中断が大変深刻で長期間続く場合、両方のシステムが機能していても、両側のシステムで BFD セッション障害が検出される可能性があります。

設定を調整することで、このようなイベントの発生をオフセットできます。

次の推奨事項は、NF が展開されているプラットフォームに基づいて提供されます。

- VPC-SI：BFD マルチホップピア設定を調整して、BFD 検出時間を 2 ー 3 秒に増やし、それに応じて再試行回数を増やします。
- VPC-DI：CF スイッチオーバーと SF 移行により、BFD パケットの生成と処理が数秒間中断される可能性があります。これらのイベントが発生したときに BFD セッションのフラップが発生しないようにするには、VPC-DI システムが関わるセッションの BFD 検出時間を 7 秒以上に設定する必要があります。

Sx 関連付けのシナリオ

次の表に、N+2 を使用する場合の CP と UP の関連付けと関連付け解除に関する情報を示します。

Table 27: N+2 Sx 関連付けのシナリオ

シナリオ	メカニズム
UP から CP への Sx 関連付け解除	• Sx-demux が VPNMgr を使って BFD モニタリングを無効にする • SAEGW サービスが削除される • UP からの Sx 関連付け解除
UP の追加	Day-0 の一環として： • UP の BFD ループバックアドレスを追加する。 • CP で BFD を設定する。 • UP グループを追加し、CP で選択できるように設定する。
UP の削除	CP で CLI コマンドを実行して、UP の IP アドレスを使ってサブスクライバをクリアし、その UP に振り向けられる新しいセッションをブロックするキーワードを指定します。 • UP 上ですべてのサブスクライバが切断されていることを確認する。 • UP で、CLI コマンドを実行して CP との関連付けを解除する。CP から UP の関連付けが解除され、CP では以降のセッションにこの UP を選択しない。すべてのセッションが切断されていることを確認する。 • CP で、UP グループから UP を削除する。 • CP で、UP グループから UP を削除する CLI コマンドを実行する（UP の BFD モニタリングも登録解除される）。 • UP および CP で BFD のモニタリング設定を無効にする。このときの CLI コマンドは no monitor-group。
UP によって開始された Sx 関連付け	CP の Sx-demux は、VPNMGr からの BFDUp および BFDDown 通知の処理を開始する。
UP によって解放された Sx 関連付け	CP の Sx-demux は、VPNMgr からの BFDUp および BFDDown 通知を無視する。

N+2 および IP アドレス指定

ループバック IP アドレス

N+2 に関連する BFD ループバックアドレスには、次のことが当てはまります。

- アクティブ CP およびスタンバイ CP の BFD ループバック IP アドレスは、Day-0 に設定する必要があります。
- BFD は、アクティブ CP とアクティブ UP の間、およびスタンバイ CP とアクティブ UP の間で動作します。そのため、3 つのコンポーネントすべてで一意の BFD ループバック IP アドレスを使用する必要があります。
- CP および UP ごとに設定された BFD ループバック IP アドレスは、Sx インターフェイスに使用されるアドレスとは異なる必要があります。また、CP の場合は、SRP インターフェイスに使用されるアドレスとも異なる必要があります。

IP アドレスの可用性

N+2 展開シナリオでは、UE は高いレート（切断レートと同等）で再接続できます。このプロセスを円滑に進めるには、十分な数の IP アドレスが UP で使用可能になっている必要があります。

CUPS IP プール管理には、アドレスの「チャンク」を使用して UP をプロビジョニングする機能が含まれています。CP で設定したチャンクサイズとプールの数は、CP から UP への高い再接続レートに比例して増やす必要があります。IP アドレスが使用できないことが原因でセッションが UP によって拒否されないようにするためです。

予測される再接続レートは、UP セッションを処理するセッションマネージャのタスク数に 1000 セッション/秒を掛けて概算できます。

アドレスキャパシティは、チャンクのサイズ（16 ～ 8192）と IP プールの数を掛けて決定されます。両方ともに CP で設定されます。

N+2 UP リカバリの設定

N+2 UP リカバリを設定するには、次の手順を実行します。

1. CP および UP で BFD を設定します。

```
configure
   context bfd_context_name
      ip route static multihop bfd mhbfd_session_name
local_endpoint_ip_address remote_endpoint_ip_address
      bfd-protocol
         bfd multihop-peer dst_ip_address interval tx_interval min_rx
rx_interval multiplier value
         #exit
      #exit
```

注：

- *bfd_ctx_name* は、BFD を設定するコンテキストの名前です。これは、Sx が設定されているコンテキストと同じである必要があります。

- *mhbfd_session_name* は BFD セッションルートの名前です。ピア接続ごとに 1 つずつ、複数のセッションルートを作成できます。
- *local_endpoint_ip_address* は、現在のコンテキストのローカルインターフェイスに対応する IPv4 または IPv6 アドレスです。
- *remote_endpoint_ip_address* は、リモート BFD ピアに対応する IPv4 または IPv6 アドレスです。
  - このルートが CP で設定されている場合、リモートアドレスはピア UP のリモートアドレスになります。
  - このルートが UP で設定されている場合、リモートアドレスはピア CP のリモートアドレスになります。
- *dst_ip_address* は、リモート BFD ピアに対応する IPv4 または IPv6 アドレスです。これは、スタティックマルチホップ BFD ルート用に設定された *remote_endpoint_ip_address* インターフェイスと同じである必要があります。リモートピアごとに 1 つずつ、複数のピアを設定できます。
- **interval** *tx_interval* は、BFD パケット間の送信間隔（ミリ秒単位）です。
- **min_rx** *rx_interval* は、BFD パケット間の最小受信間隔（ミリ秒単位）です。
- **multiplier** *value* はホールドダウンを計算するために使用する乗数値です。
- 検出時間（X）を決定するには、次の計算を使用できます。

  検出時間（X） = **interval** *tx_interval* * **multiplier** 値

  検出時間（X）の推奨値は、VPC-SI の場合は 3 秒、VPC-DI の場合は 7 秒です。

2. CP および UP でコンテキストごとに BFD ループバックを設定します。

```
configure
   context monitor_ctx_name
      monitor-protocols
         monitor-group monitor_group_name protocol bfd
            session-ctx session_ctx_name local-addr { ipv4_address |
ipv6_address } remote-address { ipv4_address | ipv6_address }
            #exit
```

注：

- *Monitor_ctx_name* は、BFD モニタリングを設定するコンテキストの名前です。これは、Sx が設定されているコンテキストと同じである必要があります。
- *Monitor_group_name* は、BFD モニタリングパラメータを指定するグループの名前です。複数のモニターグループを設定できます。
- *Session_ctx_name* は、BFD モニタリングが実行されるローカルインターフェイスを含むコンテキストの名前です。これは、Sx が設定されているコンテキストと同じである必要があります。

- **local-addr {** *ipv4_address* **|** *ipv6_address* **}** は、指定されたコンテキストのローカルインターフェイスに対応する IPv4 または IPv6 アドレスです。
- **remote-addr {** *ipv4_address* **|** *ipv6_address* **}** は、BFD モニタリングが実行されるリモートピアに対応する IPv4 または IPv6 アドレスです。
  - このモニターグループが CP で設定されている場合、リモートアドレスは UP グループのリモートアドレスになります。
  - このモニターグループが UP で設定されている場合、リモートアドレスは CP グループのリモートアドレスになります。

3. CP の特定の UP グループ内で BFD ループバック（リモート IP）を設定します。

```
configure
   user-plane-group up_group_name
      peer-node-id { ipv4_address | ipv6_address } monitor-group-name
monitor_group_name
      #exit
```

注：

- *up_group_name* は、サポートされる N+2 UP リカバリのデータ UP を含む UP グループの名前です。
  - これをデフォルトグループにすることはできません。
  - このグループには、IMS/VoLTE をサポートするための UP を含めないでください。
- **{** *ipv4_address* **|** *ipv6_address* **}** は、UP グループに含めるアクティブ UP 上の Sx インターフェイスの IPv4 または IPv6 アドレスです。グループ内で複数のピアノードを設定できます。Sx インターフェイスは、BFD のモニタリングに使用されるインターフェイスとは異なることに注意してください。
- *monitor_group_name* は、UP が関連付けられるモニタリング グループの名前です。

モニタリングおよびトラブルシューティング

コマンドの表示

show sx peers { full address *peer_ip_address* **| wide }**

show sx peers full address *peer_ip_address*

指定したピアのモニター関連情報（VPN コンテキスト名、グループ名、状態など）を表示します。

show sx peers wide

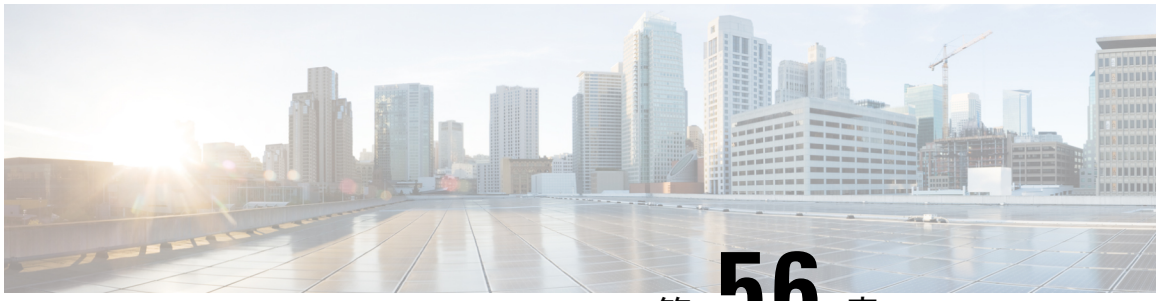
「モニター状態」が表示されます。デフォルトの状態は、アップの場合は「U」、ダウンの場合は「D」、該当なしの場合は「N」です。

show sx-service statistics all

SNMP

次の SNMP トラップを使用して、N+2 UP リカバリの正常性をモニターできます。

- StarBFDSessUp（starentTraps 1276）
- StarBFDSessDown（starentTraps 1277）
- StarSxPathFailure（starentTraps 1382）：このトラップが更新され、新しい原因コード [bfd-failure(8)] が追加されました。
- StarSxPathFailureClear（starentTraps 1383）



第 56 章

NAT のサポート

機能の概要と変更履歴

マニュアルの変更履歴

Note リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
このリリースでは、CUPS UP におけるファイアウォール NAT ポートの解放動作の変更を明確化。	21.27.x
最初の導入。	21.24 より前

機能説明

CUPS はネットワークアドレス変換（NAT）をサポートしているため、ネットワークアドレスの設定が可能です。NAT IP アドレスと NAT ポートを使用して、UE の送信元 IP または送信元ポートアドレスをカプセル化したデータパケットを自動的に転送するようにシステムを設定できます。

サポートされる NAT の組み合わせは次のとおりです。

- NAT44 オンデマンド多対 1

- NAT44 オンデマンド 1 対 1
- NAT64 オンデマンド多対 1
- NAT 64 オンデマンド 1 対 1
- NAT44 非オンデマンド多対 1
- NAT44 非オンデマンド 1 対 1
- NAT64 非オンデマンド多対 1
- NAT64 非オンデマンド 1 対 1

NAT の補足情報については、StarOS の『*NAT Administration Guide*』[英語] を参照してください。

注：StarOS『 *NAT Administration Guide*』 に記載されているすべての機能が CUPS アーキテクチャに当てはまるわけではありません。

NAT ポート解放の動作

ICMP NAT ポートの使用率は、以下の理由により、レガシーよりも CUPS ソリューションで高くなります。

- レガシーでは、ICMP応答を受信すると、次のメッセージに使用できるようにNATポートが解放されます。CUPS では、100 番目の ICMP メッセージを受信した後にのみ NAT ポートが解放されます。
- レガシーでは、要求に対する ICMP 応答が受信されない場合、20 個の NAT ポートが連続的に割り当てられ、最初のポートから解放されます。CUPS では、100 番目の ICMP パケットの後にのみ削除が行われます。

制限事項

NAT のサポートには次の制限事項があります。

- 多対 1 およびオンデマンドモードの NAT44 のみがサポートされます。
- すべてのNATプールは、接続先コンテキストの個別のユーザープレーンで設定されます。
- fw-and-nat ポリシーでの CLI アクション拒否を使用した課金アクション、および active-charging-service での flow-any-error 課金アクションはサポートされていません。
- 「dynamic-only」および「static-and-dynamic」で設定されたアクセスルール：外部サーバーからのルールはサポートされません。
- 同じレルムからの複数の IP サポートは、この機能ではサポートされていません。
- NAT プールでのネクストホップ転送はサポートされていません。
- NAT プールのポート範囲はサポートされていません。

- プライベート IP チェック CLI のスキップはサポートされていません。
- RADIUS および Gy で返される Fw-and-nat ポリシーベースの NAT ポリシーの適用はサポートされていません。
- ベアラー固有のフィルタは、access-ruledefs ではサポートされていません。
- アクセスルールは、fw-and-nat ポリシーでの open-port ポート範囲設定のトリガーをサポートしていません。
- SR/ICSR 後の NAT ポートリカバリ（fw-and-nat アクション）はサポートされていません。
- NAT 再構成タイムアウト CLI は、active-charging サービスではサポートされていません。代わりに、UP の汎用コンテキストレベル CLI を使用する必要があります。
- NAT フラグメンテーションの再構成の失敗は、基本的な CUPS の再構成に関する未解決のバグによりサポートされていません。
- NAT flow-mapping タイマーはサポートされていません
- N:M 冗長性の場合、各 UP ホストのインターフェイス設定の一部として RCM から設定される NAT IP プール、およびプール名は、すべてのアクティブなユーザープレーンで一意である必要があります。そのため、fw-and-nat ポリシーで参照される同じ NAT レルムをすべてのユーザープレーンに適用できるように、すべてのプールに NAT グループを使用することが必須になります。
- N:M 冗長性の場合、RCM を介してすべての UP でまとめて設定される NAT IP プールの総数は、IP プールの最大制限数（2,000）に従う必要があります。すべてのアクティブ UP の累積合計が最大値を超えると、スタンバイユーザープレーンの設定は失敗します。

CUPS での NAT の設定

NAT の関連設定は CP で行われ、UP にプッシュされます。プール関連の設定のみがユーザープレーンに存在します。

NAT 関連の CLI コマンドの詳細については、StarOS NAT アドミニストレーション ガイド [英語] の「NAT Configuration」の章を参照してください。

注：StarOS NAT アドミニストレーション ガイド [英語] の「NAT Configuration」の章に記載されているすべての CLI コマンドと設定を CUPS アーキテクチャに適用できるわけではありません。

設定例

コントロール プレーン

次に、CUPS で NAT を有効にするためにコントロールプレーンで必要な設定例を示します。この設定は、PFD メカニズムを介したユーザープレーンの登録時にユーザープレーンにプッシュされます。

```
configure
active-charging service ACS
     access-ruledef all
       ip any-match = TRUE
     #exit
     access-ruledef udp
       udp any-match = TRUE
     #exit
     access-ruledef tcp
       tcp any-match = TRUE
     #exit
     access-ruledef icmp
       icmp any-match = TRUE
     #exit
     fw-and-nat policy NatPolicy1
        access-rule priority 1 access-ruledef tcp permit nat-realm NAT44_GRP1
        access-rule priority 2 access-ruledef icmp permit nat-realm NAT44_GRP1
        #access-rule priority 2 access-ruledef r2 permit bypass-nat
        nat policy ipv4-only default-nat-realm NAT44_PUBLIC5
        nat binding-record edr-format NBR port-chunk-allocation port-chunk-release
     #exit

     fw-and-nat policy NatPolicy2
        access-rule priority 1 access-ruledef all permit nat-realm NAT44_PUBLIC1
        #access-rule priority 2 access-ruledef r2 permit bypass-nat
        nat policy ipv4-only
        nat binding-record edr-format NBR port-chunk-allocation port-chunk-release
     #exit

     rulebase cisco
     fw-and-nat default-policy NatPolicy1
     flow end-condition normal-end-signaling session-end timeout edr NBR
     #exit
#exit
end
```

ユーザープレーン

ISP コンテキストのユーザープレーンでは、次のプール関連の設定が必要です。

```
configure
   context ISP1-UP
      ip pool NAT44_PUBLIC1 209.165.200.225 255.255.255.224 napt-users-per-ip-address 2
 on-demand port-chunk-size 16 max-chunks-per-user 4 group-name NAT44_GRP1
      ip pool NAT44_PUBLIC2 209.165.200.226 255.255.255.224 napt-users-per-ip-address 2
 on-demand port-chunk-size 16 max-chunks-per-user 4 group-name NAT44_GRP1
      ip pool NAT44_PUBLIC3 209.165.200.227 255.255.255.224 napt-users-per-ip-address 2
 on-demand port-chunk-size 8 max-chunks-per-user 1 group-name NAT44_GRP2
      ip pool NAT44_PUBLIC4 209.165.200.228 255.255.255.224 napt-users-per-ip-address 4
 on-demand port-chunk-size 32256 max-chunks-per-user 4 group-name NAT44_GRP2
```

```
      ip pool NAT44_PUBLIC5 209.165.200.229 255.255.255.224 napt-users-per-ip-address
8064 on-demand port-chunk-size 8 max-chunks-per-user 2
      end
```

さまざまな NAT プールタイプの NAT プール関連の設定例

```
1-1 on-demand:
----------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_1_1 209.165.200.230 255.255.255.224 nat-one-to-one on-demand
nat-binding-timer 60
end

N-1 Not-on-demand:
------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_N_1 209.165.200.231 255.255.255.224 napt-users-per-ip-address 2
max-chunks-per-user 2 port-chunk-size 8
end

1-1 Not-on-demand:
------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_NOD_1_1 209.165.200.232 255.255.255.224 nat-one-to-one
end
```

Note コントロールプレーンの設定は、ユーザープレーンで設定された必須 NAT プール/グループのいずれかにマッピングされた 1 つ以上のアクセスルール定義とともに追加する必要があります。詳細については、『*Ultra Packet Core CUPS Control Plane Administration Guide*』[英語] を参照してください。

モニタリングおよびトラブルシューティング

NAT 統計の収集

次の表に、NAT 統計の収集に使用できるコマンドを示します。

最初の列には収集する統計、2 つ目の列には使用するコマンドを挙げています。

統計/情報	show コマンド
アクティブまたは休止中のセッションがある、現在のすべてのサブスクライバに関する情報。サブスクライバに関連付けられている IP アドレスを確認します。NAT レルムで使用されているすべての IP アドレスも表示されます。	**show subscribers user-plane-only full all**

統計/情報	show コマンド
NAT サブシステムの統計情報。	**show user-plane-service statistics all**
NAT 関連のすべての統計。	**show user-plane-service statistics nat all**
NAT レルム関連のすべての統計。	**show user-plane-service statistics nat nat-realm all**
NAT IP プールグループ内のすべての NAT IP プールの統計。	**show user-plane-service statistics nat nat-realm** *pool_name*
生成された NAT バインドレコードに関する情報。	**show user-plane-service edr-format statistics all**
UP の APN で fw-and-nat ポリシーの関連付けを確認します。	**show user-plane-service pdn-instance name** *name*
UP での fw-an-nat ポリシーの設定を確認します。	**show user-plane-service fw-and-nat policy all**
ポートチャンクの割り当ておよび解放のために生成された NAT バインドレコードに関する情報。	**show user-plane-service rulebase name** *name*
アクセス ruledef に関する情報。	**show user-plane-service ruledef all**
UP の rulebase で fw-and-nat ポリシーの関連付けを確認します。	**show user-plane-service rulebase name** *name*

clear コマンド

この機能をサポートする、次の clear CLI コマンドを使用できます。

- **clear user-plane-service statistics nat nat-realm all**
- **clear user-plane-service statistics nat all**

NAT パラメータしきい値の SNMP トラップ

NAT パラメータしきい値に対する次の SNMP トラップがサポートされます。

SNMP トラップ	説明
ThreshNATPortChunks	NAT ポートのチャンク使用率が、しきい値により設定された限度に達すると生成されます。
ThreshClearNATPortChunks	NAT ポートのチャンク使用率が、クリアしきい値により設定された限度に達すると生成されます。
ThreshNATPktDrop	NAT パケットドロップが、しきい値により設定された限度に達すると生成されます。

SNMP トラップ	説明
ThreshClearNATPktDrop	NAT パケットドロップが、クリアしきい値により設定された限度に達すると生成されます。
ThreshIPPoolUsed	IP プールで使用されている IP の数が、しきい値により設定された限度に達すると生成されます。
ThreshClearIPPoolUsed	IP プールで使用されている IP の数が、クリアしきい値により設定された限度に達すると生成されます。
ThreshIPPoolFree	IP プールが解放され、しきい値が定める限度に達すると生成されます。
ThreshClearIPPoolFree	IP プールが使用され、クリアしきい値が定める限度に達すると生成されます。
ThreshIPPoolAvail	IP プールが次のフローで使用可能になり、設定されたしきい値に達すると生成されます。
ThreshClearIPPoolAvail	IP プールが使用され、設定されたしきい値に達すると生成されます。

注：これらのトラップを有効にするには、それぞれの CLI をユーザープレーンで設定する必要があります。

バルク統計情報

コンテキストスキーマ

Table 28: コンテキストスキーマ

変数名	データ タイプ	カウンタタイプ	説明
nat-total-flows	Int64	Counter	NAT44 および NAT64 フローの総数
nat44-total-flows	Int64	Counter	NAT44 フローの総数
nat64-total-flows	Int64	Counter	NAT64 フローの総数
bypass-nat-total-flows	Int64	Counter	NAT44 および NAT64 バイパス NAT フローの総数
bypass-nat-ipv4-total-flows	Int64	Counter	NAT44 バイパス NAT フローの総数
bypass-nat-ipv6-total-flows	Int64	Counter	NAT64 バイパス NAT フローの総数
nat-current-flows	Int64	ゲージ	NAT44 および NAT64 フローの現在の数

変数名	データ タイプ	カウンタタイプ	説明
nat44-current-flows	Int64	ゲージ	NAT44 フローの現在の数
nat64-current-flows	Int64	ゲージ	NAT64 フローの現在の数
bypass-nat-current-flows	Int64	ゲージ	NAT44 および NAT64 バイパス NAT フローの現在の数
bypass-nat-ipv4-current-flows	Int64	ゲージ	NAT44 バイパス NAT フローの現在の数
bypass-nat-ipv6-current-flows	Int64	ゲージ	NAT64 バイパス NAT フローの現在の数
sfw-total-rxpackets	Int64	Counter	サービスによって受信されたパケットの総数
sfw-total-rxbytes	Int64	Counter	サービスによって受信されたバイトの総数
sfw-total-txpackets	Int64	Counter	サービスによって転送されたパケットの総数
sfw-total-txbytes	Int64	Counter	サービスによって転送されたバイトの総数
sfw-total-injectedpkts	Int64	Counter	サービスによって挿入されたパケットの総数
sfw-total-injectedbytes	Int64	Counter	サービスによって挿入されたバイトの総数
sfw-dnlnk-droppkts	Int64	Counter	サービスによってドロップされたダウンリンクパケットの総数
sfw-dnlnk-dropbytes	Int64	Counter	サービスによってドロップされたダウンリンクバイトの総数
sfw-uplnk-droppkts	Int64	Counter	サービスによってドロップされたアップリンクパケットの総数
sfw-uplnk-dropbytes	Int64	Counter	サービスによってドロップされたアップリンクバイトの総数

Note スキーマは CUPS のユーザープレーンでサポートされています。

ECS スキーマ

***Table 29: ECS* スキーマ**

変数名	データタイプ	カウンタタイプ	説明
nat-current-ipv4-pdn-subscribers	Int32	ゲージ	現在の NAT IPv4 PDN サブスクライバ数
nat-current-ipv6-pdn-subscribers	Int32	ゲージ	現在の NAT IPv6 PDN サブスクライバ数
nat-current-ipv4v6-pdn-subscribers	Int32	ゲージ	現在の NAT IPv4v6 PDN サブスクライバ数
nat-total-ipv4-pdn-subscribers	Int64	Counter	NAT IPv4 PDN サブスクライバの総数
nat-total-ipv6-pdn-subscribers	Int64	Counter	NAT IPv6 PDN サブスクライバの総数
nat-total-ipv4v6-pdn-subscribers	Int64	Counter	NAT IPv4v6 PDN サブスクライバの総数
nat-current-ipv4-pdn-subscribers-with-nat-ip	Int32	ゲージ	NAT IP を使用する現在の NAT IPv4 PDN サブスクライバ数
nat-current-ipv6-pdn-subscribers-with-nat-ip	Int32	ゲージ	NAT IP を使用する現在の NAT IPv6 PDN サブスクライバ数
nat-current-ipv4v6-pdn-subscribers-with-nat-ip	Int32	ゲージ	NAT IP を使用する現在の NAT IPv4v6 PDN サブスクライバ数
nat-total-ipv4-pdn-subscribers-with-nat-ip	Int64	Counter	NAT IP を使用する NAT IPv4 PDN サブスクライバの総数
nat-total-ipv6-pdn-subscribers-with-nat-ip	Int64	Counter	NAT IP を使用する NAT IPv6 PDN サブスクライバの総数
nat-total-ipv4v6-pdn-subscribers-with-nat-ip	Int64	Counter	NAT IP を使用する NAT IPv4v6 PDN サブスクライバの総数
nat-total-unsolicited-dwnlnk-pkts	Int64	Counter	受信した不正ダウンリンクパケットの合計数

変数名	データタイプ	カウンタタイプ	説明
nat-total-icmp-hu-sent-for-dwnlnk-pkts	Int64	Counter	ダウンリンクパケットで送信された ICMP ホスト到達不能の合計数

Note スキーマは CUPS のユーザープレーンでサポートされています。

NAT レルムスキーマ

NAT レルムはユーザープレーンで設定され、統計情報はコンテキストごと、レルムごとに保存されます。これらの統計変数（累積とスナップショットの両方）は、NAT レルムスキーマで使用できます。

Table 30: NAT **レルムスキーマ**

変数名	データ型	カウンタタイプ	説明
Vpnname	文字列	Info	コンテキスト名
Realmname	文字列	Info	レルム名。
nat-rlm-bind-updates	Int64	Counter	送信された暫定 AAA NBU の合計。
nat-rlm-bytes-txferred	Int64	Counter	レルムによって転送された NAT44 および NAT64 バイトの合計数（アップリンク+ダウンリンク）。
nat-rlm-bytes-nat44-tx	Int64	Counter	レルムによって転送された NAT44 バイトの合計数。
nat-rlm-bytes-nat64-tx	Int64	Counter	レルムによって転送された NAT64 バイトの合計数。
nat-rlm-ip-flows	Int64	Counter	レルムで使用された NAT44 および NAT64 フローの総数。
nat-rlm-nat44-flows	Int64	Counter	レルムによって処理された NAT44 フローの総数。
nat-rlm-nat64-flows	Int64	Counter	レルムによって処理された NAT64 フローの総数。
nat-rlm-ip-denied	Int32	Counter	NAT IP アドレスが拒否された NAT44 および NAT64 フローの総数。

変数名	データ型	カウンタタイプ	説明
nat-rlm-ip-denied-nat44	Int64	Counter	IP が拒否された NAT44 フローの総数。
nat-rlm-ip-denied-nat64	Int64	Counter	IP が拒否された NAT64 フローの総数。
nat-rlm-port-denied	Int32	Counter	ポートが拒否された NAT44 および NAT64 フローの総数。
nat-rlm-port-denied-nat44	Int64	Counter	ポートが拒否された NAT44 フローの総数。
nat-rlm-port-denied-nat64	Int64	Counter	ポートが拒否された NAT64 フローの総数。
nat-rlm-memory-denied	Int64	Counter	メモリが拒否された NAT44 および NAT64 フローの総数。
nat-rlm-memory-denied-nat44	Int64	Counter	メモリが拒否された NAT44 フローの総数。
nat-rlm-memory-denied-nat64	Int64	Counter	メモリが拒否された NAT64 フローの総数。
nat-rlm-ttl-ips	Int32	ゲージ	NAT レルムあたりのコンテキストごとの NAT パブリック IP アドレスの総数。スタティック値です。
nat-rlm-ips-in-use	Int32	ゲージ	NAT レルムあたりのコンテキストごとに、現在使用されている NAT IP アドレスの総数。
nat-rlm-current-users	Int32	ゲージ	NAT レルムを現在使用しているサブスクライバの総数。
nat-rlm-ttl-port-chunks	Int32	ゲージ	NAT レルムあたりのコンテキストごとのポートチャンクの総数。スタティック値です。
nat-rlm-chunks-in-use	Int32	ゲージ	NAT レルムあたりのコンテキストごとに現在使用されているポートチャンクの総数。
nat-rlm-port-chunk-size	Int32	ゲージ	NAT レルムのポートチャンクのサイズ。

変数名	データ型	カウンタタイプ	説明
nat-rlm-port-chunk-average-usage-tcp	Int32	ゲージ	割り当てられた TCP ポートの平均 TCP ポート使用率。つまり、割り当てられた TCP ポートのうち、使用された数。パーセンテージ値ではありません。
nat-rlm-port-chunk-average-usage-udp	Int32	ゲージ	割り当てられた UDP ポートの平均 UDP ポート使用率。つまり、割り当てられた UDP ポートのうち、使用された数。パーセンテージ値ではありません。
nat-rlm-port-chunk-average-usage-others	Int32	ゲージ	割り当てられた他のポートでの他の（ICMP または GRE）ポートの平均使用率（つまり、割り当てられた「他の」ポートのうち、使用された数）。パーセンテージ値ではありません。
nat-rlm-max-port-chunk-subs	Int64	Counter	最大数のポートチャンクを使用したサブスクライバの総数。
nat-rlm-max-port-chunk-used	Int32	Counter	使用された最大ポートチャンク数。
nat-rlm-max-cur-port-chunk-subs	Int64	ゲージ	ポートチャンクの最大数を使用している現在のサブスクライバ数。
nat-rlm-max-cur-port-chunk-used	Int32	ゲージ	アクティブなサブスクライバによって使用された最大ポートチャンク数。

EDR

通常の EDR では、次の NAT 固有の属性がサポートされています。

- sn-nat-subscribers-per-ip-address：NAT IP アドレスごとのサブスクライバ
- sn-subscriber-nat-flow-ip：NAT 対応サブスクライバの NAT IP アドレス
- sn-subscriber-nat-flow-port：NAT 対応サブスクライバの NAT ポート番号

EDR の例

```
#sn-start-time,sn-end-time,ip-protocol,ip-subscriber-ip-address,ip-server-ip-address,sn-subscriber-port,sn-server-port,
sn-nat-ip,sn-nat-port-block-start,sn-nat-port-block-end,sn-subscriber-nat-flow-ip,sn-subscriber-nat-flow-port,sn-nat-realm-name,
sn-nat-subscribers-per-ip-address,sn-nat-binding-timer,sn-nat-gmt-offset,sn-nat-port-chunk-alloc-dealloc-flag,sn-nat-port-chunk-alloc-time-gmt,
sn-nat-port-chunk-dealloc-time-gmt,sn-nat-no-port-packet-dropped,sn-closure-reason
```

```
02/18/2020 12:11:11:630,02/18/2020
12:11:11:632,1,209.165.200.225,209.165.201.1,0,0,,,,209.165.200.230,1024,,2,,,,,,0,0
02/18/2020 12:11:08:672,02/18/2020
12:11:09:671,6,209.165.200.225,209.165.201.1,1001,3000,,,,209.165.200.230,1034,,2,,,,,,0,0
02/18/2020 12:11:14:499,02/18/2020
12:11:14:499,17,209.165.200.225,209.165.201.1,1001,3000,,,,209.165.200.240,1025,,8064,,,,,,0,0
```

NAT バインドレコード

NAT IP アドレスまたは NAT ポートチャンクがサブスクライバとの間で割り当てまたは割り当て解除されるたびに、NAT バインドレコード（NBR）を生成できます。NBR の生成は、ファイアウォールと NAT ポリシーの設定で設定できます。

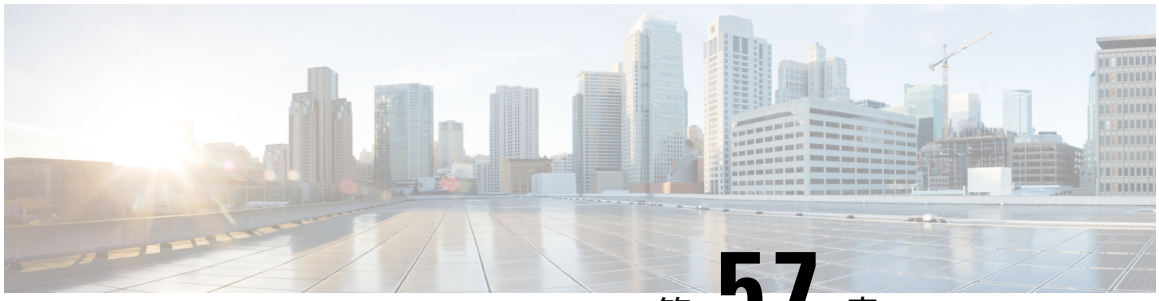
NBR の例

```
#sn-start-time,sn-end-time,ip-protocol,ip-subscriber-ip-address,ip-server-ip-address,sn-subscriber-port,
sn-server-port,sn-nat-ip,sn-nat-port-block-start,sn-nat-port-block-end,sn-subscriber-nat-flow-ip,sn-subscriber-nat-flow-port,
sn-nat-realm-name,sn-nat-subscribers-per-ip-address,sn-nat-binding-timer,sn-nat-gmt-offset,sn-nat-port-chunk-alloc-dealloc-flag,
sn-nat-port-chunk-alloc-time-gmt,sn-nat-port-chunk-dealloc-time-gmt,sn-nat-no-port-packet-dropped,sn-closure-reason
,,,209.165.200.225,,,,209.165.201.1,1024,1039,,,NAT44_PUBLIC2,2,60,+0530,1,02/18/2020
06:41:08,,,
,,,209.165.200.225,,,,209.165.201.2,1024,1031,,,NAT44_PUBLIC5,8064,60,+0530,1,02/18/2020
 06:41:14,,,
,,,209.165.200.225,,,,209.165.201.3,1024,1039,,,NAT44_PUBLIC2,2,60,+0530,0,02/18/2020
06:41:08,02/18/2020 06:42:12,,
,,,209.165.200.225,,,,209.165.201.14,1024,1031,,,NAT44_PUBLIC5,8064,60,+0530,0,02/18/2020
 06:41:14,02/18/2020 06:44:24,,
```

パケットドロップ EDR

パケットドロップ EDR の例

```
#sn-nat-no-port-packet-dropped,sn-start-time,sn-end-time,sn-subscriber-imsi
2,03/13/2020 08:28:24,03/13/2020 08:28:54,123456789012345
```



第 57 章

NAT ALG のサポート

機能の概要と変更履歴

マニュアルの変更履歴

Note リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

（注） 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。

NAT は、アプリケーション データ ストリームで送信元 IP アドレスや接続先 IP アドレスが送信されない Transmission Control Protocol/User Datagram Protocol（TCP/UDP）トラフィックで、変換サービスを実行します。該当プロトコルは次のとおりです。

- HTTP
- 簡易ファイル転送プロトコル（TFTP）
- Telnet
- Archie
- Finger
- ネットワーク タイム プロトコル（NTP）
- ネットワーク ファイル システム（NFS）
- リモートログイン（rlogin）
- リモートシェルプロトコル（RSH）
- Remote Copy Protocol（RCP）

以下のプロトコルのペイロード内にはIPアドレス情報があります。これらのプロトコルには、変換サービス用のアプリケーション レベル ゲートウェイ（ALG）のサポートが必要です。

- FTP
- H323
- Session Initiation Protocol（SIP）
- Session Description Protocol（SDP）
- TFTP
- RTSP
- ポイントツーポイント トンネリング プロトコル（PPTP）

制限事項

H323 に対する NAT64 から v4 への変換はサポートされていません。

Session Initiation Protocol ALG のコンポーネント

次のブロック図は、NATまたはファイアウォールのSIP ALGをサポートするすべてのコンポーネントを示しています。ALG-CORE と SIP APP は新しいコンポーネントです。他のコンポーネントは、拡張が必要な既存のコンポーネントです。

（注） この例はSIP ALGに固有のものです。同様のコンポーネントは、ドキュメント内の他のすべてのプロトコルに適用できます。

図 *32 : Session Initiation Protocol （SIP） ALG* のコンポーネント

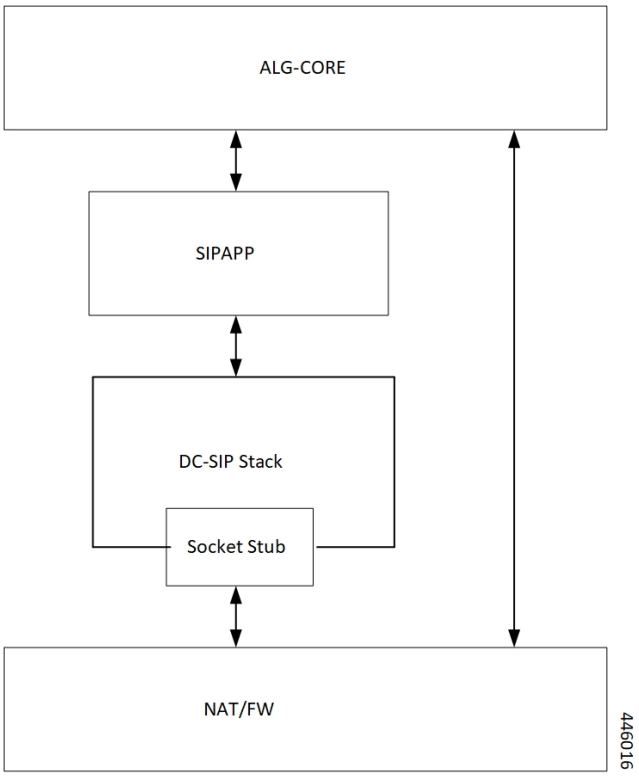


表 *31 :* コンポーネントと機能

コンポーネント	機能
ALG-CORE	• NAT/FW と対話して、ピンホールを作成/変更/クリアします。 • ALG-CORE には、HA CLP 内にピンホール情報を保存するためのロジックが組み込まれています（sip_alg_info と呼ばれる構造体への新しいポインタを定義します）。 • ALG-CORE は、受信状態とイベントに基づいてSIPAPPからのメッセージを処理します。

コンポーネント	機能
SIP アプリ	• 要求/応答のコールバックごとの新しい機能ロジック。 • コール/セッション関連の情報を維持するための新しいデータ構造（スタック callCb/TransactionCb データ構造に基づく）。 • ALG-CORE と対話するために、sip/H.323 のいくつかの一般的な UMM 構造を定義します。 • ALG-CORE によって返された情報から、プライベート IP からパブリック IP への SIP メッセージのエンコーディングを実行します。
DC SIP	DC-SIP は、SIP メッセージを解析し、トランザクションとコール状態を維持する本格的な SIP スタックです。SIP-ALG 機能の場合、DC-SIP は B2BUA として機能します。DC-SIP スタックが提供する機能は次のとおりです。 • メッセージ解析 • トランザクション管理 • コール管理 • メッセージのエンコード • 要求/応答タイプごとのコールバック。

ソケットスタブは、NAT/FW との間でパケットを送受信するコンポーネントです。

NAT/FW はソケットスタブとの間で SIP パケットを送受信し、ALG-CORE と対話するための汎用 API も提供します。

機能の仕組み

一部のネットワーク アプリケーションは、ペイロードの一部としてサーバー/クライアントの IP/ポート情報を交換します。サーバーまたはクライアントは、交換された IP/ポート情報を使用して新しいフローを作成します。サーバーまたはクライアントは、その IP/ポート情報を NAT ALG の一部として抽出し、ピンホールを介してそれらのフローを動的に許可します。

NAT の場合、サーバーまたはクライアントは IP およびトランスポートレベルで変換を行います。NAT IP と NAT ポートは、プライベート送信元 IP と送信元ポートを置き換えます。ただし、これらの変換は透過的であるため、送信側アプリケーションはこうした変換を認識しない場合があります。

たとえば、FTP NAT ALG 機能は「PORT」および「PASV 応答」メッセージを解釈します。NAT はペイロードで同じものを変換するため、FTP は NAT を介して透過的に実行されます。

NAT レイヤは、NAT 44 変換および NAT 64 変換をサポートします。NAT は、1 対 1 オンデマンド NAT 変換と多対 1 NAT 変換もサポートします。

各 ALG では、次の機能がサポートされています。

- NAT 44 1 対 1 オンデマンド NAT 変換
- NAT 44 多対 1 オンデマンド NAT 変換
- NAT 64 1 対 1 オンデマンド NAT 変換
- NAT 64 多対 1 NAT 変換

FTP

FTP は TCP ベースのプロトコルであり、2 つのフローを使用します。1 つは制御メッセージ用、もう 1 つはデータ/ファイル転送用です。FTP は、PORT および PASSIVE 応答コマンドを使用して、データフローパラメータを交換します。これらのコマンドは、ペイロードの一部として IP およびポート情報を伝送します。

RTSP

RTSP は、リアルタイムメディア転送を制御するさまざまな方法を備えた TC ベースのリアルタイムストリーミングプロトコルです。制御メッセージには、メディアを転送するためのポート情報が埋め込まれています。

PPTP

Point-to-Point Tunneling Protocol（PPTP）により、IP ネットワークを介した Point to Point Protocol（PPP）のトンネリングが実現します。PPTP は、拡張 GRE（Generic Routing Encapsulation）を使用して PPP パケットを伝送します。PPTP は制御接続を介して IP またはポート固有の情報を交換し、その情報をもとにトンネルを介してデータを転送します。

SIP

SIP はアプリケーション層の制御プロトコルであり、インターネット電話コールなどのマルチメディアセッション（会議）を確立、変更、および終了できます。SIP は要求/応答トランザクションモデルに基づいています。各トランザクションは、サーバーでメソッドまたは関数を呼び出す 1 つの要求と 1 つ以上の応答で構成されます。要求と応答には、クライアントとサー

バーの IP およびポート情報が含まれています。マルチメディアセッションを記述するための SDP メッセージ本文（SIP 要求および応答に存在する可能性あり）にも、IP およびポート情報が埋め込まれています。

メディアストリーム（音声、ビデオ）の伝送では、SIP メッセージで伝送される SDP ペイロードでは通常、Real-time Transport Protocol（RTP）が使用されます。SIP ALG はすべての SIP 通信を傍受し、ペイロード内のプライベート IP とポートを NAT IP とポートに変換します。

TFTP

Trivial File Transfer Protocol（TFTP）は、ファイル転送用のアプリケーション層プロトコルです。TFTP はシンプルなメカニズムであるため、多くの組み込み型システムがこのプロトコルを使用してサーバーからイメージやファイルがダウンロードしています。これは UDP ベースのプロトコルです。TFTP L7 ペイロードには IP やポート情報は含まれていませんが、ダウンリンクで開始されたデータフローを許可するためのピンホールが必要です。

H323

H323 は、インターネット電話コールなどのマルチメディアセッションを確立、変更、および終了できる一連のプロトコル仕様です。マルチメディアセッションの成功に関係するプロトコルは、RAS、H225、H245、およびメディアプロトコル（RTP、RTCP）です。RAS プロトコルは、H323 ゲートキーパーと端末間の通信用プロトコルです。この通信は、通信相手の他の端末を見つけるのに役立ちます。H225 と H245 は、セッションの確立、機能の交換、およびメディアパラメータの交換のために端末間で通信します。H245 メッセージには、マルチメディア通信が行われるメディアチャネルの詳細が含まれています。IP およびポート情報は、RAS、H225、および H245 メッセージに含まれています。H323 ALG は、すべての H323 通信を傍受し、ペイロード内のプライベート IP とポートを NAT IP とポートに変換します。

NAT FW 処理

パケットを処理するためのキーを受信すると、5 タプルを使用して ECS フレームワークでフローが作成されます。

- ソース IP
- ソース ポート
- プロトコル
- Destination IP
- 宛先ポート

特定の 5 タプルを持つ最初のパケットの場合は、NAT/FW ルールの照合が適用され、受け入れ可能なパケットなのか確認されます。パケットが受け入れ可能な場合は、フローが作成されます。

NAT レルム（NAT IP）の設定は、ルールの一部です。フローに適用可能な NAT レルムは、パケットと一致するルール定義から取得されます。

ルール設定は、既知のサーバーアドレスやポート番号に基づいて行われます。たとえば、FTP サービスはポート 21、SIP サービスはポート 5060 です。

そのため、既知のサーバーやポート番号への FTP 制御セッションまたは SIP 制御セッションで、一致するファイアウォールルールが検出されます。ただし、制御シグナリングに基づいて動的にメディアフロー（子フロー）のルールを設定できない場合があります。

FTP データまたは SIP メディアパケットの場合、NAT/FW ルール定義の照合は失敗し、パケットはドロップされます。

もう 1 つの要件は、同じ NAT レルムを使用するための制御シグナリングと対応するメディア接続です。制御とメディアに同じ NAT IP アドレスが適用されます。

子フロー（メディア接続）で一致する NAT/FW ルールが検出された場合でも、子フローでは、そのルールに対する正しくない NAT レルム設定が使用されます。メディアフローでは、制御接続に適用可能なレルムと同じ NAT レルムを使用する必要があります。

そのため、一致するルールがない場合でも、子フローでは制御接続用と同じ NAT レルムが使用されます。フローを実現するには、シグナリングメッセージに基づいてピンホールを作成します。ピンホールには、5 タプル情報のサブセットが含まれます。

ピンホールでは、ルールの照合（バイパスルールの照合）を行わずにトラフィックが許可され、NAT レルムがピンホールに関連付けられます。ピンホールに一致するトラフィックは許可され、ピンホールで指定された NAT レルムがパケットの通知に適用されます。

多対 1 の NAT の場合、NAT はアクティブな NAT バインディングがある場合にのみダウンリンクパケットを許可します。リモートエンドが接続（着信コール）を開始する必要がある多くのサービス（SIP など）があります。そのような状況では、ダウンリンクパケットを許可するために、ALG が必要な NAT バインディングを作成し、シグナリングメッセージを解析してピンホールに関連付ける必要があります。

次に、アップリンクおよびダウンリンクのパケット処理について説明します。

アップリンクパケット処理

アップリンクパケット処理については、次の点を参照してください。

- アップリンクパケットを受信すると、既存の 5 タプルのフローと比較されます。
- 一致するフローが存在する場合（5 タプル一致）、そのフローに関連付けられている NAT バインドがパケットに適用されます。
- 一致するフローが存在しない場合は、このフロー用に開いているピンホールがあるかどうかを確認するためにピンホールルックアップが行われます。
- ピンホールが存在する場合は、ピンホールに関連付けられた NAT バインドがパケットに適用されます。

- ピンホールが存在しない場合は、ルール照合によってそのフローの NAT 情報が決定されます。一致するルールが存在しない場合、パケットはドロップされます。

発信 SIP 要求の場合、SIP メッセージは 5060 という宛て先ポートに関連付けられます。このため、SIP トラフィックを識別するため、宛て先ポートを 5060 にしてルールを設定します。ルールに設定された対応する NAT レルムが SIP 要求に適用されます。

要求に基づくピンホールにはすべて、NAT バインドが関連付けられている必要があります。この NAT バインド割り当ては、要求を処理するための NAT レルムからの割り当てです。

ダウンリンクパケット処理

アップリンクパケット処理については、次の点を参照してください。

- ダウンリンクパケットは、アクティブな NAT バインドが存在する場合にのみ通過します。バインドルックアップが失敗すると、パケットはドロップされます。
- バインドルックアップが成功した場合、パケットに対し、アップリンクパケット処理と同じ初期フロー照合処理が行われます。
- ただし、ダウンリンクパケットの場合、多対 1 の NAT IP からのパケットに対するルール照合は行われません。パケットは、一致するフローまたは一致するピンホールがある場合のみ通過し、それ以外の場合はドロップされます。ピンホールが存在する場合は、そのピンホールを持つ NAT バインドがそのフローに適用されます。
- 1 対 1 の NAT の場合、ピンホールがなくてもルール照合が行われ、一致するルールがあればパケットは通過します。パケットを受信する NAT レルムは、そのダウンリンクフローに適用されます。

NAT ALG の設定

NAT ALG の設定コマンドを次に示します。

```
configure
  active-charging service acs_service_name
    firewall nat-alg { default | no } { ftp | pptp | rtsp | sip | h323
 }
    end
```

注：

- **default**：指定したパラメータのデフォルト設定でこのコマンドを設定します。
- **no**：すべてまたは指定した NAT ALG 設定を無効にします。無効にすると、ALG では NAT コールのペイロード変換は実行されません。
- **ftp**：File Transfer Protocol（FTP）NAT ALG を有効または無効にします。
- **pptp**：Point-to-Point Tunneling Protocol（PPTP）を有効または無効にします。

- **rstp**：Real Time Streaming Protocol（RTSP）ALG を有効または無効にします。
- **sip**：Session Initiation Protocol（SIP）NAT ALG を有効または無効にします。
- **h323**：H323 NAT ALG を有効または無効にします。

多対 1 および 1 対多の設定

ユーザープレーンでの多対 1 の設定。

```
ip pool NAT44_PUBLIC4 209.165.200.225 255.255.255.224 napt-users-per-ip-address 4
group-name NAT44_GRP2 on-demand max-chunks-per-user 4 port-chunk-size 32256
```

ユーザープレーンでの 1 対 1 の設定。

```
ip pool NAT44_PUBLIC4 209.165.200.225 255.255.255.224 nat-one-to-one on-demand group-name
 NAT44_GRP1
```

FTP NAT ALG の設定例

パケットをコントロールプレーンの FTP ALG に回送するには、次の FTP 回送ルールを設定します。

```
Config
active-charging service acs
    ruledef rt_ftp-control
      tcp either-port = 21
      rule-application routing
      multi-line-or all-lines
    #exit
    ruledef rt_ftp-data
      tcp either-port = 20
      rule-application routing
      multi-line-or all-lines
    #exit
   access-ruledef SFW_HTTP
      ip any-match = TRUE
    #exit
    access-ruledef all
      ip any-match = TRUE
    #exit
    access-ruledef ipv6_nat
      ip server-ipv6-network-prefix = 64:ff98::/96
    #exit
    rulebase prepaid
      route priority 14 ruledef rt_ftp-data analyzer ftp-data
      route priority 15 ruledef rt_ftp-control analyzer ftp-control
    #exit
    fw-and-nat policy nat_policy1
      access-rule priority 1 access-ruledef ipv6_nat permit nat-realm NAT44_GRP1
      access-rule priority 10 access-ruledef SFW_HTTP permit nat-realm NAT44_GRP1
      access-rule priority 100 access-ruledef all permit nat-realm NAT44_GRP1
      nat policy ipv4-and-ipv6
    #exit
firewall nat-alg ftp ipv4-and-ipv6
  #exit
```

RTSP NAT ALG の設定例

以下に、RTSP NAT ALG の設定例を示します。

```
Config
active-charging service acs
    ruledef rtsp-pkts
      tcp src-port = 554
      rule-application routing
    #exit
    ruledef rtsp-pkts1
      tcp dst-port = 554
      rule-application routing
    #exit
      access-ruledef SFW_HTTP
      ip any-match = TRUE
    #exit
      access-ruledef prefix1
      ip server-ipv6-network-prefix = 64:ff98::/96
    #exit
    rulebase cisco
     tcp 2msl-timeout 20
     tcp mss 1300 limit-if-present
      route priority 105 ruledef rtsp-pkts analyzer rtsp
      route priority 106 ruledef rtsp-pkts1 analyzer rtsp
      rtp dynamic-flow-detection
      fw-and-nat default-policy nat_policy1
#exit
fw-and-nat policy nat_policy1
      access-rule priority 1 access-ruledef prefix1 permit nat-realm NAT44_GRP1
      access-rule priority 10 access-ruledef SFW_HTTP permit nat-realm NAT44_GRP1
      nat policy ipv4-and-ipv6
    #exit
    firewall nat-alg rtsp ipv4-and-ipv6
```

PPTP NAT ALG の設定例

PPTP NAT ALG の設定例を以下に示します。

```
configure
active-charging service ACS
    ruledef pptp-route
      tcp either-port = 1723
      rule-application routing
      multi-line-or all-lines
     exit
     rulebase cisco
     route priority 1 ruledef pptp-route analyzer pptp
     #exit
#exit
access-ruledef all
      ip any-match = TRUE
#exit
access-ruledef ipv6_nat
ip server-ipv6-network-prefix = 101:101::/96
#exit
     rulebase cisco
     route priority 1 ruledef pptp-route analyzer pptp
     fw-and-nat default-policy nat_policy1
     #exit
      fw-and-nat policy nat_policy1
```

```
      access-rule priority 1 access-ruledef ipv6_nat permit nat-realm NAT44_GRP1
      access-rule priority 100 access-ruledef all permit nat-realm NAT44_GRP1
      nat policy ipv4-and-ipv6
    #exit
firewall nat-alg pptp ipv4-and-ipv6
#exit
```

TFTP NAT ALG の設定例

次に、コントロールプレーンでの NAT44 の設定例を示します。

```
configure
active-charging service ACS
    ruledef rt_tftp
      udp either-port = 69
      rule-application routing
      multi-line-or all-lines
    exit
      rulebase cisco
      route priority 1 ruledef rt_tftp analyzer tftp
   #exit
#exit
```

次に、コントロールプレーンでの NAT64 の設定例を示します。

```
conf
         active-charging service ACS
         ruledef rt_tftp
         udp either-port = 69
         rule-application routing
         multi-line-or all-lines
         exit
         access-ruledef all
         ip any-match = TRUE
         exit
         access-ruledef ipv6_nat
         ip server-ipv6-network-prefix = 64:ff98::/96
         exit
         rulebase cisco
         route priority 1 ruledef rt_tftp analyzer tftp
         fw-and-nat default-policy nat_policy
         #exit
        end
        conf
       context ISP1
      ip pool NAT44_PVT1 209.165.200.225 255.255.255.224 private 0 group-name NAT44_GRP1

      ip pool NAT44_PVT4 209.165.200.226 255.255.255.224 private 0 group-name NAT44_GRP1

      end
      conf
      context ISP1
      apn cisco.com
      ip address pool name NAT44_GRP1
      fw-and-nat policy nat_policy1
      exit
      end
     configure
     active-charging service ACS
     fw-and-nat policy nat_policy1
     access-rule priority 1 access-ruledef ipv6_nat permit nat-realm NAT44_GRP1
     access-rule priority 10 access-ruledef all permit nat-realm NAT44_GRP1
```

```
     nat policy ipv4-and-ipv6
     end
```

H323 NAT ALG の設定例

次に、H323 NAT ALG の設定例を示します。

```
configure
active-charging service ACS
     ruledef h323
      udp dst-port = 1719
      rule-application routing
    #exit
    ruledef h323_multi
      udp dst-port = 1718
      rule-application routing
    #exit
    ruledef h323_tcp
      tcp dst-port = 1720
      rule-application routing
    #exit
   rulebase cisco
   route priority 6 ruledef h323 analyzer h323
      route priority 7 ruledef h323_tcp analyzer h323
      route priority 8 ruledef h323_multi analyzer h323
      rtp dynamic-flow-detection
 fw-and-nat default-policy nat_policy1
     #exit
      fw-and-nat policy nat_policy1
      access-rule priority 100 access-ruledef all permit nat-realm NAT44_GRP1
      nat policy ipv4-and-ipv6
   #exit
firewall nat-alg h323 ipv4-only
#exit
```

SIP NAT ALG の設定例

次に、SIP NAT ALG の設定例を示します。

```
conf
active-charging service service_1
    ruledef sipalg
      udp dst-port = 5060
      rule-application routing
    #exit
    ruledef sipalg_tcp
      tcp dst-port = 5060
      rule-application routing
    #exit
   access-ruledef server2
      ip dst-address = 209.165.200.224/27
    #exit
    access-ruledef nat64
      ip server-ipv6-network-prefix = cccc:1111::/96
      ip any-match = TRUE
    #exit
    #exit
    rulebase base_1
      route priority 1 ruledef sipalg analyzer sip advanced description advanced
      route priority 2 ruledef sipalg_tcp analyzer sip advanced description advanced
      rtp dynamic-flow-detection
```

```
    fw-and-nat default-policy fw1
  #exit
  fw-and-nat policy fw1
    access-rule priority 2 access-ruledef server2 permit nat-realm natPool
    access-rule priority 3 access-ruledef nat64 permit nat-realm natPool
    nat policy ipv4-and-ipv6
  #exit
  firewall nat-alg sip ipv4-and-ipv6
  #exit
#exi
```

モニタリングおよびトラブルシューティング

ここでは、CUPS の NAT ALG 機能のモニタリングと障害対応で使用できる CLI コマンドについて説明します。

show コマンドと出力

ここでは、CUPS の NAT ALG 機能をサポートする show CLI コマンドについて説明します。

- **show user-plane-service statistics analyzer name rtsp**：RTSP 関連の統計情報を表示するには、このコマンドを使用します。

```
RTSP Session Stats:
   Total Uplink Bytes:             844   Total Downlink Bytes:           1440
   Total Uplink Pkts:               10   Total Downlink Pkts:               6
   Uplink RTP Bytes:                 8   Downlink RTP Bytes:          2851524
   Uplink RTP Pkts:                  2   Downlink RTP Pkts:              2741
   Uplink Retry Bytes:               0   Downlink Retry Bytes:              0
   Uplink Retry Pkts:                0   Downlink Retry Pkts:               0
   RTSP Sessions:                    1
```

- **show user-plane-service statistics analyzer name rtp**：RTP 関連の統計情報を表示するには、このコマンドを使用します。

```
RTP Session Stats:
   Total Uplink Bytes:               8   Total Downlink Bytes:        2851524
   Total Uplink Pkts:                2   Total Downlink Pkts:            2741

FastPath Statistics :
   Total FP Flows:                   1
   Total Uplink FP Bytes:            0   Total Downlink FP Bytes:     2850497
   Total Uplink FP Pkts:             0   Total Downlink FP Pkts:         2740
```

- **show user-plane-service statistics analyzer name rtcp**：RTCP 関連の統計情報を表示するには、このコマンドを使用します。

```
RTCP Session Stats:
      Total Uplink Bytes:            804   Total Downlink Bytes:            728
      Total Uplink Pkts:              16   Total Downlink Pkts:              13
```

- **show user-plane-service statistics analyzer name ftp**：FTP 関連の統計情報を表示するには、このコマンドを使用します。

```
FTP Session Stats:
   Current Control Sessions:         1        Current Data Sessions:         1
   Total Control Sessions:           1        Total Data Sessions:           3
   Uplink Control Bytes:           190        Downlink Control Bytes:      544
   Uplink Control Pkts:             23        Downlink Control Pkts:        15
```

```
   Uplink Data Bytes:               6733        Downlink Data Bytes:       12444

    Uplink Data Pkts:              5136         Downlink Data Pkts:           14
    Uplink Error Bytes:               0         Downlink Error Bytes:          0
    Uplink Error Pkts:                0         Downlink Error Pkts:           0
    Request Succeed:                 14         Request Failed:                0
    Unknown Requests:                 0         Unknown Responses:             0
    Uplink Bytes Retrans:             0         Downlink Bytes Retrans:        0
    Uplink Pkts Retrans:              0         Downlink Pkts Retrans:         0
    RETR commands:                    2         STOR commands:                 1
    Unknown packets received:                                                  0
    Data packet received without control connection:                           0
    Invalid packets:                                                           0
    Packets that could not be parsed:                                          0

  FastPath Statistics :
     Total FP Control Flows:          0
     Total FP Data Flows:             3
   Uplink :                                 Downlink :
     Total FP Control Pkts :          0       Total FP Control Pkts :        0
     Total FP Control Bytes :         0       Total FP Control Bytes:        0
     Total FP Data Pkts :             0       Total FP Data Pkts :           0
     Total FP Data Bytes :            0       Total FP Data Bytes:           0
```

- **show user-plane-service statistics analyzer name pptp**：PPTP 関連の統計情報を表示するには、このコマンドを使用します。

```
PPTP Session Stats:
  Total Uplink Bytes:              0   Total Downlink Bytes:             0
  Total Uplink Pkts:               0   Total Downlink Pkts:              0
  Total GRE Sessions:              0   Invalid PPTP Pkts:                0
  Unknown PPTP Pkts:               0

  PPTP-GRE Session Stats:
  Total Uplink Bytes:              0   Total Downlink Bytes:             0
  Total Uplink Pkts:               0   Total Downlink Pkts:              0
```

- **show user-plane-service statistics analyzer name h323**：H323 関連の統計情報を表示するには、このコマンドを使用します。

```
H323 Session Stats:
  Total Uplink Bytes              0       Total Downlink Bytes             0
  Total Uplink Packets            0       Total Downlink Packets           0
  Total H323 calls                0
  Total RAS messages              0
  Total Q931 messages             0
  Total H245 messages             0
```

  - **show user-plane-service statistics analyzer name h323 protocol ras**：H323 プロトコル RAS の統計情報を表示するには、このコマンドを使用します。

```
  Total RAS messages                  0
    RAS messages                             Uplink
     Downlink
    --------------                          ------------
  ------------
    GatekeeperRequest                          0
        0
    GatekeeperConfirm                          0
        0
    GatekeeperReject                           0
        0
    RegistrationRequest                        0
        0
```

```
 RegistrationConfirm                     0
     0
 RegistrationReject                      0
     0
 UnregistrationRequest                   0
     0
 UnregistrationConfirm                   0
     0
 UnregistrationReject                    0
     0
 AdmissionRequest                        0
     0
 AdmissionConfirm                        0
     0
 AdmissionReject                         0
     0
 LocationRequest                         0
     0
 LocationConfirm                         0
     0
 LocationReject                          0
     0
 DisengageRequest                        0
     0
 DisengageConfirm                        0
     0
 DisengageReject                         0
     0
 InfoRequest                             0
     0
 InfoRequestResponse                     0
     0
 RequestInProgress                       0
     0
 Unclassified                            0
     0
```

- **show user-plane-service statistics analyzer name h323**：H323 関連の統計情報を表示するには、このコマンドを使用します。

```
H323 Session Stats:
  Total Uplink Bytes              0       Total Downlink Bytes             0
  Total Uplink Packets            0       Total Downlink Packets           0
  Total H323 calls                0
  Total RAS messages              0
  Total Q931 messages             0
  Total H245 messages             0
```

  - **show user-plane-service statistics analyzer name h323 protocol h245** ：H323 プロトコル H245 の統計情報を表示するには、このコマンドを使用します。

```
 Total H245 messages                  0
  H245 messages                        Uplink
 Downlink
  -------------                      ------------
 ------------
  OpenLogicalChannel                          0
      0
  OpenLogicalChannelAck                       0
      0
  OpenLogicalChannelReject                    0
      0
  OpenLogicalChannelConfirm                   0
```

```
      0
 RequestChannelClose                        0
      0
 CloseLogicalChannel                        0
      0
 CloseLogicalChannelAck                     0
      0
 EndSessionCommand                          0
      0
 Unclassified                               0
      0
```

- **show user-plane-service statistics analyzer name h323 protocol q931** ：H323 プロトコル Q931 の統計情報を表示するには、このコマンドを使用します。

```
Total Q931 messages                  0
  Q931 messages                       Uplink
Downlink
  -------------                     ------------
-------------
  Alerting                                  0
      0
  CallProceeding                            0
      0
  Setup                                     0
      0
  Connect                                   0
      0
  ReleaseComplete                           0
      0
  Facility                                  0
      0
  Progress                                  0
      0
  Information                               0
      0
  Unclassified                              0
      0
```

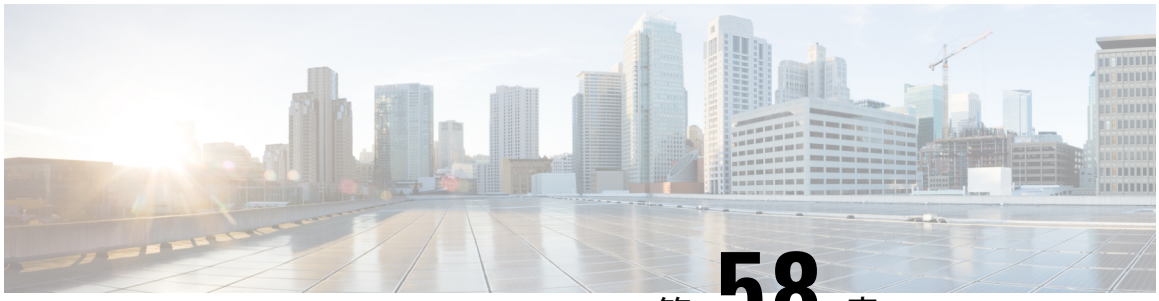
- **show user-plane-service statistics analyzer name tftp**：TFTP 関連の統計情報を表示するには、このコマンドを使用します。

```
TFTP Session Stats:
  Total Uplink Bytes:                0   Total Downlink Bytes:                0
  Total Uplink Packets:              0   Total Downlink Packets:              0
  Total Read Sessions:               0   Total Write Sessions:                0
  Total Invalid Control Packets:                                             0
  Total Invalid Data Packets:                                                0
  Total Packets with Unknown Request Type:                                   0

  TFTP DATA Session Stats:
  Total Uplink Bytes:                0   Total Downlink Bytes:                0
  Total Uplink Packets:              0   Total Downlink Packets:              0
```

- **show user-plane-service statistics analyzer name sip**：SIP 関連の統計情報を表示するには、このコマンドを使用します。

```
SIP Session Stats:
      Total Uplink Bytes:              0           Total Downlink Bytes:
0
      Total Uplink Pkts:               0           Total Downlink Pkts:
0
      Uplink Valid Pkts:               0           Downlink Valid Pkts:
```

```
0
      Uplink Retry Pkts:                0           Downlink Retry Pkts:
0
      Uplink Error Pkts:                0           Downlink Error Pkts:
0
      Total SIP Calls:                  0
SIP Advanced Session Stats:
  Total Uplink Bytes               0   Total Downlink Bytes               0
  Total Uplink Packets             0   Total Downlink Packets             0

  Total SIP Calls                  0   Current SIP Calls                  0
  Total SIP UDP Calls              0   Current SIP UDP Calls              0
  Total SIP TCP Calls              0   Current SIP TCP Calls              0

  SIP Request                          Total received         Total transmitted
        Retransmitted
  -----------                    --------------------      --------------------
  --------------------
  Register                                        0                         0
                 0
  Invite                                          0                           0
                   0
  Ack                                             0                           0
                   0
  Bye                                             0                           0
                   0
  Info                                             0                           0
                    0
  Prack                                           0                           0
                   0
  Refer                                           0                           0
                   0
  Cancel                                         0                           0
                  0
  Update                                         0                           0
                  0
  Message                                        0                           0
                 0
  Options                                         0                           0
                  0
  Publish                                           0                           0
                    0
  Subscribe                                      0                           0
                 0
  Notify                                            0                           0
                    0


  SIP Response                         Total received         Total transmitted
        Retransmitted
  ------------                   --------------------      --------------------
  --------------------
  1XX                                               0                           0
                     0
  2XX                                               0                           0
                     0
  3XX                                               0                           0
                     0
  4XX                                               0                           0
                     0
  5XX                                               0                           0
                     0
  6XX                                               0                           0
                     0
```



第 58 章

N:M 冗長性

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
このリリースでは、UP で SSH IP のインストールを無視するための新しい CLI がサポートされています。	21.26.7
最初の導入。	21.24 より前

機能説明

CUPS ユーザープレーン（UP）は、サブスクライバのデータトラフィックを伝送および固定するコアネットワーク内の非常に重要なネットワークコンポーネントです。スムーズな Quality of Experience（QoE）を実現するには、データトラフィックを維持し、最小限の中断で続行する必要があります。これは、UP でホストおよびアンカーされているすべてのデータセッションに対して堅牢な冗長性メカニズムが提供されている場合にのみ実現可能です。

すべての UP には、スタンバイ（ウォーム、ホット、またはアクティブ）の冗長 UP が必要ですが、このモデルは、サービスプロバイダーに求められるリソース要件が多く、水平方向にスケーリングを維持できる UP の数の点からも、推奨されるモデルではありません。推奨されるモデルは、すべてのアクティブ UP のスタンバイ UP として機能する複数の UP を持つ N:M モデルです。N:M 冗長性機能は、この冗長性モデルを提供します。

UP には、Redundancy and Configuration Manager（RCM）と呼ばれるシスコ独自の新しいノードがあり、UP の設定管理と冗長性機能を処理します。

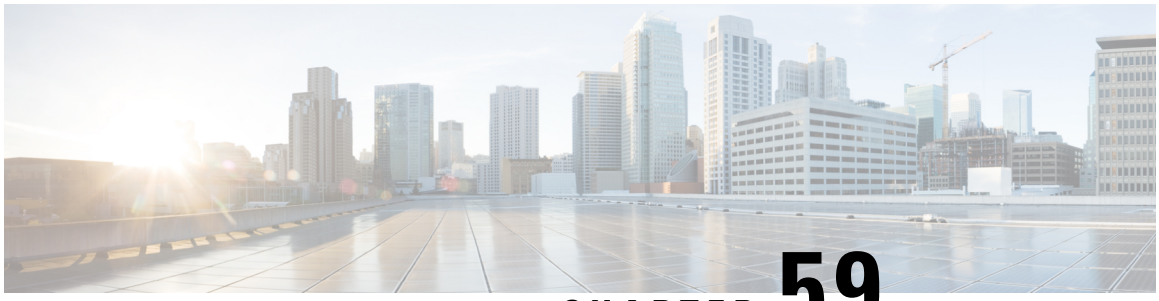
N:M 冗長性および RCM の詳細については、Redundancy and Configuration Manager コンフィギュレーションおよびアドミニストレーション ガイド [英語] を参照してください。

SSH IP インストールの無視の設定

UP で SSH IP のインストールを無視するには、次の設定を使用します。

```
configure
  context context_name
    redundancy-configuration-module module_name
      ignore-ssh-ip
      end
```

（注） この CLI が設定されていない場合、デフォルトでは NSO SSH IP が通常どおり UP で設定されます。



CHAPTER 59

Netloc と RAN/NAS 原因コード

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

Netloc と RAN/NAS 原因コード機能は、非 CUPS アーキテクチャでサポートされています。このリリースでは、この機能は CUPS アーキテクチャで認定されています。

この機能は、アクセスネットワークから PCRF に RAN や NAS の詳細なリリース原因コード情報を送信するために使用されます。

この機能は 3GPP TS 29.212 のリリース 12 の仕様に準拠しています。

サポートされている機能「netloc-ran-nas-code」および「netloc」が有効になっている場合、netloc-ran-nas-cause コードは CCR-U/CCR-T メッセージを介して PCRF に送信されます。

NetLoc-RAN-NAS-Cause をサポートする機能が有効になっており、RAN や NAS の原因がアクセス側から受信されると、Charging-Rule-Report AVP および CCR-T では、ベアラーおよびセッション削除イベントで Diameter AVP「RAN-NAS-Release-Cause」がそれぞれ追加されます。

NetLoc-RAN-NAS-Cause をサポートする機能が有効になっており、Netloc がアクセス側から受信されると、CCR-U および CCR-T では、 Diameter AVP で送信されたネットワークロケーショ

ン「3GPP-User-Location-Info」および「3GPP-MS-TimeZone」がベアラーやセッションイベントの作成、更新、削除でそれぞれ追加されます。

Netloc および RAN/NAS 原因コードの設定

この機能を有効にするには、次の設定を使用します。

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
        diameterencode-supported-featuresnetloc-ran-nas-cause
        end
```

注：

- **netloc-ran-nas-cause**：Netloc-RAN-NAS-Cause 機能を有効にします。この機能はサポートされますが、デフォルトでは無効になっています。
- サポートされている機能である [netloc-ran-nas-code] と [netloc] を有効にすると、netloc-ran-nas-cause コードが PCRF に送信されます。
- このサポートされている機能を無効にするには、次のコマンドを使用します。

  [default | no] diameter encode-supported-features

- この機能は、標準 Gx ディクショナリ（r8-gx-standard および dpca-custom8）でのみサポートされます。

第 60 章

ネットワーク提供ロケーションの表示

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

この機能により、P-GW は、TWAN-Identifier AVP、User-Location-Info-Time AVP（使用可能な場合）、S2a/S2b の場合は UE-Local-IP-Address AVP 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。

重要 Network Provided Location Indication（NPLI）は、非 CUPS アーキテクチャでサポートされている既存の機能です。このリリースでは、この機能が CUPS アーキテクチャで認定されました。詳細については、『*SAEGW Administration Guide*』[英語] の「*NetLoc for WiFi EPC*」の章を参照してください。

機能の仕組み

ベアラーの非クティブ化または UE 切断手順中に、P-GW は、TWAN-Identifier AVP 内の PCRF へのアクセスネットワーク情報と、User-Location-Info-Time AVP や UE-Local-IP-Address AVP（S2a/S2b に応じて）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、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 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。

注：CUPS では、専用ベアラーが PCRF によって作成されると、CBRsp が OCS サーバーへの CCR-I（新しいベアラーの場合は NSAPI）をトリガーするのを待ちます。この時点までこのベアラーは使用されないため、P-GW は古いアクセス側の情報を含む CCR-I を送信し、更新されたアクセス側の情報を含む新しい CCR-U をその後に送信する代わりに、更新されたアクセス側の情報を含む CCR-I メッセージを 1 つ送信します。

サポートされる機能

CBRes/DSReq/UBRes/DBC/DBRes で送信される Netloc は、Gx、Gy、および Gz インターフェイスでサポートされます。NPLI 機能は、次に対してサポートされます。

- Pure-P、Collapsed、および Pure-S セッション
- Wi-Fi セッション
- S-GW の再配置
- セッションリカバリ

制限事項

NPLI 機能には、次の制限事項があります。

- GnGp ハンドオーバーのシナリオはサポートされていません。
- UBRes の Netloc に変更がある場合、タイムゾーン変更用の CDR は生成されません。

- DSReq の Netloc に ULI の変更がある場合、CDR の serviceConditionChange は空白になります。

第 61 章

ネクストホップ転送サポート IPv4/v6 アドレス

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

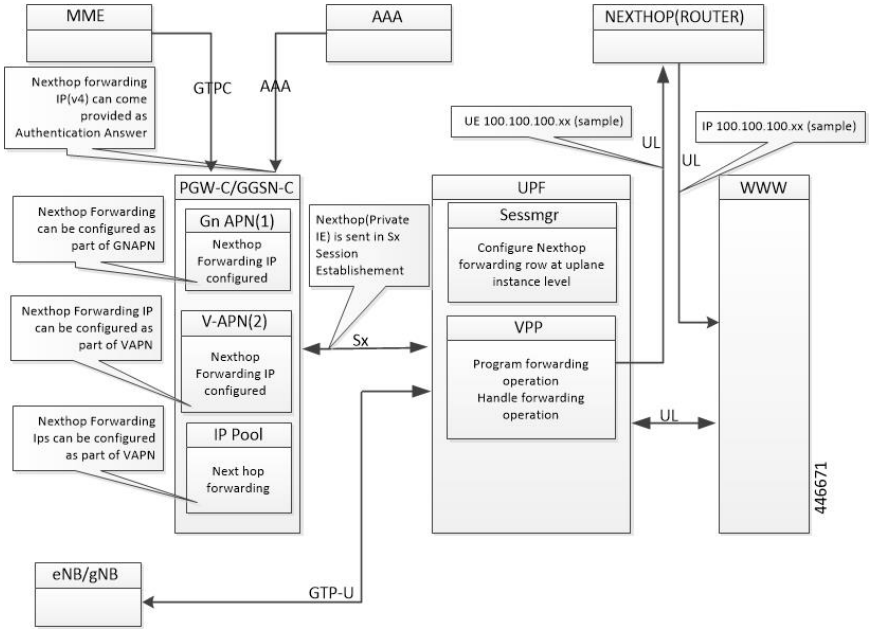
CUPS UPF のアップリンク方向では、UE IP と GI IP が異なるサブネットにある場合があり、それに応じてアップリンクパケット転送を許可するようにルーティングパスが定義されます。

機能の仕組み

アーキテクチャ

次の図は、EGCI ベースの P-GW UP 選択ソリューションの概要を示しています。

図 *33 :* ネクストホップ転送



設定の優先順位

設定	優先順位
AAA（IPv4 のみ）	1
APN（Gn/VAPN）	2
IP プール	3

構成の使用例

ケース	IP タイプ	AAA	APN	IP プール	ネクストホップ IP の選択
AAA を介した AA メッセージでのみ供給されるネクストホップ	IPv4	209.165.200.225	未設定	未設定	ネクストホップアドレスは AAA から選択される： IPv4：209.165.200.225 IPv6：NA
	IPv6	サポート対象外	未設定	未設定	

ケース	IP タイプ	AAA	APN	IP プール	ネクストホップ IP の選択
APN および IP プールで設定された AAA + IPv4 を介した AA メッセージで供給されるネクストホップ	IPv4	209.165.200.225	209.165.201.1	50.50.50.50	ネクストホップアドレスは AAA から選択される： IPv4：209.165.200.225 IPv6：NA
	IPv46	サポート対象外	未設定	未設定	
APN のみで設定された IPv4 および IPv6	IPv4	設定なし	209.165.201.1	設定なし	ネクストホップアドレスは APN から選択される： IPv4：209.165.200.225 IPv6：9001::3
	IPv6	サポート対象外	9001::3	設定なし	
IP プールのみで設定された IPv4 および IPv6	IPv4	未設定	未設定	50.50.50.50	ネクストホップアドレスは IP プールから選択される： IPv4：209.165.200.225 IPv6：5002::5
	IPv6	未設定	未設定	5002::5	
APN および IP プールで設定された AAA + IPv4 および IPv6 を介して使用可能な IPv4	IPv4	209.165.200.225	209.165.201.1	50.50.50.50	ネクストホップ IPv4 は AAA から選択される：209.165.200.225 ネクストホップ IPv6 は APN から選択される：9001::3
	IPv6	未サポート	9001::3	5002::5	
IP プールで設定された AAA + IPv4 および IPv6 を介して使用可能な IPv4	IPv4	209.165.200.225	設定なし	50.50.50.50	ネクストホップ IPv4 は AAA から選択される：209.165.200.225 ネクストホップ IPv6 は IP プールから選択される：5002::5
	IPv6	未サポート	設定なし	5002::5	
APN で設定された AAA + IPv4 および IPv6 を介して使用可能な IPv4	IPv4	209.165.200.225	209.165.201.1	設定なし	ネクストホップ IPv4 は AAA から選択される：209.165.200.225 ネクストホップ IPv6 は APN から選択される：9001::3
	IPv6	未サポート	9001::3	設定なし	

インターフェイス

次のプライベート IE が SX セッション確立メッセージに導入されます。

238	PFCP_IE_NEXTHOP	PFCP_IE_NEXTHOP								Sx セッション確立要求	プライベート IE：CUPS：ネクストホップ転送のサポート：IPv4IPv6 アドレス
		ビット									
		オクテット	7	6	5	4	3	2	1		
		1 ～ 2	タイプ = 238（10 進数）								
		3 ～ 4	長さ = n								
		5 ～ 10	PFCP_IE_NEXTHOP_ID								
		11 ～ 14	PFCP_IE_NEXTHOP_IP								

<table>
<tr>
<td>2
3
9</td>
<td>PFCP
_IE_
NEXTHOP
_ID</td>
<td colspan="8">PFCP_IE_NEXTHOP_ID</td>
<td>1 に送信します。Sx セッション確立要求の Create FAR IE 内</td>
<td rowspan="6">プライベート IE：CUPS：ネクストホップ転送のサポート：IPv4/IPv6 アドレス</td>
<td rowspan="6"></td>
</tr>
<tr>
<td colspan="8">ビット</td>
<td>2 に送信します。Sx セッション確立要求の PFCP
_IE_
NEXTHOP IE 内</td>
</tr>
<tr>
<td>オクテット</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td rowspan="4">Sx セッション確立要求の PFCP
_IE_
NEXTHOP</td>
</tr>
<tr>
<td>1 ～ 2</td>
<td colspan="8">タイプ = 239（10 進数）</td>
</tr>
<tr>
<td>3 ～ 4</td>
<td colspan="8">長さ = 5</td>
</tr>
<tr>
<td>5 ～ 10</td>
<td colspan="8"></td>
</tr>
</table>

240	PFCP_IE_NEXTHOP_IP	PFCP_IE_NEXTHOP_IP									
		ビット								Sx セッション確立要求の PFCP_IE_NEXTHOP	プライベート IE：CUPS：ネクストホップ転送のサポート：IPv4/IPv6 アドレス
		オクテット	7	6	5	4	3	2	1		
		1 ～ 2	タイプ = 240（10 進数）								
		3 ～ 4	長さ = n								
		5	予備					V4	V6		
		m ～ m+3	IPv4 アドレス								
		p ～ p+15	IPv6 Address								

ネクストホップ転送サポート IPv4/IPv6 アドレスの設定

APN Configuration モードでのネクストホップ転送の設定

APN でネクストホップ転送を設定するには、次の CLI コマンドを使用します。

```
configure
  context context_name
    apn apn_name
     nexthop-forwarding-address { ipv4v6_address | ipv4_address | ipv6_address
}
      no nexthop-forwarding-address
      end
```

注：

- **no**：ネクストホップ転送アドレスの設定を無効にします。
- **nexthop-forwarding-address {** *ipv4v6_address* | *ipv4_address* | *ipv6_address* **}**：この APN のネクストホップ転送アドレスを設定します。
  - *ipv4_address* で IPv4 アドレスを設定します。
  - *ipv6_address* で IPv6 アドレスを設定します（コロン区切りの 16 進表記をサポート）。

IP プールでのネクストホップ転送の設定

APN でネクストホップ転送を設定するには、次の CLI コマンドを使用します。

```
configure
   context context_name
      [ no ] ip pool ipv4-public nexthop-forwarding-address  ipv4_address

      [ no ] ip pool ipv6-public nexthop-forwarding-address  ipv6_address

      end
```

注：

- **no**：ネクストホップ転送アドレスの設定を無効にします。
- **nexthop-forwarding-address** *ipv4_address* | *ipv6_address*：このプールの IPv4 アドレスネクストホップ転送アドレスを設定します。
- **nexthop-forwarding-address** *ipv6_address*：このプールの IPv6 アドレスネクストホップ転送アドレスを設定します。

AAA を介したネクストホップ転送の設定

ネクストホップ転送アドレスは、AAA を使用して設定できます。このオプションを使用すると、外部で設定できます。

ネクストホップ転送の外部設定：

```
RADIUS AUTHENTICATION
  Access-Accept
   Subscriber-Nexthop-Address
```

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングと障害対応に使用できる CLI コマンドについて説明します。

show コマンドと出力

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show apn name<apn_name>

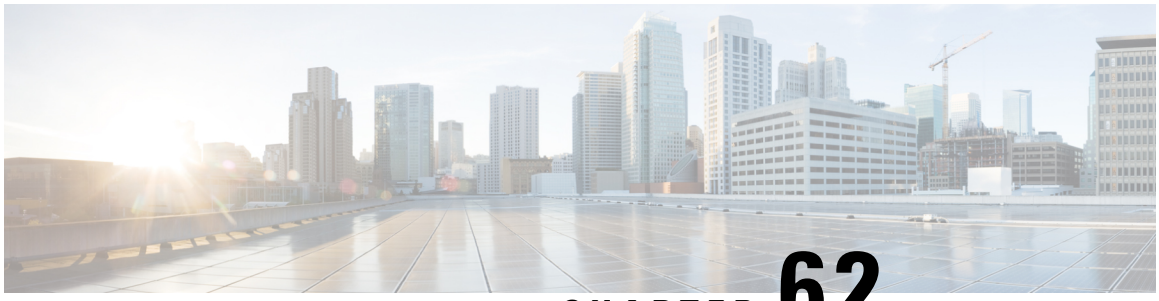
この show コマンドの出力範囲が拡張され、この機能をサポートするために導入された次のフィールドが含まれるようになりました。

- nexthop gateway addr：設定されているネクストホップ ゲートウェイ アドレスを表示します。

show subscriber user-plane-only full all

この show コマンドの出力範囲が拡張され、この機能をサポートするために導入された次のフィールドが含まれるようになりました。

- Next Hop Ip Address：設定されているネクストホップ IP アドレスを表示します。



CHAPTER 62

ネットワークトリガーによるサービスの復元

機能説明

Network Triggered Service Restoration（NTSR）機能は、S-GW で有効になっている場合に MME 障害を検出します。障害が発生した MME のサービスを受けるサブスクライバがダウンリンクデータパケットを受信すると、S-GW はラウンドロビン方式で NTSR プールから代替 MME を選択します。S-GW は、選択した MME にダウンリンクデータ通知（DDN）を送信します。このラウンドロビン方式による MME の選択は、システム全体ではなく、セッションマネージャインスタンスごとに行われます。

NTSR 機能により、MME 障害発生時のネットワークにおける DDN メッセージのロードバランシングが向上します。

CUPS モードでは、復元の対象となるベアラー、対応するダウンリンクデータがユーザープレーンにバッファリングされます。復元が設定されていないベアラーの場合、対応するトラフィックエンドポイントはユーザープレーンから削除されます。

特定の PDN から専用ベアラーが保持されていることを S-GW が検出した場合、S-GW はこの PDN のデフォルトベアラーも保持します。この場合、ダウンリンクデータはデフォルトベアラーでドロップされます。

復元保留状態でダウンリンクデータ/ベアラー更新要求/ベアラー作成要求を受信すると、SGW は MME または S4-SGSN に対して DDN 要求イベントを開始します。

MME からベアラー変更要求を受信すると、コントロールプレーンは、ユーザープレーンに Sx セッション変更要求を送信します。このとき、復元の対象となるすべてのベアラーに対して UPDATE FAR:APPLY ACTION:FORW=1 とします。

NTSR の設定

NTSR 機能には、次の設定があります。

- APN プロファイルの設定
- ピアプロファイルの設定（入力）
- NTSR プールの設定
- S-GW サービスアクセスピアマップの関連付け
- MME 復旧タイマーの設定

APN プロファイルの設定

この設定では、QCI 値と ARP 値を APN プロファイルに設定します。S-GW の入力側でパス障害が検出されると、設定された ARP/QCI 値に基づいてベアラーが保持または解放されます。S-GW では、APN プロファイルごとに最大 2 つの QCI と ARP ウォーターマークの組み合わせを設定できます。

APN プロファイルで ARP 値と QCI 値を設定するには、次のコマンドを使用します。

```
configure
  apn-profile profile_name
    ntsr { all | qci qci_value | arp-priority-watermark arp_value }
    end
```

注：

- **ntsr**：NTSR 設定を指定します。
- **qci**：NTSR の QCI 値を指定します。
- **arp-priority-watermark**：NTSR の ARP 値を指定します。
- **all**：MME 復元用の QCI 値または ARP 値を持つすべてのベアラーを識別します。

ピアプロファイルの設定（入力）

この設定では、ピアプロファイルはS-GWの入力側で設定されます。ピアプロファイルには、MME 障害発生後に MME/S4-SGSN プールを検出するために使用される、関連付けられたプール ID が含まれています。

次のコマンドを使用して、S-GW の入力側でピアプロファイルを設定します。

```
configure
  peer-profile service-type sgw-access name name
    ntsr pool-id pool_id
    end
```

注：

- **sgw-access**：S4/S11 インターフェイスに対する S-GW のピアノードのプロファイルを設定します。
- **ntsr**：NTSR 設定を指定します。
- **pool-id**：MME 障害発生後に MME/S4-SGSN プールを検出するためのプール ID を指定します。*pool_id* は、1 ～ 10 までの整数です。

NTSR プールの設定

NTSR プールの設定は、プール ID およびピアタイプに関連付けられた IP アドレスのプールを設定するために使用されます。1 つのピアタイプに 1 つのプール ID を使用できます。NTSR プールに、IPv4 または IPv6 アドレスを組み合わせて指定できます。S-GW は、最大 10 の NTSR プール、および最大 5 の IPv4v6 IP アドレスペアを指定して設定できます。

NTSR プールを設定するには、次の設定を使用します。

```
configure
  ntsr-pool pool-id pool_id peer-type [ mme | s4-sgsn ]
    [ no ] peer-ip-address { ipv4-address ipv4_address | ipv6-address
ipv6_address }
    end
```

注：

- **pool-id**：NTSR プール ID を指定します。
- **peer-type**：NTSR プール ID ピアタイプを指定します。ピアタイプは MME または S4-SGSN です。
- **peer-ip-address**：MME または S4-SGSN プールの一部として IPv4 アドレスまたは IPv6 アドレスを設定します。

S-GW サービスアクセスピアマップの関連付け

この設定では、S-GW サービスのアクセス側または入力側のピアマップが設定されます。

ピアマップを S-GW サービスに関連付けるには、次の設定を使用します。

```
configure
  context context_name
    sgw-service service_name
      associate access-peer-map peermap_name
      end
```

注：

- **access-peer-map**：S-GW サービスのアクセス/入力側のピアマップを設定します。

モニタリングおよびトラブルシューティング

show コマンドの入力と出力

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show apn-profile full all

このコマンドの出力には、この機能をサポートする次のフィールドが表示されます。

- NTSR
  - QCI
  - ARP-priority-watermark

show apn-profile full name *apn_name*

このコマンドの出力には、この機能をサポートする次のフィールドが表示されます。

- NTSR
  - QCI
  - ARP-priority-watermark

show ntsr-pool all

このコマンドの出力には、この機能をサポートする次のフィールドが表示されます。

- SGW NTSR プール
- NTSR プール ID
- NTSR プールタイプ
- NTSR プール ID
- NTSR プールタイプ

show ntsr-pool full all

このコマンドの出力には、この機能をサポートする次のフィールドが表示されます。

- NTSR pool-id
- NTSR Pool type
- peer-address-pair(s)

show ntsr-pool full pool-id *pool_id*

このコマンドの出力には、この機能をサポートする次のフィールドが表示されます。

- NTSR プール ID
- NTSR プールタイプ
- ピアアドレスペア

show ntsr-pool pool-id *pool_id*

このコマンドの出力には、この機能をサポートする次のフィールドが表示されます。

- NTSR pool-id
- NTSR Pool type

show sgw-service statistics all

このコマンドの出力には、この機能をサポートする次のフィールドが表示されます。

- ピアの障害
  - 保持
  - リストア済み
  - リリース日
- ピアの再起動
  - 保持
  - リストア済み
  - リリース日

show subscribers sgw-only full all

このコマンドの出力には、この機能をサポートする次のフィールドが表示されます。

- NTSR state
- Bearer capable restoration

show subscribers sgw-only full all

第 63 章

NSO ベースの設定管理

機能説明

4G CUPS の Cisco Network Service Orchestrator（NSO）ベースの設定管理は、以下をサポートします。

- Cisco Virtual Network Function（VNF）デバイスのオンボーディング：CP、UP、および RCM
- Day-N、Day-1、および Day-0.5 CUPS 設定プッシュ用の 4G ベース CP、UP、および RCM の一元的な設定管理
  - Day-0.5 は、RCM を使用する N:M UP 冗長性スキームに適用されます。Day-0.5 設定は、UP の RCM との通信を目的としているため、そのロールを定義し、適切な設定を後からプッシュできるようになっています。

NSO 自動化を使用した 4G CUPS 展開の顧客構成管理の管理は、再利用性、標準的な通知管理、および体系的なデバイス構成ガバナンスといった機能性も発揮します。

使用例

NSO 設定処理は、次の使用例に対応します。

1. 管理 IP を使用してすでに展開されている VNF（CP、UP、および RCM）の NSO オンボーディング：
   - すでに実行されている VNF（CP、UP、および RCM）をデバイスとして NSO にオンボーディングし、事後チェックを実行して、デバイスの到達可能性と機能を確認しま

す。これは、設定をプッシュまたは同期し、通知の通信を確立するための準備手順です。

VNF デバイスのオーケストレーション（インスタンス化と破棄）は個別のモジュールであり、設定モジュールに依存しません。デバイスをオンボーディングし、設定管理をサポートするには、特定の詳細（IP、ポート、管理ユーザー名/パスワード）が必要です。

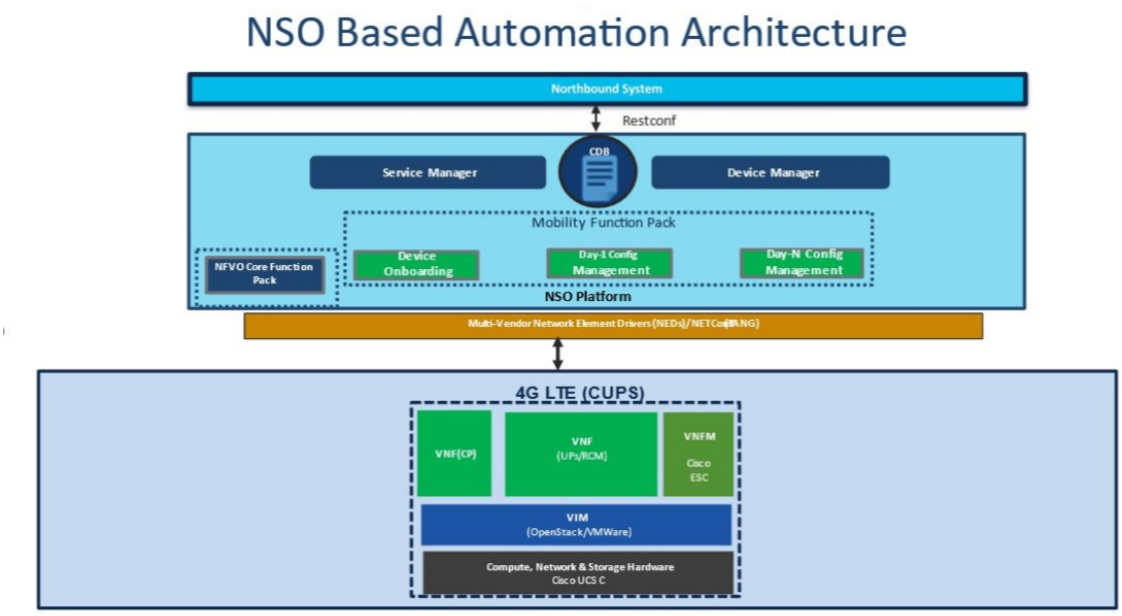
2. CP、UP、および RCM のネイティブ設定またはデバイステンプレートの保存を許可します。
   - RESTCONF/NSO-CLI を介してインターフェイスを提供し、論理名を持つデバイスの再利用可能な設定を管理します。また、ネットワーク SME やオペレータが設定を作成、変更、削除、無効化/有効化できる柔軟性を提供します。目的は、それらのアクティブな設定を選択し、CP、UP、および RCM の Day-0.5、Day-1、または Day-N の一部としてデバイスセットに適用することです。
3. デバイス論理グループ（CP/UP/RCM を含む）またはターゲットデバイスのカスタムリストに Day-N/Day-1/Day-0.5 設定を適用するための CLI/REST インターフェイスを提供します。
   - RESTCONF/NSO-CLI を介してネットワーク SME やオペレータにインターフェイスを提供し、Day-N/Day-1/Day-0.5 の設定を単一または一連のデバイス（CP、UP、または RCM）にプッシュします。このインターフェイスには、エンドユーザーに対する設定のプッシュの進行状況に関する通知やステータスが表示されます。
4. デバイスごとの設定管理のロジスティック管理（Day-N、Day-1、または Day-0.5 プッシュ）：
   - ダッシュボードユーティリティを提供し、デバイスごとに設定ログを管理します。このログは、デバイスで実行された最新のアクティビティを把握するのに役立ちます。
5. 5.（N:M の場合）RCM 通知管理の通知フレームワークを構築し、Day-N、Day-1、および Day-0.5 に関する UP への設定のプッシュを自動化します。
   - NSO で通知フレームワークを構築して、ステータスの変更に関する RCM NETCONF 通知をリッスンし、シナリオに基づいて設定を自動的にプッシュします。

機能の仕組み

-

アーキテクチャ

次の図は、ソリューションに関連するコンポーネントとフレームワークの概要を示しています。



RCM と NSO

N:M UP 冗長性シナリオでは、NSO が設定を管理している間、RCM は引き続き UP のロール（アクティブまたはスタンバイ）の調停を行い、アクティブ UP のスイッチオーバーを処理するため、このソリューションでは、設定機能が RCM から NSO に移動されるだけで、RCM は引き続き必要です。RCM の詳細については、RCM コンフィギュレーションおよびアドミニストレーション ガイド [英語] を参照してください。

コンポーネント

Cisco 4G CUPS VNF の導入と設定のワークフローは、NSO から実行されます。次に、NSO の重要なコンポーネントの一部を示します。

- **NSO デバイスマネージャ**：各 VNF コンポーネント（CP、UP、RCM）を管理し、各デバイス設定のコピーを保持し、デバイス設定プッシュの整合性を管理します。
- **NSO サービスマネージャ**：カスタマー/ユーザー入力の高レベルの抽象化ネットワークサービスモデルを定義する YANG 標準を提供します。
- **CDB**：ネットワーク設定と運用データを保存するための永続的な設定データベース。
- **モビリティ機能パック**：4G CUPS ベースの VNF オーケストレーションと設定を管理するためにカスタム構築された NSO パッケージ。
- **NFVO コア機能パック**：NSO コア NFV FP は、シスコまたは他のサードパーティの VNFM および VIM（OpenStack/VMWare など）と通信して VNF を展開するためのドライバソフトウェアです。

- **StarOS NSO NED**：設定をプッシュするために Cisco 4G CUPS VNF と接続する StarOS ベースの NSO ネットワーク エレメント ドライバ（NED）。この NED は Cisco CLI をベースとしています。StarOS NSO NED は、セキュアシェル（SSH）を使用して StarOS 管理 CLI インスタンスと通信します。
- **RCM NSO NED**：RCM ベースの NETCONF NED は、設定管理のために RCM デバイスと通信する際に使用されます。

プラットフォーム、ハードウェア、およびソフトウェアの最小要件

以下に、一元化された設定管理をサポートするためのプラットフォームおよびソフトウェアの最小要件を示します。

- サポートされるオーケストレータ：NSO
- 次のネットワーク要素の設定管理：
  - RCM：冗長性と設定の管理
  - VPC-SI：4G CUPS CP または UP として
  - VPC-DI：4G CUPS CP としてのみ
- 最小ハードウェア要件：
  - VM CPU：CPU コア x 8
  - VM RAM：基準は 16 GB RAM、サポートする StarOS デバイスごとに + 10 MB RAM
  - VM 接続：10 GBps ネットワークリンク x 1。これは、個別の VLAN またはその他のメカニズムを使用して、NSO HA と構成/展開の両方に使用できます。
  - VM ストレージ：100 GB ディスク（SSD を推奨）
- 最小ソフトウェアのバージョン

ソフトウェア	最小バージョン
Cisco NSO	6.1.6.1
StarOS NSO NED	5.52.4
Cisco NSO HCC	6.0.1
モビリティ機能パック	3.5

（注） UP、CP、および RCM で推奨される StarOS ソフトウェア イメージ バージョンは、リリース 21.23 以降です。リリースバージョンは密接に結合されておらず、NED のみに依存します。

ライセンス

NSOベースの設定管理は、ライセンスに基づくシスコの機能です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

NSO のインストール

コール フロー

この項では、4G CUPS 設定管理機能の主要なコールフローについて説明します。

コールフローは、「connect」、「sync-from」などの NSO プリミティブを参照します。プリミティブの詳細については、NSO ユーザーガイド [英語] を参照してください。

（注） 次のコールフロー図では、「NSO ノースバウンド」は NCS CLI または RESTCONF インターフェイスを意味します。

既存の 4G CUPS VNF の NSO へのオンボーディング

この項では、既存の 4G CUPS デバイスを NSO に追加するためのフローについて説明します。

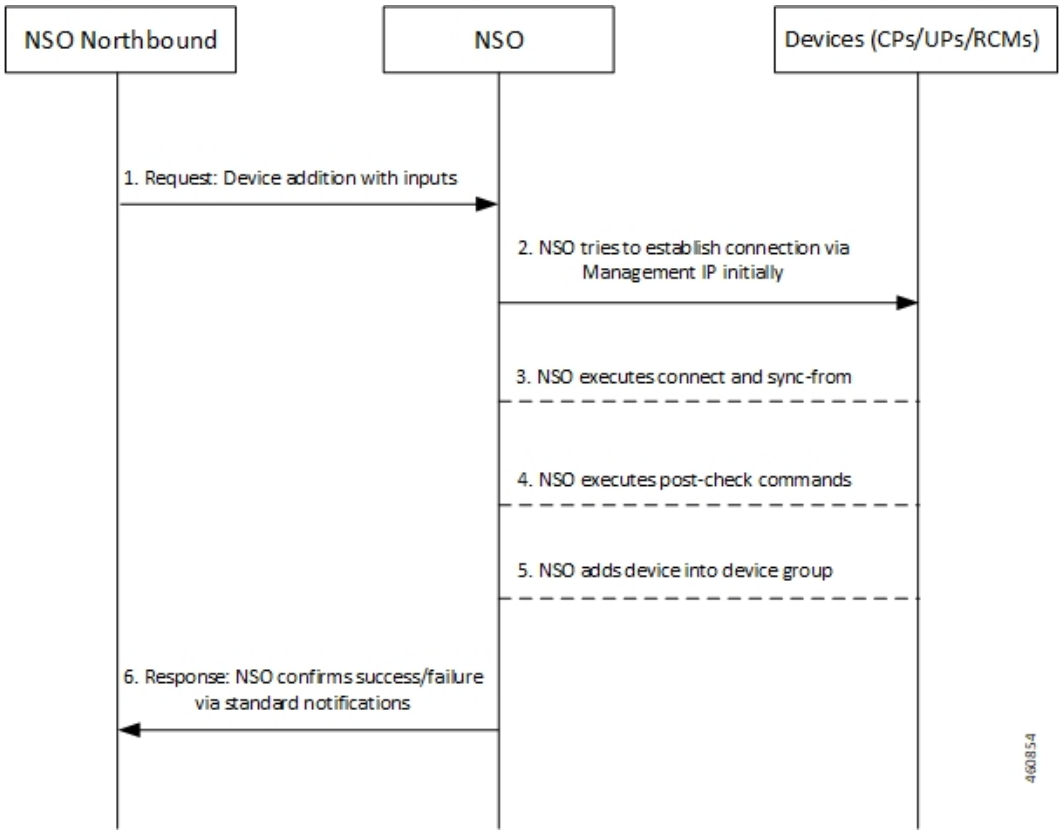


表 *32 :* コール フローの説明

ステップ	説明
1	NSO ノースバウンドが、デバイスをデバイスグループに追加するための要求を NSO に送信します。 デバイスグループは、ほぼ同一の設定を共有するデバイス（VNF）の論理グループなので、場合によっては設定が簡素化されます。
2	NSO が最初に管理 IP を介して接続を確立しようとします。
3	NSO が connect および sync-from コマンドを実行します。 NSO がデバイス上の正確な設定を認識できるように、sync-from 操作によりデバイスや VNF から既存の設定がプルされて NSO に入力されます。デバイス設定は sync-from では変更されません。
4	NSO が post-check コマンドを実行します。
5	NSO がデバイスをデバイスグループに追加します。
6	標準通知を介したデバイスの追加の成功や失敗について、NSO が NSO ノースバウンドを更新します。

4G CUPS デバイス設定のプッシュ：手動

この項では、4G CUPS デバイスの手動設定のプッシュに関するフローについて説明します。

このシナリオは、スタンドアロンまたは1:1冗長構成のCP、UP、またはRCMに当てはまります。

設定をプッシュする前に、デバイスをオンボーディングする必要があります。既存の4G CUPS VNF の NSO へのオンボーディング （547 ページ）を参照してください。

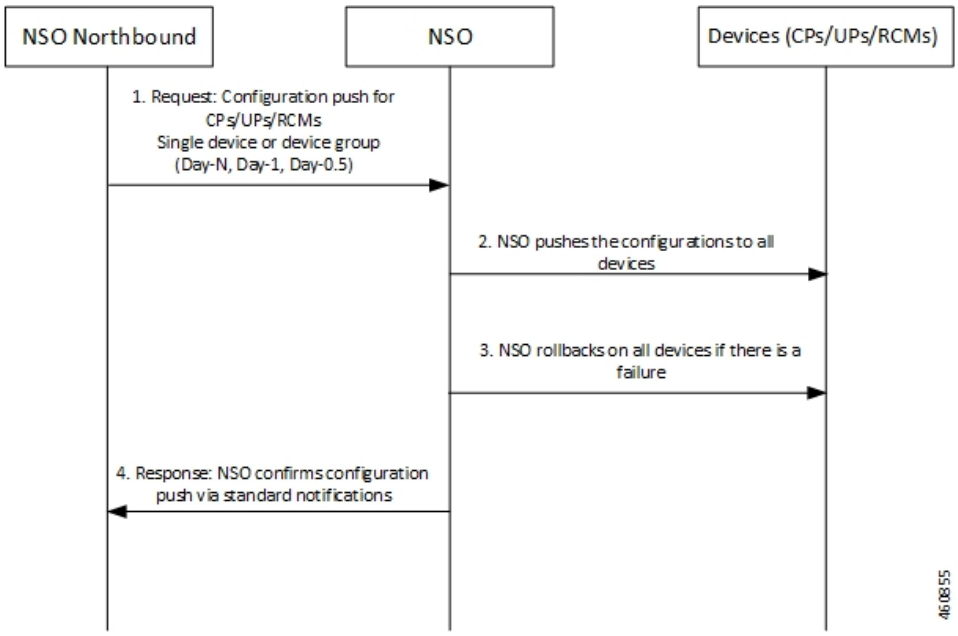


表 *33 :* コール フローの説明

ステップ	説明
1	NSO ノースバウンドが、CP、UP、RCMなどのデバイスにおける設定のプッシュを NSO に要求します。デバイスは、単一のデバイスまたはデバイスグループ（Day-N、Day-1、Day-0.5）を指定できます。
2	NSO がすべてのデバイスに設定をプッシュします。
3	障害が発生した場合、NSOがすべてのデバイスの設定をロールバックします。ロールバック操作により、デバイスに適用された設定が元に戻り、デバイスが以前の状態（設定を適用する前）に復元されます。
4	NSO が、標準通知を介して設定のプッシュに関して NSO ノースバウンドを更新します。

N:M 冗長性での NSO から 4G CUPS UP への設定のプッシュ：自動化

ここでは、NSO から 4G CUPS デバイスへの自動設定プッシュのフローについて説明します。

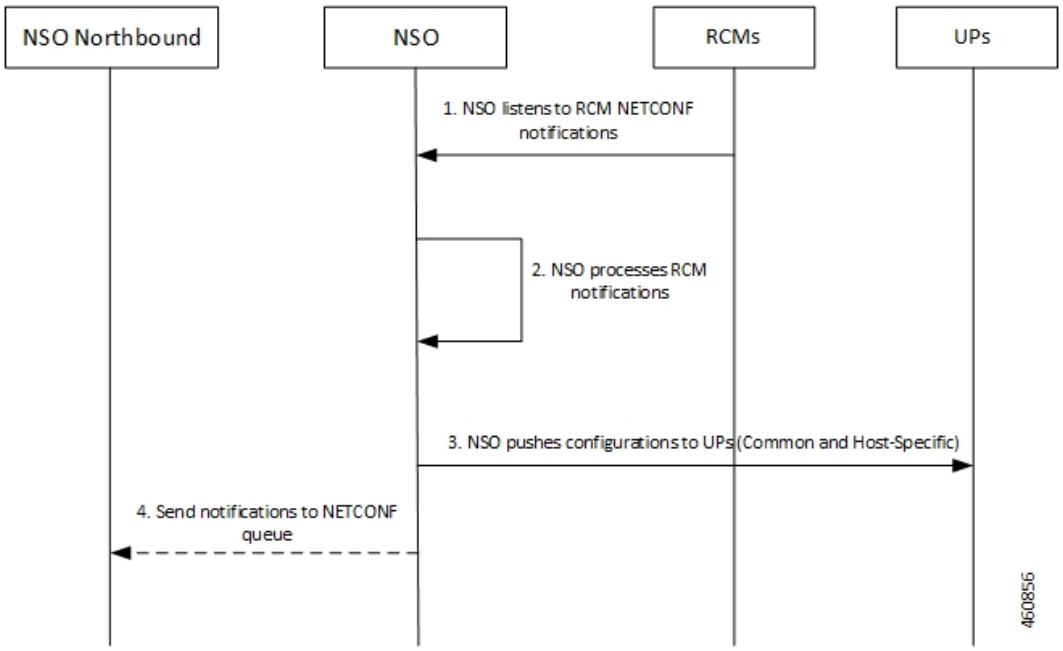


表 *34 :* コール フローの説明

ステップ	説明
1	NSO は RCM NETCONF 通知をリッスンします。 UP が RCM に接続すると、RCM は UP のロール（アクティブまたはスタンバイ）を判断します。このロールは通知で伝えられます。UP にプッシュされる設定は、そのロールによって異なります。そのため、自動設定プッシュは RCM 通知に基づいて実行されます。
2	NSO は受信した RCM 通知を処理します。
3	NSO は共通設定およびホスト固有の設定を UP にプッシュします。 共通設定とは、冗長グループ内のすべての UP で共有される設定を指します。これは通常、Enhanced Charging Service（ECS）と Access Point Name（APN）の設定です。ホスト固有の設定は、アクティブ UP に固有です。各アクティブ UP には、ホスト固有の設定が必要です。スタンバイ UP はアクティブ UP を引き継ぐ必要があるため、すべてのスタンバイ UP にはすべてのアクティブ UP のホスト固有の設定が必要です。
4	NSO は NETCONF キューに通知を送信します。

設定メタデータの事前入力

ここでは、設定メタデータの事前入力フローについて説明します。

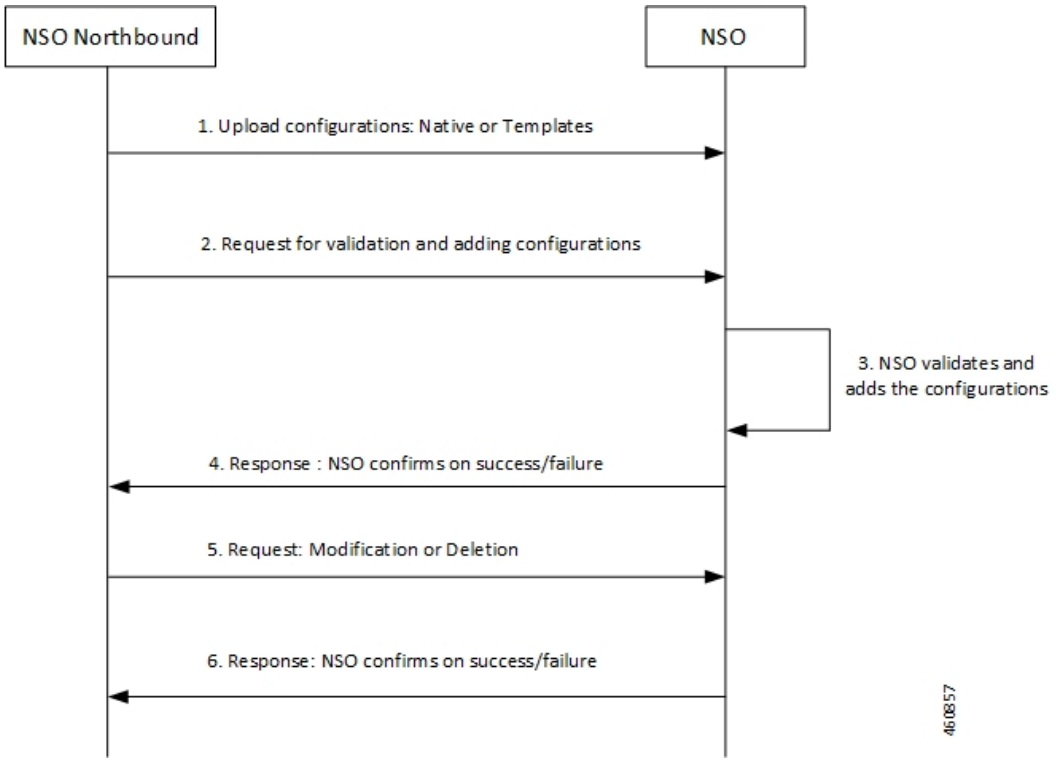


表 *35 :* コール フローの説明

手順	説明
1	NSO のノースバウンドが、設定（ネイティブまたはテンプレート）を NSO にアップロードします。
2	NSO のノースバウンドが、設定の検証と追加を NSO に要求します。
3	NSO が設定を検証して追加します。
4	デバイス追加の成功または失敗について NSO が NSO のノースバウンドを更新します。
5	NSO のノースバウンドが、設定の変更または削除を NSO に要求します。
6	成功または失敗について NSO が NSO のノースバウンドを更新します。

NSO HA スイッチオーバーの処理

この項では、NSO HA スイッチオーバーの処理フローについて説明します。

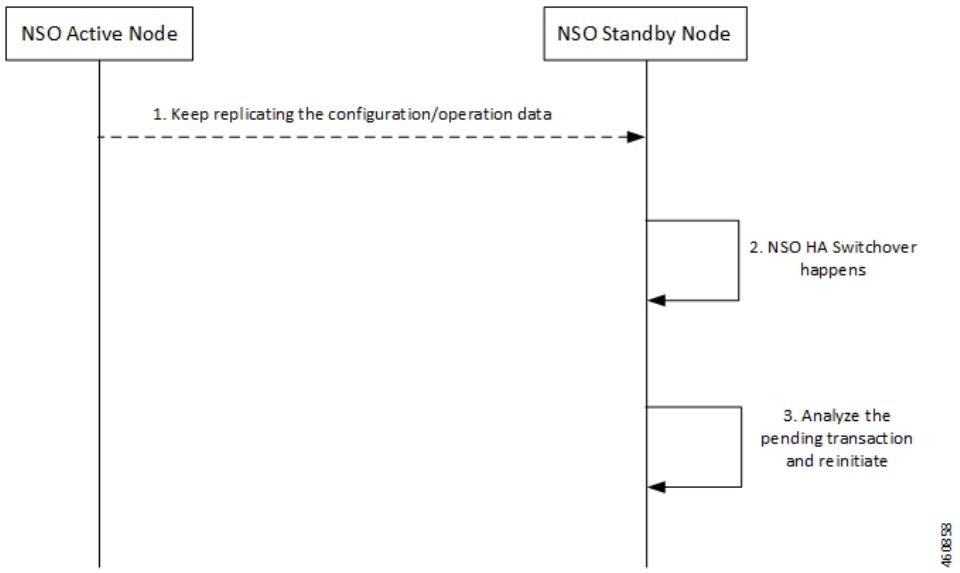


表 *36 :* コール フローの説明

ステップ	説明
1	NSO スタンバイノードが、NSO アクティブノードからの設定や動作データの複製を続けます。
2	NSO HA スイッチオーバーが、NSO スタンバイノードで発生します。
3	NSO スタンバイノードが保留中のトランザクションを分析し、プロセスを再開します。

リカバリ

障害状態から以前の状態にリカバリするために、NSO にはプッシュされた設定に対する組み込みのロールバックメカニズムがあります。1 つ以上のデバイスに設定をプッシュするには、次のオプションを使用できます。

- コミットまたは dry-run のみ
- コミット（ロールバックの生成あり）
- 単一または複数のトランザクションのスキーム
- 複数のトランザクションにおける障害処理のスキーム
- スタンバイノード、アクティブノード、または共通ノードのみをプッシュするスキーム

CP スイッチオーバー（1:1）

モビリティ機能パックは、アクティブな CP の積極的な追跡は行いません。ノースバウンドから設定のプッシュが開始されると、必要に応じて、オンデマンドで追跡します。いずれかの CP にプッシュされた設定は、その CP の起動設定として永続的に保存されます。

（注） 設定を永続的に保存するには、MOP オプションを使用する必要があります。

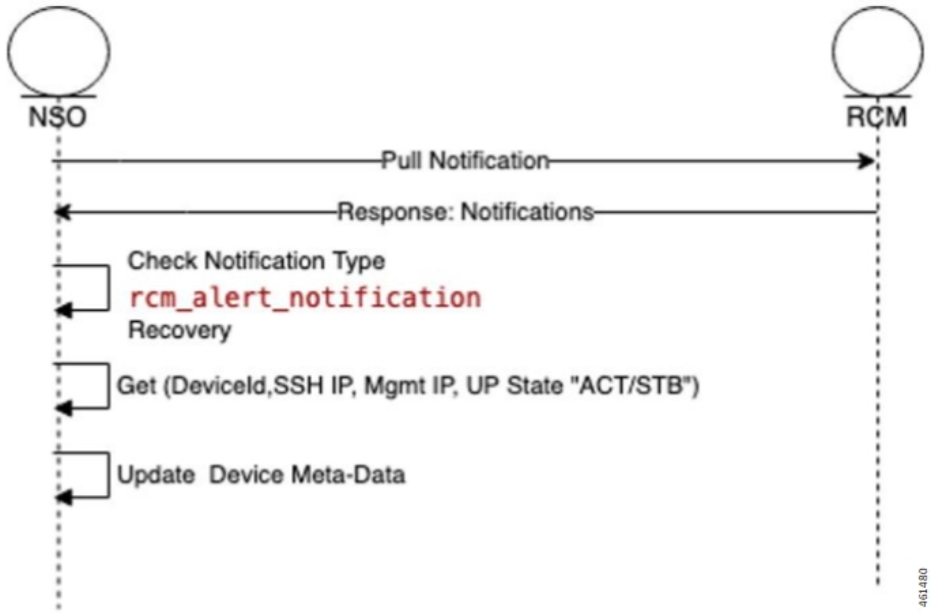
CP のスイッチオーバーでは、リブートされた CP は、必要なすべての設定を保持したまま起動することが求められます。モビリティ機能パックは、このシナリオで特別な処理を実行しません。

UP スイッチオーバー（1:1）

CP シナリオと同様に、いずれかの UP インスタンスにプッシュされた設定は、起動設定の一部として永続的に保存されます。設定を永続的に保存するには、MOP オプションを使用する必要があります。UP スイッチオーバーでは、再起動する UP は必要な設定がすべて設定された状態で自動的に起動することが期待されます。この場合、モビリティ機能パックでは特別なアクションは実行されません。

UP スイッチオーバー（N:M）

次の図は、UP リカバリ通知フローを示しています。



NSO が RCM デバイス通知に登録されると、NSO は [rcm-alert-notification] ストリームにパブリッシュされたすべての通知を取得するようになります。

NSO は、UP リカバリ通知があるたびに、次の手順を実行します。

1. アラートステータスが [Recovery] になるまで待機します。
2. デバイスの詳細（デバイス名、SSH IP、管理 IP、UP ステータス）を取得します。
3. NSO のデバイスメタデータを更新します。

アウトオブバンド設定

NSO ベースの設定管理の基本となるのが、NSO で各デバイス（VNF）の設定のコピーを維持することです。設定の変更がノースバウンドから適用されると、NSOは適用された設定と設定のローカルコピーを比較して、デバイスにプッシュする必要がある設定を決定します。これを行うには、NSO にある設定のコピーがデバイス/VNF の実際の設定と同期している必要があります。

VNF 設定が NED をバイパスしてアウトオブバンドで実行されるケースには、理由が考えられます。たとえば、Day-0 設定は必ずデバイスを NSO にオンボーディングする前に行われるため、アウトオブバンドになります（適切な VNF マネージャを介してプッシュされます）。設定プッシュ MOP は、デバイスに設定をプッシュする前に「sync-from」操作を実行します。これにより、NSO はアウトオブバンド設定を NSO のローカルコピーにプルし、試行された設定のプッシュは最新のデバイス設定に適用されます。sync-from は、NED に認識されている設定のみをプルできます。また、暗号化されたデータを処理する場合の注意事項があります。

設定の機密要素

StarOSは、パスワード、キーなどの設定内にある機密要素を暗号化します。暗号化された項目は、StarOS によってのみ復号できるため、NSO には不透明です。さらに、基になるクリアテキストが変更されない場合でも、機密項目の暗号化フォームが変更される可能性があります。その結果、NSOは、そのような項目に加えられたアウトオブバンド変更を確実に検出できません。

次のいずれかを行うことが推奨されます。

- 対応する設定をアウトオブバンドで完全に管理します。

または

- NSOのみを使用して対応する設定を管理します。つまり、最初にノースバウンドからNSOにコマンドのクリアテキストフォーマットを設定し、その後は変更のたびに設定する必要があります。

同じ設定に NSO ベースの設定管理とアウトオブバンド管理を混在させないでください。

合法的傍受

合法的傍受（LI）は、いくつかの方法で設定できます。1つの展開には、専用のLIコンテキスト機能を使用せずに、単一のコンテキスト内のすべての LI 設定が含まれ、一般的なシステム管理者に LI 管理者権限が付与されます。もう 1 つの展開には、専用の LI コンテキスト、分離された LI 設定、および一般的なシステム管理者とは別の専用の LI 管理者が含まれます。それらの中間に位置する他のバリエーションもあります。

NSO で LI 設定を管理できるようにするには、次の要件を満たす必要があります。

- LI 権限と一般的なシステム管理者権限を持っている
- クリアテキストで LI 設定を表示およびプルできる

シングル コンテキスト シナリオですべての LI 設定を含む展開の場合、NSO で LI 設定を管理する必要があります。それ以外の場合は、LI設定をアウトオブバンドで維持し、Day-0 設定の一部として提供することを推奨します。

CUPS 設定 MOP

設定 MOP は、Cisco StarOS デバイスまたは RCM に設定を適用するための Method of Procedure（MOP）です。この操作はネットワークオペレータによって呼び出され、その応答として、NSO が要求の一意のタスク ID を提供します。ネットワークオペレータは、後からタスク ID を使用して NSO をポーリングし、ステータスを取得できます。

設定 MOP は、次の 3 つの手順で構成されています。

1. デバイスのオンボーディング
2. 設定メタデータの事前入力
3. モビリティ MOP を介した設定のプッシュ

デバイスのオンボーディング

デバイスのオンボーディング手順は、モビリティ オーケストレーション ソリューションの外部でインスタンス化またはオーケストレーションされるデバイスにのみ必要です。そうでない場合、インスタンス化されたVNFは、NSOベースのモビリティ オーケストレーション ソリューションによってデバイスとして NSO に暗黙的にオンボードされます。

（注） この手順は、初回のみ必要です。後続の設定プッシュでは、この手順をスキップする必要があります。

次の例は、RESTCONF または CLI を使用して VNF をオンボードする方法をそれぞれ示しています。

RESTCONF

NSO URL のパッチ要求（http://<NSO-IP>:<PORT>/restconf/data）

次に設定例を示します。

```
{
  "data": {
    "nfv-device-onboarding:nfv-devices": {
      "device": [
        {
          "name": "<Device-or-VNF-Name>",
          "address": "<Management-Address>",
          "username": "<Management-Username>",
          "password": "<Management-Password>",
          "ned-type": "<cisco-staros/RCM>",
          "retry-options": {
            "number-of-attempts": <no-of-attempts-to-ping>,
            "delay": <delay-between-pings>
          }
        }
      ]
    }
  }
}
```

次に設定例を示します。

```
{
  "data": {
    "nfv-device-onboarding:nfv-devices": {
      "device": [
        {
          "name": "vpc-si25",
          "address": "209.165.200.225",
          "username": "admin",
          "password": "Cisco@123",
          "ned-type": "cisco-staros",
          "retry-options": {
            "number-of-attempts": 2,
            "delay": 10
          }
        }
      ]
    }
  }
}
```

CLI

次の NSO CLI コマンドを使用して、デバイスのオンボーディングを作成/入力することもできます。

```
configure
  nfv-devices device device_name address ip_address username user_name password
 password ned-type cisco-staros retry-options delay delay_value
number-of-attempts value
   commit
```

次に設定例を示します。

```
nfv-devices device dummy-device address 209.165.200.225 username admin password cisco@123
 ned-type cisco-staros retry-options delay 10 number-of-attempts 2
```

NSO の既存のデバイスは、次の削除要求 URL（ペイロードなし）を使用して削除できます：http://<NSO-IP>:<NSO-PORT>/restconf/data/nfv-device-onboarding:nfv-devices/device=<device-name>

次の NSO CLI を使用して削除することもできます。

```
configure
   no nfv-devices device device_name
   commit
```

設定メタデータの事前入力

設定プッシュ MOP では、変数の置換が可能です。これは、ほぼ同一の設定が複数のデバイス（たとえば、ICSR アクティブ/スタンバイペア）にプッシュされる場合に役立ちます。違いは、入力設定ファイルの変数として表すことができます。その後、各デバイスの特定の値を「variable: value」形式のメタデータとして入力できます。MOP は、実行時に適切な変数値を動的に置き換えます。

デバイスに事前入力されたデータがない場合、Config MOP は、設定プッシュ用に指定された設定ファイルに動的置換変数がないと想定します。設定ファイルで参照される属性値が欠落している場合、この手順は実行時に失敗します。

設定メタデータの事前入力の構造を以下に記載します。このデータの入力はネットワークスキームとデータセットに基づきます。強調表示された項目は設定をプッシュするための必須項目であり、その他の項目はオプションです。

```
container metadata-store{
    list config-metadata {
        key device-name;
        leaf device-name {
          tailf:info "onboarding device name";
          type string;
         }
 leaf schema {
   tailf:info "cluster-topology 1:1, N:M and N+2";
   type string;
 }
       list attributes {
         key attribute-name;
```

```
            leaf attribute-name {
              tailf:info "Attribute Name";
              type string;
            }
            leaf attribute-value {
              tailf:info "Attribute Value";
              type string;
              }
           }
list configuration-type {
  key config-type;
  tailf:info "Configuration type Day0.5, Day1 or DayN";
  leaf config-type {
    type string;
   }
         list files {
    key file-name;
    tailf:info "file name";
    leaf file-name {
      type string;
    }
    leaf config-scheme {
      type string;
    }
 // CP device info
    list additional-files {
      key device; //cp device
      leaf device{
        tailf:info "device name";
        type string;
```

```
        }
   list additional-file{
     key additional-file-name;
     leaf additional-file-name{
       tailf:info "file name";
       type string;
       }
     }
       }
   }
 }
  }
}
```

設定メタデータは、設定メタデータ要求を使用して入力されます。この要求は、次の YANG スキーマに従います。「input」セクションの項目は、オペレータが入力します。「output」セクションは、アクション要求の実行後に NSO によって返される内容を示します。

設定メタデータを入力または変更する NSO アクションの例を以下に示します。

```
tailf:action config-metadata-request {
          tailf:info "Invoke upgrade action on the selected devices";
          tailf:actionpoint config-metadata-request;
          input {
          list config-metadata {
   key device-name;
   leaf device-name {
     tailf:info "onboarding device name";
     type string;
   }

  list attributes {
  key attribute-name;
  leaf attribute-name {
           tailf:info "Attribute Name";
    type string;
  }
    leaf attribute-value {
    tailf:info "Attribute Value";
    type string;
        }
      }
    }
    }
```

```
    output {
  leaf status {
            type string;
          }
       }
   }
  }
```

RESTCONF

RESTCONF からこのアクションを呼び出す例を以下に示します。

URI：
http://<NSO-IP>:<NSO-REST-PORT>/restconf/data/mobility-common:config-metadata/config-metadata-request

コンテンツタイプ：application/yang-data+json

ペイロード：

```
{
        "config-metadata": {
            "device-name": "test2",
     "schema" : "1:1",
            "attributes":{
                "attribute-name":"hostname",
                 "attribute-value": "TEST"
                  },
                "attribute-name":"BACKHAUL_IP",
                 "attribute-value": "209.165.200.225"
                }
        }
}
```

結果：

```
{
    "mobility-common:output": {
        "status": "Success"
    }
}
```

CLI

次に、NCS CLI を使用してこのアクションを呼び出す例を示します。

```
ubuntu@ncs> request config-metadata config-metadata-request config-metadata { device-name
 staros-1 attributes { attribute-name hostname attribute-value TEST }
status Success
[ok][2021-07-12 08:05:01]
```

モビリティ MOP を介した設定のプッシュ

この手順は、設定 MOP の最後の手順で、新しい設定をプッシュしたり、以前にプッシュした設定をロールバックしたりできます。前述したとおり、プッシュされる設定は1つ以上のファイルに存在します。

設定 MOP プッシュ要求フロー

ネットワークオペレータが NSO API を呼び出して、デバイスの設定 MOP 自動化プロセスを開始

NSO は次の手順を実行します。

- デバイスで check-sync と sync-from または部分同期（必要な場合）を実行します。check-sync により、デバイス構成の NSO コピーが実際のデバイス構成と同期しているかどうかが確認されます。
- NSO が MOP で指定されている場合、NSO はデバイス属性（変数）を設定メタデータのデバイスツリーから読み取ったノード固有の値に置き換えます。
- NSO は、MOP で指定された入力ファイルの設定をそのデバイスに適用するか、要求で指定されている順序で一連のデバイスに適用します。設定をデバイスにプッシュするときに障害が発生した場合、そのデバイスにそれ以上の設定はプッシュされません。
- NSO は、要求で指定されている mop type（active/standby/common）に基づいて MOP を適用します。
  - mop type が「common」の場合、NSO は要求で指定されているすべてのデバイスに MOP を適用します。

    障害が発生した場合、障害が発生したデバイスへの設定プッシュは停止されます。要求で指定されている他のデバイスへの設定プッシュは続行されます。「Status」には、障害が発生したデバイスの詳細が表示されます。オペレータは、障害が発生したデバイスの設定を個別にロールバックすることができます。
  - mop type が「active」の場合、NSO は要求で指定されているすべての「アクティブ」デバイスに MOP を適用します。

    mop type 「active」は、1:1 冗長性シナリオにのみ適用されます。

    障害が発生した場合、プッシュされた設定はすべてロールバックされます。
  - mop type が「standby」の場合、NSO は要求で指定されているすべての「スタンバイ」デバイスに MOP を適用します。

    mop type「standby」は、1:1 冗長性シナリオにのみ適用されます。

    障害が発生した場合、プッシュされた設定はすべてロールバックされます。
  - mop type が「pair」の場合、NSO は最初に「スタンバイ」デバイスに MOP を適用し、成功した場合は「アクティブ」デバイスに MOP を適用します。NSO はアトミックトランザクションを実行するため、設定は両方のデバイスに適用されるか、どちらにも適用されません。

    mop type「pair」は、1:1 冗長性シナリオにのみ適用されます。

    障害が発生した場合、適用された設定はペアの両方のインスタンスからロールバックされます。

- mop type が「rcm-upf」の場合、NSO は入力デバイスに MOP を適用します。さらに、入力デバイスの RD グループを識別し、同じ RD グループに存在する他の UPF デバイスを見つけます。次に、入力デバイスに ECS/APN 設定を保存します。

  障害が発生した場合、障害が発生したデバイスへの設定プッシュは停止されます。要求で指定されている他のデバイスへの設定プッシュは続行されます。[Status] には、障害が発生したデバイスの詳細が表示されます。オペレータは、障害が発生したデバイスの設定を個別にロールバックすることができます。

- NSO は、指定された MOP のドライランおよびリバース（ロールバック）設定をネイティブフォーマットで生成し、2 つの個別のファイルに保存します。NSO は応答として、両方のファイル名と絶対ファイル パスをネットワークオペレータに返します。
  - ドライランファイルの名前は <MOP File Name>-<Device Name>-dryrun.txt になります。
  - ロールバックファイルの名前は <MOP File Name>-<Device Name>-rollback.txt になります。ファイルはタスク ID フォルダの下に生成されます。
- ネットワークオペレータがドライランの要求のみを送信した場合、NSO はドライランファイルとロールバックファイルを生成しますが、デバイスに MOP を適用しません。
- ネットワークオペレータが MOP の適用要求を送信すると、NSO はドライランファイルとロールバックファイルを生成し、MOP をデバイスに適用します。
- ネットワークオペレータは、MOP 自動化ステータスを取得するために NSO のポーリングを継続します。
- NSO はホスト（デバイス）のリストとともに、ドライランファイルとロールバックファイルの場所、およびステータス（完了/進行中/失敗）を返します。

設定 MOP ロールバック要求フロー

- ネットワークオペレータは、NSO API を呼び出して、以前に適用された設定のロールバックプロセスを開始します。
- NSO は次の手順を実行します。
  - デバイスで check-sync と sync-from または部分同期（必要な場合）を実行します。
  - NSO は、ネットワークオペレータによって指定されたタスク ID、MOP ファイル名、およびデバイス名の逆の順序で MOP ファイルのロールバックを実行します。
- MOP タイプが「pair」の場合、NSO は最初に「スタンバイ」デバイスでロールバックを実行し、ロールバックが成功すると、NSO は「アクティブ」デバイスでロールバックを実行します。
- タスク ID のみが指定されている場合は、トランザクション全体がロールバックされます。タスク ID と MOP ファイル名が指定されている場合、指定された MOP のみがすべてのデバイスに対してロールバックされます。タスク ID、MOP ファイル名、およびデバイス名

が指定されている場合、指定されたデバイスに対して指定された MOP のみがロールバックされます。

- NSOは、ロールバックを実行するためのドライランおよびリバース（ロールバック）設定をネイティブフォーマットで生成し、ファイルに保存します。NSOは応答として、両方のファイル名と絶対ファイル パスをネットワークオペレータに返します。
  - ドライランファイルの名前は <MOP File Name> -<Device Name> -dryrun.txt になります。
  - ロールバックファイルの名前は <MOP File Name> -<Device Name> -rollback.txt になります。

  ファイルはタスク ID フォルダの下に生成されます。
- ネットワークオペレータがドライラン要求のみを送信した場合、NSOはドライランファイルとロールバックファイルを生成します。
- ネットワークオペレータが MOP のロールバック要求を送信すると、NSO はドライランファイルとロールバックファイルを生成し、ロールバックを実行します。
- ネットワークオペレータは、ロールバックステータスを取得するために NSO のポーリングを継続します。
  - NSO はホスト（デバイス）のリストとともに、ドライランファイルとロールバックファイルの場所、およびステータス（完了/進行中/失敗）を返します。

MOP の自動化

モビリティ設定 MOP は、NSO からモビリティデバイスを設定するために使用できる一連のコマンドです。モビリティ設定MOP では、エンドユーザーが場所を指定して、MOP 関連の入力ファイルと出力ファイルを検索または保存できます。また、MOP のグローバル設定可能なパラメータも設定できます。

設定要件

- NSO CLI に移動し、静的アクションを使用して以下のパラメータを設定します。

1. Dry-run-mop location：Dry-run-mop ファイルには、デバイスにプッシュされた設定が含まれています。MOP の dry-run ファイルを保存する場所を入力します。
2. Rollback-mop location：ロールバックファイルは生成された構成ファイルで、デバイスの設定をロールバックするために必要です。MOPのロールバックファイルを保存する場所を入力します。
3. Config-mop-file location：入力設定 MOP ファイルを取得する場所を入力します。
4. Netconf-to-cli Conversion：NETCONF 設定をデバイス CLI 形式に変換するには、フラグを「true」に設定します。フラグが「false」に設定されている場合、dry-run ファイルはネイティブ NETCONF xml 形式で生成されます。

- 設定内の static action call コマンド：
- **static dry-run-mop /var/opt/ncs/**
  static rollback-mop /var/opt/ncs/

  確認するには、次の CLI コマンドを使用します。

  show full-configuration static

- mop-file location のグローバルパラメータ設定：

  configure
  configurable-parameters config-mop-file-loc /var/opt/ncs/

  確認するには、次の CLI コマンドを使用します。

  show full-configuration configurable-parameters config-mop-file-loc

- StarOS レベルの NED 設定の例

  1. デバイスのシステム cfg ブートファイルの設定が更新されないようにするには、次のコマンドを使用して、NCS CLI で write-memory-setting が無効になっていることを確認します。

     devices global-settings ned-settings cisco-staros
     write-memory-setting disabled

  2. デバイスに設定をコミットする際の警告を除外するには、次のコマンドを使用します。

     devices global-settings ned-settings cisco-staros behaviour
     config-warning-ignore.*Standby card not ready.*

（注） .*Standby card not ready.* は警告メッセージに置き換え可能で、無視できます。

Mop タイプペアの前提条件

- デバイスの状態（アクティブ/スタンバイ）の識別に基づいて、デバイス名の 1 つを target-device-name として指定できます。
- 次のコマンドを使用して、ピアデバイスと srp_loopback を設定します。

```
config-metadata config-metadata-request config-metadata { device-name
up2-SI device-type vpc attributes { attribute-name srp_loopback
attribute-value 209.165.200.225 } scheme 1:1 }
config-metadata config-metadata-request config-metadata { device-name
up2-SI device-type vpc attributes { attribute-name Peer_Device_Name
attribute-value up1-SI } scheme 1:1 }
```

NSO API

NSO API は、設定プッシュ機能に関連する NSO モビリティ機能パックを通じて公開されます。これらの API には、RESTCONF または CLI のいずれかを介してアクセスできます。

設定プッシュ MOP の自動化

この API は、MOP を開始して 1 つ以上のデバイスに設定をプッシュするために使用されます。これは非同期操作であり、別の API を使用してステータスをクエリできます。

API：

`mop-automation`

要求の詳細

パラメータ	書式	必須	説明
mop-file-name	リスト	—	
file-name	文字列	キー	UP、CP、または RCM に対応するデバイスの名前。
execution-order	数値	必須	MOP の実行順序。1 が最初で、使用される順序は 1、2、3… です。
target-devices	リスト	必須	デバイスのリスト
target-device-name	Leafref	キー	VNF の NSO デバイス名。NSO がオーケストレーションに使用されている場合、デバイス名は VNF 名と同じです。
operation-type	文字列	必須	**dry-run**、または **commit**

パラメータ	書式	必須	説明
mop-type	列挙体	—	

パラメータ	書式	必須	説明
			設定をプッシュする先のデバイスを決定します。使用できる値は、次のとおりです。 • **active** 1:1 冗長性ペアのアクティブインスタンスにプッシュします。冗長性ペアのいずれかのインスタンスを選んでデバイス名を入力できます（アクティブかスタンバイかは問いません）。MOPが該当するペアの現在アクティブなインスタンスを自動的に判別して、プッシュします。 • **standby** 1:1 冗長性ペアのスタンバイインスタンスにプッシュします。冗長性ペアのいずれかのインスタンスを選んでデバイス名を入力できます（アクティブかスタンバイかは問いません）。MOPが該当するペアの現在スタンバイ中のインスタンスを自動的に判別して、プッシュします。 • **pair** 1:1 冗長ペアのアクティブインスタンスとスタンバイインスタンスの両方にプッシュします。冗長性ペアのいずれかのインスタンスを選んでデバイス名を入力できます（アク

パラメータ	書式	必須	説明
			ティブかスタンバイかは問いません）。MOPは、指定されたインスタンスをもとに該当するペアの 2 つのインスタンスを自動的に判別し、最初にスタンバイインスタンスにプッシュしてから、アクティブインスタンスにプッシュします。 • **common** 要求で指定されたすべてのデバイスにプッシュします。これが**default**です。 • **rcm-upf** 単一またはすべての関連付けられたUPFに設定をプッシュします。

パラメータ	書式	必須	説明
transaction-type	列挙体	—	

パラメータ	書式	必須	説明
			使用できる値は、次のとおりです。 • **single-transaction** 指定されたすべての入力ファイルの設定が結合され、単一のトランザクションとしてデバイスにプッシュされます。 • **multiple-transaction** 各入力ファイルが、個別のトランザクションとしてデバイスにプッシュされます。これはデフォルト値です。 トランザクションは、設定変更の最小単位です。トランザクション内の設定はすべて、正常にプッシュされるか、プッシュ中に障害が発生した場合は自動的にロールバックされます。 （注） 1 つのトランザクションが複数のデバイスにまたがることはありません。各トランザクションは、1 つのデバイスに固有です。 たとえば、オペレータが 3 つのファイルをそれぞれ 2 つのデバイスにプッシュする場合、次のようになります。 • **multiple-transactions** オプションを使用すると、デバイスごと、ファイルごとに 1 つなので、トランザクショ

パラメータ	書式	必須	説明
			ンの合計数は 3 x 2 = 6 となります。 • **single-transaction** オプションを使用すると、デバイスごとに 1 つずつなので、トランザクションの合計数は 2 となります。
save-config-permanently	ブール値	—	デフォルト値は「false」です。「true」に設定すると、設定を「system.cfg」に保存できます。
timeout	数値	オプション。デフォルト値は 600 秒	デバイスがロックされるまで待機する最大秒数。

Timeout パラメータ

NSO 6.0 バージョンは、楽観的同時実行を使用してパラレリズムを向上させます。ただし、サービスを並行して実行すると、トランザクションの競合が発生する可能性があります。単一のデバイスで同時実行が設定されている場合、最初のトランザクションによってデバイスがロックされるため、後続のトランザクションは失敗します。

timeout パラメータは、デバイスロックの取得など、デバイスに関連する一部の操作が実行されるまで MFP が待機する時間を規定します。timeout パラメータが直接関係するのは、同じデバイスに同時に設定をプッシュする複数の操作がある場合です。

（注） 単一のデバイスでの同時並行処理設定は推奨されません。

mobility-mop 自動化 CLI または postman API を使用して設定をプッシュする際に **timeout** パラメータが使用されていない場合、システムは自動的にデフォルト値である 600 秒を呼び出します。

多数の設定または大きなサイズの設定をプッシュする場合は、timeout パラメータを使用して、デフォルト値を超えるタイムアウト値を設定するコールを実行できます。

次の設定例に示すように、任意の値を指定できます。

```
cloud-user@ncs# mobility-mop:action mop-automation generate-dry-run true operation-type
        commit save-config-permanently true mop-type common mop-file-name { file-name
ABC.cfg order
        1 target-devices-list { target-device-name XYZ } } timeout 900
```

タイムアウト値に -1 を指定すると、timeout パラメータを無限に設定できます。

```
cloud-user@ncs# mobility-mop:action mop-automation generate-dry-run true operation-type
        commit save-config-permanently true mop-type common mop-file-name { file-name
ABC.cfg order
        1 target-devices-list { target-device-name XYZ } } timeout -1
```

設定がプッシュされるとすぐに、別のユーザーまたは後続の設定のプッシュに向けてデバイスが解放されます。たとえば、timeout が 600 秒で、設定のプッシュが 100 秒で完了する場合、100 秒後には別のユーザーがそのデバイスに設定をプッシュできます。

応答の詳細

パラメータ	書式	必須	説明
Task-id	文字列	必須	タスクの一意の識別子。Task-id は、操作のステータスのクエリに使用されます。
Time stamp	文字列	必須	Time stamp
Error Code	文字列		エラーコード
Error Message	文字列		エラーメッセージ

CLI

NCS CLI を使用した要求の例を以下に示します。

mobility-mop:action mop-automation mop-type common transaction-type multiple-transaction operation-type commit mop-file-name { file-name dayN.txt order 1 target-devices-list { target-device-name up2-SI } }

REST API 要求：トランザクションタイプを指定しない場合

以下に、トランザクションタイプを指定せずに postman を使用する REST API 要求の例を示します。

```
POST  /restconf/data/mobility-mop:action/mop-automation
   Host: localhost:8080
     Authorization: Basic YWRtaW46YWRtaW4= Content-Type: application/vnd.yang.data+json
 cache-control: no-cache

         {
            "mop-automation": {
            "operation-type": "commit",
            "mop-type": "active",
            "generate-dry-run": "true",
            "save-config-permanently": "true",
            "mop-file-name": [
               {
                  "file-name": "up_dayN.txt" ,
                  "order": 1,
                  "target-devices-list": [
                     {
                        "target-device-name": "up2-SI"
                     }
```

```
                    ]
                }
            ]
        }
}
```

REST API 要求：トランザクションタイプを指定する場合

次に、トランザクションタイプを指定する REST API 要求の例を示します。

```
POST    /restconf/data/mobility-mop:action/mop-automation
   Host: localhost:8080
      Authorization: Basic YWRtaW46YWRtaW4= Content-Type: application/vnd.yang.data+json
 cache-control: no-cache
         Postman-Token: d2d2ddbe-5dff-4917-972a-146db6dc175f

            {
               "mop-automation": {
               "operation-type": "commit",
               "mop-type": "active",
               "transaction-type": "single-transaction",
               "mop-file-name": [
                  {
                     "file-name": "load3.txt",
                     "order": 1,
                     "target-devices-list": [
                        {
                           "target-device-name": "test3"
                        }
                     ]
                  },
                {
                    "file-name": "load4.txt",
                    "order": 2,
                    "target-devices-list": [
                 {
                    "target-device-name": "test3"
                 }
              ]
           }
       ]
   }
}
```

REST API 要求：トランザクションタイプと *mop-type* をペアとして指定しない場合

次に、トランザクションタイプと mop-type をペアとして指定しない REST API 要求の例を示します。

```
 {
    "mop-automation": {
                          "operation-type": "commit",
                          "mop-type": "pair",
                          "generate-dry-run": "true",
                          "save-1-1-config": "true",
                          "mop-file-name": [
                     {
                        "file-name": "up_dayN.txt" ,
                        "order": 1,
                        "target-devices-list": [
                  {
                     "target-device-name": "up2-SI"
                  }
```

```
            ]
        }
    ]
  }
}
```

前述の非同期要求の呼び出しが成功すると、一意のタスク ID とタイムスタンプが返され、mop-automation 要求のステータスを確認するために使用されます。

```
{
    "mobility-mop:output": {
        "task-id": "1a1f62f0-487a-4c8c-bdeb-a760c26925cc",
        "time-stamp": "2021-07-19T11:10:51+0000",
        "time-zone": "Coordinated Universal Time"
    }
}
```

[mop-type] が「rcm-upf」の MOP の自動化

「rcm-upf」という mop-type は、単一またはすべての関連付けられた UPF に設定をプッシュするために使用されます。次の 2 つのシナリオが対象です。

1. 単一の UPF に MOP を適用する場合

   UPF デバイスを指定する方法は次のとおりです。

   - [target-device-name] に「upf-device」を指定します。
   - upf-device に対応する [rcm-vip]、[group]、および [device-id] を指定します。

   上記の 2 つの方法では、要求の [only-to-target-devices] を「true」に設定する必要があります。

   ペイロードの例：

   1. [target-device-name] に「upf-device」を指定します。

```
{
    "mop-automation": {
        "operation-type": "commit",
        "mop-type": "rcm-upf",
        "generate-dry-run": "true",
        "save-config-permanently": "true",
        "only-to-target-devices": "true",
        "mop-file-name": [
            {
                "file-name": "simpleStarOsChange.txt",
                "order": 1,
                "target-devices-list": [
                    {
                        "target-device-name": "up1-device"
                    }
                ]
            }
        ]
    }
}
```

   2. upf-device に対応する [rcm-vip]、[group]、および [device-id] を指定します。

```
{
    "mop-automation": {
```

```
        "operation-type": "commit",
        "mop-type": "rcm-upf",
        "generate-dry-run": "true",
        "save-config-permanently": "true",
        "only-to-target-devices": "true",
        "mop-file-name": [
            {
                "file-name": "simpleStarOsChange.txt",
                "order": 1,
                "rcm-vip" : "rcmvip01",
                "group" : "group03",
                "device-id" : "device-id1"
            }
        ]
    }
}
```

2. 関連付けられたすべての UPF デバイスに MOP を適用する場合

   UPF デバイスを特定する方法は次のとおりです。

   - [target-device-name] にサンプル upf-device を指定します。
   - [rcm-vip] と [group] を指定します。

   ペイロードの例：

   1. [target-device-name] にサンプル upf-device を指定します。

```
  {
    "mop-automation": {
        "operation-type": "commit",
        "mop-type": "rcm-upf",
        "generate-dry-run": "true",
        "save-config-permanently": "true",
        "only-to-target-devices": "false",
        "mop-file-name": [
            {
                "file-name": "simpleStarOsChange.txt",
                "order": 1,
                "rcm-vip" : "rcmvip01",
                "group" : "group03"
            }
        ]
    }
}
```

   2. [rcm-vip] と [group] を指定します。

```
{
    "mop-automation": {
        "operation-type": "commit",
        "mop-type": "rcm-upf",
        "generate-dry-run": "true",
        "save-config-permanently": "true",
        "only-to-target-devices": "false",
        "mop-file-name": [
            {
                "file-name": "simpleStarOsChange.txt",
                "order": 1,
                "rcm-vip" : "rcmvip01",
                "group" : "group03"
            }
```

```
                ]
            }
        }
```

上記の 2 つの方法では、要求の [only-to-target-devices] を「false」に設定する必要があります。

[rcm-vip] と [group] を使用して UPF デバイスを取得する場合、次のリストに挙げる CDB のデータが使用されます。

- device-id-up-mapping
- up-rcm-mapping
- rcm-upf-mapping

MOP 自動化ステータス

NSO は、ネットワークオペレータによって渡されたタスク ID のデバイスステータスの結果を提供します。

API：

mop-automation-status

要求の詳細

パラメータ	書式	必須	説明
Task-id	文字列	必須	「MOP Automation」APIから取得したタスクの一意の識別子。

応答の詳細

パラメータ	書式	必須	説明
task-id	文字列	key	Task ID
task-status	文字列		タスク ステータス
Start-date	文字列		開始日時
End-date	文字列		終了日時
Time-zone	文字列		タイム ゾーン
Operation-type	文字列		Commit/Dry-run
Action-type	文字列		Save
devices-list	list		デバイス
Device-name	leafref	key	デバイス名
Start-date	文字列		開始日時

パラメータ	書式	必須	説明
End-date	文字列		終了日時
device-status	leafref		デバイスのステータス（Completed/In-Progress/Failed）
device-state	文字列		Active/Standby/Common /Pair/rcm-upf
files	list		ファイル
file-name	文字列	key	MOP ファイル名
順序	Uint8		MOP が実行された順序
dry-run-mop	文字列		リハーサル出力ファイルの場所
rollback-mop	文字列		ロールバック MOP の場所
Commit-queue-status	文字列		コミットキューステータス
Commit-queue-id	文字列		コミットキュー ID
Error Code	文字列		エラーコード
Error Message	文字列		エラーメッセージ
Error Code	文字列		エラーコード
Error Message	文字列		エラーメッセージ

CLI

NCS CLI を使用した要求の例を以下に示します。

```
mobility-mop:action mop-automation-status task-id
8d08e359-0bd2-48de-9a34-9192a986a486
```

REST API 要求

以下は、mop-automation のステータスを知るための REST API 要求の例です。

```
POST /restconf/data/mobility-mop:action/mop-automation-status
   Host: localhost:8080
      Authorization: Basic YWRtaW46YWRtaW4= Content-Type: application/vnd.yang.data+json
 cache-control: no-cache

      {
         "task-id": "22301071-9a6c-4f27-a0dc-b50c24124806"
      }
```

以下に、上記の要求の呼び出し後に生成される応答フォーマットの例を示します。

```
{
    "mobility-mop:output": {
```

```
        "task-id": "8d08e359-0bd2-48de-9a34-9192a986a486",
        "task-status": "COMPLETED",
        "start-date": "2021-09-06T09:08:54+0000",
        "end-date": "2021-08-06T09:09:10+0000",
        "time-zone": "Coordinated Universal Time",
        "operation-type": "commit",
        "action-type": "save",
        "devices-list": [
            {
                "device-name": "up2-SI",
                "device-status": "COMPLETED",
                "start-date": "2021-08-06T09:08:55+0000",
                "end-date": "2021-08-06T09:08:59+0000",
                "device-state": "active",
                "files": [
                    {
                        "file-name": "up_dayN.txt",
                        "order": "1",
                        "dry-run-mop":
"/var/opt/ncs//8d08e359-0bd2-48de-9a34-9192a986a486/up2-SI/up_dayN_commit_2021-08-06T090854+0000.txt",

                        "rollback-mop":
"/var/opt/ncs//8d08e359-0bd2-48de-9a34-9192a986a486/up2-SI/up_dayN_rollback_commit_2021-08-06T090854+0000.txt",

                        "commit-queue-status": "completed",
                        "commit-queue-id": "1628240937590"
                    }
                ]
            }
        ]
    }
}
```


MOP ロールバック

NSO は、ロールバック要求の入力で指定されたタスク ID、MOP ファイル、およびデバイスのロールバックプロセスを開始します。

これは、MOP で設定された構成ファイルやロールバックされた構成ファイルをロールバックする唯一のオプションです。

この API は、以前に適用された設定をロールバックします。最初に設定を適用した時に作成されたロールバックファイルが使用されます。ロールバックは、ファイルごと、すべてのファイルに対して、デバイスごと、またはすべてのデバイスに対して実行できます。

（注） ロールバックが成功するかどうかは、関連する設定がプッシュされてからシステムに加えられた変更の内容によって大きく左右されます。その後の変更によっては、設定のロールバックが意味をなさなくなるほどシステムが変更されている可能性があります。

API：

mop-rollback

要求の詳細

パラメータ	書式	必須	説明
Task-id	文字列	必須	タスク固有の識別子
mop-file-name	リスト	任意	デバイスの MOP ファイル
file-name	文字列	キー	対応するロールバックファイルを識別するために使用される元のファイル名。
target-devices	リスト	任意	デバイスリスト。指定しない場合、元のトランザクションで設定がプッシュされたすべてのデバイスにおいてロールバックが実行されます。
target-device-name	Leafref	キー	
operation-type	文字列	必須	ドライラン/コミット
timeout	数値	オプション。デフォルト値は 600 秒	デバイスがロックされるまで待機する最大秒数。

応答の詳細

パラメータ	書式	必須	説明
Task-id	文字列	必須	タスク固有の識別子 task-id は、別の API を介してロールバックのステータスを確認するために使用します。
Time stamp	文字列	必須	タイムスタンプ
Error Code	文字列	エラーコード	
Error Message	文字列	エラーメッセージ	

CLI

NCS CLI を使用した要求の例を以下に示します。

```
mobility-mop:action mop-rollback task-id
8d08e359-0bd2-48de-9a34-9192a986a486 generate-dry-run true operation-type
```

```
 commit save-config-permanently true mop-file-name { file-name
up_dayN.txt target-devices-list { target-device-name up2-SI } }
```

REST API 要求：操作タイプ「*commit*」の場合

次に、操作タイプが「commit」の REST API 要求の例を示します。

```
POST /restconf/data/mobility-mop:action/mop-rollback
   Host: localhost:8080
     Authorization: Basic YWRtaW46YWRtaW4= Content-Type: application/vnd.yang.data+json
 cache-control: no-cache
        Postman-Token: 1b687031-dc32-41 14-a69f-5984130c36a5
        {
           "mop-rollback": {
           "task-id": "0891655c-642b-4ba3-9392-6f05d4e77a63",
           "operation-type": "commit",
           "generate-dry-run": "true",
           "save-config-permanently": "true",
           "mop-file-name": [
           {
              "file-name": "up_dayN.txt",
              "target-devices-list": [
              {
                 "target-device-name": "up2-SI"
              }
           ]
        }
     ]
   }
}
```

前述の要求の呼び出しが成功すると、一意のタスク ID とタイムスタンプが返され、mop-rollback 要求のステータスを確認するために使用されます。

```
{
    "mobility-mop:output": {
        "task-id": "8d08e359-0bd2-48de-9a34-9192a986a486",
        "time-stamp": "2021-08-06T09:08:44+0000",
        "time-zone": "Coordinated Universal Time"
    }
}
```

REST API 要求：操作タイプ「*dry-run*」の場合

次に、操作タイプが「dry-run」の REST API 要求の例を示します。

```
POST /restconf/data/mobility-mop:action/mop-rollback
   Host: localhost:8080
      Authorization: Basic YWRtaW46YWRtaW4= Content-Type:
application/vnd.yang.data+json cache-control: no-cache
      Postman-Token: 1b687031-dc32-41 14-a69f-5984130c36a5
      {
         "mop-rollback": {
         "task-id": "0891655c-642b-4ba3-9392-6f05d4e77a63",
         "operation-type": "dry-run",
         "generate-dry-run": "true",
         "save-config-permanently": "true",
         "mop-file-name": [
         {
            "file-name": "up_dayN.txt",
            "target-devices-list": [
            {
                  "target-device-name": "up2-SI"
```

```
                }
            ]
        }
    ]
  }
}
```

前述の要求の呼び出しが成功すると、一意のタスク ID とタイムスタンプが返され、mop-rollback 要求のステータスを確認するために使用されます。

```
{
    "mobility-mop:output": {
        "task-id": "1a1f62f0-487a-4c8c-bdeb-a760c26925cc",
        "time-stamp": "2021-07-19T11:10:51+0000",
        "time-zone": "Coordinated Universal Time"
}
```

MOP ロールバックのステータス

NSO は、ネットワークオペレータによって渡されたタスク ID のデバイスステータスの結果を提供します。API を使用して、進行中または完了したロールバック操作のステータスをクエリします。

API：

mop-rollback-status

要求の詳細

パラメータ	書式	必須	説明
Task-id	文字列	必須	ロールバック操作におけるタスクの一意の識別子。

応答の詳細

パラメータ	書式	必須	説明
task-id	文字列	key	タスクの一意の識別子
task-status	文字列		タスク ステータス
Start-date	文字列		開始日時
End-date	文字列		終了日時
Time-zone	文字列		タイム ゾーン

パラメータ	書式	必須	説明
Operation-type	文字列		Commit/Dry-run
Action-type	文字列		ロールバック（Rollback）
devices-list	list		デバイス
Device-name	leafref	key	デバイス名
Start-date	文字列		開始日時
End-date	文字列		終了日時
device-status	leafref		デバイスのステータス（Completed/In-Progress/Failed）
device-state	文字列		Active/Standby/Common/Pair
files	list		ファイル
file-name	文字列	key	MOP ファイル名
順序	Uint8		MOP が実行された順序
dry-run-mop	文字列		リハーサル出力ファイルの場所
rollback-mop	文字列		ロールバック MOP の場所
Commit-queue-status	文字列		コミットキューステータス
Commit-queue-id	文字列		コミットキュー ID
Error Code	文字列		エラーコード
Error Message	文字列		エラーメッセージ
Error Code	文字列		エラーコード
Error Message	文字列		エラーメッセージ

CLI

NCS CLI を使用した要求の例を以下に示します。

```
mobility-mop:action mop-rollback-status task-id
fd0fb9ae-8685-420e-9490-0c6858d14148
```

REST API 要求

以下は、mop-rollback のステータスを知るための REST API 要求の例です。

```
POST /restconf/data/mobility-mop:action/mop-rollback-status
Host: localhost:8080
Authorization: Basic YWRtaW46YWRtaW4= Content-Type: application/vnd.yang.data+json
cache-control: no-cache
Postman-Token: Oe2c4bd3-2dc6-4ddb-aea9-1 1 Occf622da7
"mop-rollback -status": {
"task-id": "5733d661-9242-4867-8320-a314da592c93"
}

Below is response format generated, post invocation of the above request -
task-id fd0fb9ae-8685-420e-9490-0c6858d14148
task-status COMPLETED
start-date 2021-08-06T09:24:14+0000
end-date 2021-08-06T09:24:30+0000
time-zone Coordinated Universal Time
operation-type commit
action-type rollback
devices-list {
    device-name up2-SI
    device-status COMPLETED
    start-date 2021-08-06T09:24:14+0000
    end-date 2021-08-06T09:24:19+0000
    device-state active
    files {
        file-name up_dayN_rollback_commit_2021-08-06T090854+0000.txt
        order 1
        dry-run-mop /var/opt/ncs//fd0fb9ae-8685-420e-9490-0c6858d14148/up2-SI
/up_dayN_2021-08-06T090854+0000_rollback_commit_2021-08-06T092414+0000.txt
        rollback-mop /var/opt/ncs//fd0fb9ae-8685-420e-9490-0c6858d14148/up2-SI
/up_dayN_2021-08-06T090854+0000_commit_2021-08-06T092414+0000.txt
        commit-queue-status completed
        commit-queue-id 1628241856973
    }
}
```

ドライランおよびリバースドライラン MOP の確認

ドライラン MOP およびリバースドライラン MOP を確認するには、ドライラン MOP およびリバースドライラン MOP の静的データの設定時に提供されたそれぞれのファイルの場所に移動します。

MOP 実行用の構成ファイルへの変数の追加

MOP 自動化パッケージでは、MOP での変数の指定がサポートされているため、MOP が適用されるデバイスに基づいてランタイムに変数が入力されます。たとえば、次の MOP が指定され、デバイス TXPCF003 で実行されたとします。

```
config context local administrator $Host_name password Nsotest123$ exit
 end
```

ホスト名は、次のアクションコールを使用して設定できます。

```
config-metadata config-metadata-request config-metadata { device-name
up2-SI device-type vpc attributes { attribute-name Host_name
attribute-value TXPCF003} scheme 1:1 }
```

生成される dry-run MOP は次のとおりです。

```
config context local administrator TXPCF003 password Nsotest123$ exit
end
```

N:M 冗長性での UP 設定のプッシュとリカバリ

N:M シナリオでは、RCM が各 UP のロール（アクティブとスタンバイ）を決定します。任意の M 個のスタンバイインスタンスが任意の N 個のアクティブインスタンスを引き継げる必要があるため、プッシュされる設定は異なり、動的に変化します。これは、すべての設定を UP に永続的に保存できるわけではないことも意味します。

RCM は、UP 起動や UP スイッチオーバーなどの関連イベントに対して NETCONF 通知を発行します。NSO は NETCONF 通知をリッスンし、必要に応じて必要な設定を適用します。

UP の設定は以下の論理コンポーネントで構成されます。

- Day-0 設定：これは主に、UP の管理インターフェイスを到達可能にするための基本設定です。この設定は、VNFM による UP 展開時にプッシュされ、再起動後も変わらないと想定されています。

（注） 必要な

```
rcm-configmgr CLI
```

コマンドは、NSOベースの設定のプッシュを機能させるために、Day-0 設定の一部として UP で設定する必要があります。このコマンドは、RCMがソリューションで使用されているかどうかに関係なく必要です。このコマンドを設定しない場合、ECS 設定のプッシュは非表示になります。

- Day-0.5 設定：UP が RCM に接続できるようにする設定です。この設定は、UP 展開の直後（NSO が VM を展開している場合）に自動的に、または手動で MOP の設定のプッシュを実行して、Day-0 設定とともにプッシュしたり、NSO とは別にプッシュしたりできます。この設定は、再起動後も永続的に保存されると想定されています。
- 共通設定：これは、アクティブかスタンバイかに関係なく、すべての UP に共通の設定で、ECS と APN の設定のみ該当します。この設定は、NSO に事前入力する必要があります。NSO は、RCM から通知を受信すると、この設定をプッシュします。この設定は、起動設定の一部として永続的に保存されるのではなく、各 UP でファイルとしてローカルに保存され、再起動のたびに NSO によって自動的に再適用されます。

- ホスト固有の設定：これは、アクティブな各 UP に固有の設定で、主に各種サービスの IP アドレスです。各アクティブ UP には、そのアクティブインスタンスに固有の設定がプッシュされます。各スタンバイインスタンスには、すべてのアクティブ UP に関する結合されたホスト固有の設定がプッシュされます。この設定は、NSO に事前入力されている必要があります。NSO は、RCM からの通知に基づいて、必要に応じてこの設定を各 UP にプッシュします。
- ホスト固有の設定：RCM コピー：これは各 UP のホスト固有の設定ですが、RCM 互換形式でフォーマットされています。この設定は RCM にプッシュする必要があります。RCM は設定にはほとんど関係しませんが、UP スイッチオーバー時における設定の否定の実行には関係します。設定の否定とは、特定のアクティブ UP を引き継ぐスタンバイ UP から、他のすべてのアクティブ UP の設定を削除することを意味します。たとえば、3:1 のシナリオで、Active3 UP がダウンしたとします。スタンバイには、Active1、Active2、および Active3 のホスト固有の設定があり、スタンバイが Active3 を引き継ぐため、RCM はスイッチオーバーの一環としてそのスタンバイから Active1 と Active2 の設定を無効にします。

NSO での NETCONF 通知サブスクリプション

RCM から送信されたすべての通知は、NSO によってキャプチャされます。NSO は通知をフィルタリングし、RCM 関連の通知を処理します。

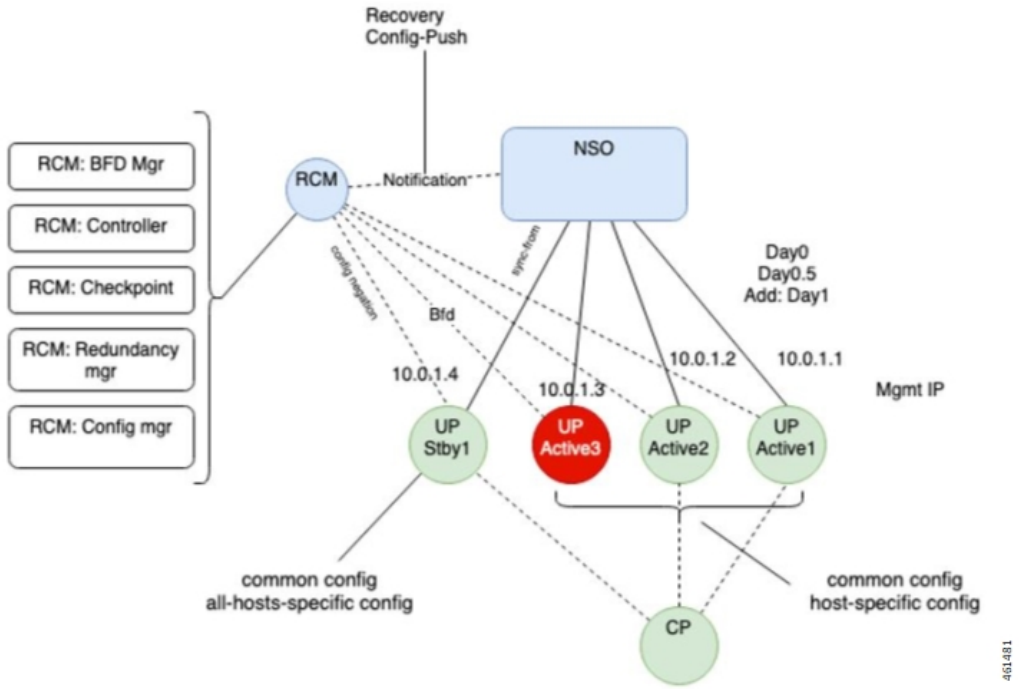
次の表では、処理可能な RCM UP 通知のタイプと、それらの通知が NSO によってどのように処理されるかについて説明します。

	リカバリ	設定のプッシュ	
	UP リカバリ	**UP リブート**	**新規 UP**
アクティブ UP	NSO でデバイスメタデータを更新します。	**ホスト固有の設定をプッシュします** 。 共通設定がデバイスにない場合は、共通設定ファイルを再プッシュします。 NSO でデバイスメタデータを更新します。	
スタンバイ UP	該当なし	**ホスト固有の設定をすべてプッシュします。** 共通設定がデバイスにない場合は、共通設定ファイルを再プッシュします。 NSO でデバイスメタデータを更新します。	

RCM UP リカバリ通知の処理

UP 障害が発生した場合、RCM は BFD マネージャを介して障害を検出し、NSO が受信した通知をプッシュします。RCM は UP のスイッチオーバーを処理して、選択されたスタンバイ UP をアクティブ UP にします。スタンバイ UP はすでに必要なすべての設定を備えているため、スタンバイ UP がスイッチオーバーするためのこの設定管理プロセスにそれほど時間はかかりません。

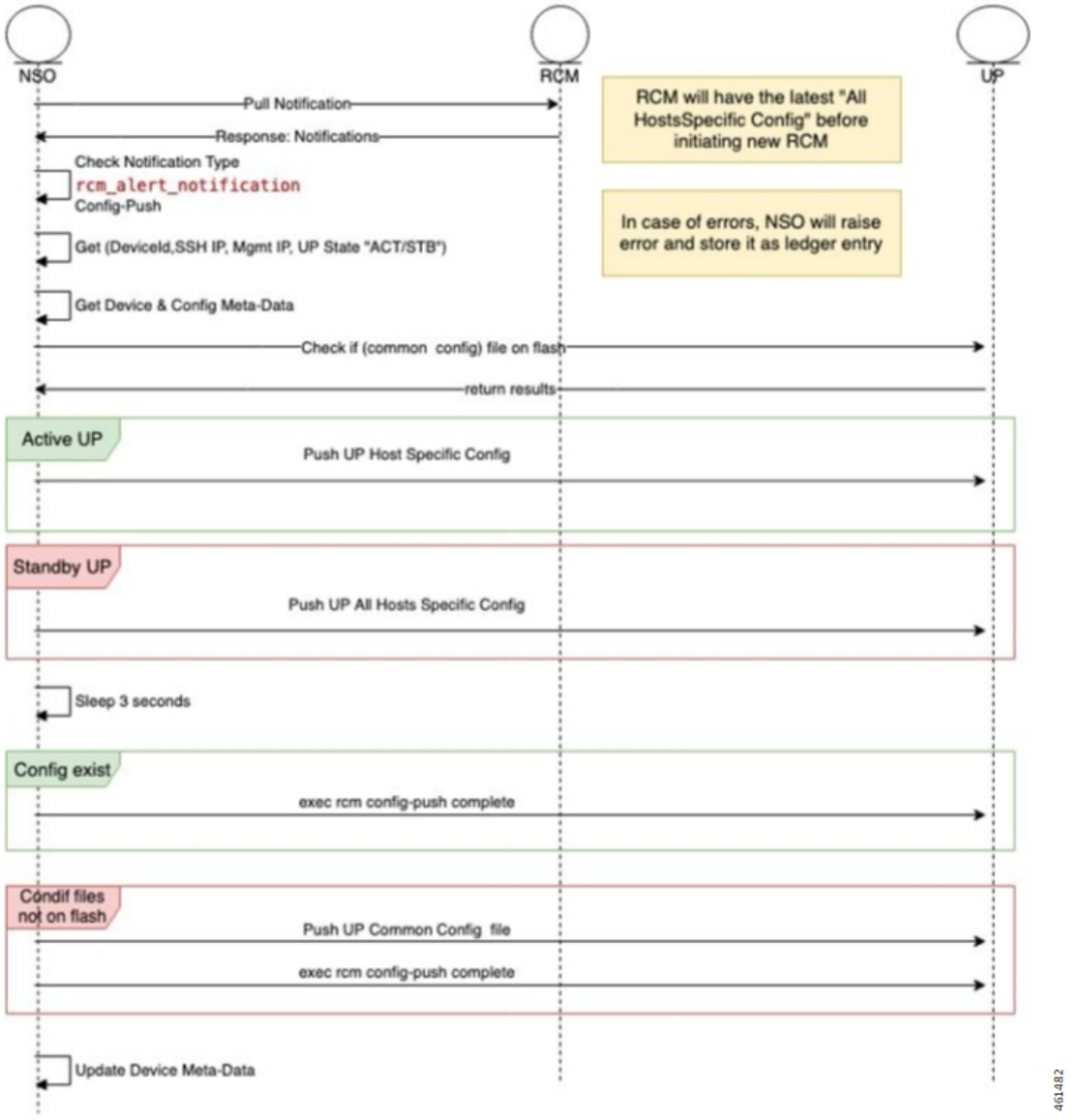
この図は、RCM による UP 通知の処理を示しています。



RCM UP 設定プッシュ通知

RCM は、起動中の新しい UP、またはリカバリのためにリブート中の既存の UP があると、設定のプッシュ通知を生成します。

次の図は、RCM による UP 設定のプッシュ通知の処理を示しています。



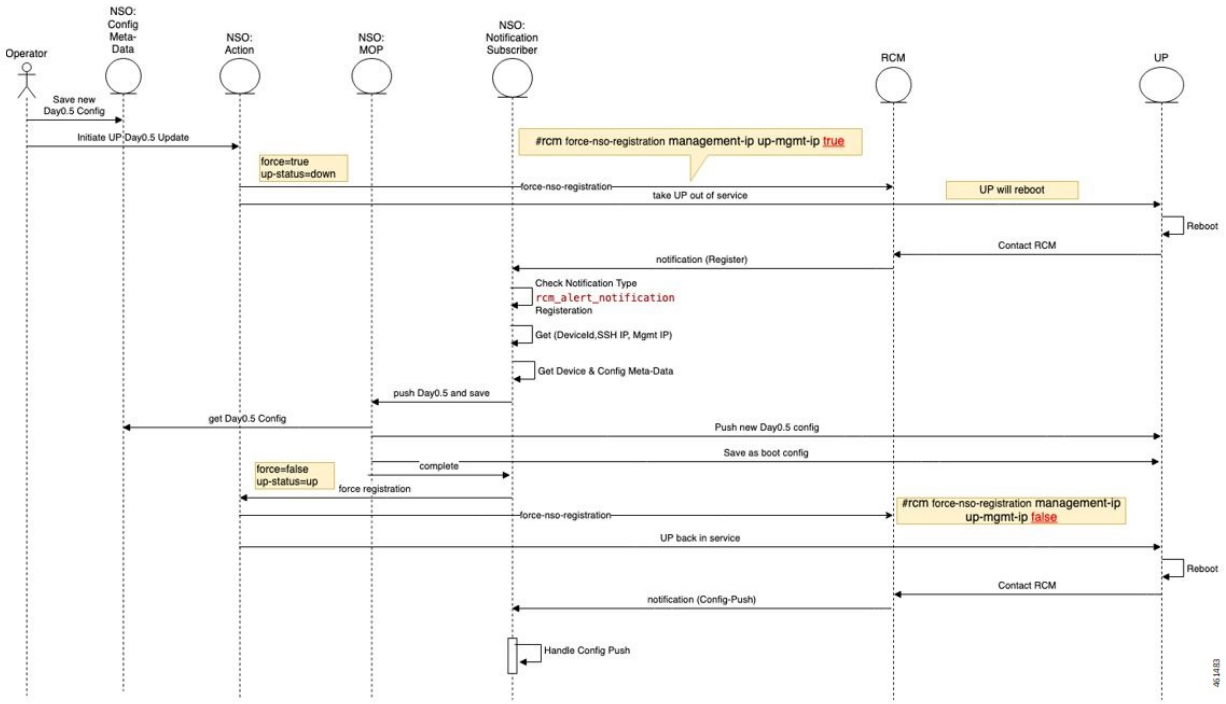
NSO は、UP 設定のプッシュ通知があるたびに、次の手順を実行します。

1. アラートステータスが [config-push] になるまで待機します。
2. デバイスの詳細（デバイス名、SSH IP、管理 IP、UP ステータス）を取得します。
3. NSO からデバイスメタデータを取得します。
4. UP フラッシュに共通ファイルが存在するかを確認します。
5. UP の状態がアクティブの場合、NSO はモビリティ MOP を使用して UP ホストに固有の構成ファイルをプッシュします。
6. UP 状態がスタンバイの場合、NSO はモビリティ MOP を使用して UP のすべてのホストに固有の構成ファイルをプッシュします。

7. 3 秒間スリープします。
8. 共通の構成ファイルが存在する場合、NSO は UP で live-status コマンドを実行してそれを適用します。
9. 共通の構成ファイルが存在しない場合、NSO はモビリティ MOP を使用して共通の構成ファイルを UP にプッシュし、UP で live-status コマンドを実行してこれを適用します。
10. NSO のデバイスメタデータを更新します。

UP Day-0.5 の更新

UP の Day-0.5 設定を変更するには、UP をリブートする必要があります。このため、変更中は UP はダウン状態となります。RCM は、特定の UP がリブートされると必ず強制的に通知を送信するコマンドを使用して、このユースケースをサポートします。この通知がトリガーとなって、NSO は新しい Day-0.5 設定をプッシュします。



1. NSO config-metadata で UP の Day-0.5 設定を更新する必要があります。
2. UP デバイス名と管理 IP アドレスを指定して、UP の Day-0.5 変更アクションを開始する必要があります。
3. NSO アクションは、UP のリブート時に NSO 登録を強制する RCM コマンドを実行します。

```
rcm force-nso-registration management-ip MGMT-IP  true
```

4. NSO アクションによって UP はダウン状態になります。このとき、次の 2 つのシナリオのいずれかとなります。
   1. スタンバイ UP：NSO アクションは UP でリロードコマンドを実行します。
   2. アクティブ UP：NSO アクションは、UP の management-ip とスタンバイ UP の management-ip を指定して、RCM で計画的スイッチオーバーコマンドを実行します。スタンバイ UP の management-ip は、UP グループの NSO デバイスメタデータから取得できます。
5. UP のリブート後（アクティブ UP またはスタンバイ UP）、RCM は [Registration] タイプの通知を生成し、これを NSO が受信します。
6. NSO RCM サブスクライバは、登録通知を受信すると、新しい MOP プロセスを開始して、対象となる UP の Day-0.5 設定をプッシュします。
7. NSO RCM サブスクライバは、継続して MOP ステータスを収集します。MOP が完了すると、NSO は UP で次のコマンドを実行します。

   rcm-config-push-complete
8. NSO RCM サブスクライバは、次のコマンドを実行して NSO アクションを呼び出し、force-notification コマンドを無効にします。

   rcm force-nso-registration management-ip *MGMT-IP* **false**
9. NSO アクションは、reload コマンドを実行して UP を起動します。
10. UP がリブートすると、RCM は Config-Push 通知を生成します。この通知は、通常どおり NSO によって処理されます。

設定プッシュの前提条件

設定のプッシュの前提条件を次に示します。

1. UP の場合：

   require rcm-configmgr

   CLI コマンドは、Day-0 設定の一部として事前に設定する必要があります。このコマンドは、N:M、1:1、およびスタンドアロンのシナリオに必要です。設定することで、ECS 設定の適切な動作が有効になります。
2. UP の場合、該当する場合は、CP から、または UP で PFD プッシュを無効にする必要があります。すべての UP 設定は、NSO から直接プッシュされます。これは、N:M、1:1、およびスタンドアロンのシナリオに当てはまります。
3. RCM Ops Center コンフィギュレーション モードの CLI は、次のように設定する必要があります。

   k8 smf profile rcm-config-ep config-mode NSO

   k8 smf profile rcm-config-ep switchover deployment false

4. オーバーライドする必要があるデフォルトの StarOS NED 設定がいくつかあります。

   1. 設定の変更はすべて、デバイスの起動設定（system.cfg）に自動的に保存されます。N:M 冗長性が使用されている場合、UP の変更の設定はそのロールによって異なるため、自動保存は望ましくないので、次の CLI 設定コマンドを使用してグローバルに無効化する必要があります。

      devices global-settings ned-settings cisco-staros write-memory-setting disabled

      1:1 またはスタンドアロン展開のみを使用する場合は、この設定をそのまま保持できます。

      N:M と 1:1/スタンドアロンを組み合わせて使用する場合は、前述のように設定の保存を無効にしてから、1:1/スタンドアロンに対する手動設定のプッシュで「save-config-permanently」パラメータを融合します。自動設定のプッシュの場合、モビリティ機能パックが必要に応じて自動的に設定を保存します。

   2. NEDは警告をエラーとして扱い、設定のプッシュを失敗させます。多くの場合、警告は無視できるため、設定のプッシュを続行する必要があります。警告の正規表現を使用して、選択した警告を無視するように NED を設定できます。次に例を示します。

      devices global-settings ned-settings cisco-staros behaviour config-warning-ignore .*not recommended to change the dictionary.*

      その他の一般的な例は次のとおりです。

      ned-settings cisco-staros behaviour config-warning-ignore .*About to overwrite boot.*

      ned-settings cisco-staros behaviour config-warning-ignore .*Standby card not ready.*

      最後の例は、SI への設定のプッシュに必要です。

5. RCM は SSH IP の概念をサポートしています。SSH IP は、機能を提供している VM に関係なく、特定のアクティブ UP を明確に追跡する方法です。NSO ベースのソリューションでは、SSH IP は使用されませんが、ダミーの SSH IP を設定する必要があります。これは、管理インターフェイスでセカンダリ IP アドレスとして設定されます。この設定におけるエラーを回避するには、Day-0.5 の一部として次の設定を推奨します。

   configure

   redundancy-configuration-module rcm *rcm*

   nso-ssh-ip context local interface-name *local1* **mask** *255.255.255.224*

6. NSO から VNF への読み取りおよび書き込み操作にかかる時間は、遅延に応じ変化する場合があります。遅延時間は、次に示されているように調整可能です。調整は、本当に遅延が原因である読み取りまたは書き込みエラーの問題が発生した場合にのみ行います。通常は、デフォルト設定で十分です。

   devices global-settings read-timeout 180

   devices global-settings write-timeout 180

制限事項と制約事項

このリリースでは、NSO ベースの設定管理機能に次の制限事項があります。

- 実稼働 NSO インスタンスは、一般的な Linux フレーバー（RedHat、Cisco Linux、Ubuntu、CentOS など）でのみ実行できます。
- Day-1 設定のみが RCM 通知で UP にプッシュされます。他の設定はプッシュされません。
- Day-N 設定の変更を後でプッシュする場合は、その変更を Day-1 設定ファイルとマージして、今後 RCM 通知で自動的にプッシュされるようにする必要があります。
- 事前に入力された設定ファイルに変更がある場合、それらは自動的にプッシュされません。すべてのターゲットデバイスに手動でプッシュする必要があります。次の自動プッシュの設定変更のみが考慮されます。

  N:M の UP の場合、事前に入力された設定ファイルは、それらを使用する VNF が少なくとも 1 つある場合、NSO（HA ペアとして実行されている場合は両方のインスタンス）で保持する必要があります。
- 設定コマンドはサポートされていません。設定ファイル内の show CLI コマンドはサポートされていません。
- NSO から管理する設定は、対応する NED（CP、UP の場合は StarOS NED、RCM の場合は RCM NED）によって認識される必要があります。現在、すべての StarOS 設定コマンドがサポートされているわけではありません。CUPS フィールド展開で最もよく使用される設定のみがサポートされています。欠落しているコマンドをサポートするには、新しい NED が必要です。
- ネイティブ StarOS CLI のサポートは 100% ではありません。サポートされている CLI コマンドの大部分はネイティブの StarOS CLI 形式で使用できますが、NSO が対応する StarOS CLI のバリアントのみを受け入れる場合もあります。このような CLI については、付録 A：互換性のない StarOS ネイティブ コマンド シンタックス （593 ページ）を参照してください。設定 MOP の「ドライラン」機能を使用すると、設定のプッシュを実行する前に、互換性がないかサポートされていない CLI によるエラーを検出できます。
- 操作中に要求を処理する NSO がダウンした場合、設定のプッシュが失敗する可能性があります。これは、手動と自動の両方の設定プッシュに当てはまります。また、NSO HA 展開とスタンドアロン NSO 展開の両方に当てはまります。障害の正確な種類に応じて、オペレータの介入が必要になる場合があります。
- N:M の冗長性シナリオの Day-0.5 設定変更ワークフローは、このリリースでは完全には機能しません。このリリースでの回避策は次のとおりです。

  1. 冗長グループから UP を削除します（アクティブだった場合は、最初にスタンバイにします）。
  2. UP は Day-0 および現在の Day-0.5 設定で起動します。
  3. UP で Day-0.5 設定を変更し、ブート設定として永続的に保存します。

4. UP を冗長グループに追加します。UP は RCM に登録され、残りの設定は NSO によって自動的にプッシュされます。

- このリリースでは、rcm-upf の MOP タイプを使用してアクティブな課金設定の変更をプッシュする場合、N:M 冗長シナリオでの Day-N 設定のプッシュには、事前の追加手順が必要です。MOP を呼び出す前に、その冗長グループ内のすべての UP でファイル */flash/mobility_production.cfg* を手動で削除する必要があります。
- 標準の StarOS CLI NED は、特定の機密設定データをクリアテキストとしてローカルに保存します。NSO では、NACM ルールを使用して機密設定データへのアクセスを制限できます。それでも懸念が残る場合は、シスコのアカウント担当者に連絡して、この機密データをローカルで暗号化する NED バージョンを入手してください。この暗号化は NED と NSO に固有であることに注意してください。StarOS は独自に機密データを暗号化するため、この 2 つの暗号化は個別のものです。NSO がローカルで機密データを暗号化する場合、StarOS デバイスに送信する前に復号します（SSH 経由で送信されるため、転送中に暗号化されますが、StarOS CLI ではクリアテキストとして受信されます）。
- N:M 冗長性シナリオでは、RCM は SSH IP の概念をサポートします。NSO ベースのソリューションでは、SSH IP を使用しません。ただし、FCS（3.0.0 および 21.25）の場合、ソリューションの SSH IP を指定する必要があります。ルーティング不可能なプライベートアドレスを含む任意のアドレスで十分です。このアドレスは、UP の管理インターフェイスでセカンダリアドレスとして設定されます。また、UP の SSH IP 設定要件に関する注意事項については、設定プッシュの前提条件 （589 ページ）の項を参照してください。

トラブルシューティング

障害対応では、次のオプションを使用できます。

1. タスク ID のダッシュボード出力を使用して、詳細を確認できます。次に例を示します。

   ```
   mobility-mop:action mop-automation-status task-id 12d5fc33-2f9e-44e3-81e3-14043d4ee39d
   ```

2. 障害が発生した場合、一部のアラームが発生する可能性があります。これらを確認するには、

   show alarms

   CLI コマンドを使用します。

3. 詳細なログは、*/var/log/ncs/ncs-java-vm.log* ファイルで確認できますが、これは開発者のデバッグ向けです。

付録 A：互換性のない StarOS ネイティブ コマンド シンタックス

ここでは、NED ではすでにサポートされているものの（下に太字で表示するもの）、StarOS ネイティブ コマンド シンタックスとの互換性がないコマンドを示します。

モード	コマンド	説明
context xxx/ggsn-service yyy	**ip qos-dscp qci 9 af31 gtpc af41**	「ip qos-dscp qci 9 af31」と 「ip qos-dscp gtpc af41」を個別に受け付けます。デバイスにプッシュするときは、両方合わせてプッシュします。
context xxx/apn yyy	apn fnetcoriolis **default max-contexts** **default cc-roaming** **default ipv6 address alloc-method** exit	「no max-contents」、「no cc-roaming」、および「no ipv6 addres alloc-method」を受け付けて、デバイスに対して「default xxx」を生成します。
context xxx/crypto map yyy (ikev2-pv4)/payload zzz match ipv4	crypto map ipsec_tunnel ikev2-ipv4 keepalive interval 4 timeout 1 num-retry 4 payload mypaiload match ipv4 **default lifetime** exit	「no lifetime」を受け付けて、デバイスに対して「default lifetime」を生成します。
active-charging service xxx/credit-control group yyy/	credit-control group cc-m2mpt quota validity-time 600 diameter reauth-blacklisted-content content-based-rar **default diameter send-ccru on-rar always** **default diameter mscc-per-ccr-update** exit	「no xxx」を受け付けて、デバイスに対して「default xxx」を生成します。

モード	コマンド	説明
context xxx/ikev2-ikesa transform-set yyy	ikev2-ikesa transform-set transformset_li **default encryption** **default group** **default hmac** **default lifetime** **default prf** exit	「no xxx」を受け付けて、デバイスに対して「default xxx」を生成します。
global config mode	**end** および **#exit**	rload はこれらのコマンドを受け付けません。
global config mode	snmp trap enable	相当するコマンド：no snmp trap suppress
active-charging service xxx/ruledef yyy または「!」を含むすべてのコマンド	active-charging service ecs ruledef rd-webredirect-apn-sl2sfr **bearer 3gpp imsi !range imsi-pool imsi-NOREDIRECT** exit	二重引用符で囲まれているか、バックスラッシュでエスケープされていない限り、rload は「!」記号を認識しません。
active-charging service xxx/ruledef yyy %NN を含むすべての URL	ruledef rd1 www url = http://itunes.apple.com/WebObjects/MZStore.woa/wa/viewSoftware**%3f**id=362713555&amp exit	%3f は「\」でエスケープする必要があります。

モード	コマンド	説明
context xxx/gtpp group yyy	gtpp group sgw **no gtpp attribute node-id** **no gtpp attribute losdv** **no gtpp trigger time-limit** **no gtpp trigger tariff-time-change** **no gtpp trigger serving-node-change-limit** **no gtpp trigger inter-plmn-sgsn-change** **no gtpp trigger qos-change** **no gtpp trigger rat-change** **no gtpp trigger ms-timezone-change** **no gtpp trigger uli-change**	これらのコマンドは、NED ではデフォルト設定として処理されますが、StarOS では処理されません。
context xxx/ims-auth-service yyy	p-cscf table 1 row-precedence 1 ipv4-address 209.165.200.227 secondary **ipv4-address** 209.165.200.229	ハイライトしたキーワードは、セカンダリ IP アドレスに対してのみ ipv4-address に変更する必要があります。
context xxx/ims-auth-service yyy	default signaling-flag	代わりに「no signalling-flag」を使用します。
context xxx/ims-auth-service yyy	default traffic-policy general-pdp-context no-matching-gates direction downlink	代わりに、「no traffic-policy general-pdp-context no-matching-gates direction downlink」を使用します。
context xxx/ims-auth-service yyy	p-cscf table 1 row-precedence 1 ipv6-address 2001:860:ffff:feb6::a secondary **ipv6-address** 2001:860:ffff:feb4::9	ハイライトしたキーワードは、セカンダリ IP アドレスに対してのみ ipv6-address に変更する必要があります。
context xxx/hexdump-module	default file rotation volume time-stamp monitor- subscriber-file-name	相当するコマンド： no file rotation volume no file time-samp no file monitor-subscriber-file-name
context xxx/hexdump-module	default file rotation volume	相当するコマンド： no file rotation volume

モード	コマンド	説明
context xxx/hexdump-module	default file time-stamp	相当するコマンド： no file time-stamp
context xxx/hexdump-module	default subscriber-file-name	相当するコマンド： no subscriber-file-name
context xxx/hexdump-module	default hexdump transfer-mode	相当するコマンド： no hexdump transfer-mode
context xxx/hexdump-module	default hexdump push-interval	相当するコマンド： no hexdump push-interval
context xxx/edr-module active-charging-service	default cdr transfer-mode push via transfer-mode	相当するコマンド： no cdr transfer-mode push
context xxx/session-event-module	default event transfer-mode push via transfer-mode	相当するコマンド： no event transfer-mode push
context xxx/router bgp NNN	context gy router bgp 64650 neighbor 209.165.200.226 remote-as 15557 **no neighbor 209.165.200.226 capability graceful-restart**	StarOS にはデフォルト設定として、グレースフルリスタート機能があります。NED は、これとは逆の方法でこれらのコマンドを処理します。 （注） この CLI は、StarOS CLI NED バージョン 5.50 以降でサポートされています。

付録 B：RCM を使用した N:M 展開の設定例

ホスト固有の設定：UP

次に、2 つのアクティブ UP のホスト固有の設定例を示します。設定はそれぞれの UP にプッシュされます。

最初のアクティブ UP

```
config
context EPC2
interface loop1_up1 loopback
```

```
ip address 209.165.200.225 255.255.255.224

interface loop2_up1 loopback
ip address 209.165.200.226 255.255.255.224

interface loop3_up1 loopback
ip address 209.165.200.227 255.255.255.224

interface loop4_up1 loopback
ip address 209.165.200.228 255.255.255.224

interface loop5_up1 loopback
ip address 209.165.200.229 255.255.255.224

exit
exit

context EPC2
sx-service sx_up1
instance-type userplane
bind ipv4-address 209.165.200.229
exit

exit
exit

context EPC2
gtpu-service pgw-gtpu_up1
bind ipv4-address 209.165.200.226
exit
gtpu-service saegw-sxu_up1
bind ipv4-address 209.165.200.227
exit
gtpu-service sgw-engress-gtpu_up1
bind ipv4-address 209.165.200.228
exit
gtpu-service sgw-ingress-gtpu_up1
bind ipv4-address 209.165.200.225

exit
exit
config
context EPC2
user-plane-service up_up1
associate gtpu-service pgw-gtpu_up1 pgw-ingress
associate gtpu-service sgw-ingress-gtpu_up1 sgw-ingress
associate gtpu-service sgw-engress-gtpu_up1 sgw-egress
associate gtpu-service saegw-sxu_up1 cp-tunnel
associate sx-service sx_up1
associate fast-path service
associate control-plane-group g1
exit

exit
exit
```

2 番目のアクティブ UP

```
config
context EPC2
interface loop1_up2 loopback
ip address 209.165.200.230 255.255.255.224

interface loop2_up2 loopback
```

```
ip address 209.165.200.231 255.255.255.224

interface loop3_up2 loopback
ip address 209.165.200.232 255.255.255.224

interface loop4_up2 loopback
ip address 209.165.200.233 255.255.255.224

interface loop5_up2 loopback
ip address 209.165.200.234 255.255.255.224

exit
exit

context EPC2
sx-service sx_up2
instance-type userplane
bind ipv4-address 209.165.200.234
exit

exit
exit

context EPC2
gtpu-service pgw-gtpu_up2
bind ipv4-address 209.165.200.231
exit
gtpu-service saegw-sxu_up2
bind ipv4-address 209.165.200.232
exit
gtpu-service sgw-engress-gtpu_up2
bind ipv4-address 209.165.200.233
exit
gtpu-service sgw-ingress-gtpu_up2
bind ipv4-address 209.165.200.230

exit
exit

context EPC2
user-plane-service up_up2
associate gtpu-service pgw-gtpu_up2 pgw-ingress
associate gtpu-service sgw-ingress-gtpu_up2 sgw-ingress
associate gtpu-service sgw-engress-gtpu_up2 sgw-egress
associate gtpu-service saegw-sxu_up2 cp-tunnel
associate sx-service sx_up2
associate fast-path service
associate control-plane-group g1
exit

exit
exit
```

ホスト固有の設定：RCM

RCM のホスト固有の設定例を以下に示します。この設定は RCM にプッシュされます。

最初のアクティブ RCM

```
config
control-plane-group g1
```

```
 redundancy-group 1
  host Active1
   peer-node-id ipv4-address 209.165.200.240
  exit
 exit
exit
context EPC2
 interface-loopback loop1_up1
  redundancy-group 1
   host Active1
    ipv4-address 209.165.200.224/27
   exit
  exit
 exit
 interface-loopback loop2_up1
  redundancy-group 1
   host Active1
    ipv4-address 209.165.201.0/27
   exit
  exit
 exit
 interface-loopback loop3_up1
  redundancy-group 1
   host Active1
    ipv4-address 209.165.202.128/27
   exit
  exit
 exit
 interface-loopback loop4_up1
  redundancy-group 1
   host Active1
    ipv4-address 192.0.2.0/24
   exit
  exit
 exit
 interface-loopback loop5_up1
  redundancy-group 1
   host Active1
    ipv4-address 198.51.100.0/24
   exit
  exit
 exit
 user-plane-service up_up1
  redundancy-group 1
   host Active1
    associate control-plane-group g1
    associate fast-path service
    associate sx-service sx_up1
    associate gtpu-service pgw-gtpu_up1 pgw-ingress
    associate gtpu-service saegw-sxu_up1 cp-tunnel
    associate gtpu-service sgw-engress-gtpu_up1 sgw-egress
    associate gtpu-service sgw-ingress-gtpu_up1 sgw-ingress
   exit
  exit
 exit
 gtpu-service pgw-gtpu_up1
  redundancy-group 1
   host Active1
    bind ipv4-address 209.165.201.0
   exit
  exit
 exit
 gtpu-service saegw-sxu_up1
  redundancy-group 1
```

```
   host Active1
    bind ipv4-address 209.165.202.128
   exit
  exit
 exit
 gtpu-service sgw-engress-gtpu_up1
  redundancy-group 1
   host Active1
    bind ipv4-address 192.0.2.0
   exit
  exit
 exit
 gtpu-service sgw-ingress-gtpu_up1
  redundancy-group 1
   host Active1
    bind ipv4-address 198.51.100.123
   exit
  exit
 exit
 sx-service sx_up1
  redundancy-group 1
   host Active1
    bind ipv4-address 198.51.100.0
    instance-type userplane
   exit
  exit
 exit
exit
```

2 番目のアクティブ RCM

```
config
control-plane-group g1
 redundancy-group 1
  host Active2
   peer-node-id ipv4-address 209.165.200.240
  exit
 exit
exit
context EPC2
 interface-loopback loop1_up2
  redundancy-group 1
   host Active2
    ipv4-address 209.165.200.224/27
   exit
  exit
 exit
 interface-loopback loop2_up2
  redundancy-group 1
   host Active2
    ipv4-address 209.165.201.0/27
   exit
  exit
 exit
 interface-loopback loop3_up2
  redundancy-group 1
   host Active2
    ipv4-address 209.165.202.128/27
   exit
  exit
 exit
 interface-loopback loop4_up2
  redundancy-group 1
   host Active2
```

```
    ipv4-address 192.0.2.0/24
   exit
  exit
 exit
 interface-loopback loop5_up2
  redundancy-group 1
   host Active2
    ipv4-address 198.51.100.0/24
   exit
  exit
 exit
 user-plane-service up_up2
  redundancy-group 1
   host Active2
    associate control-plane-group g1
    associate fast-path service
    associate sx-service sx_up2
    associate gtpu-service pgw-gtpu_up2 pgw-ingress
    associate gtpu-service saegw-sxu_up2 cp-tunnel
    associate gtpu-service sgw-engress-gtpu_up2 sgw-egress
    associate gtpu-service sgw-ingress-gtpu_up2 sgw-ingress
   exit
  exit
 exit
 gtpu-service pgw-gtpu_up2
  redundancy-group 1
   host Active2
    bind ipv4-address 209.165.201.0
   exit
  exit
 exit
 gtpu-service saegw-sxu_up2
  redundancy-group 1
   host Active2
    bind ipv4-address 209.165.202.128
   exit
  exit
 exit
 gtpu-service sgw-engress-gtpu_up2
  redundancy-group 1
   host Active2
    bind ipv4-address 192.0.2.0
   exit
  exit
 exit
 gtpu-service sgw-ingress-gtpu_up2
  redundancy-group 1
   host Active2
    bind ipv4-address 198.51.100.123
   exit
  exit
 exit
 sx-service sx_up2
  redundancy-group 1
   host Active2
    bind ipv4-address 198.51.100.0
    instance-type userplane
   exit
  exit
 exit
exit
```

共通の設定

以下に共通の設定例を示します。これは、すべてのアクティブ UP とすべてのスタンバイ UP にプッシュされます。

```
config
 active-charging service ACS
 idle-timeout udp 60
 statistics-collection ruledef all
 host-pool IPv6_VoLTE_Phone_Host_7
 ip 209.165.200.224/27
 ip 64:ff9b::d3f6:6b00/120
 ip 2001:e60:6000::/46
 ip 2001:e60:6004::/46
 ip range 209.165.200.225 to 209.165.200.234
 ip range 64:ff9b::e00:4f12 to 64:ff9b::e00:4f14
 ip range 64:ff9b::3d6e:ff52 to 64:ff9b::3d6e:ff59
 ip range 64:ff9b::d3f6:682c to 64:ff9b::d3f6:683e
 exit
 port-map M_learning_Port
 port range 1 to 9500
 port range 10001 to 30000
 exit
 port-map OTM_Advertisement_port
 port 90
 port 9090
 exit
 ruledef ICMP
 ip protocol = 1
 exit
 ruledef ICMPv6
 ip protocol = icmpv6
 exit
 ruledef IPv6_VoLTE_Phone_1
 udp either-port range port-map M_learning_Port
 ip server-ip-address range host-pool IPv6_VoLTE_Phone_Host_7
 exit
 ruledef RD-allTraffic
 ip any-match = TRUE
 exit
 ruledef RD_Charge
 ip server-ip-address = 209.165.201.0/27
 exit
 ruledef catchall
 ip any-match = TRUE
 exit
 ruledef googles
 icmpv6 any-match = TRUE
 exit
 ruledef qci1
 tcp any-match = TRUE
 exit
 ruledef route-ims-ipv6-nexthop
 ip uplink = TRUE
 ip version = ipv6
 exit
 ruledef optIn
 ip any-match = TRUE
 exit
 group-of-ruledefs GoR_FOTA
 add-ruledef priority 1 ruledef FOTA_SAMSUNG
 add-ruledef priority 2 ruledef FOTA_LG
 add-ruledef priority 3 ruledef FOTA_LG_2
```

```
 add-ruledef priority 5 ruledef FOTA_PANTECH_2
 add-ruledef priority 8 ruledef IOS_OTA_Update
 add-ruledef priority 9 ruledef GOTA_google
 add-ruledef priority 10 ruledef FOTA_Hybrid_Egg
 add-ruledef priority 11 ruledef FOTA_SAMSUNG_2
 add-ruledef priority 12 ruledef FOTA_SAMSUNG_3
 add-ruledef priority 13 ruledef FOTA_SAMSUNG_4
 add-ruledef priority 15 ruledef FOTA_SAMSUNG_5
 add-ruledef priority 16 ruledef FOTA_LG_4
 add-ruledef priority 17 ruledef FOTA_LG_5
 add-ruledef priority 18 ruledef FOTA_HUAWEI_Egg
 add-ruledef priority 20 ruledef KTF_DMS_FOTA
 add-ruledef priority 21 ruledef FOTA_Nlabs
 add-ruledef priority 22 ruledef FOTA_LTE_Beam
 add-ruledef priority 23 ruledef FOTA_S_Mobile
 add-ruledef priority 24 ruledef FOTA_Giga_Genie
 add-ruledef priority 100 ruledef SAMSUNG_SKT_issue
 add-ruledef priority 104 ruledef new_FOTA_Pantech
 add-ruledef priority 106 ruledef new_FOTA_KTtech
 add-ruledef priority 107 ruledef new_IOS_OTA_Log
 add-ruledef priority 114 ruledef new_FOTA_LG_3
 add-ruledef priority 200 ruledef IoT_FOTA_mexus
 add-ruledef priority 201 ruledef IoT_FOTA_acnt
 add-ruledef priority 202 ruledef IoT_FOTA_amtel
 exit
 packet-filter qci1
 ip protocol = 1
 ip remote-port = 1001
 priority 1
 exit
 packet-filter subscriber-pools
 exit
 charging-action CA-nothing
 content-id 5
 exit
 charging-action CA_Chargeable_2
 content-id 1
 billing-action egcdr
 exit
charging-action CA_Charge
exit
 charging-action DSI
 billing-action egcdr
 flow action discard
 tft packet-filter permit_all
 exit
 charging-action ca11
 service-identifier 22
 billing-action egcdr
 cca charging credit
 flow action discard
 flow limit-for-bandwidth id 4
 exit
 charging-action catchall
 content-id 10
 billing-action egcdr
 cca charging credit rating-group 10 preemptively-request
 exit
 charging-action qci1
 billing-action egcdr
 cca charging credit rating-group 1 preemptively-request
 qos-class-identifier 1
 tft packet-filter qci1
 exit
```

```
 bandwidth-policy bw-policy
 flow limit-for-bandwidth id 2 group-id 2
 flow limit-for-bandwidth id 4 group-id 4
 flow limit-for-bandwidth id 10 group-id 12
 flow limit-for-bandwidth id 562 group-id 562
 group-id 2 direction downlink peak-data-rate 225280 peak-burst-size 2253 violate-action
 discard
 group-id 4 direction uplink peak-data-rate 450560 peak-burst-size 4506 violate-action
discard
 group-id 10 direction uplink peak-data-rate 1153434 peak-burst-size 11534 violate-action
 discard
 group-id 11 direction uplink peak-data-rate 10000 peak-burst-size 10000 violate-action
 discard
 exit
 rulebase 5G-DF
 tcp packets-out-of-order timeout 30000
 no retransmissions-counted
 edr sn-charge-volume count-dropped-units
 bandwidth default-policy bw-policy
 exit
 rulebase RB-allTraffic
 action priority 100 ruledef RD-allTraffic charging-action CA_Charge
 egcdr threshold interval 3600
 egcdr threshold volume total 4000000
 exit
 rulebase RB_Charge
 action priority 10 ruledef RD_Charge charging-action CA_Charge
 exit
 rulebase cisco
 billing-records egcdr
 action priority 12 ruledef catchall charging-action catchall monitoring-key 123
 egcdr threshold interval 120
 egcdr threshold volume total 1000000
 exit
 rulebase cisco_dynamic
 action priority 11 dynamic-only ruledef qci1 charging-action qci1
 action priority 10000 ruledef catchall charging-action catchall
 egcdr threshold interval 120
 egcdr threshold volume total 100000
 exit
 rulebase P2P
 transactional-rule-matching
 dynamic-rule order first-if-tied
 tethering-detection application ip-ttl value 62
 flow end-condition timeout normal-end-signaling session-end charging-edr flow-edr
 billing-records egcdr
 edr transaction-complete http charging-edr http-edr
 flow control-handshaking charge-to-application all-packets
 egcdr threshold interval 3600
 egcdr threshold volume total 4000000000
 no cca quota retry-time
 cca diameter requested-service-unit sub-avp volume cc-total-octets 5000
 p2p dynamic-flow-detection
 no tft-notify-ue-def-bearer
 exit
 rulebase default
 exit
 rulebase wap_adult
      transactional-rule-matching
      tcp mss 1320 limit-if-present
      flow end-condition handoff timeout normal-end-signaling session-end charging-edr
flow-edr
      billing-records egcdr radius
      action priority 28 ruledef catchall charging-action CA_Chargeable_2
```

```
      action priority 29 ruledef catchall charging-action CA_Chargeable_2
      edr transaction-complete http charging-edr http-edr
     flow control-handshaking charge-to-application  mid-session-packets tear-down-packets

      egcdr threshold volume total 3000000
#exit
 service-scheme ss1
 exit
 credit-control group DCCA_grp1
 diameter origin endpoint Gy
 diameter peer-select peer minid-Gy
 pending-traffic-treatment noquota buffer
 pending-traffic-treatment quota-exhausted buffer
 pending-traffic-treatment validity-expired pass
 exit
 credit-control group default
 pending-traffic-treatment noquota pass
 pending-traffic-treatment quota-exhausted buffer
 exit
 policy-control charging-rule-base-name active-charging-rulebase
 policy-control burst-size auto-readjust duration 3
 exit
 context ecs
 apn cisco.com
 ip context-name ecs
 exit
 apn starent.com
 ip context-name ecs
 exit
end
```

スタンバイ設定（Active1 + Active2）

```
config
context EPC2
interface loop1_up1 loopback
ip address 198.51.100.123 255.255.255.224

interface loop2_up1 loopback
ip address 209.165.201.0 255.255.255.224

interface loop3_up1 loopback
ip address 209.165.202.128 255.255.255.224

interface loop4_up1 loopback
ip address 192.0.2.0 255.255.255.224

interface loop5_up1 loopback
ip address 198.51.100.0 255.255.255.224

exit
exit

context EPC2
sx-service sx_up1
instance-type userplane
bind ipv4-address 198.51.100.0
exit

exit
exit

context EPC2
```

```
gtpu-service pgw-gtpu_up1
bind ipv4-address 209.165.201.0
exit
gtpu-service saegw-sxu_up1
bind ipv4-address 209.165.202.128
exit
gtpu-service sgw-engress-gtpu_up1
bind ipv4-address 192.0.2.0
exit
gtpu-service sgw-ingress-gtpu_up1
bind ipv4-address 198.51.100.0

exit
exit

context EPC2
user-plane-service up_up1
associate gtpu-service pgw-gtpu_up1 pgw-ingress
associate gtpu-service sgw-ingress-gtpu_up1 sgw-ingress
associate gtpu-service sgw-engress-gtpu_up1 sgw-egress
associate gtpu-service saegw-sxu_up1 cp-tunnel
associate sx-service sx_up1
associate fast-path service
associate control-plane-group g1
exit

exit
exit

config
context EPC2
interface loop1_up2 loopback
ip address 209.165.200.230 255.255.255.224

interface loop2_up2 loopback
ip address 209.165.200.231 255.255.255.224

interface loop3_up2 loopback
ip address 209.165.200.232 255.255.255.224

interface loop4_up2 loopback
ip address 209.165.200.233 255.255.255.224

interface loop5_up2 loopback
ip address 209.165.200.234 255.255.255.224

exit
exit

context EPC2
sx-service sx_up2
instance-type userplane
bind ipv4-address 209.165.200.234
exit

exit
exit

context EPC2
gtpu-service pgw-gtpu_up2
bind ipv4-address 209.165.200.231
exit
gtpu-service saegw-sxu_up2
bind ipv4-address 209.165.200.232
```

```
exit
gtpu-service sgw-engress-gtpu_up2
bind ipv4-address 209.165.200.233
exit
gtpu-service sgw-ingress-gtpu_up2
bind ipv4-address 209.165.200.230

exit
exit

context EPC2
user-plane-service up_up2
associate gtpu-service pgw-gtpu_up2 pgw-ingress
associate gtpu-service sgw-ingress-gtpu_up2 sgw-ingress
associate gtpu-service sgw-engress-gtpu_up2 sgw-egress
associate gtpu-service saegw-sxu_up2 cp-tunnel
associate sx-service sx_up2
associate fast-path service
associate control-plane-group g1
exit

exit
exit
```

第 64 章

4G CUPS に対する NSO オーケストレーション

機能説明

Cisco Network Service Orchestrator（NSO）ベースの VNF オーケストレーションを使用すると、新たに作成された仮想ネットワーク機能（VNF）デバイス（CP、UP、RCM など）のライフサイクルを管理できます。

Cisco NSO Orchestration for 4G CUPS ソリューションは、次の機能を提供します。

- NSO CLI、Web インターフェイス、または NSO RESTCONF API によるインスタンス化
- インスタンス化が成功した場合の CP、UP、RCM などの VNF デバイスのオンボーディング
- インスタンス化が成功した後の Day-0.5 および Day-1 CUPS 設定のプッシュ
- VNF デバイスのデコミッション

使用例

NSO オーケストレーション ソリューションは、次のユースケースに対応します。

1. 新しい CP、UP、RCM のインスタンス化

   CUPS で新しい 4G ベースの VNF（CP、UP、RCM）をインスタンス化します。CP は、仮想化パケット コア シングル インスタンス（VPC-SI）または仮想化パケットコア分散インスタンス（VPC-DI）にすることができますが、UP は VPC-SI のみにすることができます。

   障害が発生した場合は、ユーザーに通知されます。

2. CP、UP、RCM の終了

   CUPS で 4G ベースの VNF（CP、UP、RCM）を終了します。

   障害が発生した場合は、ユーザーに通知されます。

3. VNF ダッシュボードの現在のステータスの更新

   VNF のダッシュボードに現在のステータスを表示します。

4. CP、UP、RCM の論理グループの設定

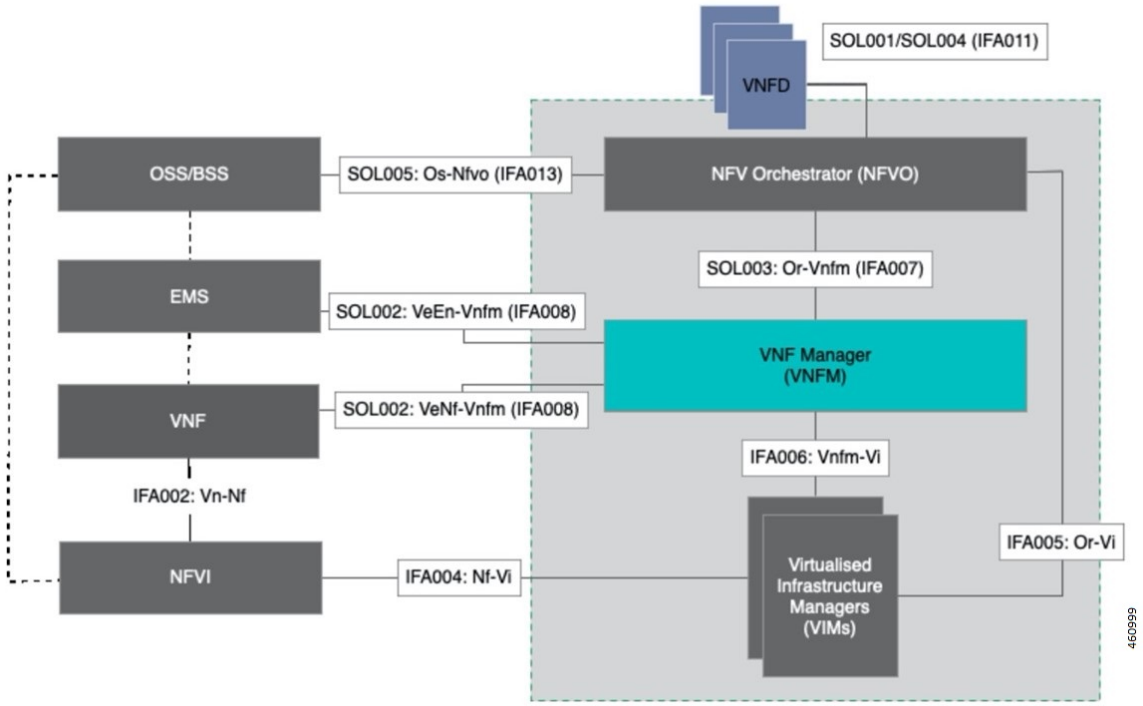
   CP、UP、および RCM をグループ化するように NSO でデバイスグループを設定し、対応する VNF をデバイスグループに追加します。

機能の仕組み

アーキテクチャ

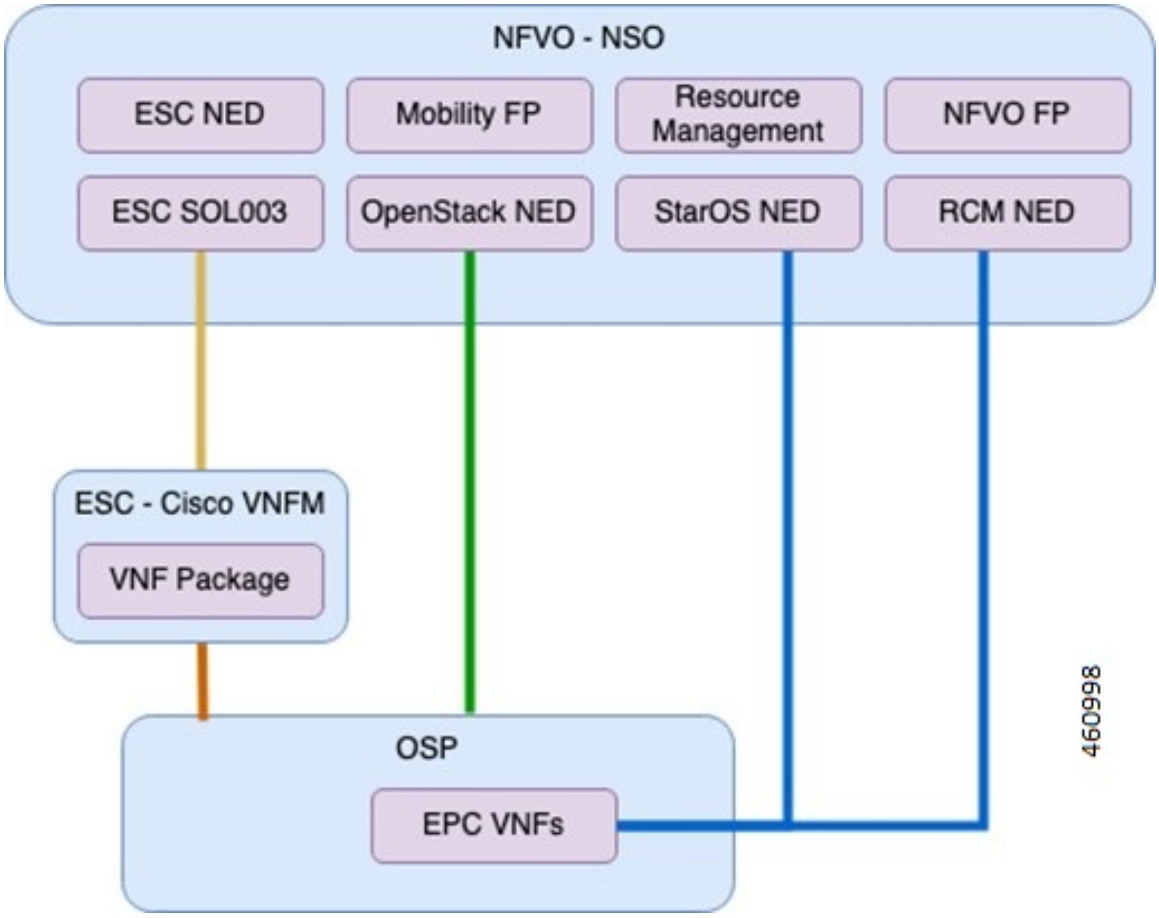
Cisco NSO オーケストレーション エンジン ソフトウェア モジュールは、ネットワーク機能の仮想化オーケストレータ（NFVO）機能を処理します。NFV ソリューションは、次の図に示すように、ETSI NFV 管理およびオーケストレーション（MANO）モデルに従います。

図 *34 : NVF* ソリューション アーキテクチャ



次の図は、ソリューションに関連するコンポーネントとフレームワークの概要を示しています。

図 *35 : NFV* ソリューションのコンポーネント



コンポーネント

以下に、NSO の重要なコンポーネントの一部を示します。

- **Cisco NFVO 機能パック** ：

  Cisco NFVO 機能パックには、MANO 仕様（SOL006）に準拠した YANG モデルが含まれます。

  Cisco NFVO 機能パックには、VNF マネージャ（VNFM）および OpenStack に MANO 記述子のインスタンス化ロジックを実装する **cisco-etsi-nfvo** のモデルが含まれています。仮想ネットワーク機能（VNF）とネットワークサービス（NS）は、このパッケージの主要なサービスです。ノースバウンドユーザーは、これらのサービスとやり取りして VNF またはネットワークサービスを開始します。

  また、リソース オーケストレーション（RO）機能を含む **cisco-etsi-nfvo-ro** のモデルも含まれます。リソース オーケストレーションは、仮想化インフラストラクチャ マネージャ（VIM）の物理リソースの割り当てを管理します。これらの物理リソースは、VNF または NS によって使用されます。

- **NSO の StarOS NED**：

  StarOS ベースのネットワーク エレメント ドライバ（NED）は、設定をプッシュするために Cisco 4G CUPS VNF と接合します。

- **NSO の RCM NED**：

  RCM ベースの NETCONF NED は、NSO と RCM デバイス間の通信を確立するために使用されます。

- **Cisco ESC SOL003 NED**：

  この NED は、ETSI SOL3 準拠デバイスに使用されます。Elastic Services Controller（ESC）も、SOL3 準拠デバイスとして NSO に追加されます。

- **NFV アプリケーション モビリティ パッケージ**：

  これは、VNF ライフサイクル管理と VNF ダッシュボードの更新を提供するカスタムパッケージです。

プラットフォームおよびソフトウェアの最小要件

NSO オーケストレーションをサポートするために必要なプラットフォームとソフトウェアの最小要件は次のとおりです。

- サポートされる VIM：OpenStack
- サポートされる VNFM：Cisco ESC
- サポートされるオーケストレータ：NSO
- ネットワーク要素：
  - RCM
  - VPC-SI（UP/CP）
  - VPC-DI（CP）

表 *37*：ソフトウェア バージョン

ソフトウェア	最小バージョン
Redhat OpenStack	13（Queens） （注） VMWare や OSP 16 は、サポートおよび検証の対象外です。
Cisco ESC	5.5.0.86
Cisco NSO	6.1.6.1
OpenStack NED	4.2.30

ソフトウェア	最小バージョン
ESC NED	5.10.0.97
StarOS NSO NED	5.52.4
Cisco NFVO FP	4.7.3
Mobility FP	3.5
NSO リソース管理	3.5.2
Cisco NSO HCC	6.0.1

この機能は、次の ETSI MANO 仕様をサポートします。

表 *38 : ETSI MANO* の仕様

仕様	サポートされるバージョン	説明
SOL001	v2.5.1	VNF 記述子のフォーマットと構造を定義します
SOL003	v2.4.1	Or-Vnfm 参照ポイント上のすべてのインタラクションを定義します

ネットワークおよびハードウェア要件

ネットワーク要件：

次の表に、NSO および ESC のネットワーク要件を示します。

表 *39 : NSO* および *ESC* ネットワーク要件

アプリケーション	[Management IP]	オーケストレーション	HA ペア間の接続
NSO（2 VM + VIP）	3	3	遅延が 30 ミリ秒未満の 100 Mbps の L2 接続
ESC（2 VM + VIP）	3	3	遅延が 30 ミリ秒未満の 100 Mbps の L2 接続

ハードウェア要件

次の表に、最大 250 の VNF をサポートするための NSO および ESC 仮想マシンの仕様を示します。

表 *40 : NSO* および *ESC VM* の仕様

アプリケーション	VM の数	VM CPU コア数	VM RAM	VM ストレージ	VM 接続
NSO	2	8	サポート対象のすべての StarOS デバイス用に 16 GB RAM の基準＋10 MB RAM	100 GB ディスク（SSD を推奨）	10 Gbps ネットワークリンク X 1
ESC	2	4	16 GB	100 GB	

ライセンス

4G CUPS の NSO オーケストレーションは、ライセンス供与されたシスコの機能です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

コール フロー

この項では、4G CUPS オーケストレーション機能の主要なコールフローについて説明します。

VNF オンボーディング

この項では、VNF オンボーディングフローについて説明します。

図 *36 : VNF* オンボーディング

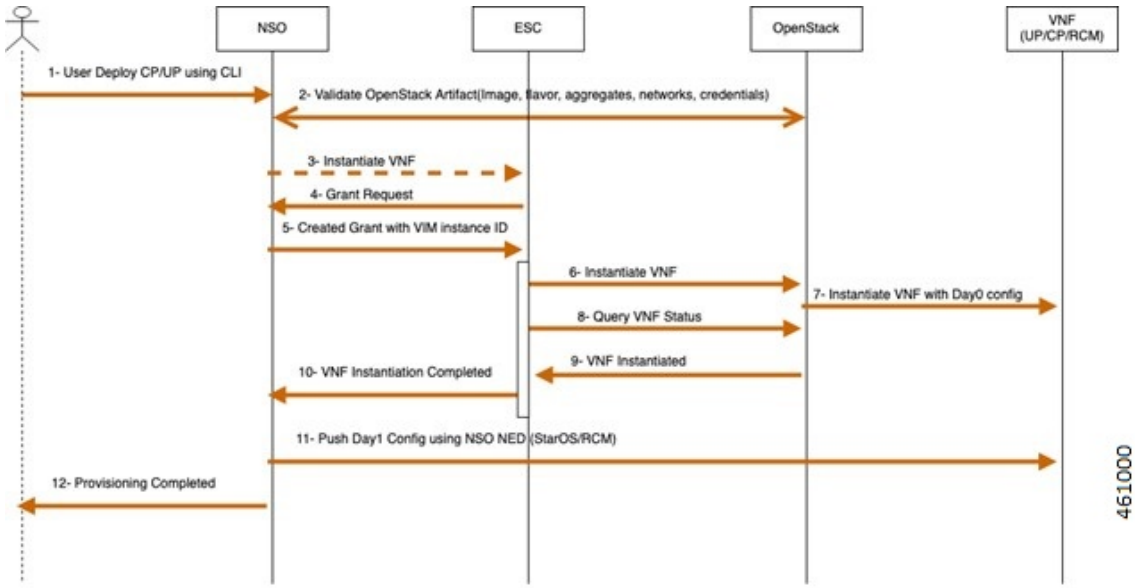


表 *41 :* コール フローの説明

ステップ	説明
1	ネットワークオペレータが、NSO CLI を使用して VNF（CP、UP、または RCM）をインスタンス化します。対象には、VNF をホストする VIM ID、および ESC が含まれます。
2	NSO が OpenStack を介してユーザーから提供されたデータを検証します。
3	NSO が ESC で VNF をインスタンス化するために SOL.003 要求を送信します。
4	ESC が NSO に付与要求を送信します。
5	NSO が VIM インスタンス ID を使用してリソース付与メッセージを ESC に送信します。
6	ESC が OpenStack API を使用して VNF をインスタンス化します。
7	OpenStack が VNF を起動します。
8	ESC が OpenStack に VNF ステータスをクエリします。
9	OpenStack が VNF-Up メッセージで応答します。
10	ESC が VNF のインスタンス化について NSO に通知します。
11	NSO が Day-1 設定を VNF にプッシュします。
12	NSO が VNF のプロビジョニングが完了したことをオペレータに通知します。

P2P モジュールのインストール

モビリティ機能パックでは、VNF 展開の一部として P2P モジュールのインストールをサポートします。P2P モジュールは、デバイスのオンボーディング後にインストールされます。P2P モジュールファイルは、VNF を展開する前に NSO にアップロードしておく必要があります。設定可能なパラメータによって、ファイルの場所と、P2P のインストールが必要かどうかを示します。

P2P のインストールが完了すると、MFP 3.4.2 以降のバージョンでは、新しくインスタンス化された VNF の P2P のデフォルト優先順位は「99」になります。MFP 3.4.2 より前のバージョンでは、P2P のデフォルト優先順位は「10」から始まります。「mobility-library」アクションコマンドを使用して P2P の優先順位をアップグレードするには、「付録 *C*」の手順を参照してください。

VNF の終了

ここでは、VNF の終了フローについて説明します。

図 *37 : VNF* の終了フロー

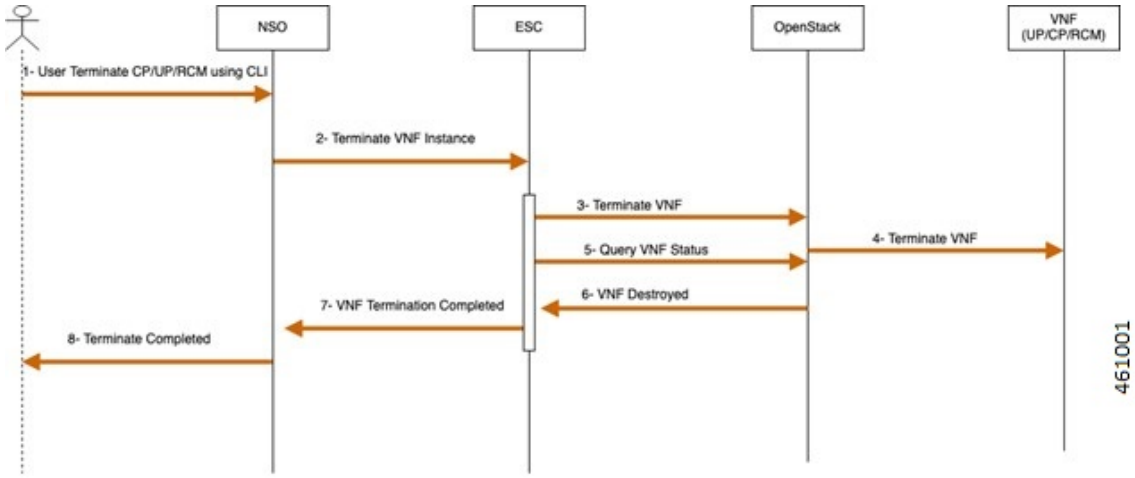


表 *42 :* コール フローの説明

手順	説明
1	オペレータは NSO CLI を使用して VNF（CP、UP、RCM）を終了します。これには、VNF ID、VNF をホストする VIM ID、および ESC が含まれます。
2	NSO は、ESC で VNF を終了するために SOL.003 要求を送信します。
3	ESC は OpenStack API を使用して VNF を終了します。
4	OpenStack は VNF を終了します。
5	ESC は OpenStack に VNF ステータスをクエリします。
6	OpenStack は VNF 破棄メッセージで応答します。
7	ESC は NSO に VNF の終了を通知します。
8	NSO は、VNF の終了が完了したことをオペレータに通知します。

リカバリ

自動修復は現在サポートされていません。

障害状態から以前の状態に回復するには、次の手順を実行します。

- VNFのインスタンス化をキャンセルまたは終了します。システムが元の状態に戻ります。

- VNF 終了プロセスをキャンセルまたは再作成します。システムが元の状態に戻ります。

制限事項

このリリースの 4G CUPS 機能の NSO オーケストレーションには、次の制限事項があります。

- 実稼働 NSO インスタンスは、一般的な Linux フレーバー（RedHat、Cisco Linux、Ubuntu、CentOS など）でのみ実行できます。
- 展開を処理する NSO/ESC インスタンスがダウンすると、VNF 展開が失敗する可能性があります。これは、ESC/NSO HA とスタンドアロン ESC/NSO の両方の展開に当てはまります。障害の正確な種類に応じて、オペレータの介入が必要です。展開後に自動設定がプッシュされる場合、展開は成功しても、NSO 障害のタイミングによっては、後続の設定のプッシュが失敗する可能性があります。

NSO パッケージのインストール

NSO オーケストレーション ソリューションは、NED およびその他の NSO パッケージのコレクションを使用します。以下に、各種パッケージとそのロールに関する詳細なリストを示します。これらのパッケージのインストール手順については、該当する NSO バージョンの『*NSO Administration Guide*』[英語] のパッケージに関する章を参照してください。

1. **NSO NED パッケージ**

   ほとんどの NSO NED パッケージは公開され、個別にダウンロードできます。詳しいダウンロード方法については、シスコの担当者にお問い合わせください。

   ncs-6.1-rcm-nc.v21.28.mx_20240415-072244Z.tar.gz：NSO からの RCM デバイス通信用の RCM NETCONF ベース NED

   ncs-6.1.6-cisco-staros-5.52.4.tar.gz：NSO からの StarOS デバイス（SI または DI）通信用の CLI ベース NED

   ncs-6.1.1-etsi-sol003-1.13.18.tar.gz：NSO からの ESC 通信用の ETSI SOL003 ベース NED

   ncs-6.1-openstack-cos-4.2.30.tar.gz：NSO からの Openstack 通信用の Openstack NED

   ncs-6.1.2.1-cisco-etsi-nfvo-4.7.3.tar.gz：NSO からの ESC 通信用の NETCONF ベース NED

   ncs-6.1.2.1-esc-5.10.0.97.tar.gz：NSO からの ESC 通信用の ETSI SOL ベース NED

2. **NSO カスタムパッケージ**

   NSO カスタムパッケージは、モビリティ VNF オーケストレーション用のカスタムビルドパッケージです。これらのパッケージは、モビリティ機能パックの tar アーカイブにバンドルされています。

   Mobility-common.tar.gz：設定およびデバイスメタデータの共通パッケージ

nfv-common.tar.gz：VNF オーケストレーション関連の共通ユーティリティの共通パッケージ

nfv-device-onboarding.tar.gz：NSO デバイスのオンボーディングをサポートするパッケージ

nfv-vim.tar.gz：Openstack 関連の事前チェック機能のパッケージ

nfv-vnf-lcm.tar.gz：VNF のインスタンス化および終了ロジックのパッケージ

mop-common.tar.gz：設定 MOP 関連の共通ユーティリティの共通パッケージ

Mobility-mop.tar.gz：モビリティ MOP 設定プッシュ用パッケージ

3. **オーケストレーションに必要な VNF パッケージ（SOL003/SOL004）**

   特定の VNF のオンボーディングに使用される VNF パッケージです。これらのパッケージはガイドラインとしてのみ提供されます。ほとんどの場合、特定のパッケージは導入環境に合わせてカスタマイズされます。

   VPC-SI-2P-IMAGE-BOOT：SI インスタンス化の参照用 SOL003/SOL004 CSAR パッケージ

   RCM-IMAGE-BOOT：RCM インスタンス化の参照用 SOL003/SOL004 CSAR パッケージ

   VPC-DI-2P-1DI-ENCRYPTVOLBOOT：2 つの CF と 4 つの SF を使用した VPC DI インスタンス化の参照用 SOL003/SOL004 CSAR パッケージ。SF には 2 つのサービスネットワークがあります。

   VPC-DI-2P-1DI-ENCRYPTVOLBOOT-LTD：2 つの CF と 2 つの SF を使用した VPC DI インスタンス化の参照用 SOL003/SOL004 CSAR パッケージ。SF には 2 つのサービスネットワークがあります。

   VPC-DI-2P-1DI-ENCRYPTVOLBOOT-LTD-1S-NETWORK：2 つの CF と 2 つの SF を使用した VPC DI インスタンス化の参照用 SOL003/SOL004 CSAR パッケージ。SF のサービスネットワークは 1 つのみです。

   create-zip.sh：SOL001 定義または Day-0 スクリプトに変更がある場合に、SOL003 パッケージを再構築するシェルスクリプト。

（注） すでにモビリティ機能パックを使用している場合は、「付録*B*：モビリティ機能パック（*MFP*）の一般的なアップグレード手順」の手順を参照してください。

VNF オーケストレーション/展開および自動設定管理

このソリューションには、以下のタスクが含まれます。

- VNF オーケストレーションの設定メタデータの事前入力。
- VNF（CP、UP、RCM）のオーケストレーション/展開
- VNF 展開後の自動デバイスオンボーディング

- 展開後の自動設定プッシュ

VNF オーケストレーションの設定メタデータの事前入力

設定メタデータの事前入力は、自動モードで展開後の設定を NSO からプッシュするために重要です。このデバイスに事前入力されたデータがない場合、NSO は VNF とオンボードを NSO のデバイスとしてインスタンス化します。

設定メタデータの事前入力には次の構造があり、このデータの入力はネットワークスキームとデータセットに基づいています。

```
container
metadata-store {
         list config-metadata {
             key device-name;
             leaf device-name {
                 tailf:info "onboarding device name";
                 type string;
             }
             leaf redundancy_scheme {
                 tailf:info "cluster-topology 1:1, N:M and N+2";
                 type string;
             }
             leaf device-type {
                 tailf:info "Onboarding device type vpc or rcm";
                 type string;
             }
             list attributes {
                 key attribute-name;
                 leaf attribute-name {
                     tailf:info "Attribute Name";
                     type string;
                 }
                 leaf attribute-value {
                     tailf:info "Attribute Value";
                     type string;
                 }
             }
             list configuration-type {
                 key config-type;
                 tailf:info "Configuration type Day0.5, Day1 or DayN";
                 leaf config-type {
                     type string;
                 }
                 list files {
                     key file-name;
                     tailf:info "file name";
                     leaf file-name {
                         type string;
                     }
                     leaf config-scheme {
                         type string;
                     }
                     // CP device info
                     list additional-files {
                         key device;
                         //cp device
                         leaf device {
                             tailf:info "device name";
                             type string;
```

```
                        }
                        list additional-file {
                            key additional-file-name;
                            leaf additional-file-name {
                                tailf:info "file name";
                                type string;
                            }
                        }
                    }
                }
            }
        }
    }
```

次の表に、パラメータの説明を示します。

パラメータ	説明
device-name	VNF に対応する NSO デバイスの名前。VNF 名と同じ。
redundancy_scheme	冗長スキームのタイプ。N + 2 はスタンドアロン（冗長性なし）
device-type	VPC（SI および DI の場合）または RCM（RCM の場合）
configuration-type	Day-0.5 は、N:M 冗長性のための特別な設定です。この設定により、UP は RCM に接続できます。この設定は永続的に保存されます。
	Day-1 は設定の大部分を占めます。
	Day-N は通常、動作中の設定に変更されます。NSO オーケストレーション フローには適用されません。
file-name	プッシュされるプライマリ構成ファイル
config-scheme	このパラメータの値は、次のいずれかです。 **Common**：設定は、ロール（アクティブまたはスタンバイ）に関係なく、すべての UP にプッシュされます。 **host-specific**：このスキームは、設定がすべての UP（アクティブまたはスタンバイ）にプッシュされるため、「Common」に似ていますが、設定は「Common」設定の後にのみプッシュされます。そのため、「Common」設定に依存する設定を提供できます。例：コントロール プレーン グループの設定。 **allHostSpecific**：すべてのアクティブ UP のホスト固有の設定の集合が含まれます。設定は、N:M に対するすべてのスタンバイ UP にプッシュされます。 **"Active1", "Active2",... "ActiveN"**：それぞれのアクティブ UP のホスト固有の設定。特定の UP にのみプッシュされます。 **"Active1-rcm", "Active2-rcm", .. "ActiveN-rcm"**：この設定は RCM 形式であり、RCM にプッシュされます。RCM は、スタンバイが特定のアクティブデバイスを引き継ぐ際に設定の否定を実行するためにこのスキームを必要とします。

パラメータ	説明
additional-files	このパラメータは、関連する設定を他のデバイスにプッシュします（たとえば、UP のオンボーディング時に設定を CP にプッシュします）。このパラメータはまだサポートされていません。
attribute-name	このパラメータは、動的置換用の構成ファイル内の属性（変数）を識別し、$attribute_name としてフォーマットされます。
attribute-value	属性の値

次に、設定メタデータを入力または変更する NSO アクションの例を示します。

```
container
  config-metadata {
         // config true;
         tailf:action config-metadata-request {
             tailf:info "Invoke upgrade action on the selected devices";
             tailf:actionpoint config-metadata-request;
             input {
                 list config-metadata {
                     key device-name;
                     leaf device-name {
                         tailf:info "onboarding device name";
                         type string;
                     }
                     leaf device-type {
                         tailf:info "Onboarding device type vpc or rcm";
                         type enumeration {
                             enum vpc;
                             enum rcm;
                         }
                     }
                     leaf redundancy_scheme {
                         tailf:info "cluster-topology 1:1, N:M and N+2";
                         type enumeration {
                             enum 1:1;
                             enum N:M;
                             enum RCUPS;
                         }
                     }


                     list configuration-type {
                         key config-type;
                         tailf:info "Configuration type Day0.5, Day1 or DayN";
                         leaf config-type {
                             type enumeration {
                                 enum Day0.5;
                                 enum Day1;
                                 enum DayN;
                             }
                         }
                         list files {
                             key file-name;
                             tailf:info "file name";
                             leaf file-name {
                                 type string;
                             }
                             leaf config-scheme {
                                 type enumeration {
                                     enum common;
```

```
                                    enum host-specific;
                                    enum host-specific-common;
                                }
                            }
                            // CP device info
                            list additional-files {
                                key device;
                                //cp device
                                leaf device {
                                    tailf:info "device name";
                                    type string;
                                }
                                list additional-file {
                                    key additional-file-name;
                                    leaf additional-file-name {
                                        tailf:info "file name";
                                        type string;
                                    }
                                }


                                }
                            }
                        }
                    }
                    list attributes {
                        key attribute-name;
                        leaf attribute-name {
                            tailf:info "Attribute Name";
                            type string;
                        }
                        leaf attribute-value {
                            tailf:info "Attribute Value";
                            type string;
                        }
                    }
                }
                leaf delete-config-data {
                    type boolean;
                    default false;
                }
            }
            output {
                leaf status {
                    type string;
                }
                leaf message {
                 type string;
                }
            }
        }
    }
```

次の例に示されているように、このアクションは RESTCONF から呼び出せます。

URI：
http://<NSO-IP>:<NSO-REST-PORT>/restconf/data/mobility-common:config-metadata/config-metadata-request

メソッド：POST

コンテンツタイプ：application/yang-data+json

ペイロード：

```
{
        "config-metadata": {
            "device-name": "test2",
     "schema" : "1:1",
            "attributes":{
                "attribute-name":"test",
                 "attribute-value": "gh"
                  },
            "configuration-type":{
                "config-type": "Day0.5",
                "files":{
                    "file-name":"/home/ubuntu/tmo_action/test.txt"
                    },
                "files":{
                    "file-name":"/home/ubuntu/tmo_action/day0.5.txt"
                    }

            }
        }
}
```

結果：

```
{
    "mobility-common:output": {
        "status": "Success
/home/ubuntu/tmo_action/test.txt ==> syntax error: unknown command,Error: on line 3:
kkkl,
/home/ubuntu/tmo_action/day0.5.txt ==> Success"
    }
}
```

次の例に示されているように、このアクションは NCS CLI を使用して呼び出せます。

```
ubuntu@ncs> request config-metadata config-metadata-request config-metadata { device-name
 staros-1 attributes { attribute-name hostname attribute-value TEST } configuration-type
 { config-type Day0.5 files { file-name /home/ubuntu/tmo_action/test.txt } files {
file-name /home/ubuntu/tmo_action/day0.5.txt } } schema 1:1  }
status Success
/home/ubuntu/tmo_action/test.txt ==> syntax error: unknown command,Error: on line 3:
kkkl,
/home/ubuntu/tmo_action/day0.5.txt ==> Success
[ok][2021-07-12 08:05:01]
```

注：

- Config-metadata-request アクションには内部設定バリデータがあります。設定バリデータを使用すると、設定をプッシュする前に、構文や特定のセマンティックエラー（範囲外の値など）を検出できます。設定の検証には、少なくとも NSO でオンボーディングされているデバイス（real-one または NetSim）が必要です。

  設定可能なパラメータは次のとおりです。

  ```
  container
  configurable-parameters {
     leaf config-pre-validation-vpc-device-name {
             type string;
     leaf config-pre-validation-rcm-device-name {
             type string;
     }
  }
  ```

このファイルの設定の検証も任意です。設定を検証しない場合は、設定可能なパラメータを使用してこの機能をオフにできます。設定の検証がオフになっている場合、構成ファイルにエラーがあると設定のプッシュエラーが発生するため、ロールバックする必要があります。

```
container
configurable-parameters {
   leaf config-pre-validation-required {
           type boolean;
           default false;
   }
   }
  }
```

この設定メタデータには、設定可能なすべてのパラメータが含まれています。

デバイスとしての ESC および OpenStack のオンボーディング

ESC のインストールについては、ESC のマニュアルを参照してください。VNF の設定またはオンボーディングとインスタンス化の前に、次の設定手順を実行します。

NFV 用の NSO および ESC 環境のセットアップ

1. ユーザー名とパスワードを使用して ESC ホストに SSH 接続します。

   ```
   ssh esc@<esc-ip>
   ```

2. Sudo ユーザーになります。

   sudo su

3. 次のファイルを編集します。`vi /opt/cisco/esc/esc_database/etsi-production.properties`

4. 以下に示されているように情報を編集し、ファイルを保存します（Spring ユーザーとパスワードは変更しないでください）。適宜NSOの詳細を変更します。通信にはローカルサブネット管理 IP のみを使用し、ESC/NSO 通信間のフローティング IP は使用しないでください。

   ```
   spring.security.user.name=esc
   spring.security.user.password=$1$J7BUBX$Ce4vqA6JcrWCggRpYrPYg1

   security.pam.service=
   server.additionalConnector.port=8253
   server.additionalConnector.key-alias=esc
   server.esc.key-alias=esc

   nfvo.apiRoot=<NSO-IP>:9191
   nfvo.httpScheme=http
   nfvo.userName=<NSO-User-name>
   nfvo.password=<NSO-Password>
   nfvo.authenticationType=BASIC

   server.host=<ESC-Orch-IP>
   http.enabled=true
   https.enabled=false
   certificate.validation=false
   ```

```
spring.datasource.password=${PGSQL_PASSWORD}
spring.flyway.password=${PGSQL_PASSWORD}
```

5. 次に示されているように、**escadm** サービスを再起動します。

```
escadm restart
Stopping esc_service: [OK]
Stopping escadm service: [OK]
Starting escadm service: [OK]
#
```

6. 次に示されているように、escadmの正常性を確認します（数分かかる場合があります）。

```
escadm health
============== ESC =================
vimmanager (pgid 18651) is running
monitor (pgid 18688) is running
mona (pgid 18741) is running
snmp is disabled at startup
etsi (pgid 19316) is running
pgsql (pgid 18944) is running
portal (pgid 19355) is running
confd (pgid 18978) is running
escmanager (pgid 19131) is running
=====================================
ESC HEALTH PASSED
```

7. NSO にログインし、環境に応じて設定を変更し、ファイルに保存します。

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <nfv xmlns="urn:etsi:nfv:yang:etsi-nfv-descriptors">
  <settings xmlns="http://cisco.com/ns/nso/cfp/cisco-etsi-nfvo">
    <image-server>
      <ip-address><NSO-IP></ip-address>
      <port>8010</port>
      <document-root>/var/opt/ncs/vnfpackages</document-root>
    </image-server>
    <etsi-sol3>
      <server>
        <ip-address><NSO-IP></ip-address>
        <port>9191</port>
        <use-ssl>false</use-ssl>
        <document-root>/var/opt/ncs</document-root>
        <auth-enabled>true</auth-enabled>
        <auth-types>
          <basic>
            <username><NSO-USERNAME></username>
            <password><NSO-PASSWORD></password>
          </basic>
        </auth-types>
      </server>
      <vnfm-behaviour>
        <vnfm-behaviour-override>
          <id>default-sol3</id>
          <rpc-behaviour>
            <rpc>
              <include>
                <vim-info>false</vim-info>
              </include>
            </rpc>
            <modify>
              <pre>
                <rpc>false</rpc>
              </pre>
```

```
            <post>
              <rpc>true</rpc>
            </post>
          </modify>
        </rpc-behaviour>
        <grant>
          <store-history>false</store-history>
          <heal>
            <authorise-grant>true</authorise-grant>
          </heal>
        </grant>
        <onboarding>
          <store-details>true</store-details>
        </onboarding>
      </vnfm-behaviour-override>
    </vnfm-behaviour>
  </etsi-sol3>
 </settings>
 </nfv>
</config>
```

8. パッケージフォルダ内のパッケージをすべてコンパイルし、パッケージのリロードを実行します。

```
ubuntu@test-nso:/var/opt/ncs/packages$ ncs_cli -C
User ubuntu last logged in 2021-09-23T08:00:34.649202+00:00, to test-nso, from
209.165.200.225 using cli-ssh
ubuntu connected from 209.165.200.225 using ssh on test-nso
ubuntu@ncs# packages reload
```

9. 次に示されているように、ファイルをロードマージします。この手順では、NSO を NFVO として有効にし、9191 ポートで NFVO サービスを実行します。

```
ubuntu@test-nso:~$ vi config.xml
ubuntu@test-nso:~$ ncs_cli -C

User ubuntu last logged in 2021-08-04T09:10:55.819283+00:00, to test-nso, from
209.165.200.226 using cli-ssh
ubuntu connected from 209.165.200.227 using ssh on test-nso
ubuntu@ncs# config
Entering configuration mode terminal
ubuntu@ncs(config)# load merge config.xml
Loading.
1.54 KiB parsed in 0.01 sec (128.38 KiB/sec)
ubuntu@ncs(config)# commit
```

10. NSO ユーザー名を「ncsadmin」グループに追加して NACM ルールを更新します。

```
ubuntu@test-nso:~$ ncs_cli -C

User ubuntu last logged in 2021-08-06T09:56:26.370979+00:00, to test-nso, from
209.165.200.227 using cli-ssh
ubuntu connected from 209.165.200.227 using ssh on test-nso
ubuntu@ncs# config
Entering configuration mode terminal
ubuntu@ncs(config)# nacm groups group ncsadmin user-name ubuntu
ubuntu@ncs(config-group-ncsadmin)# commit
```

11. 必要なパッケージを NSO の標準の場所（通常は/var/opt/ncs/packages）にコピーします。

12. パッケージのリロードを実行し、パッケージのステータスを確認します。すべてのパッケージのステータスが UP である必要があります。

```
ubuntu@test-nso:~$ ncs_cli -C

User ubuntu last logged in 2021-08-06T09:58:39.866838+00:00, to test-nso, from
209.165.200.227 using cli-ssh
ubuntu connected from 209.165.200.227 using ssh on test-nso
ubuntu@ncs# packages reload
ubuntu@ncs# show packages package oper-status

NAME                UP  PROGRAM CODE ERROR  JAVA UNINITIALIZED PYTHON UNINITIALIZED
 *
------------------------------------------------------------------------------
cisco-etsi-nfvo        X      -                     -             -

cisco-rcm-nc-1.0       X      -                     -             -

cisco-staros-cli-5.38  X      -                     -             -

esc                    X      -                     -             -

etsi-sol003-gen-1.13   X      -                     -             -

mobility-common        X      -                     -             -

mop-automation         X      -                     -             -

mop-common             X      -                     -             -

nfv-common             X      -                     -             -
nfv-device-onboarding  X      -                     -             -

nfv-vim                X      -                     -             -

nfv-vnf-lcm            X      -                     -             -

openstack-cos-gen-4.2  X      -                     -             -
```

13. 通知ストリームを設定します。/etc/ncs/ncs.confファイルを更新して、「nfv-events」ストリームを追加します。

```
<ncs-config>
    <event-streams>
      <notifications>
        <stream>
          <name>nfv-events</name>
          <description>Generic netconf notification stream for NFV
events</description>
          <replay-support>true</replay-support>
          <builtin-replay-store>
            <enabled>true</enabled>
            <dir>${NCS_RUN_DIR}/state</dir>
            <max-size>S10M</max-size>
            <max-files>50</max-files>
          </builtin-replay-store>
        </stream>
      </event-streams>
    </notifications>
</ncs-config>
```

14. sudo ユーザーとして NSO を再起動します。

```
/etc/init.d/ncs stop
Stopping ncs (via systemctl):                              [  OK  ]
/etc/init.d/ncs start
Starting ncs (via systemctl):                              [  OK  ]
```

15. デバイスオンボーディング API を介して、NSO のデバイスとして NETCONF、ESC、ETSI SOL003 ESC、および OpenStack をオンボードします。

    1. デバイスとして OpenStack をオンボードします。次に、例を示します。特定の展開に合わせてカスタマイズします。これは、コンフィギュレーション モードで NSO CLI を使用して設定できます。authgroup については、NSO のマニュアルを参照してください。

    ```
    devices device openstack
    address 209.165.200.228
    port 5000
    authgroup openstack
    device-type generic ned-id openstack-cos-gen-4.2
    ```

    2. ESC ETSI インターフェイスをデバイスとしてオンボードします。次に、例を示します。特定の展開に合わせてカスタマイズします。

    ```
    devices device esc-etsi
    address 209.165.200.229
    port 8250
    authgroup esc-etsi
    device-type generic ned-id etsi-sol003-gen-1.13
    ```

    3. ESC ネイティブ NETCONF インターフェイスをデバイスとしてオンボードします。次に、例を示します。特定の展開に合わせてカスタマイズします。

    ```
    devices device esc-netconf
    address 209.165.200.229
    ssh host-key ssh-rsa
    key-data "AAAAB3NzaC1yc2EAAAADAQABAAABAQDYwNCaa3ghJtnJSvn/
    aSPjCuoMKmssZds+J5d9JCOS\n3h3V/fCtJwiH7qMgMXnNc0LEr1fZhxQ4kg5o/
    IafmoYD7N+w/ECqWEp68sjeN+AftiZ9J74D\n+/KDonffgBCHxIVEo0XHYlojrtmpg/
    EH9/N3fQgoSzEhGItGG4uMaAzbWr1pO8AApOPlPi4r\nciL4Qemi6u4i/
    HGFr8MqQp5qcMFd8O30OlB1q1vKn9sq/9sL6EzqyUd2lMounDglEQYMgi8J\
    nyG6upsOFuvhiYRC9qfHML45quyepsJdVi2Li2QwUJLa89EDh148RlhLTJs4s2iAwBGNdvLdK\ntzLu2VGyWKqH"
    !
    authgroup esc-netconf
    device-type netconf ned-id esc
    ```

16. 次に示されているように、さまざまなデバイスについてデバイスの追加ステータスを追跡します。

```
ubuntu@test-nso:~$ ncs_cli -C

User ubuntu last logged in 2021-08-06T10:09:23.550686+00:00, to test-nso, from
209.165.200.227 using cli-ssh
ubuntu connected from 209.165.200.227 using ssh on test-nso
ubuntu@ncs# show vnf-status instances esc-netconf

INSTANCE ID  TIMESTAMP   FUNCTION TYPE OPERATION  STATUS   STATUS MESSAGE
------------------------------------------------------------------------------------------
esc-netconf  2021-07-21 *    -          init   success   Device Onboarding
initialized
             2021-07-21 *    -          init   success   Device Onboarding
initialized
```

```
              2021-07-21 *    - fetch-ssh-keys  success   fetch-ssh-keys was
successful
              2021-07-21 *    -         connect success   connect was successful
              2021-07-21 *    -       sync-from success   sync-from was successful
             2021-07-21 *    - device-config   success   Subscribed to ESC Netconf
    notification escEvent Stream
              2021-07-21 *    -          ready  success   Device Successfully
onboarded
```

VNF のインスタンス化の前提条件

VNF 展開要求を送信する前に、次の設定の変更を行います。

1. **設定パラメータ**

   必要に応じて、次の設定パラメータを設定します。

   - configurable-parameters device-ping-sleeptimesec 30（デフォルト値は 30 秒）
   - configurable-parameters device-ping-retries 150（デフォルト値は 30）。RCM の場合は、より大きな値（150 など）に設定します。
   - configurable-parameters p2p-required true（デフォルト値は false）
   - configurable-parameters p2p-soFile-path /var/opt/ncs/patch_libp2p-2.64.1418.so.tgz

2. **設定メタデータの事前入力**

   Config-metadata を設定する場合、デバイス名は VNF インスタンス名と同じにする必要があります。

   次の例に示されているように、このアクションは RESTCONF から呼び出せます。

   URI：
   http://<NSO-IP>:<NSO-REST-PORT>/restconf/data/mobility-common:config-metadata/config-metadata-request

   メソッド：POST

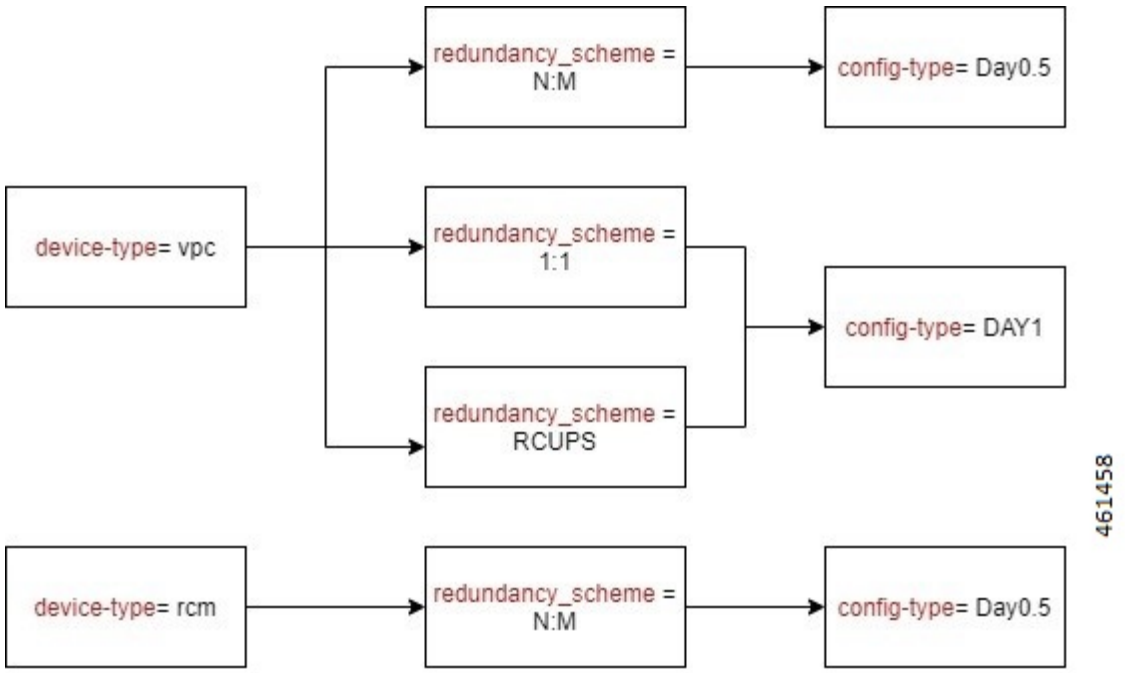
   コンテンツタイプ：application/yang-data+json

   サンプル ペイロード：

```
{
        "config-metadata": {
            "device-name": "test2",
    "schema" : "1:1",
            "attributes":{
                "attribute-name":"test",
                 "attribute-value": "gh"
                  },
            "configuration-type":{
                "config-type": "Day1",
                "files":{
                    "file-name":"/home/ubuntu/tmo_action/test.txt"
                    },
                "files":{
                    "file-name":"/home/ubuntu/tmo_action/day0.5.txt"
                    }
```

```
                }
            }
        }
```

設定メタデータを事前入力する際は、次の図に示されている基準に従ってください。



VNF のインスタンス化

VNF は設定時にインスタンス化されます。したがって、VNF をインスタンス化するには、VNF 設定を NSO にロードする必要があります。VNF には、SOL006 VNFD への参照が含まれます。また、Openstack テナントネットワークや IP アドレスなどの VIM アーティファクトへの参照もあります。VNF の YANG 定義の詳細については、付録 A：VNF の YANG の定義を参照してください。

VNF のインスタンス化には、次のようにさまざまなコンポーネントが関係します。

- TOSCA VNF パッケージとしてパッケージ化された ETSI SOL001 VNFD テンプレート
- VNF パッケージと同じ名前または ID を持つ ETSI SOL006 VNFD
- NSO 独自の VNF インスタンス

モビリティ機能パックには、いくつかのサンプル VNF パッケージが付属しており、対応する SOL006 VNFD も含まれています。これらのサンプルはベースとして使用できますが、展開に合わせた追加のカスタマイズが必要です。以下に、VNF の設定例を示します。

```
{
   "nfv-vnf-lcm:nfv-vnf":[
```

```
{
   "network-function-type":"VPC-SI",
   "name":"test026",
   "vnfd":"VPC-SI-2P-IMAGE-BOOT",
   "instantiation-level":"default",
   "deployment-flavor":"default",
   "mgmt-user-name":"admin",
   "mgmt-password":"Csco@123",
   "host-name":"vpc-si",
   "domain-name":"cisco.com",
   "ntp-server":"209.165.201.1",
   "name-server":"209.165.201.2",
   "location":{
      "vim":{
         "name":"openstack",
         "project":"test",
         "zone-id":"nova"
      },
      "vnfm":"esc-etsi"
   },
   "network":[
      {
         "type":"VIM_NETWORK_MANAGEMENT",
         "extent":"external",
         "name":"test-mgmt",
         "subnet-name":"test-mgmt-subnet"
      },
      {
         "type":"VIM_NETWORK_ORCHESTRATION",
         "extent":"external",
         "name":"test-orch",
         "subnet-name":"test-orch-subnet"
      },
      {
         "type":"VIM_NETWORK_SERVICE_1",
         "extent":"external",
         "name":"service1",
         "subnet-name":"service1"
      },
      {
         "type":"VIM_NETWORK_SERVICE_2",
         "extent":"external",
         "name":"service2",
         "subnet-name":"service2"
      }
   ],
   "unit":[
      {
         "type":"VPC-SI",
         "image":"core-si-21.23",
         "flavor":"core-si",
         "connection-point":[
            {
               "name":"nic0",
               "ip-address":[
                  {
                     "id":0,
                     "fixed-address":[
                        "209.165.201.3"
                     ]
                  }
               ],
               "security-group":[
                  "default"
```

```
                        ],
                        "network-type":"VIM_NETWORK_ORCHESTRATION"
                     },
                     {
                        "name":"nic1",
                        "ip-address":[
                           {
                              "id":0,
                              "fixed-address":[
                                 "209.165.201.4"
                              ]
                           }
                        ],
                        "security-group":[
                           "default"
                        ],
                        "network-type":"VIM_NETWORK_MANAGEMENT"
                     },
                     {
                        "name":"nic2",
                        "ip-address":[
                           {
                              "id":0,
                              "fixed-address":[
                                 "209.165.201.5"
                              ]
                           }
                        ],
                        "security-group":[
                           "default"
                        ],
                        "network-type":"VIM_NETWORK_SERVICE_1"
                     },
                     {
                        "name":"nic3",
                        "ip-address":[
                           {
                              "id":0,
                              "fixed-address":[
                                 "209.165.201.6"
                              ]
                           }
                        ],
                        "security-group":[
                           "default"
                        ],
                        "network-type":"VIM_NETWORK_SERVICE_2"
                     }
                  ]
               }
            ],
            "extra-parameters":[
               {
                  "name":"BOOTUP_TIME",
                  "value":"100"
               },
               {
                  "name":"LICENSE_KEY",
                  "value":"\"VER=1|DOI=1624646484|DOE=1640457684|ISS=3|NUM=212017|
CMT=SWIFT_License|LSG=5000000|LEC=10000000|LGT=5000000|FIS=Y|FR4=Y|FTC=Y|FSR=Y|
FPM=Y|FID=Y|FI6=Y|FLI=Y|FFA=Y|FCA=Y|FTP=Y|FTA=Y|FDR=Y|FDC=Y|FGR=Y|FAA=Y|FDQ=Y|
FEL=Y|BEP=Y|FAI=Y|FCP=Y|LCF=5000000|LPP=5000000|LSF=5000000|FLS=Y|FSG=Y|
LGW=5000000|HIL=XT2|LSB=5000000|LMM=5000000|FIB=Y|FND=Y|FAP=Y|FRE=Y|FHE=Y|
FUO=Y|FUR=Y|FOP=Y|FRB=Y|FCF=Y|FVO=Y|FST=Y|FSI=Y|FRV=Y|F6D=Y|F13=Y|FIM=Y|
```

```
FLP=Y|FSE=Y|FMF=Y|FEE=Y|FHH=Y|FIT=Y|FSB=Y|FDS=Y|LSE=5000000|FLR=Y|FLG=Y|
FMC=Y|FOC=Y|FOS=Y|FIR=Y|FNE=Y|FGD=Y|LIP=5000000|FOE=Y|FAU=Y|FEG=Y|FL2=Y|
FSH=Y|FLF=Y|FSP=Y|FNI=Y|FCI=Y|FME=Y|FCN=Y|FUB=Y|FSF=Y|FGO=Y|FPE=Y|FWI=Y|
FAC=Y|FIE=Y|FSM=Y|FAG=Y|FNQ=Y|FEW=Y|FAR=Y|FOX=Y|FPW=Y|FAM=Y|FGX=Y|FWT=Y|
FUA=Y|LDT=5000000|LEX=5000000|LVL=5000000|LQP=5000000|LMP=5000000|
LCU=10000000|LUU=10000000|FXS=Y|FLC=Y|FRT=Y|FSX=Y|FBS=Y|FRD=Y|FXM=Y|
LTO=10000000|FNS=Y|LNS=5000000|SIG=MC0CFBge/
0TZha2Ta7c1L5CLOL2tgDIDAhUAhIKwZxXEJJpr9Xk5buNyzZStrNM\""
            }
         ]
      }
   ]
}
```

以下に、RCM VNF のインスタンス化の例をもう 1 例示します。

```
{
    "nfv-vnf-lcm:nfv-vnf": [
      {
        "network-function-type": "RCM",
        "name": "RCM-ahhashem-sol003-78",
        "vnfd": "RCM-IMAGE-BOOT",
        "instantiation-level": "default",
        "deployment-flavor": "default",
        "mgmt-user-name": "luser",
        "mgmt-password": "$8$40/jVMTHJY+Jrd7mZiwqdrKEIz6Kc5Pt2Qvnwi0/65g=;”
        "host-name": "rcm",
        "domain-name": "cisco.com",
        "ntp-server": "209.165.201.1",
        "name-server": "209.165.201.1",
        "location": {
          "vim": {
            "name": "openstack",
            "project": "ahhashem",
            "zone-id": "nova"
          },
          "vnfm": "esc-etsi"
        },
        "network": [
          {
            "type": "VIM_NETWORK_MANAGEMENT",
            "name": "ahhashem-mgmt",
            "extent": "external",
            "subnet-name": "ahhashem-mgmt-subnet"
          },
          {
            "type": "VIM_NETWORK_ORCHESTRATION",
            "name": "ahhashem-orch",
            "extent": "external",
            "subnet-name": "ahhashem-orch-subnet"
          },
          {
            "type": "VIM_NETWORK_SERVICE_1",
            "name": "service1",
            "extent": "external",
            "subnet-name": "service1"
          } ,
          {
            "type": "VIM_NETWORK_SERVICE_2",
            "name": "service2",
            "extent": "external",
            "subnet-name": "service2"
          }
        ],
        "unit": [
```

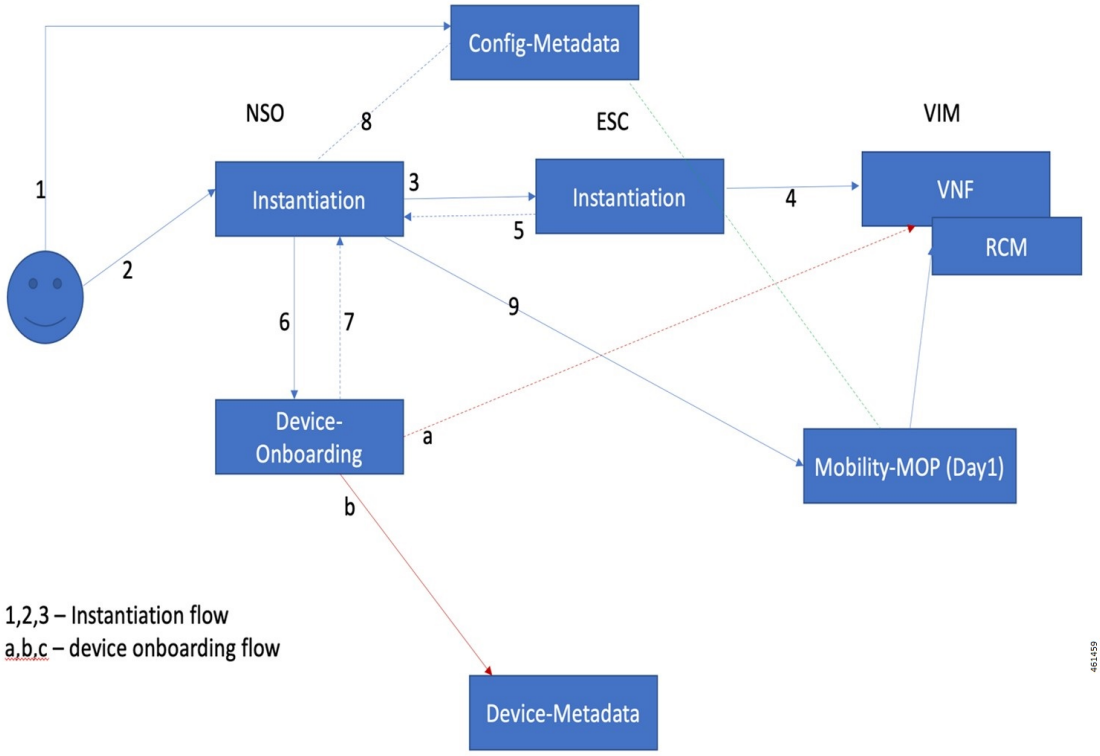
```
  {
    "type": "RCM",
    "image": "core-rcm-21.23",
    "flavor": "mkal-rcm-hugepages",
    "connection-point": [
      {
        "name": "nic0",
        "ip-address":{
            "id": 1,
            "fixed-address": ["209.165.201.7"]
        },
        "security-group": ["default"],
        "network-type": "VIM_NETWORK_ORCHESTRATION"
      },
      {
        "name": "nic1",
        "ip-address":{
            "id": 1,
            "fixed-address":["209.165.201.8"]
        } ,
        "security-group": ["default"],
        "network-type": "VIM_NETWORK_MANAGEMENT"
      },
      {
        "name": "nic2",
        "ip-address": {
            "id": 1,
            "fixed-address": ["209.165.201.9"]
        },
        "security-group": ["default"],
        "network-type": "VIM_NETWORK_SERVICE_1"
      } ,
      {
        "name": "nic3",
        "ip-address": {
            "id": 1,
            "fixed-address": ["209.165.201.10"]
        },
        "security-group": ["default"],
        "network-type": "VIM_NETWORK_SERVICE_2"
      }

    ]
  }
],
"extra-parameters": [
  {
    "name": "VIM_VM_NAME",
    "value": "RCM-ahhashem-sol003-78"
  },
  {
    "name": "HOST_NAME",
    "value": "rcm"
  },
    {
      "name": "NIC0_TYPE",
      "value": "virtual"
    },
    {
      "name": "NIC1_TYPE",
      "value": "virtual"
    },
    {
      "name": "NIC2_TYPE",
```

```
                "value": "direct"
              },
              {
                "name": "NIC3_TYPE",
                "value": "direct"
              },
              {
                "name": "MGMT_USER_NAME",
                "value": "luser"
              },
              {
                "name": "MGMT_PASSWORD_ROUND4096",
                "value": "$6$rounds=4096$P2wdTbEBO0LHmHi$OwbVEIarMbt
Qxbu5Us5kW0n0MOWp3QN9eVRX7WjvLm4xTJvFpl6vHez3XkKm39XJJ7dGRRIsZqXfcZRjQBA7E."
              },
              {
                  "name": "SERVICE_INTERFACE_IP_1",
                  "value": "209.165.201.9"
              },
              {
                  "name": "SERVICE_INTERFACE_IP_2",
                  "value": "209.165.201.11"
              },
              {
                "name": "NTP_SERVER",
                "value": ["209.165.201.12","209.165.201.13","209.165.201.14"]
              }

          ]
        }
      ]
    }
```

VNF のインスタンス化 - コンポーネントのインタラクションとフロー

次の図は、エンドツーエンドのインスタンス化の自動化について、その全体のフローを示しています。

図 *38 : VNF* のインスタンス化のインタラクション



手順の詳細：

1. ネットワークオペレータは、名前、タイプ、ダイナミック属性、構成ファイルなど、VNF のインスタンス化に必要なすべての詳細を把握しています。構成ファイルを NSO ファイルシステムに配置し、自動化のための NSO 設定 DB に詳細を登録します。

   このステップには、以下のタスクが含まれます。

   - ネットワークオペレータは、構成ファイルを NSO ファイルシステムに Secure Copy（SCP）でコピーします。このコピー先は NFS であるか、NSO HA 環境で複製されている必要があります。
   - すべての属性値ペア、ダイナミック置換値、Day-0.5、または Day-1 設定を登録します。
   - 構成ファイルの検証を有効にし、テスト支援デバイスの詳細を入力します。
   - 再検証フラグが「true」に設定されている場合、設定メタデータアクションがすべての構成ファイルを内部的に検証します。検証が行われない場合は、設定の適用中に失敗します。

2. ネットワークオペレータは、すべての詳細を含む VNF のインスタンス化用ペイロードを準備します。次に、ペイロードを呼び出してインスタンスを作成します。基本的な検証が行われ、命令が処理されます。

このステップには、以下のタスクが含まれます。

- 命令を呼び出す前に、パスワードの長さ、イメージ、フレーバー、ネットワークの存在などの入力情報を OpenStack で検証します。

3. NSO が内部で命令を処理し、ESC VNF のインスタンス化命令を準備します。

   このステップには、以下のタスクが含まれます。

   - サービスの NSO フットプリントを作成します。
   - CSAR を検証します。
   - SOL3/SOL4 入力を使用して ESC VNF のインスタンス化命令を呼び出します。
   - ESC 通知（ETSI と NETCONF の両方）のリッスンを開始します。

4. ESC が SOL3/SOL4 の入力検証を実行し、VIM で命令を作成します。

   このステップには、以下のタスクが含まれます。

   - ESC が VNF のインスタンス化を呼び出します。
   - VNF の呼び出しが成功すると、VNF をモニターするモノモニターが作成されます。
   - ETSI および NETCONF 通知を通じて更新を NSO に返します（成功、失敗いずれの場合も）。

5. ESC は、ETSI または NETCONF 通知を通じて、進行状況に関する定期的な更新を NSO に返します。

   このステップには、以下のタスクが含まれます。

   - ESC は、進行状況に関する ETSI および NETCONF 通知を継続的に送信します。
   - ETSI 通知は、展開～初期化、処理、および完了通知で構成されます。
   - NETCONF 通知は、VM ステータスに関するより詳細な情報を提供します。
   - 失敗すると、適切なエラーメッセージが表示されます。

6. ESC から VNF のインスタンス化完了メッセージを受信すると、NSO は NSO デバイスとしてオンボーディングします。

   このステップには、以下のタスクが含まれます。

   - インスタンス化ロジックが入力ペイロードから詳細を取得し、デバイスのオンボーディングロジックを呼び出します。
   - NSO がデバイスから fetch-ssh-host-key を実行します。
   - NSO が接続チェックを実行します。
   - NSO が sync-from を実行します。
   - NSO がデバイスで「show version」などの事後チェックコマンドを実行します。

- NSO がデバイスを NSO デバイスツリーに追加します。

7. NSO のインスタンス化ロジックは、デバイスの追加が完了するまで待機します。

   このステップには、以下のタスクが含まれます。

   - NSO がデバイスのオンボーディングプロセスが完了したかどうかを確認します。
   - デバイスのオンボーディングが失敗した場合、NSO は実行を停止します。

8. NSO のインスタンス化ロジックは、事前に入力された設定メタデータを読み取り、プッシュされる設定を解釈します。

   このステップには、以下のタスクが含まれます。

   - 事前に入力された設定メタデータを読み取り、device-name に基づいて Day-0.5 または Day-1 構成ファイルを解釈します（デバイス名は VNF 名に基づきます）。
   - RCM ベースの N:M スキームの場合、Day-0.5 がプッシュされます。
   - 1:1 の場合、Day-1 がプッシュされます。
   - 不足している情報がある場合は、インスタンス化が完了し、処理が停止します。

9. NSO は、設定メタデータから構成ファイルを取得し、モビリティ MOP 入力フォーマットを作成し、設定のプッシュ用 MOP を呼び出します。

   このステップには、以下のタスクが含まれます。

   - モビリティ MOP を呼び出し、task-id を取得します。
   - 定期的に task-id のステータスを確認します。
   - 1:1 の CP または UP ペア（MOP 経由）の場合、デバイスのフラッシュに設定を永続的に保存します。
   - 完了ステータスが vnf-status 元帳で更新されます。

VNF のインスタンス化ステータスの確認

vnf-status コマンドを定期的に使用して、VNF インスタンス化のステータスを確認できます。

失敗、処理中、または完了に関連するメッセージはすべて、ステータスメッセージに追加されます。

```
show vnf-status instances vnf-instance-name
INSTANCE ID TIMESTAMP TYPE OPERATION STATUS STATUS MESSAGE
------------------------------------------------------------------------
<VNF-Name> <Time-Stamp> <type> <function> <status> <message-if-any>
```

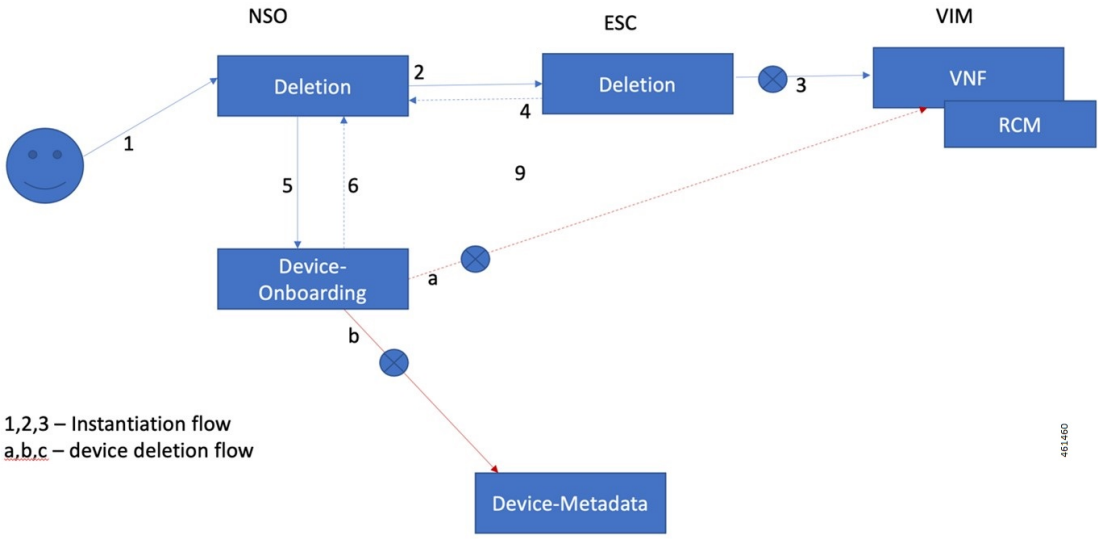
VNF ダッシュボード

VNF のインスタンス化手順と VNF の現在のステータスは、NSO ベースのダッシュボードに表示されます。

VNF の削除

次のフロー図は、エンドツーエンドの削除の自動化に関する完全なフローを示しています。

図 *39 : VNF* 削除の連携動作



詳細な手順：

1. ネットワークオペレータが、実行中または失敗状態になっている既存インスタンスのデコミッションまたは削除を決定します。

   このステップには、以下のタスクが含まれます。

   - ネットワークオペレータが、削除タイプを含む VNF 名を提供します。
   - NSO が VNF の存在を検証します。

2. NSO が VNF インスタンスのステータスを確認し、NSO 側で失敗したインスタンスがある場合、ESC を呼び出して VIM から削除するか、ロールバックを実行します。

   このステップには、以下のタスクが含まれます。

   - NSO が、ESC にインスタンスをプッシュするか、ロールバックを実行する（NSO 内でインスタンスが失敗した場合）かを決定します。
   - NSO が ESC への非同期要求を行い、通知が来るまで待機します。

3. ESC がクリーンアップを実行し、VNF モニターを削除します。
4. ESC が NSO への ETSI/NETCONF 通知を生成します。
5. NSO が ESC 通知を処理し、次の処理を実行します。

- インスタンスを削除するためにデバイス オンボーディング パッケージを呼び出します。
- 「nfv-vnf-inventory」からエントリを削除します。

6. デバイス オンボーディング パッケージによって NSO からデバイスが削除され、VNF 元帳でステータスが更新されます。

VNF の削除ステータスの確認

vnf-status コマンドを使用して、VNF の削除ステータスを確認できます。

失敗、処理中、または完了に関連するメッセージがあれば、ステータスメッセージに追加されます。

```
show vnf-status instances vnf-instance-name
INSTANCE ID TIMESTAMP TYPE OPERATION STATUS STATUS MESSAGE
------------------------------------------------------------------------
<VNF-Name> <Time-Stamp> <type> <function> <status> <message-if-any>
```

設定メタデータの削除

これは手動の手順であり、NSOアクションを使用して設定メタデータを削除する必要があります。設定メタデータを保持しても影響はありません。

NSO ファイルシステムの構成ファイルの削除

NSO ファイルシステムから構成ファイルを手動で削除する必要があります。構成ファイルのデータを保持しても影響はありません。

自動化プロセス：VNF の展開、オンボーディング、および設定のプッシュ

自動化プロセスには、次のセクションが含まれます。

入力ペイロードを使用した VNF のインスタンス化

必要な変更を加えた後、入力ペイロードを使用してインスタンス化要求を送信します。VNFインスタンス化の自動化プロセスが開始されます。

入力ペイロードのサンプルについては、VNF のインスタンス化の項を参照してください。

NSO でのデバイスとしての VNF のオンボーディング

インスタンス化が成功すると、VNF は NSO のデバイスとしてオンボーディングされます。デバイス名は VNF 名と同じになります。

VPC デバイスへの P2P モジュールのインストール

「device-type」が VPC で、configurable-parameters の「p2p-required」が「true」に設定され、「p2p-soFile-path」が定義されている場合、P2P ファイルをデバイスのフラッシュディレクトリにコピーしてから P2P モジュールをアップグレードします。

P2P モジュールがデバイスにインストールされます。

オンボーディングされたデバイスへの設定のプッシュ

次に、自動設定のプッシュ中に使用される静的パラメータを示します。

- operation-type：Commit
- mop-type：Common
- save-config-permanently：デフォルトは false で、デバイスタイプが「vpc」の場合は true に設定されます。

構成ファイルを使用した設定のプッシュが完了すると、タスク ID が生成されます。タスク ID を使用して設定のプッシュのステータスをチェックし、ステータスに基づいて元帳エントリが更新されます。

（注） NSO は RCM で設定の監査を実行しません。NSO は設定のプッシュ中に RCM が再起動した場合、再起動の完了時に設定を再プッシュしないため、設定を手動で再プッシュする必要があります。NSO は、設定のプッシュの失敗についてオペレータに警告します。RCM に正常にプッシュされた設定は、その RCM を再起動しても保持されます。

付録 A：VNF の YANG の定義

ここでは、VNF の YANG 定義の例を示します。

```
module nfv-vnf-lcm {
  namespace "http://com/cisco/cx/servicepack/nfv/vnflcm";
  prefix nfv-vnf-lcm;

  import ietf-inet-types { prefix inet; }
  import tailf-common { prefix tailf; }
  import tailf-ncs { prefix ncs; }
  import nfv-common { prefix nfv-common; }
  import tailf-kicker { prefix kicker; }
  include nfv-vnf-lcm-nano {
    revision-date 2020-02-14;
  }

  organization "Cisco-AS";

  contact "Cisco AS";

  description "Generic NFV VNF LCM service package";
```

```
revision 2020-10-22 {
  description "Active Inventory and LCM Auto/on-demand heal support";
}

revision 2020-07-01 {
  description "Re-branded per new naming convention";
}

revision 2020-02-14 {
  description "First version, ready for testing";
}

notification vnf-lcm {
  description "Notification about Network Function Operation";
  uses nfv-common:network-function-notification;
}

notification vnf-alarm {
  description "VNF alarms";
  uses nfv-common:vnf-alarm;
}

container nfv-vnf-inventory {
  tailf:info "CDB model to persist the VNFs, associated project, VIM and the
      VM details";
  config false;
  tailf:cdb-oper {
    tailf:persistent true;
  }

  list vnf {
    tailf:info "VNFs with associated VMs and status";
    key name;
    leaf name {
      tailf:info "VNF Name";
      type string;
    }
    leaf vnfd {
      type string;
      tailf:info "Associated VNFD name";
    }
    leaf project {
      type string;
      tailf:info "Associated vim tenant/project";
    }
    leaf vim {
      type string;
      tailf:info "Associated VIM";
    }
    leaf status {
      type string;
      tailf:info "Overall VNF status";
    }
    list vm {
      tailf:info "Associated VMs and the status";
      key name;
      leaf name {
        type string;
        tailf:info "VM name";
      }
      leaf type {
        type string;
        tailf:info "VM Type";
      }
```

```
      leaf flavor {
        type string;
        tailf:info "VIM flavor that is used to deploy the VM";
      }
      leaf host {
        type string;
        tailf:info "Compute host where the VM has been deployed";
      }
      list connection-point {
        key nic-id;
        leaf nic-id {
          type uint8;
          tailf:info "NIC id of the connection point";
        }
        leaf ip-address {
          type inet:ip-address;
          tailf:info "IP address of the connection point";
        }
      }
      leaf status {
        type string;
        tailf:info "VM status";
      }
    }

    leaf netconf-notification-done {
        tailf:hidden nfv-internal;
        type empty;
    }
  }
}

list nfv-vnf {
  description "Generic RFS model for VNF LCM";

  key "network-function-type name";

  leaf network-function-type {
    tailf:info "virtual network function type";
    type enumeration {
      enum "VPC-SI";
      enum "VPC-DI";
      enum "CSR1KV";
      enum "GENERIC";
      enum "VCU";
      enum "VDU";
      enum "EMS";
      enum "RCM";
    }
  }

  leaf name {
    tailf:info "Unique service id";
    type string;
  }

  leaf vnfd {
    mandatory true;
    type string;
    tailf:info "VNFD to use for this type of Network Function that has to be
          onboarded on the target VIM.";
  }

  uses ncs:service-data;
```

```
  ncs:servicepoint nfv-vnf-lcm;
  uses ncs:nano-plan-data;

  tailf:action heal {
    tailf:info "Heal VNF";
    tailf:actionpoint nfv-lcm-heal-ap;
    input {
    }
    output {
      uses nfv-common:standard-action-response;
    }
  }

 tailf:action start {
           tailf:info "Start VNF";
           tailf:actionpoint nfv-lcm-start-ap;
           input {
           }
           output {
               uses nfv-common:standard-action-response;
           }
       }

 tailf:action stop {
           tailf:info "Stop VNF";
           tailf:actionpoint nfv-lcm-stop-ap;
           input {
           }
           output {
               uses nfv-common:standard-action-response;
           }
       }

tailf:action scale {
           tailf:info "Scale-In VNF";
           tailf:actionpoint nfv-lcm-scale-ap;
           input {
               leaf scale-type {
                   mandatory true;
                   tailf:info "SCALE IN or OUT";
                   type enumeration {
                       enum "OUT";
                       enum "IN";
                   }
               }

               leaf no-of-instances {
                   tailf:info "Number of scale IN or OUT instances. Default is 1";
                   type uint32;
                   default 1;
               }

               leaf vdu-type {
                   mandatory true;
                   tailf:info "vdu-type as CF/SF/VPC-SI etc";
                   type string;
               }

           }
           output {
               uses nfv-common:standard-action-response;
           }
       }
```

```
  tailf:action retry {
        tailf:info "Stop VNF";
        tailf:actionpoint nfv-lcm-retry-ap;
        input {
        }
        output {
            uses nfv-common:standard-action-response;
        }
    }

leaf instantiation-level {
  type string;
  default "default";
  tailf:info "Instantiation level defined in VNFD to use. This will determine
        the number of VMs/VDUs to be deployed.";
}

leaf deployment-flavor {
  type string;
  default "default";
  tailf:info "Deployment flavor defined in the VNFD to use. Describes a specific
        deployment version of a VNF with specific requirements for capacity
        and performance.";
}
leaf mgmt-user-name {
  type nfv-common:identifier;
  description " Management login username specific to this VNF. Default values
        can be configured per VNF type.";
}

leaf mgmt-password {
  tailf:suppress-echo "true";
  type tailf:aes-cfb-128-encrypted-string;
  description "Management login password specific to this VNF.";
}

leaf host-name {
  type inet:domain-name;
  description "Hostname to use to communicate with this network function";
}

leaf domain-name {
  type inet:domain-name;
  description "Domain name used to construct Fully Qualified Domain Name by
        concatenating with VM hostname: <hostname>.<domain>";
}

leaf ntp-server {
  description "NTP server to use for VNFs deployed in this data center";
  type inet:host;
}

leaf name-server {
  type inet:ip-address;
  description "Name server";
}

container location {
  container vim {
    leaf name {
      description "NFVI this Network Function is deployed on.";
      type leafref {
        path "/ncs:devices/ncs:device/ncs:name";
      }
```

```
      //must "/ncs:devices/ncs:device[ncs:name=current()]/ncs:platform/ncs:name
      //          = 'Openstack'" {
      //  error-message "Please select Openstack devices only";
      //}
    }
    leaf project {
      type nfv-common:identifier;
      description "VIM project used to instantiate VNFs";
      mandatory true;
    }
    leaf zone-id {
      type string;
      default "nova";
      description "VIM zone id";
    }
    //TODO might need to support user domain and project domain
  }
  leaf vnfm {
    mandatory true;
    type leafref {
      path "/ncs:devices/ncs:device/ncs:name";
    }
    //must "/ncs:devices/ncs:device[ncs:name=current()]/ncs:platform/ncs:name
    //        = 'ETSI SOL'" {
    //  error-message "Please select ETSI-SOL VNFM devices only";
    //}
    description "ESC VNFM onboarded";
  }
}
list network {
  key type;
  leaf type {
    type nfv-common:identifier;
  }
  leaf name {
    type nfv-common:identifier;
    mandatory true;
  }
  leaf extent {
    type nfv-common:network-extent;
  }
  leaf subnet-name {
    when "../extent='external'";
    type nfv-common:identifier;
    mandatory true;
  }
}

list unit {
  description "Virtual Deployment Unit, a single VM.";
  key type;

  leaf type {
    description "VDU type as defined in the VNFD of this Network Function.";
    type nfv-common:identifier;
  }
  leaf image {
    type string;
    description " Image to use for this type of Network Function. Must have been
            be onboarded on the target VIM.";
  }
  leaf flavor {
    mandatory true;
    type string;
```

```
          description " Flavor to use for this type of Network Function. Must have been
                  onboarded on the target VIM.";
        }
        list storage-volume {
          key id;
          description "Out of band Storage volumes to use for this network function";
          leaf id {
            type string;
          }
          leaf volume-name {
            type string;
            description "Storage Volume to use for this type of Network function";
          }
        }
        list connection-point {
          key name;
          description " Network connection point such as a network interface card, as
                  defined in the descriptor.";
          leaf name {
            mandatory true;
            type nfv-common:identifier;
          }

          list ip-address {
              key id;
              ordered-by user;
              leaf id {
               type uint8;
                  tailf:info "IP Address ID for connection points";
              }
              leaf-list fixed-address {
                  ordered-by user;
                  description " IP address(es) to assign this network interface for both
scaled and non-scaled VNF's. Both IPv4 and
                              IPv6 is possible to allow for dual-stack cases if this VNF
requires
                              it for Internet access.";
                  type inet:ip-address;
               }
          }

          list vip {
            key address;
            ordered-by user;
            description " Virtual IP address(es) to assign this network interface. Both
                      IPv4 and IPv6 is possible to allow for dual-stack cases if this
                      VNF requires it for Internet access. Setting this will populate
                      allowed-address-pair list in the CVIM";

            leaf address {
              type inet:ip-address;
            }
            leaf netmask {
              type inet:ip-address;
              mandatory true;
            }
          }
          leaf-list security-group {
            type nfv-common:identifier;
            description "Security group(s) to apply to this network interface.";
          }
          leaf network-type {
            type leafref {
              path "../../../network/type";
```

```
        }
        description "Network used for this connection-point.";
      }
    }
  }
  list extra-parameters {
    description "VNF instance specific additional parameters defined in the VNFD.
          This will override the values configured in the VNFD";
    key name;
    leaf name {
      type string {
        pattern "[A-Za-z0-9_]+";
      }
    }
    leaf value {
      type string;
    }
  }
}

 list nfv-retry-vnfs {
      tailf:info "Retry VNF's to tweak the notifications";
      config false;
      tailf:cdb-oper {
          tailf:persistent true;
      }
      tailf:hidden nfv-internal;

      key name;
      leaf name {
          tailf:info "VNF Name";
          type string;
      }
  }
}
```

付録 B：モビリティ機能パック（MFP）の一般的なアップグレード手順

この付録では、次の手続きについて説明します。

- NSO 5.7.5.1-MFP 3.4.1 から NSO 5.8.10-MFP 3.4.2 へのアップグレード （649 ページ）
- NSO バージョンを変更せずに MFP 3.4.1 から MFP 3.4.2 にアップグレード （656 ページ）

NSO 5.7.5.1-MFP 3.4.1 から NSO 5.8.10-MFP 3.4.2 へのアップグレード

NSO 5.7.5.1-MFP 3.4.1 から NSO 5.8.10-MFP 3.4.2 にアップグレードするには、次の手順を使用します。この場合、MFP バージョンのアップグレードと同時に NSO バージョンのアップグレードを行います。

1. NSO 5.8.10 インストール bin ファイルを */tmp* フォルダにコピーし、NSO をバージョン 5.8.10 にアップグレードします。
2. */opt/ncs* で新しい NSO バージョン 5.8.10 へのシンボリックリンクを設定します。

3. MFP 3.4.2 のパッケージと NED をコピーし、*/var/opt/ncs/packages* フォルダの中身と置き換えます。
4. **start-with-package-reload** オプションを使って NSO を再起動します。これで、MFP 3.4.1 が 3.4.2 にアップグレードされ、NSO が NSO 5.7.5.1 から 5.8.10 にアップグレードされます。

以下に、NSO 5.7.5.1-MFP 3.4.1 から NSO 5.8.10-MFP 3.4.2 にアップグレードするための詳しい手順を示します。

（注） アップグレードが完了していない場合は、後でリカバリが必要になった場合に備えて、必ずバックアップを作成しておくことを推奨します。

データをバックアップするには、次の設定を使用します。

```
$ sudo su
# source /etc/profile.d/ncs.sh
# /etc/init.d/ncs stop
# ncs-backup
# exit
$
```

1. NSO 5.7.5.1 で MFP 3.4.1 を実行します。

```
root@test-nso:/var/opt/ncs# ncs --version
5.7.5.1

root@ncs# show packages package package-version
                         PACKAGE
NAME                     VERSION
----------------------------------
cisco-etsi-nfvo          4.7.2
cisco-rcm-nc-1.6         1.6
cisco-staros-cli-5.43    5.43.4
esc                      5.7.0.73
etsi-sol003-gen-1.13     1.13.16
mobility-common          3.4.1
mobility-rcm-subscriber  3.4.1
mop-automation           3.4.1
mop-common               3.4.1
nfv-common               3.4.1
nfv-device-onboarding    3.4.1
nfv-vim                  3.4.1
nfv-vnf-lcm              3.4.1
openstack-cos-gen-4.2    4.2.26

root@ncs# show packages package oper-status
packages package cisco-etsi-nfvo
 oper-status up
packages package cisco-rcm-nc-1.6
 oper-status up
packages package cisco-staros-cli-5.43
 oper-status up
packages package esc
 oper-status up
packages package etsi-sol003-gen-1.13
 oper-status up
packages package mobility-common
 oper-status up
```

```
packages package mobility-rcm-subscriber
 oper-status up
packages package mop-automation
 oper-status up
packages package mop-common
 oper-status up
packages package nfv-common
 oper-status up
packages package nfv-device-onboarding
 oper-status up
packages package nfv-vim
 oper-status up
packages package nfv-vnf-lcm
 oper-status up
packages package openstack-cos-gen-4.2
 oper-status up
root@ncs#

root@ncs# show devices list
NAME         ADDRESS        DESCRIPTION  NED ID                  ADMIN STATE
-----------------------------------------------------------------------------
esc-etsi     64.1.0.6       -            etsi-sol003-gen-1.13    unlocked
esc-netconf  64.1.0.6       -            esc                     unlocked
openstack    10.225.202.49  -            openstack-cos-gen-4.2   unlocked
root@ncs#
```

2. NSO 5.7.5.1 で MFP 3.4.1 を使用して、テスト用 VNF VPC-SI デバイスをインスタンス化します。

```
root@ncs#
System message at 2023-10-09 07:52:05...
Commit performed by ubuntu via http using rest.
root@ncs#
System message at 2023-10-09 07:52:05...
Commit performed by ubuntu via http using rest.
root@ncs#
System message at 2023-10-09 07:52:07...
Commit performed by ubuntu via http using rest.
root@ncs#
System message at 2023-10-09 07:52:07...
Commit performed by ubuntu via http using rest.
root@ncs#
System message at 2023-10-09 07:52:08...
Commit performed by ubuntu via http using rest.

root@ncs# show vnf-status instances S1-Test-00001 | tab
                                        FUNCTION

INSTANCE ID    TIMESTAMP                TYPE      OPERATION       STATUS      STATUS
 MESSAGE
-------------------------------------------------------------------------------------
S1-Test-00001  2023-10-09 07:50:55.198  VPC-SI    deploy          init        init

               2023-10-09 07:51:38.595  VPC-SI    deploy          processing
processing
               2023-10-09 07:52:01.639  VPC-SI    deploy          processing
processing
             2023-10-09 07:52:03.997  VPC-SI    deploy         completed   completed

               2023-10-09 07:53:43.293  -         init            success     Device
 Onboarding initialized
               2023-10-09 07:53:43.874  -         fetch-ssh-keys  success
fetch-ssh-keys was successful
             2023-10-09 07:53:45.285  -         connect         success     connect
```

```
 was successful
             2023-10-09 07:53:46.785  -        sync-from      success     sync-from
 was successful
              2023-10-09 07:53:46.964  -         ready          success     Device
 Successfully onboarded
              2023-10-09 07:54:13.305  -         config-read    success     Config
 MetaData is empty or null

root@ncs# show devices list
NAME           ADDRESS        DESCRIPTION  NED ID                 ADMIN STATE
-----------------------------------------------------------------------------
S1-Test-00001  64.1.0.110     -            cisco-staros-cli-5.43  unlocked
esc-etsi       64.1.0.6       -            etsi-sol003-gen-1.13   unlocked
esc-netconf    64.1.0.6       -            esc                    unlocked
openstack      10.225.202.49  -            openstack-cos-gen-4.2  unlocked
root@ncs#
```

3. NSO 5.8.10 インストール bin ファイルを */tmp* フォルダにコピーし、NSO をバージョン 5.8.10 にアップグレードします。

```
root@test-nso:/var/opt/ncs# cd /tmp
root@test-nso:/tmp# ls -lrt
total 397840
-rwxrwxrwx 1 ubuntu   ubuntu   203071802 Nov 18  2022
nso-5.7.5.1.linux.x86_64.installer.bin
drwx------ 3 root     root          4096 Sep 10 03:02
systemd-private-d7c0f02148d447358a1b6b5995f1f339-systemd-resolved.service-O5tL4V
drwx------ 3 root     root          4096 Sep 10 03:02
systemd-private-d7c0f02148d447358a1b6b5995f1f339-systemd-logind.service-Uj4bic
drwx------ 3 root     root          4096 Sep 10 03:02 snap.lxd
drwx------ 2 ubuntu   ubuntu        4096 Sep 12 09:45 ssh-WxVBdtyvgGzB
drwx------ 2 ubuntu   ubuntu        4096 Sep 12 19:28 ssh-kRFako4TgqJp
drwx------ 2 ubuntu   ubuntu        4096 Sep 12 20:25 ssh-wyrZqTmiA4o1
drwx------ 2 ubuntu   ubuntu        4096 Sep 12 20:50 ssh-a10wclKRgSP2
-rwxrwxrwx 1 ubuntu   ubuntu   204258218 Sep 13 05:38
nso-5.8.10.linux.x86_64.installer.bin
drwx------ 2 ubuntu   ubuntu        4096 Sep 13 12:21 ssh-ReWAFnmi3qSl
drwx------ 2 ubuntu   ubuntu        4096 Sep 13 12:54 ssh-dn16O8f1nkaz
drwx------ 2 ubuntu   ubuntu        4096 Sep 20 05:49 ssh-DtgyHvctQ5S0
drwxr-xr-x 2 root     root          4096 Oct  9 07:01 hsperfdata_root
drwxr-xr-x 2 nsoadmin nsoadmin      4096 Oct  9 07:01 hsperfdata_nsoadmin

root@test-nso:/tmp# sh ./nso-5.8.10.linux.x86_64.installer.bin --system-install
--install-dir /opt/ncs --config-dir /etc/ncs --run-dir /var/opt/ncs --log-dir
/var/log/ncs --run-as-user nsoadmin --non-interactive
INFO  Using temporary directory /tmp/ncs_installer.63734 to stage NCS installation
bundle
INFO  Using /opt/ncs/ncs-5.8.10 for static files
INFO  Doing install for running as user nsoadmin
INFO  Unpacked ncs-5.8.10 in /opt/ncs/ncs-5.8.10
INFO  Found and unpacked corresponding DOCUMENTATION_PACKAGE
INFO  Found and unpacked corresponding EXAMPLE_PACKAGE
INFO  Found and unpacked corresponding JAVA_PACKAGE
INFO  Generating default SSH hostkey (this may take some time)
INFO  SSH hostkey generated
INFO  Generating self-signed certificates for HTTPS
INFO  Environment set-up generated in /opt/ncs/ncs-5.8.10/ncsrc
INFO  NSO installation script finished
INFO  Found and unpacked corresponding NETSIM_PACKAGE
cp: cannot stat '/sbin/arping': No such file or directory
WARN  Failed to copy /sbin/arping command - capability not set
INFO  Found ncs.crypto_keys, not migrating
INFO  The following files have been installed with elevated privileges:
  /opt/ncs/ncs-5.8.10/lib/ncs/lib/core/pam/priv/epam: setuid-root
```

```
  /opt/ncs/ncs-5.8.10/lib/ncs/erts/bin/ncs.smp: capability cap_net_bind_service
  /opt/ncs/ncs-5.8.10/lib/ncs/bin/ip: capability cap_net_admin

INFO  NCS installation complete

root@test-nso:/tmp# /etc/init.d/ncs stop
Stopping ncs: .

root@test-nso:/tmp# cd /opt/ncs
root@test-nso:/opt/ncs# ls -lrt
total 24
drwxr-xr-x 17 root     root 4096 Oct  9 06:41 ncs-5.7.5.1
-rw-r--r--  1 root     root    9 Oct  9 06:41 user
-rw-r--r--  1 root     root   80 Oct  9 06:41 installdirs
lrwxrwxrwx  1 root     root   11 Oct  9 06:41 current -> ncs-5.7.5.1
drwxr-xr-x  2 nsoadmin root 4096 Oct  9 06:41 packages
drwxr-xr-x  2 nsoadmin root 4096 Oct  9 06:41 downloads
drwxr-xr-x 17 root     root 4096 Oct  9 09:43 ncs-5.8.10

Set the current NSO to version 5.8.10 using symbolic link

root@test-nso:/opt/ncs# rm -f current
root@test-nso:/opt/ncs# ln -s ncs-5.8.10 current

root@test-nso:/opt/ncs# ls -lrt
total 24
drwxr-xr-x 17 root     root 4096 Oct  9 06:41 ncs-5.7.5.1
-rw-r--r--  1 root     root    9 Oct  9 06:41 user
-rw-r--r--  1 root     root   80 Oct  9 06:41 installdirs
drwxr-xr-x  2 nsoadmin root 4096 Oct  9 06:41 packages
drwxr-xr-x  2 nsoadmin root 4096 Oct  9 06:41 downloads
drwxr-xr-x 17 root     root 4096 Oct  9 09:43 ncs-5.8.10
lrwxrwxrwx  1 root     root   10 Oct  9 09:44 current -> ncs-5.8.10
```

4. */var/opt/ncs/packages* フォルダにある以前の MFP 3.4.1 のパッケージと NED を参照し、新しい MFP 3.4.2 のパッケージと NED に置き換えます。

```
root@test-nso:/opt/ncs# cd /var/opt/ncs/packages/
root@test-nso:/var/opt/ncs/packages# ls -lrt
total 20104
-rw-rw-r-- 1 ubuntu ubuntu 2191794 Jan 25  2023 ncs-5.7.5.1-cisco-rcm-nc-1.6.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu 2694132 Jan 25  2023 ncs-5.7.3-etsi-sol003-1.13.16.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu  655190 Jan 25  2023 ncs-5.7.2.1-esc-5.7.0.73.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu 2685815 Jan 25  2023
ncs-5.7.2.1-cisco-etsi-nfvo-4.7.2.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu 2702317 Jan 25  2023 ncs-5.7.2-openstack-cos-4.2.26.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu 9606799 Jan 25  2023 ncs-5.7.2-cisco-staros-5.43.4.tar.gz
-rwxrwxrwx 1 ubuntu ubuntu     435 Jan 25  2023 compile-all-packages.sh
-rwxrwxrwx 1 ubuntu ubuntu     275 Jan 25  2023 Ha-Mop.sh
drwxrwxr-x 6 ubuntu ubuntu    4096 Oct  9 06:55 nfv-common
drwxrwxr-x 7 ubuntu ubuntu    4096 Oct  9 06:56 nfv-device-onboarding
drwxrwxr-x 8 ubuntu ubuntu    4096 Oct  9 06:56 nfv-vim
drwxrwxr-x 9 ubuntu ubuntu    4096 Oct  9 06:57 nfv-vnf-lcm
drwxrwxr-x 8 ubuntu ubuntu    4096 Oct  9 07:00 mobility-common
drwxrwxr-x 7 ubuntu ubuntu    4096 Oct  9 07:01 mop-common
drwxrwxr-x 8 ubuntu ubuntu    4096 Oct  9 07:01 mobility-mop
drwxrwxr-x 7 ubuntu ubuntu    4096 Oct  9 07:01 mobility-rcm-subscriber

root@test-nso:/var/opt/ncs/packages# rm -rf *
root@test-nso:/var/opt/ncs/packages# ls -lrt
total 0
root@test-nso:/var/opt/ncs/packages#

Copy the MFP 3.4.2 packages along with NEDS:
```

```
root@test-nso:/var/opt/ncs/packages# ls -lrt
total 26328
-rw-rw-r-- 1 ubuntu ubuntu 2191794 Sep 25 05:40 ncs-5.7.5.1-cisco-rcm-nc-1.6.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu 2694132 Sep 25 05:40 ncs-5.7.3-etsi-sol003-1.13.16.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu  655190 Sep 25 05:40 ncs-5.7.2.1-esc-5.7.0.73.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu 2685815 Sep 25 05:40
ncs-5.7.2.1-cisco-etsi-nfvo-4.7.2.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu 2702317 Sep 25 05:40 ncs-5.7.2-openstack-cos-4.2.26.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu 9606799 Sep 25 05:40 ncs-5.7.2-cisco-staros-5.43.4.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu  824211 Sep 25 05:40 nfv-vnf-lcm.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu  307054 Sep 25 05:40 nfv-vim.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu  197449 Sep 25 05:40 nfv-device-onboarding.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu   59217 Sep 25 05:40 nfv-common.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu 3905393 Sep 25 05:40 mop-common.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu  113829 Sep 25 05:40 mobility-rcm-subscriber.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu  243790 Sep 25 05:40 mobility-mop.tar.gz
-rw-rw-r-- 1 ubuntu ubuntu  746045 Sep 25 05:40 mobility-common.tar.gz
```

5. **start-with-package-reload** オプションを使って NSO を再起動します。これで、NSO 5.8.10 で MFP が 3.4.1 から 3.4.2 にアップグレードされます。

```
root@test-nso:/var/opt/ncs/packages# source /etc/profile.d/ncs.sh

root@test-nso:/var/opt/ncs/packages# /etc/init.d/ncs start-with-package-reload
Starting ncs: .

root@test-nso:/var/opt/ncs/packages# ncs --version
5.8.10

root@test-nso:/var/opt/ncs/packages# ncs_cli -C

root connected from 127.0.0.1 using console on test-nso
root@ncs# show packages package package-version
                        PACKAGE
NAME                    VERSION
-----------------------------------
cisco-etsi-nfvo         4.7.2
cisco-rcm-nc-1.6        1.6
cisco-staros-cli-5.43   5.43.4
esc                     5.7.0.73
etsi-sol003-gen-1.13    1.13.16
mobility-common         3.4.2
mobility-rcm-subscriber 3.4.2
mop-automation          3.4.2
mop-common              3.4.2
nfv-common              3.4.2
nfv-device-onboarding   3.4.2
nfv-vim                 3.4.2
nfv-vnf-lcm             3.4.2
openstack-cos-gen-4.2   4.2.26

root@ncs# show packages package oper-status
packages package cisco-etsi-nfvo
 oper-status up
packages package cisco-rcm-nc-1.6
 oper-status up
packages package cisco-staros-cli-5.43
 oper-status up
packages package esc
 oper-status up
packages package etsi-sol003-gen-1.13
 oper-status up
packages package mobility-common
```

```
 oper-status up
packages package mobility-rcm-subscriber
 oper-status up
packages package mop-automation
 oper-status up
packages package mop-common
 oper-status up
packages package nfv-common
 oper-status up
packages package nfv-device-onboarding
 oper-status up
packages package nfv-vim
 oper-status up
packages package nfv-vnf-lcm
 oper-status up
packages package openstack-cos-gen-4.2
 oper-status up
root@ncs#

root@ncs# show devices list
NAME           ADDRESS        DESCRIPTION  NED ID                 ADMIN STATE
-------------------------------------------------------------------------------
S1-Test-00001  64.1.0.110     -            cisco-staros-cli-5.43  unlocked
esc-etsi       64.1.0.6       -            etsi-sol003-gen-1.13   unlocked
esc-netconf    64.1.0.6       -            esc                    unlocked
openstack      10.225.202.49  -            openstack-cos-gen-4.2  unlocked
```

6. mop-automation メソッドにより、NSO 5.8.10 で MFP 3.4.2 を使用して、以前の MFP 3.4.1 および NSO 5.7.5.1 でインスタンス化されたテスト用 VNF VPC-SI デバイスに設定をプッシュします。

```
root@test-nso:/var/opt/ncs# cat day1config.cfg
config
port ethernet 1/1
description test-description-1/1-by-mop18oct
no shutdown
exit

root@ncs# mobility-mop:action mop-automation generate-dry-run true operation-type
commit mop-type common mop-file-name { file-name day1config.cfg order 1
target-devices-list { target-device-name S1-Test-00001 } } save-config-permanently
true
task-id 036f5e94-364b-4d5f-a95e-4663fe5ed08a
time-stamp 2023-10-09T10:18:19+0000
time-zone Coordinated Universal Time
root@ncs#

root@ncs# mobility-mop:action mop-automation-status task-id
036f5e94-364b-4d5f-a95e-4663fe5ed08a
task-id 036f5e94-364b-4d5f-a95e-4663fe5ed08a
task-status COMPLETED
start-date 2023-10-09T10:18:19+0000
end-date 2023-10-09T10:18:23+0000
time-zone Coordinated Universal Time
operation-type commit
action-type save
devices-list {
    device-name S1-Test-00001
    device-status COMPLETED
    start-date 2023-10-09T10:18:19+0000
    end-date 2023-10-09T10:18:23+0000
    device-state common
    files {
        file-name day1config.cfg
```

```
        order 1
        dry-run-mop
/var/opt/ncs//036f5e94-364b-4d5f-a95e-4663fe5ed08a/S1-Test-00001/day1config_commit_2023-10-09T101819+0000.cfg

        rollback-mop
/var/opt/ncs//036f5e94-364b-4d5f-a95e-4663fe5ed08a/S1-Test-00001/day1config_rollback_commit_2023-10-09T101819+0000.cfg

        commit-queue-status completed
        commit-queue-id 1696846701998
    }
}

root@test-nso:/var/opt/ncs# cat
/var/opt/ncs//036f5e94-364b-4d5f-a95e-4663fe5ed08a/S1-Test-00001/day1configroot@test-nso:/var/opt/ncs#
 cat
/var/opt/ncs//036f5e94-364b-4d5f-a95e-4663fe5ed08a/S1-Test-00001/day1config_commit_2023-10-09T101819+0000.cfg
config
port ethernet 1/1
 description test-description-1/1-by-mop18oct
exit
end

root@test-nso:/var/opt/ncs# cat
/var/opt/ncs//036f5e94-364b-4d5f-a95e-4663fe5ed08a/S1-Test-00001/day1configroot@test-nso:/var/opt/ncs#
 cat
/var/opt/ncs//036f5e94-364b-4d5f-a95e-4663fe5ed08a/S1-Test-00001/day1config_rollback_commit_2023-10-09T101819+0000.cfg
config
port ethernet 1/1
 no description
exit
end
```

NSO バージョンを変更せずに MFP 3.4.1 から MFP 3.4.2 にアップグレード

NSO バージョンを変更せずに MFP 3.4.1 から MFP 3.4.2 にアップグレードするには、次の手順を使用します。

1. MFP 3.4.2 のパッケージと NED をコピーし、*/var/opt/ncs/packages* フォルダの中身と置き換えます。
2. **ncs_cli** でパッケージのリロードを実行して、MFP バージョンが 3.4.2 にアップグレードされていることを確認します。NSO を再起動します。

付録 C：P2P 優先順位のアップグレード

mobility-library アクションコマンドを使用して P2P 優先順位をアップグレードするには、次の手順を実行します。

1. P2P ファイルの配置とパス設定を含む事前チェックを実行し、その後に VNF のインスタンス化を行います。

```
[cloud-user@qwerty ncs]$ ncs --version
5.8.10

[cloud-user@qwerty ncs]$ ncs_cli -C

User cloud-user last logged in 2023-09-20T03:23:18.655123+00:00, to qwerty, from
```

```
10.65.51.122 using cli-ssh
cloud-user connected from 10.65.51.122 using ssh on qwerty
cloud-user@ncs# show packages package package-version
                          PACKAGE
NAME                      VERSION
-----------------------------------
cisco-etsi-nfvo           4.7.2
cisco-rcm-nc-1.6          1.6
cisco-staros-cli-5.43     5.43.4
esc                       5.7.0.73
etsi-sol003-gen-1.13      1.13.16
mobility-common           3.4.2
mobility-rcm-subscriber   3.4.2
mop-automation            3.4.2
mop-common                3.4.2
nfv-common                3.4.2
nfv-device-onboarding     3.4.2
nfv-vim                   3.4.2
nfv-vnf-lcm               3.4.2
openstack-cos-gen-4.2     4.2.26

cloud-user@ncs# show packages package oper-status
packages package cisco-etsi-nfvo
 oper-status up
packages package cisco-rcm-nc-1.6
 oper-status up
packages package cisco-staros-cli-5.43
 oper-status up
packages package esc
 oper-status up
packages package etsi-sol003-gen-1.13
 oper-status up
packages package mobility-common
 oper-status up
packages package mobility-rcm-subscriber
 oper-status up
packages package mop-automation
 oper-status up
packages package mop-common
 oper-status up
packages package nfv-common
 oper-status up
packages package nfv-device-onboarding
 oper-status up
packages package nfv-vim
 oper-status up
packages package nfv-vnf-lcm
 oper-status up
packages package openstack-cos-gen-4.2
 oper-status up

[cloud-user@qwerty ncs]$ ls -lrt
total 4740
drwxrwxrwx.  2 nsoadmin   root             6 Sep  5 03:36 scripts
drwxrwxrwx.  2 nsoadmin   root             6 Sep  5 03:36 streams
drwxrwxrwx.  2 nsoadmin   root             6 Sep  5 03:36 backups
-rwxrwxrwx.  1 nsoadmin   root          1513 Sep  5 03:36 INSTALLATION-LOG
drwxrwxrwx.  3 nsoadmin   nsoadmin        22 Sep  5 03:37 target
drwxrwxrwx.  7 cloud-user cloud-user     204 Sep  5 03:56 vnfpackages
-rwxrwxrwx.  1 root       root            87 Sep  5 06:26 day1config.cfg
-rwxrwxrwx.  1 root       root            31 Sep  5 06:47 rcm-day1config.cfg

-rwxrwxrwx.  1 root       root       4253395 Sep  8 03:19
patch_libp2p-2.69.0.1534.so.tgz
```

```
-rwxrwxrwx.  1 cloud-user cloud-user     142 Sep 10 14:11 daynconfig.cfg

drwxrwxrwx. 10 nsoadmin   root          4096 Sep 18 02:20 packages
-rwxrwxrwx.  1 nsoadmin   nsoadmin       333 Sep 18 02:31 storedstate

drwxrwxrwx.  2 nsoadmin   root            98 Sep 18 08:59 cdb

drwxrwxrwx.  2 nsoadmin   root         20480 Sep 19 23:23 rollbacks
drwxrwxrwx.  5 nsoadmin   root          4096 Sep 19 23:26 state

cloud-user@ncs# config
Entering configuration mode terminal
cloud-user@ncs(config)# configurable-parameters p2p-required true
cloud-user@ncs(config)# configurable-parameters p2p-soFile-path
/var/opt/ncs/patch_libp2p-2.69.0.1534.so.tgz
cloud-user@ncs(config)# commit
Commit complete.
cloud-user@ncs(config)# exit

cloud-user@ncs# show vnf-status instances UP-Test001-p2p
                                          FUNCTION

INSTANCE ID     TIMESTAMP               TYPE      OPERATION       STATUS      STATUS
 MESSAGE
-------------------------------------------------------------------------------------------------
UP-Test001-p2p  2023-09-19 23:29:42.335  VPC-SI    deploy          init        init

                2023-09-19 23:30:19.377  VPC-SI    deploy          processing
processing
                2023-09-19 23:30:47.948  VPC-SI    deploy          processing
processing
                2023-09-19 23:30:49.269  VPC-SI    deploy          completed
completed
               2023-09-19 23:31:55.555  -         init            success     Device
 Onboarding initialized
                2023-09-19 23:31:56.061  -         fetch-ssh-keys  success
fetch-ssh-keys was successful
              2023-09-19 23:31:57.005  -         connect         success     connect
 was successful
                2023-09-19 23:31:58.353  -         sync-from       success
sync-from was successful
               2023-09-19 23:31:58.523  -         ready           success     Device
 Successfully onboarded
               2023-09-19 23:37:29.386  -         config-read     success     Config
 MetaData is empty or null

[cloud-user@qwerty ncs]$ ssh admin@64.1.0.96
The authenticity of host '64.1.0.96 (64.1.0.96)' can't be established.
RSA key fingerprint is SHA256:TKCql7DQvty52OHp8WzGt0lYKiloAtEmMt1xAMQ23a0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Csco@123
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '64.1.0.96' (RSA) to the list of known hosts.
Cisco Systems QvPC-SI Intelligent Mobile Gateway
admin@64.1.0.96's password:
Last login: Tue Sep 19 23:32:04 -0400 2023 on pts/1 from 64.1.0.7.

No entry for terminal type "xterm-256color";
using dumb terminal settings.

[local]vpc-si# show module p2p verbose
Module p2p
   Priority  card   version  loaded    location      update/rollback time    status
```

```
       99      1  2.69.1534    2/2    /var/opt/lib   Tue Sep 19 23:32:35 2023
success                                <<<<<<< p2p priority starting from 99 instead
 of 10
        X      1  1.161.656    0/2            /lib                   (never)     N/A

[local]vpc-si#
[local]vpc-si#
[local]vpc-si# exit
Connection to 64.1.0.96 closed.
[cloud-user@qwerty ncs]$
[cloud-user@qwerty ncs]$
[cloud-user@qwerty ncs]$ ncs_cli -C

User cloud-user last logged in 2023-09-20T03:30:52.813071+00:00, to qwerty, from
10.65.51.122 using rest-http
cloud-user connected from 10.65.51.122 using ssh on qwerty
cloud-user@ncs#
cloud-user@ncs#
```

2. P2P 優先順位の実際のアップグレードには、**mobility-library** アクションコマンドを使用します。

```
cloud-user@ncs# mobility-library configure-library library-name p2p device-list {
device-name UP-Test001-p2p }
status success
message Configured Successfully

cloud-user@ncs#
cloud-user@ncs#
cloud-user@ncs# exit
[cloud-user@qwerty ncs]$ ssh admin@64.1.0.96
Cisco Systems QvPC-SI Intelligent Mobile Gateway
admin@64.1.0.96's password:
Last login: Tue Sep 19 23:41:37 -0400 2023 on pts/1 from 64.1.0.7.

No entry for terminal type "xterm-256color";
using dumb terminal settings.

[local]vpc-si# show module p2p verbose
Module p2p
   Priority  card   version  loaded    location      update/rollback time     status
>      98      1  2.69.1534    2/2    /var/opt/lib   Tue Sep 19 23:41:39 2023
success
*      99      1  2.69.1534    2/2    /var/opt/lib                   (never)     N/A
        X      1  1.161.656    0/2            /lib                   (never)     N/A

>  current module priority is 98
*  some modules have not unloaded from the p2p application and are still in use

[local]vpc-si#
```

第 65 章

NSH トラフィックステアリング

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
このリリースでは、トラフィックステアリングおよび L2 up-appliance-group BFD 設定の後処理ルール条件の照合がサポートされています。	21.23.22
このリリースでは、トラフィックステアリングの後処理ルール条件の照合と、インターフェイス名を使用して実行できる L2 up-appliance-group BFD 設定のサポートが追加されています。	21.27

改訂の詳細	リリース
最初の導入。	21.24 より前

機能説明

3GPP EPC アーキテクチャにより、Gi インターフェイス上の各種サービス機能間でデータトラフィックをステアリングできます。トラフィック ステアリング アーキテクチャは、ネットワーク サービス ヘッダー（NSH）サービス チェーン プロトコルに基づいています。EPC ゲートウェイは、NSHをサポートするアプライアンスを含む複数のサービスチェーン全体でトラフィックを誘導するため、トラフィックステアリングを実行する必要があります。

NSH トラフィックステアリングには、次の 2 つのモードがあります。

- スタンドアロン モード
- サンドイッチモード

この機能により、お客様の要件に基づいて、トラフィックの課金とステアリングを互いに独立させることができます。お客様は、最小限の構成拡張によって、トラフィックをステアリングするためのさまざまなトラフィックカテゴリを既存のユースケースシナリオ内に加えることができます。

トラフィックステアリングの後処理ルール条件の照合

単純なトラフィック分類は、複数のルールベースにまたがる膨大な数の課金ルールにより、トラフィックステアリングの操作および設定プロセスを簡素化するのに役立ちます。

- サービス スキーム フレームワークのトリガー条件では、後処理 ruledef 名の照合がサポートされています。
- トラフィックの後処理ルールとして設定された L3/L4 ruledef がトラフィックステアリングされます。
- トリガーアクションは、トラフィックステアリングの後処理ルールの照合に関するトリガー条件をサポートしています。
- トリガー条件の後処理 ruledef 名は、PFD プッシュと RCM でサポートされています。

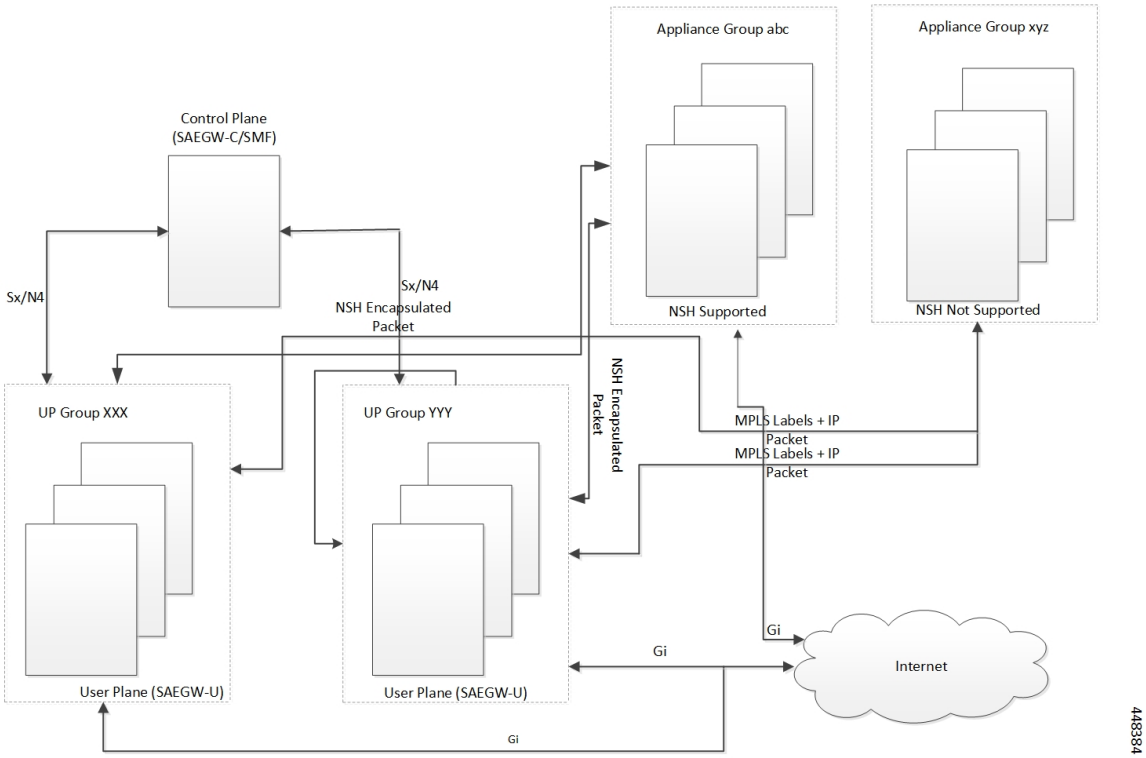
インターフェイス名を使用した UP アプライアンスグループでの BFD インスタンス ID の設定

トラフィックステアリングの場合、 **up-appliance-group** 内の Bidirectional Forwarding Detection（BFD）インスタンス ID の設定は、IP 設定とともにインターフェイス名を使用して有効になります。

アーキテクチャ：スタンドアロンモード

次の図は、NSHアプライアンス向けのCUPSベースゲートウェイのアーキテクチャセットアップを示しています。

図 *40 : NSH* トラフィック ステアリング アーキテクチャ：スタンドアロンモード



この機能は、NSH がサポートするアプライアンスの Service Function Chaining をサポートします。ゲートウェイは、各アプライアンスのインスタンスまたはグループに基づいて、トラフィックをステアリングするための適切なステアリング方式またはカプセル化方式を選択するように設定されます。

表 *43 :* 通話フロー

ステップ	説明
1.	SAEGW-U で受信した UL パケットは、適切な SFC に関連付けられた設定済みポリシーに基づいて分類されます。

ステップ	説明
2 に送信します。	Saegw は、SFP のスティッキ性（MSISDN スティッキ性）またはサービスと負荷の可用性に基づいて SFP の選択を実行します。UL トラフィックは、選択した SFP で NSH（IP-UDP）カプセル化されてステアリングされ、必要に応じてコンテキストヘッダーが入力されます。
3.	NSH アプライアンスは、NSH パケットを受信すると、IP パケット（場合によってはコンテキストヘッダーも）を処理し、Gi インターフェイスを介してパケットを送信します。
4.	接続先サーバーは、Gi インターフェイスから SAEGW-U に DL パケットを送信します。DL トラフィックは、選択した SFP で NSH（IP-UDP）カプセル化されてステアリングされ、必要に応じてコンテキストヘッダーが入力されます。
5.	NSH アプライアンスは、NSH パケットを受信すると、IP パケット（場合によってはコンテキストヘッダーも）を処理し、パケットを SAEGW-U にヘアピンします。
6.	NSH パケットを受信した SAEGW-U： • 受信したペイロードのカプセル化を解除します。 • IP パケット（場合によってはコンテキストヘッダーも）を処理し、Gn インターフェイスを介してパケットを UE に送信します。

コンポーネント

トラフィック ステアリング アーキテクチャは、次の主要コンポーネントで構成されています。

コントロールプレーン（SAEGW-C）

CP はサブスクライバのトラフィックのステアリング方法に関する情報を UP に送信します。UP はサブスクライバに対して定義されたポリシーに基づいて、サブスクライバ データ トラフィックのすべてまたは一部のみをステアリングします。さまざまなタイプのサブスクライバ トラフィックをさまざまなサービス機能チェーンに誘導できます。

CP はローカルに設定されたポリシーに基づいて、PCRF から Ts-subscription-scheme AVP を受信した後、サブスクライバのサービスチェーン名を選択します。

ユーザープレーン（SAEGW-U）

UP は CP から受信したポリシーに基づいて、サブスクライバ データ トラフィックを 1 つ以上のサービス機能チェーンに誘導します。

UP は、次の機能も実行します。

- 特定のサービス機能チェーン（SFC）のサービス機能パス（SFP）を選択します。
- アプライアンスにトラフィックを転送しながら、サブスクライバのスティッキ性を維持します。
- ノードやアプライアンスに障害が発生した場合は、サブスクライバ データ トラフィックを再選択し、新しいノードに誘導します。
- SFP の**インサービス**および **アウトオブサービス**のステータスを管理します。
- SFC 内でサービスを提供できる SFP の数に応じて、SFC ステータスを管理します。

NSH

NSH アプライアンスの正常性をモニタリングするために、各 SAEGW-U/UPF はアプライアンスの負荷と有用性統計のモニタリングを担当します。

- OAM NSH パケットメカニズムを使用して、アプライアンスのステータスをモモニターします。
- 設定のモニタリング頻度は 1 ～ 20 秒で、デフォルトの間隔は 1 秒です。
- OAM 要求がタイムアウトした場合は、再試行します。タイムアウトと再試行の値については、タイムアウトは 1 ～ 5 秒（デフォルトは 3 秒）、再試行は 1 ～ 3 回（デフォルトは 2 回）の範囲で値を設定できます。
- アプライアンスの有用性ステータスに加えて、アプライアンスの現在の負荷が監視されます。SF のさまざまなインスタンス間で最適なロードバランシングを維持するために、現在の負荷をモニターします。この負荷ステータスは、NSH の OAM 応答パケットを介して返されます。

制限事項

NSH トラフィックステアリングには、次の制限があります。

- NSH アプライアンスで、インターフェイスのフラグメンテーションが発生しないようにする必要があります。NSH アプライアンス インターフェイスへの MTU を Gn/Gi インターフェイスよりも大きくします。

- HTTP パイプライン化セッション、ミッドフロー HTTP 部分パケット、および TCP アウトオブオーダーパケットの場合、L7 条件で SFP 再評価が要求されると、NSH アプライアンスに到達しません。
- メイン設定から SFP ID 設定を削除しても、show configuration では依然として SFP ID が表示されます。commit CLI を使用して SFP ID を VPP にコミットすると、SFP ID は削除されます。
- トラフィックステアリング統計は、トラフィックステアリングの候補となるパケットを示します。トラフィックステアリング統計では、クォータの枯渇によってドロップされたパケットもカウントされますが、これらは依然としてトラフィックステアリングの候補です。
- NSH SRC/バインド IP アドレスまたはアプライアンス IP アドレスの変更が NSH アプライアンスのインスタンス設定で必要になった場合は、インスタンスを削除してから、それに関連付けられている SFP を削除し、SFP と新しいインスタンスを変更した IP アドレスとともに配置する必要があります。後でコミットを実行します。
- ノード障害が発生して、連続データが受信されると、ステアリング統計に不一致が生じる可能性があります。ダウンしている SFP でステアリングされたデータは、統計に反映されません。
- マルチ PDN コールの場合、NSH インスタンスのスティッキ性は各サブスクライバセッションに制限されます。
- ICSR や SFP の削除などの設定変更が原因で SAEGW-U の状態が変更された場合、この時間枠でアプライアンスからヘアピンバックされているパケットがドロップされる可能性があります。それ以降のすべての着信パケットは、通常どおりに処理されます。
- フローの最初のパケットが DL パケット（セッションリカバリ）の場合、最初のパケットだけがドロップされますが、再送信されたパケットと後続のすべてのパケットは通常どおりに送信されます。
- NSH 形式のタグが変更された場合、タグタイプ stream-fp-md エンコード、reverse-stream-fp-md 、secondary-srv-path-hdr、および rate-group は、既存のフローではなく、新しいフローに対して有効になります。NSH 形式の残りのタグの変更は新しいセッションに適用されますが、既存のセッションのトラフィックは古い形式のタグで続行されます。このようなケース、特にタグの変更や削除の場合、アプライアンスが NSH パケットで受信したタグ値と一致せず、あいまいな動作につながる可能性があります。そのため、NSH 形式のタイプの変更は慎重に行ってください。
- サーバーによって開始された TCP フローは、トラフィックステアリングでは考慮されません。
- NSH トラフィックをキャプチャするための Monsub サポートは現在使用できません。
- アプライアンスレベルの制限（トラフィックタイプなど）に対処するためには、サービススキームのポリシー選択の設定で、そのようなアプライアンスを含むサービスチェーンの選択対象からそのようなトラフィックを柔軟に除外できます。

- N:M 構成の場合、サービススキームの設定（トリガーアクション、トリガー条件、サービススキーム、サブスクライバクラス、サブスクライバベース）は、UP の Day-0 設定で行う必要があります。UP の一般的な設定では、サービススキームが設定されていると、競合状態になり、ユーザープレーンのセッションマネージャでサービススキームが断続的に設定されなくなり、トラフィックステアリング機能で障害が発生します。
- L2 ステアリングの OAM 統計は部分的にサポートされています。
- HTTP 連結パケットの場合のパケットは、パケット内の最後の HTTP GET で一致したポリシーに基づいてステアリングされたトラフィックを指します。
- アプライアンスがダウンした場合、次のアップリンクパケットがフローで回復したときに、フローを再評価するためにオンロードされます。新しい SFP の選択が行われ、トラフィックが新しいアプライアンスに誘導されます。

機能の仕組み：スタンドアロンモード

パケットフロー

この項では、NSH トラフィック ステアリング アーキテクチャのパケットフローについて説明します。

アップリンクパケット数

図 *41 :* アップリンクパケットフロー

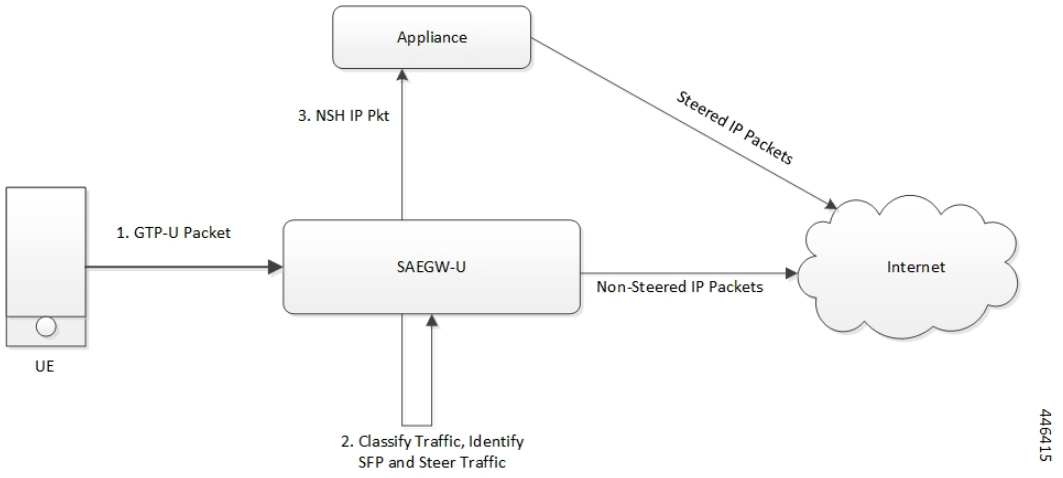


表 *44 :* アップリンクパケットフローの説明

手順	説明
1	UE が、サブスクライバのデータパケットを SAEGW-U に送信します。
2	SAEGW-U が、サブスクライバポリシーに基づいてサブスクライバのデータトラフィックを分類し、SFC を識別して適宜 SFP を選択します。
3	SAEGW-U が、NSH RFC に従って NSH カプセル化を使用してアップリンク（UL）パケットをステアリングし、NSH アプライアンスに送信します。 SAEGW-U が、ステアリングされていない IP パケットをサーバーに送信します。
4	アップリンクパケットを受信した NSH 対応アプライアンスが、特定の基準に基づいてパケットをサーバーに転送するか決定します。

ダウンリンクパケット数

図 *42 :* ダウンリンクパケットフロー

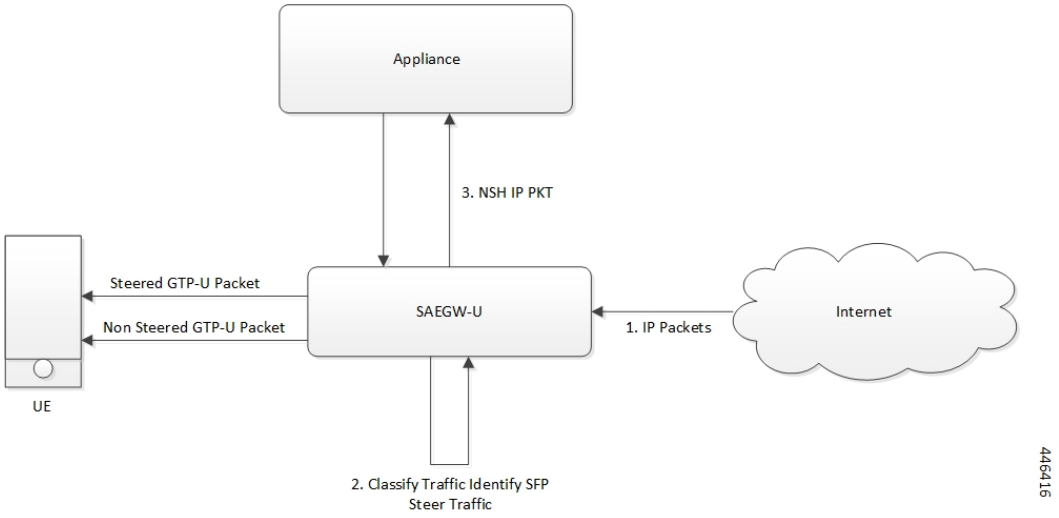


表 *45 :* ダウンリンクパケットフローの説明

手順	説明
1	SAEGW-U が、サーバーからダウンリンク（DL）パケットを受信します。
2	SAEGW-U が SFP を選択します。

手順	説明
3	SAEGW-U が、メタデータを NSH コンテキストヘッダーとして追加し、NSH 対応アプライアンスに転送します。
4	NSH 対応アプライアンスが、SAEGW-U によって送信されたいくつかのメタデータタグを使用してパケットを SAEGW-U に送り返します。
5	パケットを受信した SAEGW-U が、サブスクライバ課金ポリシーに基づいてサブスクライバのデータトラフィックを分類します。
6	SAEGW-U がデータパケットをサブスクライバに送信します。

NSH トラフィックステアリング要件

トラフィック ステアリング ソリューションにおける NSH アプライアンスの統合の動作は次のとおりです。

- SAEGW-U は NSH アプライアンスセッションのスティック性を維持し、サブスクライバセッションのすべてのフローが同じアプライアンスインスタンスを選択するようにします。
- すべてのアプライアンスインスタンスの負荷容量を定義するために設定できるオプション（50%、100% など）があります。NSH アプライアンスによる負荷ステータスがこのしきい値を超えた場合、既存のサブスクライバだけがそれまでのインスタンスを続行できます。このインスタンスは、負荷ステータスがしきい値を下回るまで、新しいサブスクライバに割り当てられません。
- NSH アプライアンスが DEAD 状態と検出された場合、このアプライアンスインスタンスに関与する SFP 上のすべてのトラフィックが再分類され、トラフィックは別のアプライアンスインスタンスに移動します。このようなアプライアンスは ALIVE 状態に戻っても、新しいサブスクライバの選択には使用できません。
- トラフィックステアリングは、セッション中に有効または無効にできます。セッション中にトラフィックステアリングを有効にすると、新しいフローはトラフィックステアリングの対象になります。古いフローは、トラフィックステアリングなしで続行されます。
- SR/ICSR 後のトラフィック ステアリング セッションのスティッキ性に対する SR/ICSR サポートは維持されます 。
- マルチアプライアンス SFP の場合、設定には次の 2 つの形式があります。
  - アプライアンスがトラフィックの開始（TWH パケットなど）を確認する必要がある場合は、すべてのアプライアンスに関与する SFP が選択されます。設定ポリシーに従って分類が行われると、トラフィックは不適格なアプライアンスから脱落する可能性があります。
  - アプライアンスが中間フローに関与する場合、特定のアプライアンスがさらにトラフィック分類の対象になると、アプライアンスが関与するように設定されます。

- トラフィックステアリング統計は、トラフィックステアリングの候補となるパケットを示します。トラフィックステアリング統計では、クォータの枯渇によってドロップされたパケットもカウントされますが、これらはトラフィックステアリングの候補です。
- ノード障害が発生して、連続データが受信されると、ステアリング統計に不一致が生じる可能性があります。ダウンしている SFP でステアリングされたデータは、統計に反映されません。
- NSH アプライアンスインスタンスの設定で NSH リモート IP アドレスまたは SRC バインド IP を変更する場合は、次の手順を実行します。
  - 次に、インスタンスを削除します。
  - 次に、関連付けられている SFP を削除します。
  - 変更後の IP アドレスで SFP と新しいインスタンスを配置します。
  - 後でコミットを実行します。

この機能では、次のトラフィック ステアリング システムの制限値がサポートされています。

トラフィック ステアリング オブジェクト	上限
アプライアンスグループの総数	16
アプライアンスグループごとのインスタンスの総数	256
SFC の総数	16
SFP の総数	64000

デフォルトのサービスチェーン

オペレータは、トラフィックステアリングが有効になっているサブスクライバのすべてのトラフィックが特定のアプライアンスを通過する必要があるといったユースケースを扱うことがあります。このような要件に対応すると同時に、それを実現するための簡単な設定メカニズムを提供するために、デフォルトのサービスチェーンの概念が導入されました。たとえば、サブスクライバが 2 つのアプライアンス（APP1 と APP2）を持つサブスクライバとコミュニケーションを取り、APP2 ですべてのトラフィックを表示する必要がある場合、APP2 を含むサービスチェーンがデフォルトのサービスチェーンとして設定されます。

したがって、トラフィックステアリングが有効になっているサブスクライバの場合、次のような状況下では、特定のトラフィックについてはサービスチェーン APP1+APP2 を使用できない可能性があります。

- APP1+APP2 サービスチェーンを選択しようとしている特定のフローに適切なポリシーが設定されていない。

- APP1+APP2 サービスチェーンが選択されたが、APP1 インスタンスが最小インスタンスしきい値を下回っている。このような場合、APP1+APP2 サービスチェーンは使用できません。
- APP1+APP2 サービスチェーンが選択されたが、SFP を選択できなかった。

このようにサービスチェーンが使用できない場合、フローは設定済みのデフォルトサービスチェーンにフォールバックし、フローに対する APP2 サービス処理が保証されます。

デフォルトのサービスチェーンが設定されていない場合、トラフィックはステアリングされずに送信されます。

SFP の選択

SFP の選択は、次のいずれかに基づきます。

- MSISDN スティッキ性（事前設定済み）
- 負荷の可用性

MSISDN スティッキ性

MSISDN スティッキ性は MS-ISDN に依存し、対応するノードを提供します。ノードが使用可能で、SFP の一部である場合は、その SFP がデータ（UL/DL）用に選択されます。現在、MSISDN スティッキ性は L2 ノードでのみ使用可能であり、L2 ノードのみ、または L2 と NSH が混在するサービスチェーンが存在する可能性があります。サービスチェーンの SFP はすべて、同じノードタイプのセットになっています。このタイプには、L2、L2+NSH、または NSH（のみ）があります。

サブスクライバのスティッキ性（L2 と NSH の両方）は、そのノードが使用可能になるまでサービスチェーン全体でサブスクライバに対して維持され、ノードがダウンするか設定から削除されると、サブスクライバは（SFP 選択に基づいて）別の SFP に移動できます。スティッキ性が失われた場合には、ログとトラップが生成されます。

負荷の可用性

負荷の可用性とは負荷のキャパシティであり、現在の負荷は SFP ごとに保持されます（SFP の一部であるすべてのインスタンスの最小値）。SFP は、負荷の可用性に基づいて、使用可能リスト、過負荷リスト、またはブロック対象リストに分類されます。ブロック対象リストはノードがダウンしている SFP を対象としているため、SFP の選択には、使用可能リストと過負荷リストのみが使用されます。使用可能リストの SFP は、古いコール/セッションおよび新しいコール/セッションの両方に使用できます。過負荷リスト（負荷の可用性＝0）は、スティッキ性（存在する場合）を維持する場合にのみ使用されます。つまり、古いコール/セッション専用です。SFP が選択されると、その SFP は負荷に応じて、またスティッキ性の維持のために、過負荷リストに移動する場合があります。古いコール/セッションには同じ SFP が使用され、新しいコールには SFP 選択の使用可能リストにある残りの SFP が使用されます。

インライン機能とのインターワーキング

次のインライン機能とのインターワーキングのサポートは、既存の実装の範囲には含まれていません。

- IPv4/v6 再アドレス指定
- NAT44 および NAT64
- Next Hop Forwarding
- L2 マーキング

NSH コンテキストヘッダーの評価グループのエンコーディングは、次の予想される動作に合わせてサポートされています。

- エンコードされた評価グループ値は、各パケットが一致するルールに対応するため、単一のフローのパケットでは、異なる評価グループが設定されているか、または設定されていない異なるルール間をフローが移動すると、評価グループが変更されるか、またはエンコードされません。
- SAEGW により、評価グループフィールドに評価グループ値が入力されます（設定されている場合）。コンテンツ ID のみが設定されている場合、この値がフィールドに入力されます。パケットの一致ルールに関連付けられているルールがない場合、評価グループに対応する TLV フィールドは送信されません。
- SAE-GW で遅延ルールの照合が実行され、ルールが一致しない状態でパケットが送信される場合、パケットの評価グループ TLV はエンコードされません。

L2 および NSH トラフィックステアリング機能の設定：スタンドアロンモード

ここでは、CP と UP の両方で L2 および NSH トラフィックステアリング CUPS 機能を設定するために使用できる CLI コマンドについて説明します。

コントロールプレーンの設定

CP を設定するには、次の手順を実行します。

1. 次の CLI コマンドは、[active-charging service] で CP を設定するための設定例です。

```
configure
  active-charging service ACS
  policy-control services-framework

  trigger-action ta1
    up-service-chain sc_L3
  exit
  trigger-action ta2
    up-service-chain  L3
```

```
  exit

  trigger-condition tc1
    rule-name = rule1
    rule-name = rule2
    multi-line-or
  exit

  trigger-condition tc2
    any-match = TRUE
  exit

  service-scheme scheme1
    trigger rule-match-change
      priority 1 trigger-condition tc1 trigger-action ta1
    exit
    trigger subs-scheme-received
      priority 1 trigger-condition tc2 trigger-action ta2
    exit

    subs-class class1
      subs-scheme = s1
    exit
    subscriber-base base1
      priority 1 subs-class class1 bind service-scheme scheme1
    exit
end
```

注：

- **subs-scheme**：この名前は、Gx インターフェイスを介して PCRF から受信した subscription-scheme AVP 値と一致する必要があります。
- **up-service-chain SecNet**：この値は、UP で設定されている up-service-chain と一致する必要があります。
- **rule-name**：この値には、静的/事前定義/GoR/ダイナミックルールを使用できます。

2. トラフィックステアリング AVP は現在、Diameter ディクショナリ custom44 でサポートされています。Diameter ディクショナリにより、TS 関連の AVP が Gx インターフェイスを介して受信されるとき、および Sx メッセージで UP に送信されるときに、CP はこれらの AVP を適切に復号できます。

   CP でディクショナリを設定するための設定例を以下に示します。

```
configure
  context ISP1
    ims-auth-service IMSGx
    policy-control
    diameter dictionary dpca-custom44
  exit
end
```

GX を介して CCA-I/CCA-U/RAR で受信する TS 関連 AVP の値の例を以下に示します。

```
    [V] Services:
      [V] Service-Feature:
        [V] Service-Feature-Type: TS (4)
        [V] Service-Feature-Status: ENABLE (1)
        [V] Service-Feature-Rule-Install:
          [V] Service-Feature-Rule-Definition:
```

```
[V] Service-Feature-Rule-Status: ENABLE (1)
[V] Subscription-Scheme: scheme
[V] Profile-Name: Gold
```

ユーザープレーンの設定

UP を設定するには、次の手順を同じ順序で実行します。

次の CLI コマンドは、L2 および NSH がサポートされているアプライアンスへのデータ送信に使用されるコンテキストに、インターフェイスを追加するための設定例です。

1. L2 および NSH がサポートされているアプライアンスへのデータ送信に使用されるコンテキストにインターフェイスを追加します。

   以下に設定例を示します。

```
configure
require tsmon
end
configure
   context ISP1-UP
   interface <ts_ingress>
   ip address <ip_address>
   ipv6 address <ipv6_address_secondary>
   exit
   end

configure
   context ISP2-UP
   interface <ts_egress>
   ip address <ip_address>
   ipv6 address <ipv6_address_secondary>
   exit
   end
```

2. 新たに追加されたインターフェイスを UP の物理ポートにバインドします。

   次に設定例を示します。

```
configure
   port ethernet 1/11
   vlan 1240
   no shutdown
   bind interface ts_ingress ISP1-UP
   exit
   exit
   port ethernet 1/12
   vlan 1240
   no shutdown
   bind interface ts_egress ISP2-UP
   exit
   exit
   end
```

3. TS 関連の設定を UP に追加します。

   次に設定例を示します。

```
config

ts-bind-ip IP_UP01 ipv4-address 209.165.200.225 ipv6-address 4001::106

  nsh
```

```
node-monitor ipv4-address 209.165.200.226 ipv6-address 4001::107 poll-interval 1
retry-count 2 load-report-threshold 5 (node-monitor  is mandatory for NSH appliances,
 default values are poll-interval=1, retry-count=2, load-report-threshold=5)
    up-nsh-format format1
      tag-value 250 imsi encode
      tag-value 66 msisdn encode
      tag-value 4 rating-group encode
      tag-value 1 stream-fp-md encode decode
      tag-value 2 reverse-stream-fp-md encode decode
      tag-value 76 subscriber-profile encode
      tag-value 3 secondary-srv-path-hdr encode
      tag-value 5 rat-type encode
      tag-value 51 mcc-mnc encode
      tag-value 255 apn encode
      tag-value 25 sgsn-address encode
    #exit
  #exit
  traffic-steering
    up-service-chain sc_L3
      sfp-id 9 direction uplink up-appliance-group L2 instance 1 up-appliance-group
 L3 instance 1
     sfp-id 10 direction downlink up-appliance-group L3 instance 1 up-appliance-group
 L2 instance 1
     sfp-id 11 direction uplink up-appliance-group L2 instance 2 up-appliance-group
 L3 instance 1
     sfp-id 12 direction downlink up-appliance-group L3 instance 1 up-appliance-group
 L2 instance 2
     sfp-id 13 direction uplink up-appliance-group L2 instance 1 up-appliance-group
 L3 instance 2
     sfp-id 14 direction downlink up-appliance-group L3 instance 2 up-appliance-group
 L2 instance 1
     sfp-id 15 direction uplink up-appliance-group L2 instance 2 up-appliance-group
 L3 instance 2
     sfp-id 16 direction downlink up-appliance-group L3 instance 2 up-appliance-group
 L2 instance 2
     sfp-id 17 direction uplink up-appliance-group L2 instance 3 up-appliance-group
 L3 instance 1
     sfp-id 18 direction downlink up-appliance-group L3 instance 1 up-appliance-group
 L2 instance 3
     sfp-id 19 direction uplink up-appliance-group L2 instance 4 up-appliance-group
 L3 instance 1
     sfp-id 20 direction downlink up-appliance-group L3 instance 1 up-appliance-group
 L2 instance 4
     sfp-id 21 direction uplink up-appliance-group L2 instance 3 up-appliance-group
 L3 instance 2
     sfp-id 22 direction downlink up-appliance-group L3 instance 2 up-appliance-group
 L2 instance 3
     sfp-id 23 direction uplink up-appliance-group L2 instance 4 up-appliance-group
 L3 instance 2
     sfp-id 24 direction downlink up-appliance-group L3 instance 2 up-appliance-group
 L2 instance 4
    #exit
    up-service-chain L3
      sfp-id 1 direction uplink up-appliance-group L3 instance 1
      sfp-id 2 direction downlink up-appliance-group L3 instance 1
      sfp-id 3 direction uplink up-appliance-group L3 instance 2
      sfp-id 4 direction downlink up-appliance-group L3 instance 2
    #exit
    up-appliance-group L3
      steering-type nsh-aware
      up-nsh-format format4
      min-active-instance 1
      instance 1 ip address 40.40.40.3
      instance 2 ip address 40.40.40.4
```

```
    #exit
    up-appliance-group L2
      steering-type l2-mpls-aware
      min-active-instance 1
      instance 1 ingress slot/port 1/13 vlan-id 2136 egress slot/port 1/12 vlan-id
2136  ingress-context ingress ip address 4101::1 egress-context egress ip address
4101::2
      instance 2 ingress slot/port 1/13 vlan-id 2137 egress slot/port 1/12 vlan-id
2137  ingress-context ingress ip address 4201::1 egress-context egress ip address
4201::2
      instance 3 ingress slot/port 1/13 vlan-id 2138 egress slot/port 1/12 vlan-id
2138  ingress-context ingress ip address 4301::1 egress-context egress ip address
4301::2
      instance 4 ingress slot/port 1/13 vlan-id 2139 egress slot/port 1/12 vlan-id
2139  ingress-context ingress ip address 4401::1 egress-context egress ip address
4401::2
    #exit
```

4. **show configuration** CLI コマンドを使用して前述の設定を確認します。次に、**commit** CLI コマンドを実行して設定を有効にします。

```
configure
  traffic-steering
    commit
end
```

設定時の注意事項

ここでは、この機能を適切に設定するために必要な次のガイドラインについて説明します。

- 前項で説明したのと同じ順序で、UPのTS関連の設定を行います。この方法により、トラフィックをL2に誘導するために使用されるインターフェイスが設定で適切に適用されます。
- [up-appliance-group] のインスタンスを変更または削除する必要がある場合は、まず [up-service-chain] の関連するすべての sfp-id を削除する必要があります。
- コールの開始後に関連するインスタンスと sfp-id に対して前述の変更を行う必要がある場合は、問題を回避するため、sfp-id を削除して再設定します。
- up-appliance-groupインスタンスを設定する前に、インターフェイスに変更を適用します。インターフェイスへの変更が後になってから適用される場合は、まずup-service-chain設定を削除してから、up-appliance-group設定を削除します。インターフェイスの変更が完了したら、サービスチェーンとアプライアンスグループを再設定します。
- インターフェイスまたはsfpidを削除するために、UPサービスチェーンとアプライアンスグループ全体を削除することはできません。

N:M トラフィックステアリング

N:M トラフィックステアリングの設定手順は次のとおりです。

1. すべてのアクティブ UP の RCM ホスト固有の設定で TS-bind IP を設定します。

2. RCM の共通設定で必要なアクティブな課金 ruledef、ルールベース設定、およびトラフィックステアリング設定（up-nsh 形式、up-appliance-group および up-service-chain、commit CLI）を設定し、コミットします。
3. 必要な ts-mon、RCM 設定、L3 サーバーモニタリング用のノードモニター CLI、L2 の BFD 関連インターフェイス設定、およびトラフィックステアリング用のサービススキーマ設定（トリガー条件、トリガーアクションなど）が設定されている Day-0 設定を使用して、アクティブおよびスタンバイ UP をリロードします。
4. RCM がすべての UP に設定をプッシュすることを確認します。すべてのサービスがすべての UP で稼働していることを確認します。
5. VPP fastpath テーブルに SST、SSMT、および SST テーブルが作成されていること、また、グローバルテーブルが正しく作成されていることを確認します。
6. up-service-chain の SFP ステータスを確認し、SFP が使用可能な状態であることを確認します。

設定

以下に設定例を示します。

- **Day-0 設定**：次の設定は Day-0 設定の一部です。
  - 前述の「設定」の項で説明したように、L3 アプライアンスをモニターするには ts-mon および Node-monitor CLI が必要です。各 UP には、L3 アプライアンスをモニターする独自の物理 IP があります。
  - L2 の BFD 関連のインターフェイス設定。VLAN 設定および IP インターフェイス関連の設定。
  - サービススキーマ設定（トリガー条件、サービススキームなど）。

（注） 最適化により、サービススキーマ設定を共通設定に移動する予定です。現在、サービススキームの設定を変更する必要がある場合は、すべての UP で手動で変更する必要があります。

UP の設定例

L3 モニタリング

```
config
require ts-mon
nsh
 node-monitor ipv4-address 209.165.200.227 poll-interval 5 retry-count 5
load-report-threshold 20
exit

    interface ISP1_TO_PDN
      ip address 209.165.200.227 255.255.255.224
```

```
    ipv6 address 4001::254/64 secondary
  #exit
```

（注） UP2 では、IP は 40.40.40.454 にできます。これはその UP に固有の物理 IP アドレスです。

L2 モニタリング：

```
config
  context ingress
    bfd-protocol
      bfd multihop-peer 209.165.200.228 interval 50 min_rx 50 multiplier 20
      bfd multihop-peer 209.165.200.229 interval 50 min_rx 50 multiplier 20
      bfd multihop-peer 209.165.200.230 interval 50 min_rx 50 multiplier 20
    #exit
    interface TS_SecNet_v4 loopback
      ip address 209.165.200.231 255.255.255.224

    #exit
    interface TS_SecNet_v4_1 loopback
      ip address 209.165.200.232 255.255.255.224

    #exit
    interface TS_SecNet_v4_2 loopback
      ip address 209.165.200.233 255.255.255.224

    #exit
    interface TS_Secnet_ingress
      ip address 209.165.200.234 255.255.255.224

    #exit
    interface TS_Secnet_ingress1
      ip address 209.165.200.235 255.255.255.224

    #exit
    interface TS_Secnet_ingress2
      ip address 209.165.200.236 255.255.255.224

    #exit

    ip route static multihop bfd bfd1 209.165.200.231 209.165.200.228

    ip route static multihop bfd bfd2 209.165.200.232 209.165.200.229

    ip route static multihop bfd bfd3 209.165.200.233 209.165.200.230

    ip route 209.165.200.228 255.255.255.224 209.165.200.237 TS_Secnet_ingress

    ip route 209.165.200.229 255.255.255.224 209.165.200.238 TS_Secnet_ingress1

    ip route 209.165.200.230 255.255.255.224 209.165.200.239 TS_Secnet_ingress2

  #exit
end
```

```
config
  context egress
    bfd-protocol
    bfd multihop-peer 209.165.200.231 interval 50 min_rx 50 multiplier 20
      bfd multihop-peer 209.165.200.232 interval 50 min_rx 50 multiplier 20
      bfd multihop-peer 209.165.200.233 interval 50 min_rx 50 multiplier 20
```

```
    #exit
    interface TS_SecNet_v4 loopback
      ip address 209.165.200.228 255.255.255.224
    #exit
    interface TS_SecNet_v4_1 loopback
      ip address 209.165.200.229 255.255.255.224
    #exit
    interface TS_SecNet_v4_2 loopback
      ip address 209.165.200.230 255.255.255.224
    #exit
    interface TS_Secnet_egress
      ip address 209.165.200.237 255.255.255.224
    #exit
    interface TS_Secnet_egress1
      ip address 209.165.200.238 255.255.255.224
    #exit
    interface TS_Secnet_egress2
      ip address 209.165.200.239 255.255.255.224
    #exit
    subscriber default
    exit
    aaa group default
    #exit
    ip route static multihop bfd bfd4 209.165.200.228 209.165.200.231
    ip route static multihop bfd bfd5 209.165.200.229 209.165.200.232
    ip route static multihop bfd bfd6 209.165.200.230 209.165.200.233
    ip route 209.165.200.231 255.255.255.224 209.165.200.234 TS_Secnet_egress
    ip route 209.165.200.232 255.255.255.224 209.165.200.235 TS_Secnet_egress1
    ip route 209.165.200.233 255.255.255.224 209.165.200.236 TS_Secnet_egress2
  #exit
end
```

すべてのインターフェイスをポートと VLAN にバインドするための 1 つのインターフェイス設定例。

```
port ethernet 1/11
    vlan 1608
      no shutdown
      bind interface TS_Secnet_ingress ingress
    #exit
    vlan 1609
      no shutdown
      bind interface TS_Secnet_ingress1 ingress
    #exit
    vlan 1610
      no shutdown
      bind interface TS_Secnet_ingress2 ingress
    #exit
  #exit
  port ethernet 1/13
    no shutdown
    vlan 1608
      no shutdown
      bind interface TS_Secnet_egress egress
    #exit
    vlan 1609
      no shutdown
      bind interface TS_Secnet_egress1 egress
    #exit
    vlan 1610
      no shutdown
      bind interface TS_Secnet_egress2 egress
    #exit
```

サービススキーマ設定：

```
trigger-action ta1
      up-service-chain sc_L3
    #exit
    trigger-action default
      up-service-chain default
    #exit
    trigger-condition tc1
      rule-name = udp
      rule-name = http-pkts
      rule-name = tcp
      rule-name = dynamic2
      multi-line-or all-lines
    #exit
    trigger-condition tc2
      rule-name = qci8
      rule-name = qci1
      multi-line-or all-lines
    #exit
   trigger-condition defualt
     any-match = TRUE
   #exit
    service-scheme scheme1
      trigger rule-match-change
        priority 1 trigger-condition tc1 trigger-action ta1
        priority 2 trigger-condition tc2 trigger-action ta1
      #exit
      trigger subs-scheme-received
        priority 1 trigger-condition default trigger-action default
      #exit
     #exit
    subs-class class1
      subs-scheme = gold
    #exit
    subscriber-base base1
      priority 1 subs-class class1 bind service-scheme scheme1
    #exit
```

- **ホスト固有の設定**：次の設定は、ホスト固有の設定の一部です。
  - 各アクティブ UP の TS-bind IP 設定は、RCM におけるホスト固有の設定の一部です。

```
svc-type upinterface
redundancy-group 1
host Active1
host 391 " context ISP1-UP"
host 436 " interface ISP1_TO_PDN_v6 loopback"
host 437 " ipv6 address 4000::106/128"
host 438 " #exit"
host 439 " interface ISP1_TO_PDN_v4 loopback"
host 440 " ip address 209.165.200.240 255.255.255.224"
host 441 " #exit"
host 471 "ts-bind-ip up1 ipv4-address 209.165.200.240 ipv6-address 4000::106"
host 472 " exit"
host Active2
host 600 " context ISP1-UP"
host 601 " interface ISP1_TO_PDN_v6 loopback"
host 602 " ipv6 address 4000::107/128"
host 603 " #exit"
host 604 " interface ISP1_TO_PDN_v4 loopback"
host 605 " ip address 209.165.200.241 255.255.255.224"
host 606 " #exit"
```

```
host 607 "ts-bind-ip up2 ipv4-address 209.165.200.241 ipv6-address 4000::107"
host 608 " exit"
```

（注） TS-bind IP はループバック IP アドレスで、その物理 IP アドレスは、Day-0 設定の一部です。

- **共通設定**：次の設定は、共通設定の一部です。
  - トラフィックステアリング設定（up-nsh format、up-appliance-group、および up-service-chain config）。

（注） 低いVLANで入力が設定されていると仮定すると、アップリンクデータフローの場合、パケットは入力 VLAN ID で SN に送信され、出力 VLAN ID で SN から受信されます。同様に、ダウンリンクデータフローの場合、パケットは出力 VLAN ID で SN に送信され、入力 VLAN ID で SN から受信されます。

```
nsh
    up-nsh-format L3-format
      tag-value 7 imsi encode
      tag-value 4 rating-group encode
      tag-value 1 stream-fp-md encode decode
      tag-value 2 reverse-stream-fp-md encode decode
      tag-value 76 subscriber-profile encode
      tag-value 3 secondary-srv-path-hdr encode
      tag-value 5 rat-type encode
      tag-value 51 mcc-mnc encode
      tag-value 255 apn encode
      tag-value 25 sgsn-address encode
    #exit

  #exit
  traffic-steering
  up-appliance-group L2
steering-type l2-mpls-aware
min-active-instance 1
instance 1 ingress slot/port 1/12 vlan-id 1608 egress slot/port 1/13 vlan-id 1608
ingress-context ingress ip address 209.165.200.231egress-context egress ip address
209.165.200.228 load-capacity 100
instance 2 ingress slot/port 1/12 vlan-id 1609 egress slot/port 1/13 vlan-id 1609
ingress-context ingress ip address 209.165.200.232egress-context egress ip address
209.165.200.229 load-capacity 80
instance 3 ingress slot/port 1/12 vlan-id 1610 egress slot/port 1/13 vlan-id 1610
ingress-context ingress ip address 209.165.200.233egress-context egress ip address
209.165.200.230 load-capacity 90
exit
    up-appliance-group L3_only
      steering-type nsh-aware
      up-nsh-format new
      min-active-instance 1
      instance 1 ip address 209.165.200.242 load-capacity 80
      instance 2 ip address 209.165.200.243 load-capacity 90
    #exit
```

```
    up-service-chain sc_L3
      sfp-id 1 direction uplink up-appliance-group L2 instance 1 up-appliance-group
 L3_only instance 2
      sfp-id 2 direction downlink up-appliance-group L3_only instance 2
up-appliance-group L2 instance 1
     sfp-id 10 direction uplink up-appliance-group L2 instance 2 up-appliance-group
 L3_only instance 2
      sfp-id 11 direction downlink up-appliance-group L3_only instance 2
up-appliance-group L2 instance 2
     sfp-id 12 direction uplink up-appliance-group L2 instance 3 up-appliance-group
 L3_only instance 2
      sfp-id 13 direction downlink up-appliance-group L3_only instance 2
up-appliance-group L2 instance 3
     sfp-id 14 direction uplink up-appliance-group L2 instance 1 up-appliance-group
 L3_only instance 1
      sfp-id 15 direction downlink up-appliance-group L3_only instance 1
up-appliance-group L2 instance 1
     sfp-id 16 direction uplink up-appliance-group L2 instance 2 up-appliance-group
 L3_only instance 1
      sfp-id 17 direction downlink up-appliance-group L3_only instance 1
up-appliance-group L2 instance 2
     sfp-id 18 direction uplink up-appliance-group L2 instance 3 up-appliance-group
 L3_only instance 1
      sfp-id 19 direction downlink up-appliance-group L3_only instance 1
up-appliance-group L2 instance 3
    #exit
 up-service-chain default
sfp-id 200 direction uplink up-appliance-group L3_only instance 1
sfp-id 201 direction downlink up-appliance-group L3_only instance 1
sfp-id 202 direction uplink up-appliance-group L3_only instance 2
sfp-id 203 direction downlink up-appliance-group L3_only instance 2
#exit
commit
exit
```

検証用の show CLI

ユーザープレーンと RCM の show CLI を次に示します。

- ユーザープレーン：**Show srp checkpoints stats/ Show srp checkpoints stats debug-info**

  ```
  laas-setup# show srp checkpoint statistics | grep UPLANE_TRAFFIC_STEERING_INFO
  ```

- RCM：**under rcm checkpoint manager**

  ```
  "numTSInfo": 0
  ```

モニタリングと障害対応：スタンドアロンモード

ここでは、この機能のモニタリングおよび障害対応の方法を説明します。

コントロールプレーンの show コマンド

ここでは、CP でこの機能をモニターするための show コマンドについて説明します。

show active-charging sessions full all

（注） *TS Subscription Scheme Name*：active-charging-service で設定されたサービススキームから適用する必要があるサブスクリプションスキームが表示されます。この active-charging-service は、Gx インターフェイスを介して PCRF から受信されます。

ユーザープレーンの show コマンド

ここでは、UP でこの機能をモニターするための show コマンドについて説明します。

Show Commands for Configuration

ここでは、この機能の設定の確認に使用できる show コマンドについて説明します。

- **show user-plane-service traffic-steering up-service-chain all**
- **show user-plane-service traffic-steering up-service-chain name** *up-service-chain name*
- **show user-plane-service traffic-steering up-service-chain sfp-id** *sfp-id*

データ統計の show コマンド

ここでは、この機能に関連するデータ統計の確認に使用できる show コマンドについて説明します。

- **show user-plane-service inline-services traffic-steering statistics up-service-chain all v**
- **show user-plane-service inline-services traffic-steering statistics up-service-chain all**
- **show user-plane-service inline-services traffic-steering statistics up-service-chain sfp-id** *sfp-id*
- **show user-plane-service inline-services traffic-steering statistics up-appliance-group all verbose**
- **show user-plane-service inline-services traffic-steering statistics up-appliance-group name** *appliance group name*
- **show user-plane-service inline-services traffic-steering statistics up-appliance-group name** *appliance group name* **instance** *appliance instance*

TS のサービスチェーンと SFP 関連付けを確認する show コマンド：

ここでは、サービスチェーンと SFP 関連付けの確認に使用できる show コマンドについて説明します。

- **show subscriber user-plane-only flows**
- **show subscribers user-plane-only callid** <*call-id*> **flows**

OAM 統計の show コマンド

ここでは、この機能に関連する OAM 統計の確認に使用できる show コマンドについて説明します。

- **show user-plane-service inline-services traffic-steering oam all**
- **show user-plane-service inline-services traffic-steering oam summary**

- **show user-plane-service inline-services traffic-steering oam l3-steering summary**
- **show user-plane-service inline-services traffic-steering oam l3-steering monitors** *<ip address>*
- **show user-plane-service inline-services traffic-steering oam l3-steering monitors all**
- **show user-plane-service inline-services traffic-steering oam l3-steering monitors up-appliance-group***<name>*
- **show user-plane-service inline-services traffic-steering oam l2-steering monitors all**
- **show user-plane-service inline-services traffic-steering oam l2-steering monitors up-appliance-group** *<name>*
- **show user-plane-service inline-services traffic-steering oam l2-steering summary**
- **clear user-plane-service traffic-steering oam statistics**
- **clear user-plane-service traffic-steering oam l3-steering statistics**

現在、BFD はセッション統計をクリアする API を提供していないため、次の traffic-steering OAM clear コマンドが拡張され、l2-steering 統計が追加されました。

- clear user-plane-service traffic-steering
  - OAM：OAM をクリアします。
  - statistics：ユーザー プレーン トラフィック ステアリング統計をクリアします。
- clear user-plane-service traffic-steering OAM
  - L3-steering：L3-steering OAM をクリアします。
  - statistics：OAM 統計をクリアします。

show configuration コマンド

次の設定は、この機能の **show configuration** コマンドのサンプルスニペットです。

```
nsh
  up-nsh-format format4
    tag-value 250 imsi encode
    tag-value 66 msisdn encode
    tag-value 4 rating-group encode
    tag-value 1 stream-fp-md encode decode
    tag-value 2 reverse-stream-fp-md encode decode
    tag-value 76 subscriber-profile encode
    tag-value 3 secondary-srv-path-hdr encode
    tag-value 5 rat-type encode
    tag-value 51 mcc-mnc encode
    tag-value 255 apn encode
    tag-value 25 sgsn-address encode
  #exit
traffic-steering
  up-service-chain L3
    sfp-id 65535 direction uplink up-appliance-group L3 instance 1
    sfp-id 65536 direction downlink up-appliance-group L3 instance 2
    sfp-id 65537 direction downlink up-appliance-group L3 instance 1
```

```
      sfp-id 65538 direction uplink up-appliance-group L3 instance 2
    #exit
    up-service-chain sc_L3
      sfp-id 9 direction uplink up-appliance-group L2 instance 1 up-appliance-group L3
instance 1
      sfp-id 10 direction downlink up-appliance-group L3 instance 1 up-appliance-group
L2 instance 1
      sfp-id 11 direction uplink up-appliance-group L2 instance 2 up-appliance-group L3
 instance 1
      sfp-id 12 direction downlink up-appliance-group L3 instance 1 up-appliance-group
L2 instance 2
      sfp-id 13 direction uplink up-appliance-group L2 instance 1 up-appliance-group L3
 instance 2
      sfp-id 14 direction downlink up-appliance-group L3 instance 2 up-appliance-group
L2 instance 1
      sfp-id 15 direction uplink up-appliance-group L2 instance 2 up-appliance-group L3
 instance 2
      sfp-id 16 direction downlink up-appliance-group L3 instance 2 up-appliance-group
L2 instance 2
      sfp-id 17 direction uplink up-appliance-group L2 instance 3 up-appliance-group L3
 instance 1
      sfp-id 18 direction downlink up-appliance-group L3 instance 1 up-appliance-group
L2 instance 3
      sfp-id 19 direction uplink up-appliance-group L2 instance 4 up-appliance-group L3
 instance 1
      sfp-id 20 direction downlink up-appliance-group L3 instance 1 up-appliance-group
L2 instance 4
      sfp-id 21 direction uplink up-appliance-group L2 instance 3 up-appliance-group L3
 instance 2
      sfp-id 22 direction downlink up-appliance-group L3 instance 2 up-appliance-group
L2 instance 3
      sfp-id 23 direction uplink up-appliance-group L2 instance 4 up-appliance-group L3
 instance 2
      sfp-id 24 direction downlink up-appliance-group L3 instance 2 up-appliance-group
L2 instance 4
    #exit
    up-appliance-group L3
      steering-type nsh-aware
      up-nsh-format format4
      min-active-instance 1
      instance 1 ip address 209.165.200.225
      instance 2 ip address 4001::3
    #exit
    up-appliance-group L2
      steering-type l2-mpls-aware
      min-active-instance 1
      instance 1 ingress slot/port 1/13 vlan-id 2136 egress slot/port 1/12 vlan-id 2136
  ingress-context ingress ip address 4101::1 egress-context egress ip address 4101::2
load-capacity 100
      instance 2 ingress slot/port 1/13 vlan-id 2137 egress slot/port 1/12 vlan-id 2137
  ingress-context ingress ip address 4201::1 egress-context egress ip address 4201::2
load-capacity 60
      instance 3 ingress slot/port 1/13 vlan-id 2138 egress slot/port 1/12 vlan-id 2138
  ingress-context ingress ip address 4301::1 egress-context egress ip address 4301::2
load-capacity 20
      instance 4 ingress slot/port 1/13 vlan-id 2139 egress slot/port 1/12 vlan-id 2139
  ingress-context ingress ip address 4401::1 egress-context egress ip address 4401::2
load-capacity 100
    #exit
  #exit
  ts-bind-ip nshsrcip ipv4-address 209.165.200.226 ipv6-address 4001::106
  #exit
    context egress
    bfd-protocol
```

```
    bfd multihop-peer 4101::1 interval 50 min_rx 50 multiplier 20
    bfd multihop-peer 4201::1 interval 50 min_rx 50 multiplier 20
    bfd multihop-peer 4301::1 interval 50 min_rx 50 multiplier 20
    bfd multihop-peer 4401::1 interval 50 min_rx 50 multiplier 20
  #exit
  interface ts_egress1
    ipv6 address 4101::2/64
    ip mtu 1600
  #exit
  interface ts_egress2
    ipv6 address 4201::2/64
    ip mtu 1600
  #exit
  interface ts_egress3
    ipv6 address 4301::2/64
    ip mtu 1600
  #exit
  interface ts_egress4
    ipv6 address 4401::2/64
    ip mtu 1600
  #exit
  subscriber default
  exit
  aaa group default
  #exit
  gtpp group default
  #exit
  ipv6 route static multihop bfd bfd1 4101::2 4101::1
  ipv6 route static multihop bfd bfd2 4201::2 4201::1
  ipv6 route static multihop bfd bfd3 4301::2 4301::1
  ipv6 route static multihop bfd bfd4 4401::2 4401::1
  ip igmp profile default
  #exit
#exit
context ingress
  bfd-protocol
    bfd multihop-peer 4101::2 interval 50 min_rx 50 multiplier 20
    bfd multihop-peer 4201::2 interval 50 min_rx 50 multiplier 20
    bfd multihop-peer 4301::2 interval 50 min_rx 50 multiplier 20
    bfd multihop-peer 4401::2 interval 50 min_rx 50 multiplier 20
  #exit
  interface ts_ingress1
    ipv6 address 4101::1/64
    ip mtu 1600
  #exit
  interface ts_ingress2
    ipv6 address 4201::1/64
    ip mtu 1600
  #exit
  interface ts_ingress3
    ipv6 address 4301::1/64
    ip mtu 1600
  #exit
  interface ts_ingress4
    ipv6 address 4401::1/64
    ip mtu 1600
  #exit
  subscriber default
  exit
  aaa group default
  #exit
  gtpp group default
  #exit
  ipv6 route static multihop bfd bfd1 4101::1 4101::2
```

```
  ipv6 route static multihop bfd bfd2 4201::1 4201::2
  ipv6 route static multihop bfd bfd3 4301::1 4301::2
  ipv6 route static multihop bfd bfd4 4401::1 4401::2
  ip igmp profile default
  #exit
#exit
  context ISP1-UP
  ip access-list IPV4ACL
    redirect css service ACS any
    permit any
  #exit
  ipv6 access-list IPV6ACL
    redirect css service ACS any
    permit any
  interface TO-ISP12
    ipv6 address 4001::106/64
    ip address 209.165.200.226 255.255.255.224 secondary
    ip mtu 2000
  #exit
    port ethernet 1/12
  no shutdown
  vlan 2135
    no shutdown
    bind interface TO-ISP12 ISP1-UP
  #exit
  vlan 2136
    bind interface ts_egress1 egress
  #exit
  vlan 2137
    no shutdown
    bind interface ts_egress2 egress
  #exit
  vlan 2138
    no shutdown
    bind interface ts_egress3 egress
  #exit
  vlan 2139
    no shutdown
    bind interface ts_egress4 egress
  #exit
#exit
port ethernet 1/13
  no shutdown
  vlan 2137
    no shutdown
    bind interface ts_ingress2 ingress
  #exit
  vlan 2138
    no shutdown
    bind interface ts_ingress3 ingress
  #exit
  vlan 2139
    no shutdown
    bind interface ts_ingress4 ingress
  #exit
  vlan 2136
    no shutdown
    bind interface ts_ingress1 ingress
  #exit
#exit
```

ユーザープレーンの 1:1 冗長性に関する show コマンド

show srp checkpoint statistics | grep ts-sfp

```
call-recovery-uplane-internal-audit-ts-sfp-failure: 0
```

SFP の可用性に関する show コマンド

show user-plane traffic-steering up-service-chain <all> <name> <sfp-id>

SNMP トラップ

この機能をサポートするために、次の SNMP トラップが追加されました。

- UPlaneTsMisConfig：アプライアンスグループに関連付けられている SFP がない場合。
- UPlaneTsNoSelectedSfp：SFP を選択できない場合。
- UPlaneTsServiceChainOrApplianceDown：サービスチェーンまたはアプリケーションノードが使用できなくなった場合。アプリケーショングループの最小インスタンスが使用できなくなると、サービスチェーンは使用できなくなります。
- UPlaneTsServiceChainOrApplianceUp：サービスチェーンまたはアプリケーションノードインスタンスが使用可能になったため、アプライアンスのノードステータスが更新されたとき。

バルク統計情報

UP サービスチェーンスキーマ

変数名	データ タイプ	カウンタタイプ	説明
up-svc-chain-name	文字列	情報（Info）	UP サービスチェーンの名前
up-svc-chain-status	Int32	情報（Info）	UP サービスチェーンのステータス
up-svc-chain-load-status	Int32	ゲージ	UP サービスチェーンの負荷ステータス
up-svc-chain-sfp-stickiness-miss-count	Int32	Counter	UP サービスチェーンの SFP スティッキ性の欠落数
up-svc-chain-sfp-not-selected-count	Int32	Counter	SFP が選択されていない UP サービスチェーンの数
up-svc-chain-associated-calls	Int32	ゲージ	UP サービスチェーンの関連コール

変数名	データ タイプ	カウンタタイプ	説明
up-svc-chain-associated-flows	Int32	ゲージ	UPサービスチェーンの関連フロー
up-svc-chain-total-uplink-pkts	Int64	Counter	UP サービスチェーンの合計アップリンクパケット数
up-svc-chain-total-uplink-bytes	Int64	Counter	UP サービスチェーンの合計アップリンクバイト数
up-svc-chain-total-downlink-pkts	Int64	Counter	UPサービスチェーンの合計ダウンリンクパケット数
up-svc-chain-total-downlink-bytes	Int64	Counter	UPサービスチェーンの合計ダウンリンクバイト数

Up-appliance-group Schema

変数名	データ タイプ	カウンタタイプ	説明
up-appl-group-name	文字列	情報（Info）	UP アプライアンスのグループ名
up-appl-group-status	Int32	情報（Info）	UP アプライアンスグループのステータス
up-appl-group-load-status	Int32	ゲージ	UP アプライアンスグループの負荷ステータス
up-appl-group-node-down-count	Int32	Counter	UP アプライアンスグループのノードダウン数
up-appl-group-associated-sfps	Int32	ゲージ	UP アプライアンスグループに関連付けられた SFP
up-appl-group-num-times-loaded-state	Int32	Counter	UP アプライアンスグループのノードダウン状態の回数
up-appl-group-total-uplink-pkts	Int64	Counter	UP アプライアンスグループの合計アップリンクパケット数
up-appl-group-total-uplink-bytes	Int64	Counter	UP アプライアンスグループの合計アップリンクバイト数
up-appl-group-total-downlink-pkts	Int64	Counter	UP アプライアンスグループの合計ダウンリンクパケット数
up-appl-group-total-downlink-bytes	Int64	Counter	UP アプライアンスグループの合計ダウンリンクバイト数

次の CLI コマンドは、この機能のバルク統計情報の設定例です。

```
config
   bulkstats collection
   bulkstats mode
   file 1
   up-service-chain schema TS format "\nup-service-chain-name = %up-svc-chain-name%
   \nup-service-chain-status=%up-svc-chain-status%\nup-service-chain-load-status =
   %up-svc-chain-load-status%\nup-service-chain-associated-calls =
   %up-svc-chain-associated-calls%\nup-service-chain-associated-flows =
   %up-svc-chain-associated-flows%\nup-service-chain-total-uplink-pkts =
   %up-svc-chain-total-uplink-pkts%\nup-service-chain-total-uplink-bytes =
   %up-svc-chain-total-uplink-bytes%\nup-service-chain-total-downlink-pkts =
   %up-svc-chain-total-downlink-pkts%\nup-service-chain-total-total-downlink-bytes
   = %up-svc-chain-total-downlink-bytes%\n\n"
```

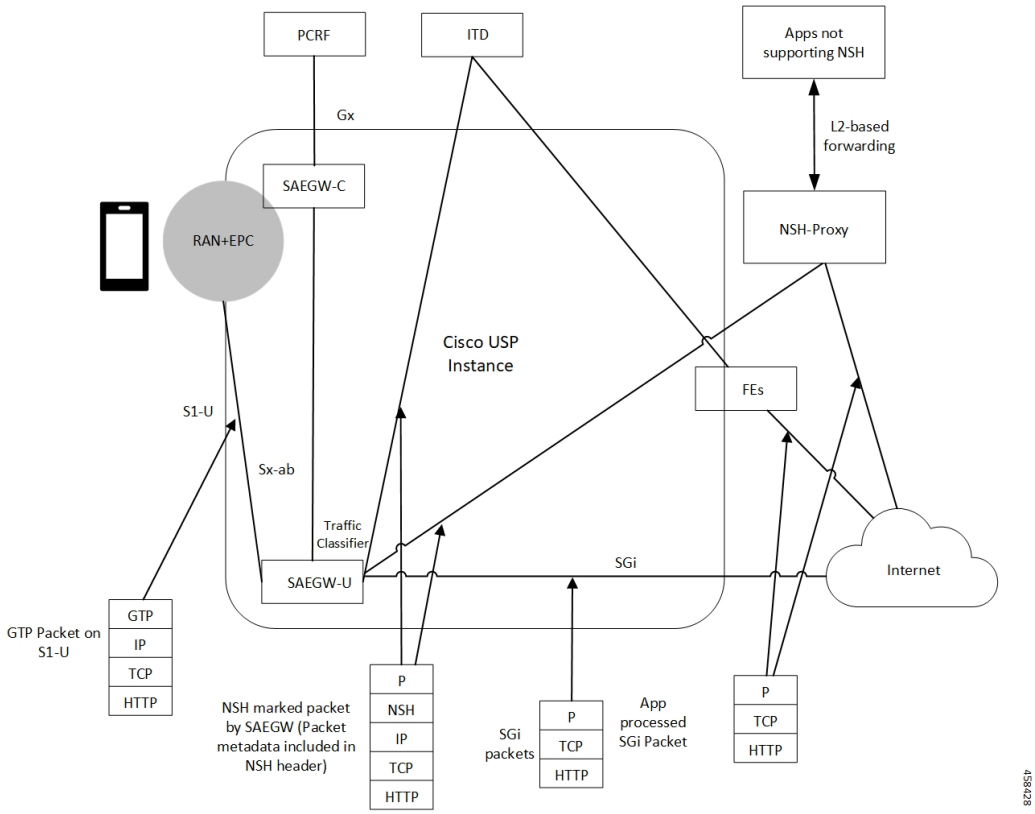
機能説明：サンドイッチモード

サンドイッチモードは、NSH ベースのトラフィックステアリング（TS）アプローチに対応して、サービス機能アプライアンスのフォワーディングエンジン（FE）ノードに必要なメタデータを提供します。

サンドイッチ モード ソリューションは、Cisco USP インスタンスで Cisco Nexus 9000 シリーズ NX-OS Intelligent Traffic Director（ITD）を活用します。ITD の詳細については、Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director コンフィギュレーション ガイド [英語] を参照してください。

アーキテクチャ：サンドイッチモード

次の図は、外部サービス機能アプライアンスとシスコの SAEGW-U（ユーザープレーン）の統合を示しています。



サンドイッチ モード ソリューションには、次の機能が含まれています。

- SAEGW-U は、アップリンク方向でのみ Gi パスを出る該当パケットに NSH ベースの該当メタデータを追加します。
- サンドイッチモードで実行中の ITD は、これらのパケットを（送信元 IP に基づいて）FE にロードバランシングできます。
- SAEGW-U は、FE に対して正常性チェックを実行せず、その存在を認識しません。
- ITD ノードは、セッションレベルで「スティック性」を維持できます。ITD は、NSH-Outer-IP-SRC-Header を調べてこれを行います。
- アップリンク方向では、送信元 IP は「UE-IP」（内部 IP ヘッダーのコピー）です。宛先 IP は「server-IP-internet」です。
- ダウンリンク方向では、NSH ヘッダーはなく、パケットはインターネットから FE に直接送信されます。SAEGW-U では、送信元 IP は「Server-IP」、宛先 IP は「UE-IP」です。
- SAEGW-U はトラフィック分類を実行し、特定のフローのサービスチェーンを選択します。
- SAEGW-U のサービスチェーンには複数のアプライアンスを含めることができ、ステアリング機能はこれらのアプライアンスを処理できます。
- SAEGW-U は、アップリンクパケットの NSH ヘッダーのみをエンコードします。

- SAEGW-U は、元の UE-IP ヘッダーから送信元 IP の詳細を直接コピーします。SAEGW-U は、外部ヘッダー SRC および DEST ポートに NSH ポート 6633 を使用します。宛先 IP（設定されている場合）はアプライアンス IP です。
- NSH ヘッダーを持つダウンリンク パケットを受信すると、SAEGW-U はそのようなパケットをドロップします。
- SAEGW-U は、FE や ITD の正常性チェックを実行しません。SAEGW-U は、ITD を常に使用可能として扱います。
- SAEGW-U は、NSH ベースヘッダー、サービスヘッダー、およびコンテキストヘッダー（メタデータを含む）を使用して、ITD に向かうすべてのアップリンクパケット（サービス機能アプライアンスによって認定）をエンコードします。
- TS アプリケーションは、一度に 1 つのモード（サンドイッチモードまたはスタンドアロンモード）でのみ動作します。

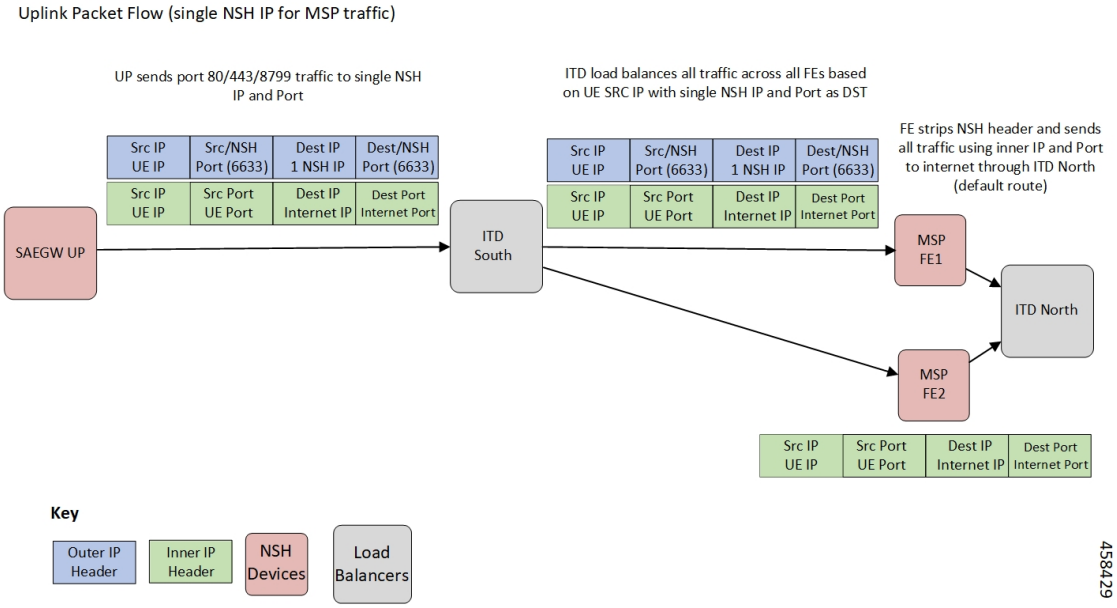
（注）
- サンドイッチモードの場合、**require tsmon** CLI コマンドを設定しないでください。
- サンドイッチモードからスタンドアロンモード、およびその逆に変更した場合は、再起動が必要です。

機能の仕組み：サンドイッチモード

サンドイッチモードのパケットフロー

アップリンクパケット数

次の図は、アップリンクパケットフローを示しています。



次に、パケットフローについて説明します。

1. GTP-U パケットが SAEGW-U に到着すると、SAEGW-U が GTP ヘッダーのカプセル化を解除し、フローのサブスクライバを特定します。
2. SAEGW-Uがトラフィック分類を実行し、フローのサービスチェーンを関連付けます。サービス機能アプライアンス（ITD）を含むサービスチェーンを、TCP/UDP/HTTP/HTTPS に応じて分類されるトラフィックに関連付けるように SAEGW-U が設定されます。
3. サービス機能アプライアンスに送信される NSH 変数ヘッダーのパラメータをエンコードするために、サービスチェーンに関連付けられた NSH 形式を SAEGW-U が検索します。

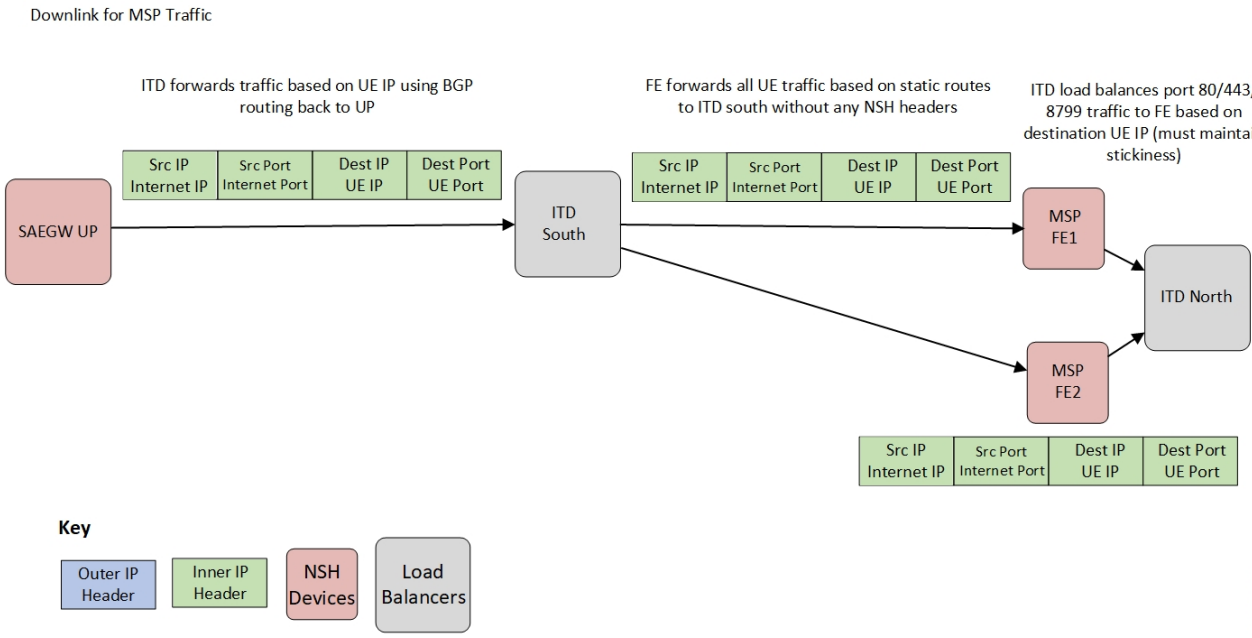
   次に、アップリンクパケット用に選択された SFP が 200 である NSH ヘッダーの例を示します。

```
**************NSH Base Header**************
                   Version: 0
                   OAM Bit: 0
                    Length: 4
                   MD Type: 2
               Next Protocol: 1

**************NSH Service Header**************
   Service Path Identifier: 200
             Service Index:   1

**************Start NSH Context Header**************
                  TLV Type: <MSISDN tag configured in UP>
                  TLV Len: 15
                  TLV Value: 123456789012340 (unencrypted msisdn)

                  TLV Type: <MCCMNC tag configured in UP>
                  TLV Len: 6
                  TLV Value: 404122 (mcc-mnc value)

                  TLV Type: <RAT TYPE tag configured in UP>
                  TLV Len: 1
```

```
                        TLV Value: 3 (rat type value)

                        TLV Type: <APN tag configured in UP>
                        TLV Len: 64
                        TLV Value: APN1 (apn value)

                        TLV Type: <Sub Profile tag configured in UP>
                        TLV Len: 32
                        TLV Value: Profile-1 (Sub Profile name)

                        TLV Type: <SGSN addr tag configured in UP>
                        TLV Len: 4
                        TLV Value: 169090600 (SGSN Addr(in network byte order))

**************End NSH Context Header**************
```

ダウンリンクパケット数

次の図は、ダウンリンクパケットフローを示しています。



次に、パケットフローについて説明します。

1. パケットはインターネットサーバーから FE に直接送信されます。FE がパケットを処理し、SAEGW-U にパケットを送信します。

   SRC IP/ポートはサーバー IP/ポートで、DEST IP/ポートは UE IP/ポートです。

2. SAEGW-U がパケットを処理し、サービスチェーン内に他のサービス機能アプライアンスがある場合は、追加処理のためにパケットを送信します。サービスチェーンが完了すると、パケットはルールの照合や分類と課金のために通常のダウンリンクパケット処理パスに送信されます。

3. SAEGW-U が、GTP-U ヘッダーがあるパケットをカプセル化し、UE に送信します。

（注） ダウンリンクパケットは NSH エンコードできません。SAEGW-U では同様のパケットはすべてドロップされます。

TCP および UDP トラフィック

アップリンクトラフィック

- アプライアンス向けのステアリングに適したすべての TCP トラフィックと UDP トラフィックは同様に扱われます。
- UL パケットは、設定された NSH コンテキストヘッダー要素を使用してアプライアンスにステアリングされます。NSH サービスヘッダーは SI=1 でエンコードされるため、SI 推論がさらに実行され、SI=0 の場合、パケットは Gi インターフェイスを介して送信されます。
- 外部ヘッダーの SRC IP は、内部ヘッダーの SRC IP（つまり、UE SRC IP）と同じです。
- 外部ヘッダーの SRC ポートは、NSH ポート 6633 です。
- 外部ヘッダーの DST IP は、設定されたアプライアンス IP です。
- 外部ヘッダーの DST ポートは、NSH ポート 6633 です。

ダウンリンクトラフィック

ダウンリンクパケットは ITD を介して FE から受信されるため、FE にステアリングされることなく、通常の IP パケットとして処理されます。

- SAEGW-U で受信した UL パケットは、適切な SFC に関連付けられた設定済みポリシーに基づいて分類されます。
- SAEGW-U は、アプライアンスインスタンスと選択されたステアリングのサービスと負荷の可用性に基づいて SFP の選択を実行します。アップリンクトラフィックは NSH（IP-UDP）でカプセル化され、必要に応じて、入力されたコンテキストヘッダーを使用して、選択した SFP でステアリングされます。
- NSH アプライアンスは、NSH パケットを受信すると、IP パケット（場合によってはコンテキストヘッダー）を処理し、Gi インターフェイスを介してパケットを送信します。
- ダウンリンクパケットは、Gi インターフェイスを介して接続先サーバーから SAEGW-U に送信されます。

トラフィックステアリングのサービススキームの選択

service-scheme は、次の 2 つの方法のいずれかで選択できます。

1. Gx/PCRF：

   PCRF は、次の AVP を介してトラフィックステアリングを有効にします。

```
        [V] Services:
          [V] Service-Feature:
            [V] Service-Feature-Type: TS (4)
            [V] Service-Feature-Status: ENABLE (1)
            [V] Service-Feature-Rule-Install:
              [V] Service-Feature-Rule-Definition:
                [V] Service-Feature-Rule-Status: ENABLE (1)
                [V] Subscription-Scheme: gold
                [V] Profile-Name: L3_profile
```

続いて、TSプロファイルとTSサブスクライバスキームがSxメッセージングを介してユーザープレーンに送信されます。

```
        SUBSCRIBER PARAMS:
...
...
...
            TS-Profile: L3_profile

            TS-Subscriber-Scheme: gold
```

Gx/PCRF ベースのトラフィックステアリングの場合、service-scheme 設定で **trigger subs-scheme-received** CLI コマンドが必要です。

2. Service-scheme フレームワーク（Gx/PCRF AVP なし）：

   トラフィックステアリングは、Subscription-scheme AVP がなくても PCRF から有効にできます。

   trigger sess-setup CLI コマンドは、**up-service-chain** を指定したトリガーアクションでは必須です。次に設定例を示します。

```
service-scheme scheme1
trigger sess-setup
  priority 1 trigger-condition subs-scheme-check trigger-action ta2
exit

trigger-condition subs-scheme-check
  any-match = TRUE
exit

trigger-action ta1
  up-service-chain SN-L3_profile

exit
```

デフォルトのサービスチェーン

TS 対応サブスクライバの場合、次の状況では、特定のトラフィックでサービスチェーン（APP1+APP2）が使用できなくなる可能性があります。

- APP1+APP2 サービスチェーンを選択しようとしている特定のフローに適切なポリシーが設定されていない。
- APP1+APP2 サービスチェーンが選択されたが、APP1 インスタンスが最小インスタンスしきい値を下回っている。このような場合、APP1+APP2 サービスチェーンは使用できません。

- APP1+APP2 サービスチェーンが選択されたが、SFP を選択できなかった。

このようにサービスチェーンが使用できない場合、フローは設定済みのデフォルトサービスチェーンにフォールバックし、フローに対する APP2 サービス処理が保証されます。

デフォルトのサービスチェーンが設定されていない場合、トラフィックはステアリングされずに送信されます。

Gx/PCRF を介した TS 対応の場合、デフォルトのサービスチェーンは **trigger subs-scheme-received** で定義されます。

Gx/PCRF AVP を使用しないサービス スキーム フレームワークを介した TS 対応の場合、デフォルトのサービスチェーンは **trigger sess-setup** で定義されます。

SFP の選択

NSH ベースのアプライアンスのみを使用するサービスチェーンの場合：

ダウンリンクパケットの場合、NSH アプライアンスがないため、SFP はありません。

L2 および NSH ベースのアプライアンスが混在するサービスチェーンの場合：

SFP は、L2 の「スティッキネス」に基づいて選択されます。同じ NSH ベースのアプライアンスが存在し、SFP の選択に常に使用できます。

ダウンリンクパケットの場合、SFP の選択は L2 アプライアンスのみに基づいています。

NSH ベースのアプライアンスの負荷の可用性に基づいた SFP の選択は実行されません。NSH とアプライアンスは常に使用可能と見なされます。

制限事項と制約事項

この機能には次の既知の制限事項があります。

- スタンドアロンモードからサンドイッチモードに、またはその逆に変更するには、リロードと設定変更が必要です。
- トラフィックステアリングが PCRF から、またはサービススキームフレームワークを使用してローカルで有効になっている場合、そのセッションでトラフィックステアリングを無効にすることはできません。
- マルチ アプライアンス サービス チェーン（L2 および L3 ステアリング）の場合、V4 および V6 トラフィックの SFP は異なります。ただし、両方の SFP は L2 アプライアンスの MSISDN ベースのスティッキ性を維持します。

NSH トラフィックステアリングの設定：サンドイッチモード

この項では、CP と UP の両方で NSH トラフィックステアリング：サンドイッチモードを設定するために使用できる CLI コマンドについて説明します。

CP の設定

CP を設定するには、次の手順を実行します。

1. アクティブ課金サービスを設定します。

   次に設定例を示します。

```
configure
  active-charging service ACS
  policy-control services-framework

  trigger-action ta1
   up-service-chain sn-L3-sc  <<<< (This should match the up-service-chain configured
 on UP)
  exit

  trigger-action ta2
   up-service-chain  L3-sc    <<<< (This should match the up-service-chain configured
 on UP)
  exit

  trigger-condition tc1
    rule-name = rule1           <<<<< (This can be static/predef/gor/dynamic rules)
    rule-name = rule2
    multi-line-or
  exit

  trigger-condition tc2
    any-match = TRUE
  exit

  service-scheme scheme1
    trigger rule-match-change
      priority 1 trigger-condition tc1 trigger-action ta1
    exit
    trigger subs-scheme-received      <<<<< (For default service chain selection)
      priority 1 trigger-condition tc2 trigger-action ta2
    exit

    subs-class class1
      subs-scheme = gold  <<<<<<< (This name should match the subscription-scheme
AVP value received from PCRF over Gx)
    exit

    subscriber-base base1
      priority 1 subs-class class1 bind service-scheme scheme1
    exit
end
```

2. トラフィックステアリング AVP は現在、Diameter ディクショナリ custom44 でサポートされています。Diameter ディクショナリにより、TS 関連の AVP が Gx インターフェイスを介して受信されるとき、および Sx メッセージで UP に送信されるときに、CP はこれらの AVP を適切に復号できます。

   CP でディクショナリを設定するための設定例を以下に示します。

```
configure
  context ISP1
    ims-auth-service IMSGx
    policy-control
    diameter dictionary dpca-custom44
  exit
end
```

CCA-I/CCA-U/RAR の Gx を介して受信する TS 関連 AVP の値の例を以下に示します。

```
    [V] Services:
      [V] Service-Feature:
        [V] Service-Feature-Type: TS (4)
        [V] Service-Feature-Status: ENABLE (1)
        [V] Service-Feature-Rule-Install:
          [V] Service-Feature-Rule-Definition:
            [V] Service-Feature-Rule-Status: ENABLE (1)
            [V] Subscription-Scheme: gold
            [V] Profile-Name: L3
```

UP の設定

UP を設定するには、次の手順を同じ順序で実行します。

1. サービス チェーン アプライアンスにデータを送信するために使用されるコンテキストにインターフェイスを追加します。

   次に設定例を示します。

```
configure
  context ISP1-UP
    interface ts_ingress
    ip address 209.165.200.225 255.255.255.224
    ipv6 address 4101::1/64 secondary
  exit
end

configure
  context ISP2-UP
    interface ts_egress
    ip address 209.165.200.225 255.255.255.224
    ipv6 address 4101::2/64 secondary
  exit
end
```

2. 新たに追加されたインターフェイスを UP の物理ポートにバインドします。

   次に設定例を示します。

```
configure
  port ethernet 1/11
    vlan 1240
      no shutdown
```

```
      bind interface ts_ingress ISP1-UP
    exit
  exit
  port ethernet 1/12
    vlan 1240
      no shutdown
      bind interface ts_egress ISP2-UP
    exit
  exit
end
```

3. TS 関連の設定を UP に追加します。

   次に設定例を示します。

```
configure
  ts-bind-ip IP_UP01 ue-src-ip ipv4-address 209.165.200.225     <<<< See Notes below


  nsh
    up-nsh-format nfo
      tag-value 1  apn encode
      tag-value 2  imsi encode
      tag-value 3  mcc-mnc encode
      tag-value 4  msisdn encode
      tag-value 5  rat-type encode
      tag-value 10 rating-group encode
      tag-value 11 sgsn-address encode
      tag-value 12 subscriber-profile encode
    exit
  exit

  traffic-steering
    up-service-chain L3
      sfp-id 1 direction uplink up-appliance-group L3 instance 1
    exit

    up-service-chain sn_L3
     sfp-id 3  direction uplink   up-appliance-group L2 instance 1 up-appliance-group
 L3 instance 1
      sfp-id 4  direction downlink up-appliance-group L2 instance 1
     sfp-id 5  direction uplink   up-appliance-group L2 instance 2 up-appliance-group
 L3 instance 1
      sfp-id 6  direction downlink up-appliance-group L2 instance 2
     sfp-id 7  direction uplink   up-appliance-group L2 instance 3 up-appliance-group
 L3 instance 3
      sfp-id 8  direction downlink up-appliance-group L2 instance 3
     sfp-id 9  direction uplink   up-appliance-group L2 instance 4 up-appliance-group
 L3 instance 3
      sfp-id 10 direction downlink up-appliance-group L2 instance 4

    exit
    up-appliance-group L3
      steering-type nsh-aware
      up-nsh-format nfo
      min-active-instance 1
      instance 1 ip address 40.40.40.3
    exit
    up-appliance-group L2
      steering-type l2-mpls-aware
      min-active-instance 1
      instance 1 ingress slot/port 1/13 vlan-id 2136 egress slot/port 1/12 vlan-id
2136  ingress-context ingress ip address 4101::1 egress-context egress ip address
4101::2
```

```
      instance 2 ingress slot/port 1/13 vlan-id 2137 egress slot/port 1/12 vlan-id
2137  ingress-context ingress ip address 4201::1 egress-context egress ip address
4201::2
      instance 3 ingress slot/port 1/13 vlan-id 2138 egress slot/port 1/12 vlan-id
2138  ingress-context ingress ip address 4301::1 egress-context egress ip address
4301::2
      instance 4 ingress slot/port 1/13 vlan-id 2139 egress slot/port 1/12 vlan-id
2139  ingress-context ingress ip address 4401::1 egress-context egress ip address
4401::2
    exit
```

注：

- **ts-bind-ip** *name* **ue-src-ip { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **}**：パケットが ITD に送信される UP インターフェイスの IP アドレスを指定します。

4. **show configuration** CLI コマンドを使用して前述の設定を確認します。次に、**commit** CLI コマンドを実行して設定を有効にします。

```
configure
  traffic-steering
    commit
end
```

スタンドアロンとサンドイッチの両モードでの後処理 Ruledef の設定

up-service-chain トリガーアクションは、トリガー条件を含めて、トラフィックをステアリングするために rulebase 内の ruledef の後処理設定で使用されます。複数の課金 ruledef がある場合でも、HTTP、HTTPS、およびその他のプロトコルのポート番号を使用して単一の後処理 ruledef が定義されます。この単一の後処理 ruledef 名は、トラフィックステアリングで使用されるトリガー条件で照合されます。

次の設定を使用して、トラフィックをステアリングするための ruledef の後処理を設定します。

```
configure
  active-charging service service_name
    rulebase rulebase_name
      post-processing priority priority_number ruledef ruledef_name
charging-action charging_action_name
      end
```

次の設定を使用して、後処理 ruledef のトリガー条件を設定します。

```
configure
  trigger-condition trigger_condition_name
    rule-name rule_name
    post-processing-rule-name post_processing_rule_name
    end
```

UPアプライアンスグループでのインターフェイス名を使用したBFDインスタンスIDの設定

トラフィックステアリング中に、**up-appliance-group** 内で、インターフェイス名と IP 設定を使用して BFD インスタンス ID が設定されます。

次の設定を使用して、トラフィックをステアリングするための BFD インスタンス ID を設定します。

```
configure
  traffic-steering
    up-appliance-group up_appliance_group_name
      steering-type steering_type
      instance instance_id ingress slot/port slot_or_port_number vlan-id
vlan_id egress slot/port slot_or_port_number vlan-id vlan_id ingress-context
ingress interface-name interface-name egress-context egress interface-name
 interface-name
      end
```

（注）

- 特定の L2 **up-appliance-group** では、BFD インスタンス ID は IP アドレスを使用して、または対応するインターフェイス名を使用し、特定の **ingress** または **egress** に関する **interface-name** を使用して設定されます。
- **interface-name** を使用した BFD モニタリングの **up-appliance-group** 設定が完了し、BFD の登録が完了するまで最大 5 分かかります。
- BFD の登録が成功すると、IP アドレスと **interface-name** が **show user-plane traffic-steering up-appliance-group all** の出力で使用可能になります。
- BFD モニタリングを使用して **up-appliance-group** で使用されている **interface-name** の IP アドレスが変更された場合は、**up-appliance-group** を再設定する必要があります。

NSHトラフィックステアリングのモニタリングとトラブルシューティング：サンドイッチモード

ここでは、この機能のモニタリングと障害対応で使用できる CLI コマンドについて説明します。

SNMP トラップの詳細については、この章の「SNMP トラップ （688 ページ）」の項を参照してください。

バルク統計情報の詳細については、この章の「バルク統計情報 （688 ページ）」の項を参照してください。

コマンドの表示

この項では、この機能をサポートするために使用可能な show CLI コマンドについて説明します。

CP コマンド

機能をモニターおよび障害対応するには、CP で次の show CLI コマンドを使用します。**show active-charging sessions full all**

TS Subscription Scheme Name：active-charging-service で設定されたサービススキームから適用する必要があるサブスクリプションスキームが表示されます。この active-charging-service は、Gx インターフェイスを介して PCRF から受信されます。

UP コマンド

機能をモニターおよび障害対応するには、UP で次の show CLI コマンドを使用します。

- トラフィックステアリングの設定チェック
  - **show user-plane-service traffic-steering up-service-chain all**
  - **show user-plane-service traffic-steering up-service-chain name** *up_service_chain_name*
  - **show user-plane-service traffic-steering up-service-chain sfp-id** *sfp_id*
  - **show user-plane traffic-steering up-appliance-group name** *name* **instance-id** *id*
  - **show user-plane traffic-steering up-appliance-group name** *name*
  - **show user-plane traffic-steering up-appliance-group all**
  - **show user-plane traffic-steering up-service-chain name** *name*
  - **show user-plane traffic-steering up-service-chain sfp-id** *id*
  - **show user-plane traffic-steering up-service-chain all**
- トラフィックステアリングの統計情報
  - **show user-plane-service inline-services traffic-steering statistics up-service-chain all verbose**
  - **show user-plane-service inline-services traffic-steering statistics up-service-chain all**
  - **show user-plane-service inline-services traffic-steering statistics up-service-chain sfp-id** *sfp_id*
  - **show user-plane-service inline-services traffic-steering statistics up-appliance-group name** *appliance_group_name*
  - **show user-plane-service inline-services traffic-steering statistics up-appliance-group name** *appliance_group_ name* **instance** *appliance instance*
  - **show user-plane-service statistics trigger-action all**
- サービスチェーンと SFP 関連付け

- **show subscriber user-plane-only flows**
- **show subscribers user-plane-only callid** *call_id* **flows**

show user-plane traffic-steering up-appliance-group all

機能のモニタリングや障害対応には、次の show CLI コマンドを使用します。

- **show in interface-name out interface-name**

第 66 章

静的ルールと事前定義ルールのパケットフロー説明管理手順

機能説明

パケットフロー記述管理手順の機能を使用することで、コントロールプレーンは、ユーザープレーンの静的ルールと事前定義ルール、およびその他の課金情報を設定できます。

機能の仕組み

CUPS より前は、静的および事前定義されたルールの処理は、ルール定義、ルールベース、および課金アクションに応じて実行されました。ルールベースは静的ルールの照合順序の優先順位を示し、関連する課金アクションも提供します。

CUPS アーキテクチャでは、L3/L4 の静的ルールと事前定義されたルールを処理するには、ルール定義、ルールベース、および課金アクションがユーザープレーンで利用可能な状態である必要があります。コントロールプレーンは、PFD 管理メッセージを使用して、関連するユーザープレーンにこのすべての情報を送信します。

この情報をコントロールプレーンからユーザープレーンに送信するために、CUPS アーキテクチャは次の 2 つのモジュールを使用します。

- **Sx-U Demux**：複数のコントロールプレーンノードでノードレベルのメッセージをすべて処理します。
- **Sx-C Demux**：ユーザープレーンサービスとのノードレベルのメッセージ交換、つまり PFD 管理メッセージ、Sx 関連付けメッセージ、ハートビート関連メッセージを処理します。

1. コントロールプレーンがすべての設定で初期化され、ユーザープレーンが初期設定で初期化されると、デバッグモードCLIコマンドを使用してPFD管理要求メッセージが開始されます。debugコマンドについては、「モニタリングとトラブルシューティング」の項を参照してください。
2. debug CLIコマンドが実行されると、Sx-C Demuxは、PFD管理要求または応答メッセージを使用して、すべてのルール定義、ルールベース、および課金アクションの設定をユーザープレーンにプッシュします。
3. ユーザープレーンのSx-U Demuxは、PFD管理要求メッセージを受信すると、設定を復号してからユーザープレーンノードの各セッションマネージャインスタンスに送信し、SCTに保存します

コントロールプレーンからユーザープレーンへの一括設定の移動

push config-to-up all CLIコマンドを使用して、一連の設定をコントロールプレーン（CP）からユーザープレーン（UP）にプッシュできます。セッションコントローラでは、常時設定タイマーが実行されます。このタイマーが終了すると、各種設定が指定されたすべてのセッションマネージャに一括でプッシュされます。セッションコントローラは、CPから受信したさまざまな設定タイプのスキップリストを保持します。Sx Demuxが設定をプッシュすると、設定タイプに応じたスキップリストに保存されます。

スキップリストが最大長に達すると、特定の設定タイプのリスト全体がセッションコントローラからすべてのセッションマネージャにプッシュされます。このプロビジョニングにより、設定ごとに個別にメッセージを送信するのではなく、設定が単一のメッセージでまとめて送信されるため、proclet間のメッセンジャーイベント/メッセージの数が削減されます。

一括設定プッシュでは、次の設定タイプがサポートされます。

- Ruledef
- 課金アクション
- アクション優先回線
- 回送ルール設定
- Group of Ruledef設定
- Group of Ruledefのルール設定
- Rulebase L3/L4/L7情報設定
- APN設定
- ACSサービス設定
- サービスチェーン設定
- NSHフォーマット
- NSHフィールド

- トラフィック ステアリング グループ
- ECS のホストプール設定
- ECS のポートマップ設定
- ECS のサービス スキーム フレームワーク設定
- ECS の X-Header フォーマット
- ECS のコンテンツ フィルタリング カテゴリのポリシー ID

現在、CP から UP への設定の伝達は、UP 登録時に CP と UP の間で Sx 関連付けが発生した場合、または **push config-to-up all** CLI がトリガーされた場合にのみ発生します。設定の伝達中は、すべての設定が CP から UP にプッシュされます。UP 登録が行われた後、新しい設定が追加されるか、既存の設定が変更されると、CP から更新済みの設定を受信するため、UP をリブートして登録する必要があります。この時点では、設定の更新が UP に伝達されていないためです。

push config-to-up all CLI を実行すると、設定全体がすべての登録済み/関連付け済みの UP に伝達されます。入力としてピアアドレスを指定することで、設定を特定の UP に伝達することもできます。設定は、その CP に関連付けられている UP にのみプッシュされます。

push config-to-up all CLI では、UP の既存の設定は削除されません。また、CP には存在しない UP の不要な設定もフラッシュアウトされません。CP からプッシュされた設定は、現在 UP に存在するものとマージされます。UP の既存の設定はフラッシュアウトされません。CP と UP 間の設定監査はサポートされません。

CP の設定からルール、rulebase アクションの優先順位、ホストプール、およびポートマップが削除されると、CP から UP に自動的にプッシュされます。ルールの追加または変更は、CLI を使用してプッシュする必要があります。

ruledef でルール行の変更（追加または削除）がサポートされるようになりました。変更されたルール行は、既存のフロー、新しいフロー、または新規コールのルール照合の候補となります。

CUPS では（RCM を使用しない場合）、変更はコントロールプレーンで行われ、PFD メカニズムを介してユーザープレーンにプッシュされます。CUPS では（RCM を使用する場合）、変更は RCM で行われ、ユーザープレーンにプッシュされます。変更は、コントロールプレーンで並行して個別に行われます。

次の表に、設定変更による新規コールと既存のコールへの影響について示します。

設定の変更	既存のコールへの影響（既存のフロー）	既存のコールへの影響（新しいフロー）	新規コールへの影響
既存の ruledef の内容/新しいルールの追加	設定変更後、既存のフローにルール照合が適用される。	設定の変更が新しいフローに適用される。新しいフローの場合、あらゆる方向で新たにルール照合が発生し、ruledefの変更が既存のコールの新しいフローに適用される。	設定の変更が新規コールに適用される。新しいフローの場合、あらゆる方向で新たにルール照合が発生し、ruledef の変更が新規コールのフローに適用される。
ruledef なし	使用中のルールは、そのアクションの優先順位が rulebase から削除されない限り、削除できない。	設定変更後、既存のフローにルール照合が適用される。	設定の変更が新規コールに適用される。
新規 Group of Ruledefs（GoR）/既存の Group of Ruledefs の内容の変更（GoR へのルールの追加または削除）	設定変更後、既存のフローにルール照合が適用される。	設定の変更が新しいフローに適用される。新しいフローの場合、あらゆる方向で新たにルール照合が発生し、GoR の変更が既存のコールの新しいフローに適用される。	設定の変更が新規コールに適用される。新しいフローの場合、新たにルール照合が発生し、GoR の変更が新規コールのフローに適用される。
GoR なし	使用中のルールは、そのアクションの優先順位が rulebase から削除されない限り、削除できない。	設定変更後、既存のフローにルール照合が適用される。	設定の変更が新規コールに適用される。
GoR にルールなし	設定変更後、既存のフローにルール照合が適用される。	新しいフローで新たにルール照合が行われ、設定の変更が有効になる。	新しいフローで新たにルール照合が行われ、設定の変更が有効になる。
アクションの優先順位の変更/アクションの優先順位の追加	設定の変更が既存のフローに適用される。	設定の変更が新しいフローに適用される。	設定の変更が新規コールに適用される。
アクションの優先順位なし	設定の変更が既存のフローに適用される。	設定の変更が新しいフローに適用される。	設定の変更が新規コールに適用される。
rulebase なし	rulebase なしの設定はサポートされない。	rulebase なしの設定はサポートされない。	rulebase なしの設定はサポートされない。

設定の変更	既存のコールへの影響（既存のフロー）	既存のコールへの影響（新しいフロー）	新規コールへの影響
APN なし	APN なしの設定はサポートされない。	APN なしの設定はサポートされない。	APN なしの設定はサポートされない。
IP ソース違反	既存のコールへの影響なし	既存のコールへの影響なし	設定の変更が新規コールに適用される。

制限事項

CP が VPC-DI 上にある場合、多数の UP に接続されている CP の一括設定があるシステムで、CP から UP への PFD 設定のプッシュの遅延が発生する可能性があります。

この遅延は、VPC-DI がカード間通信プロセスを備えたマルチカードシャーシであり、各ピアの UP の共有/システム設定タスク（SCT）から設定を取得するのに時間がかかるために発生します。

CP が VPC-SI 上にある場合、遅延は観測されません。

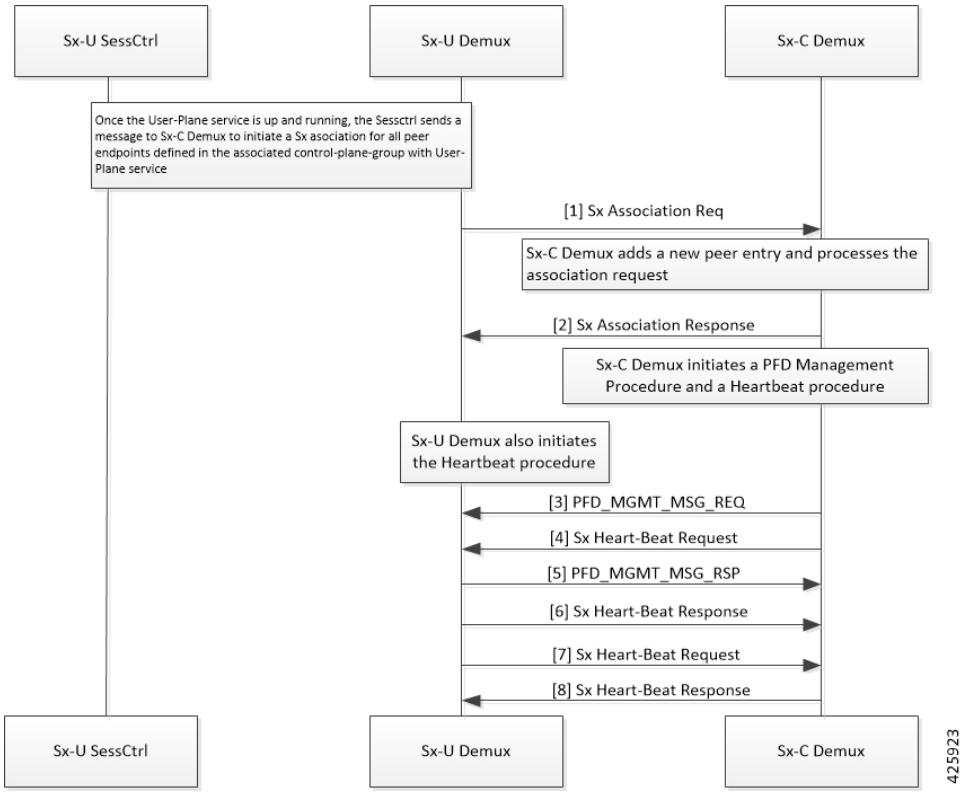
Sx 関連付け

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。

CUPS 環境では、コントロールプレーンとユーザープレーンのエンティティは、通信を確立する前に相互に関連付けを実行する必要があります。

Sx 関連付け手順は、3GPP TS 29.244 で定義されています。これらはノードレベルのメッセージであるため、コントロールプレーンの Sx-C Demux とユーザープレーンの Sx-U Demux によって処理されます。

通話フロー



次に、Sx 関連付けの仕組みの概要を示します。

1. Sx 関連付けセットアップ要求がコントロールプレーンまたはユーザープレーンによって開始されます。

重要 このリリースでは、ユーザープレーンからの Sx 関連付けセットアップ要求のみがサポートされています。

2. ユーザープレーンが Sx 関連付けセットアップ要求を開始するには、オペレータがグローバル コンフィギュレーション モードで **control-plane-group** を設定し、**control-plane-group** をユーザープレーンサービスに関連付ける必要があります。この章の「Sx 関連付けセットアップ要求の設定」の項を参照してください。
3. ピアノード ID（現在は IPv4 または IPv6 アドレス）は **control-plane-group** で設定されます。
4. 現在、ユーザープレーンでは、Sx-U Demux は Sx 関連付けセットアップ要求に送信される Sx サービスアドレスを（ノード ID と同様に）使用します。IPv4 と IPv6 の選択は、設定された **peer-node-id** によって異なります。
5. ユーザープレーンでユーザープレーンサービスが起動すると、Sx-U Demux がコントロールプレーンに Sx 関連付け要求を送信します。Sx-C Demux が、Sx 関連付け応答を検証し、ユーザープレーンに送信します。

6. コントロールプレーンが Sx 関連付け要求を処理し、ユーザープレーンに応答を送信すると、設定を送信するためにユーザープレーンに向けて Prime PFD メッセージを開始します。また、コントロールプレーンは、関連付けられたユーザープレーンでハートビート手順を開始します。
7. Sx 関連付け応答を受信すると、ユーザープレーンもコントロールプレーンに向けてハートビート手順を開始します。
8. Sx 関連付けセットアップ要求を受信したときにコントロールプレーンの準備ができていない（SAEGW サービスが稼働していない）場合、Sx 関連付けセットアップ要求は拒否されます。ユーザープレーンは **association reattempt-timeout** の後に Sx 関連付けセットアップ要求を再試行します。この章の「Sx 関連付け再試行タイムアウトの設定」の項を参照してください。

特定のユーザープレーンのセッションの解放

特定のユーザープレーンを停止するには、次の CLI コマンドを使用して、そのユーザープレーンに属するすべてのサブスクライバを最初にクリアすることを推奨します。

clear subscribers saegw-only uplane-address *user_plane_address* **no-select-up**

この CLI コマンドを実行すると、指定されたユーザープレーンに属するすべてのセッションが正常に解放され、そのユーザープレーンは「セッション選択に使用不可」としてマークされます。そのユーザープレーンは関連付けられた状態のままですが、セッションの選択には使用できません。

セッションをクリア後、ユーザープレーンで次のいずれかの CLI コマンドを実行して、コントロールプレーンからの関連付けを削除します。

no user-plane-service *service_name*

または

no peer-node-id { ipv4-address *ipv4_address* **| ipv6-address** *ipv6_address* **}**

前述の CLI コマンドの詳細については、このガイドの「ユーザープレーンサービスの設定」および「ピアノード ID の設定」の項を参照してください。

ユーザープレーンから既存のセッションのみを解放するには、次の CLI コマンドを使用します。

clear subscribers saegw-only uplane-address *user_plane_address*

この場合、ユーザープレーンは関連付けられた状態のままで、セッションの選択に使用できることに注意してください。

（注） **clear subscribers** コマンドが UP で実行されると、CP には通知されず、セッションは実行中であると見なされます。

ICSR のサポート

Sx コントロールプレーンの場合、Demux ICSR がサポートされます。関連するすべてのピア情報は、セッションマネージャを介してスタンバイシャーシの Sx コントロールプレーンの Demux にチェックポイントされます。

Demux のリカバリのサポート

SX コントロールプレーンの Demux リカバリと計画外の Demux カードの移行がサポートされています。リカバリ中に、関連するすべてのピア情報がセッションマネージャから Sx コントロールプレーンの Demux にリカバリされます。

現在、Sx-Demux のリカバリ後、Sx コントロールプレーンの Demux ではピアエントリとピア ID の各 VPNmgr で監査が実行されません。エラーが発生した場合、IP プールの管理と UP の選択に関連して、VPNMgr と SxMgr の間でコールのドロップと非同期状態が発生する可能性があります。

コントロール プレーン グループの設定

次の CLI コマンドを使用して、[Global Configuration] モードでコントロール プレーン グループを設定します。コントロール プレーン グループには、ユーザープレーンが関連付けられるコントロール プレーン エンドポイントがリストされます。

```
configure
  [ no ] control-plane-group control_plane_group_name
  end
```

注：

- **control-plane-group** *control_plane_group_name*：ユーザープレーンでコントロール プレーン グループを設定します。*control_plane_group_name* は、1 ～ 63 文字の文字列である必要があります。
- 以前に設定済みの場合は、**no control-plane-group** *control_plane_group_name* CLI コマンドを使用して、コントロール プレーン グループの設定を削除します。

Sx 関連付けの設定

この項では、この機能をサポートするために使用可能な CLI コマンドについて説明します。

Sx の関連付けセットアップ要求の設定

次の CLI コマンドを使用して、[Control Plane Group Configuration] モードでピアノード ID と Sx 関連付けに関連する属性を有効にします。

```
configure
  control-plane-group control_plane_group_name
    sx-association { initiated-by-cp | initiated-by-up }
    end
```

注：

- **sx-association**：コントロールプレーンまたはユーザープレーンによって開始される Sx 関連付けセットアップ要求を設定します。デフォルト値は **initiated-by-up** です。
- **initiated-by-cp**：Sx 関連付けセットアップ要求は、コントロールプレーンによって開始されます。

重要 このリリースでは、このキーワードはサポートされません。

- **initiated-by-up**：Sx 関連付けセットアップ要求は、ユーザープレーンによって開始されます。

コントロール プレーン グループとユーザープレーンサービスの関連付け

重要 コントロール プレーン グループとユーザープレーンサービスの関連付けは、ユーザープレーンサービスを起動するためのオプションパラメータです。ユーザープレーンに関連付けられているコントロール プレーン グループがあり、その設定に従って Sx 関連付けを開始することが想定されている場合、ユーザープレーンは定義されたコントロールプレーンエンドポイントに Sx 関連付け要求を送信します。

次の CLI コマンドを使用して、ユーザープレーンサービスをコントロール プレーン グループに関連付けます。

```
configure
  context context_name
    user-plane-service service_name
      [ no ] associate control-plane-group control_plane_group_name
      end
```

注：

- **no**：ユーザープレーンサービスからコントロール プレーン グループの関連付けを削除します。
- **control-plane-group** *control_plane_group_name*：ユーザープレーンサービスが Sx 関連付けを実行するコントロール プレーン グループを関連付けます。コントロール プレーン グループ名は、1 ～ 63 文字の文字列である必要があります。

ユーザープレーンサービスのコンフィギュレーション モードおよび関連する CLI コマンドの詳細については、「*CUPS* でのユーザープレーンの設定」の章を参照してください。

ピアノード ID の設定

コントロールプレーンノード ID を設定するには、次の CLI コマンドを使用します。

```
configure
  control-plane-group control_plane_group_name
    [ no ] peer-node-id { ipv4-address ipv4_address | ipv6-address
```

```
ipv6_address }
      end
```

注：

- **no**：従っているオプションを削除します。
- **ipv4-address**：IPv4 アドレスを設定します。
- **ipv6-address**：IPv6 アドレスを設定します（コロン区切りの 16 進表記をサポート）。
- **peer-node-id** は、開始する必要があるコントロールプレーン sx-service アドレスであり、セットアップ要求を受信して応答する必要があります。
- 現在、5 つのノード ID をコントロール プレーン グループに追加できます。

Sx 関連付け再試行タイムアウトの設定

Sx サービスの関連付け再試行タイムアウトには、次の設定を使用します。

```
configure
  context context_name
    sx-service service_name
      sx-protocol association reattempt-timeout timeout_seconds
      end
```

注：

- **association**：Sx 関連付けパラメータを設定します。
- **reattempt-timeout** *timeout_seconds*：Sx サービスの関連付け再試行タイムアウトを秒単位（30 ～ 300 の範囲）で設定します。デフォルトは 60 です。
- ユーザープレーンが起動すると、SSI で 2 分間、ASR 5500 で 10 分間待機して、コントロールプレーンとの関連付けのセットアップが開始されます。これは、関連付けのセットアップ後にコントロールプレーンから送信される設定メッセージをユーザープレーンシステムが処理する準備が、完全に整っていることを確認するために行われます。各待機時間は、reattempt-timeout を使用して変更できます。

Sx の関連付け SNMP トラップの設定

Sx 関連付けが検出されると、SNMP トラップ（通知）がシステムによって自動生成されます。

Sx 関連付けが検出された際の SNMP トラップを有効にするには、次の設定を使用します。

```
configure
  snmp trap enable SxPeerAssociated
  end
```

Sx 関連付けがリリースされた際の SNMP トラップを有効にするには、次の設定を使用します。

```
configure
  snmp trap enable SxPeerAssociationRelease
  end
```

コントロールプレーンからユーザープレーンへの一括設定の移動

次の設定を使用して、コントロールプレーンからユーザープレーンに一括設定を移動します。

push config-to-up all peer-ip-addr*IP_Address*

注：

- **all**：関連するすべてのユーザープレーンに設定をプッシュします。
- **peer-ip-addr**：指定したユーザープレーンに設定をプッシュします。設定を受信するには、ユーザープレーンを関連付ける必要があります。*IP_Address*（IPv4 または IPv6）では、ユーザープレーンノードの IP アドレスを指定します。
- IP プール関連の設定は、前述の設定を使用してプッシュされません。

Sx の関連付けのモニタリングと障害対応

ここでは、Sx 関連付け手順のモニタリングと障害対応で使用できる CLI コマンドを紹介します。

SNMP トラップ

Sx 関連付けのステータスを追跡するため、次のトラップを使用できます。

- **sn_trap_sx_peer_node_associated**：Sx 関連付けが検出された際にトリガーされる情報トラップ。コントロールプレーンとユーザープレーンの両方で、次の情報が共有されます。
  - Context Name
  - サービス名
  - ノード タイプ
  - ノード ID（Node ID）
  - Peer Node Type
  - Peer Node ID
  - Group-Name
- **sn_trap_sx_peer_node_association_release**：Sx 関連付けの解除が検出された際にトリガーされる情報トラップ。コントロールプレーンとユーザープレーンの両方で、次の情報が共有されます。
  - Context Name
  - サービス名
  - ノード タイプ
  - ノード ID（Node ID）
  - Peer Node Type

- Peer Node ID
- Group-Name

show コマンドと出力

この項では、Sx 関連付けのサポートにおける show コマンドおよびコマンドの出力について説明します。

show control-plane-group all

この show コマンドの出力には、Sx 関連付けをサポートするフィールドが表示されます。

- Control Plane Group
  - Name:
  - Sx-Association:
  - Node-Id:
  - Node-Id:

show user-plane-service name <name>

この show コマンドの出力には、Sx の関連付けをサポートする次のフィールドが表示されます。

- サービス名
  - Service-Id
  - Context
  - Status
  - PGW Ingress GTPU Service
  - SGW Ingress GTPU Service
  - SGW Egress GTPU Service
  - Control Plane Tunnel GTPU Service
  - Sx Service
  - Control Plane Group

show sx peers

この show コマンドの出力には、Sx 関連付けをサポートするフィールドが表示されます。

- ノードタイプ：
  - （C）：CPLANE
  - （U）：UPLANE

- ピアモード：
  - （A）：アクティブ
  - （S）：スタンバイ
- 関連付け状態：
  - （i）：アイドル
  - （I）：開始済み
  - （A）：関連付け済み
  - （R）：リリース中
- 設定状態：
  - （C）：設定済み
  - （N）：未設定
- IP プール：
  - （E）：有効
  - （D）：無効
- Sx サービス ID
- グループ名
- ノード ID（Node ID）
- ピア ID
- リカバリタイムスタンプ
- 再起動回数
- Current Sessions
- 最大セッション数（Max Sessions）

show snmp trap history

このコマンドの出力には、次のフィールドが含まれています。

- タイムスタンプ
- Trap Information

モニタリングおよびトラブルシューティング

この項では、この機能のサポートにおける debug コマンドと show コマンドやコマンドの出力について説明します。

コマンドや出力の表示

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show user-plane-service charging-action all

このコマンドを実行すると、次の出力が表示されます。

```
Service Name: default
Charging Action Name: charge-action-qci8
Content ID: 0
Service ID: 0
EDRs: Disabled
EGCDRs: Enabled
Rf: Disabled
UDRs: Enabled
Flow Idle Timeout: 300 (secs)
Limit For Flow Type: Disabled
Bandwidth ID: 0
Limit For Uplink Bandwidth: Disabled
Limit For Downlink Bandwidth: Disabled
Throttle-Suppress Timeout: n/a
QoS Renegotiate Traffic-Class: Disabled
QoS Class Identifier: 8
IP Type of Service: Not Configured
Content Filtering: Enabled
Credit-Control: Disabled
Flow Action:
Redirect URL: Disabled
Redirect URL from OCS: Disabled
Redirect to Video Server: Disabled
Clear Quota Retry Timer: Disabled
Conditional Redirect: Disabled
Discard: Disabled
Terminate-Flow: Disabled
Terminate-Session: Disabled
Rulebase Change: Disabled
Billing Action:
Event Data Record: Disabled
GGSN charging Data Record: Enabled
Rf Accounting: Disabled
User Data Record: Enabled
Radius Accounting Record: Disabled
Charge Volume: ip bytes
PCO-Custom1 value: n/a
Flow-Mapping Idle Timeout: 300 (secs)
DNS Proxy Bypass: Disabled
Discard on Readdressing Failure: Disabled
Video Bitrate: Not Configured (default/no(0) is interpreted as bitrate=QOS MBR (GGSN/PGW))
Strip URL:
CAE-Readdressing: Disabled
TFT notification to UE : Enabled
Service Detection:
```

```
Session Update:
QOS: Disabled
Packet Filter Name
==================
Predefined Rule Deactivation: Disabled
Config URRID : 0x800050
Charging Action Name: charge-action-qci9
Content ID: 0
Service ID: 0
EDRs: Disabled
EGCDRs: Enabled
Rf: Disabled
UDRs: Enabled
Flow Idle Timeout: 300 (secs)
Limit For Flow Type: Disabled
Bandwidth ID: 0
Limit For Uplink Bandwidth: Disabled
Limit For Downlink Bandwidth: Disabled
Throttle-Suppress Timeout: n/a
QoS Renegotiate Traffic-Class: Disabled
QoS Class Identifier: 8
IP Type of Service: Not Configured
Content Filtering: Enabled
Credit-Control: Disabled
Flow Action:
Redirect URL: Disabled
Redirect URL from OCS: Disabled
Redirect to Video Server: Disabled
Clear Quota Retry Timer: Disabled
Conditional Redirect: Disabled
Discard: Disabled
Terminate-Flow: Disabled
Terminate-Session: Disabled
Rulebase Change: Disabled
Billing Action:
Event Data Record: Disabled
GGSN charging Data Record: Enabled
Rf Accounting: Disabled
User Data Record: Enabled
Radius Accounting Record: Disabled
Charge Volume: ip bytes
PCO-Custom1 value: n/a
Flow-Mapping Idle Timeout: 300 (secs)
DNS Proxy Bypass: Disabled
Discard on Readdressing Failure: Disabled
Video Bitrate: Not Configured (default/no(0) is interpreted as bitrate=QOS MBR (GGSN/PGW))
Strip URL:
CAE-Readdressing: Disabled
TFT notification to UE : Enabled
Service Detection:
Session Update:
QOS: Disabled
Packet Filter Name
==================
Predefined Rule Deactivation: Disabled
Config URRID : 0x800050
Charging Action Name: ggsn-ingress
Content ID: 10
Service ID: 0
EDRs: Disabled
EGCDRs: Disabled
Rf: Disabled
UDRs: Enabled
Flow Idle Timeout: 300 (secs)
```

```
Limit For Flow Type: Disabled
Bandwidth ID: 0
Limit For Uplink Bandwidth: Disabled
Limit For Downlink Bandwidth: Disabled
Throttle-Suppress Timeout: n/a
QoS Renegotiate Traffic-Class: Disabled
QoS Class Identifier: Not Configured
IP Type of Service: Not Configured
Content Filtering: Enabled
Credit-Control: Disabled
Flow Action:
Redirect URL: Disabled
Redirect URL from OCS: Disabled
Redirect to Video Server: Disabled
Clear Quota Retry Timer: Disabled
Conditional Redirect: Disabled
Discard: Disabled
Terminate-Flow: Disabled
Terminate-Session: Disabled
Rulebase Change: Disabled
Billing Action:
Event Data Record: Disabled
GGSN charging Data Record: Disabled
Rf Accounting: Disabled
User Data Record: Enabled
Radius Accounting Record: Disabled
Charge Volume: ip bytes
PCO-Custom1 value: n/a
Flow-Mapping Idle Timeout: 300 (secs)
DNS Proxy Bypass: Disabled
Discard on Readdressing Failure: Disabled
Video Bitrate: Not Configured (default/no(0) is interpreted as bitrate=QOS MBR (GGSN/PGW))
Strip URL:
CAE-Readdressing: Disabled
TFT notification to UE : Enabled
Service Detection:
Session Update:
QOS: Disabled
Packet Filter Name
==================
Predefined Rule Deactivation: Disabled
Config URRID : 0x800050
Total charging action(s) found: 3
```

show user-plane-service charging-action name *charging-action-name*

このコマンドを実行すると、次の出力が表示されます。

```
Charging Action Name: charge-action-qci1
Content ID: 0
Service ID: 0
EDRs: Disabled
EGCDRs: Enabled
Rf: Disabled
UDRs: Enabled
Flow Idle Timeout: 300 (secs)
Limit For Flow Type: Disabled
Bandwidth ID: 0
Limit For Uplink Bandwidth: Disabled
Limit For Downlink Bandwidth: Disabled
Throttle-Suppress Timeout: n/a
QoS Renegotiate Traffic-Class: Disabled
QoS Class Identifier: 1
```

```
IP Type of Service: Not Configured
Content Filtering: Enabled
Credit-Control: Disabled
Flow Action:
Redirect URL: Disabled
Redirect URL from OCS: Disabled
Redirect to Video Server: Disabled
Clear Quota Retry Timer: Disabled
Conditional Redirect: Disabled
Discard: Disabled
Terminate-Flow: Disabled
Terminate-Session: Disabled
Rulebase Change: Disabled
Billing Action:
Event Data Record: Disabled
GGSN charging Data Record: Enabled
Rf Accounting: Disabled
User Data Record: Enabled
Radius Accounting Record: Disabled
Charge Volume: ip bytes
PCO-Custom1 value: n/a
Flow-Mapping Idle Timeout: 300 (secs)
DNS Proxy Bypass: Disabled
Discard on Readdressing Failure: Disabled
Video Bitrate: Not Configured (default/no(0) is interpreted as bitrate=QOS MBR (GGSN/PGW))
Strip URL:
CAE-Readdressing: Disabled
TFT notification to UE : Enabled
Service Detection:
Session Update:
QOS: Disabled
Packet Filter Name
==================
Predefined Rule Deactivation: Disabled
Config URRID : 0x800050
Total charging action(s) found: 1
```

show user-plane-service rule-base all

このコマンドを実行すると、次の出力が表示されます。

```
Service Name: default
Rule Base Name: prepaid
Charging Action Priorities:
Name Type Priority Charging-action Timedef Description
================================================================================
rule-qci8 RD 1 charge-action-qci8 - -
rule-qci7 RD 2 charge-action-qci7 - -
rule-qci6 RD 3 charge-action-qci6 - -
rule-qci5 RD 4 charge-action-qci5 - -
rule-qci4 RD 5 charge-action-qci4 - -
rule-qci3 RD 6 charge-action-qci3 - -
rule-qci2 RD 7 charge-action-qci2 - -
rule-qci1 RD 8 charge-action-qci1 - -
rule-qci9 RD 9 charge-action-qci9 - -
ip-any-rule RS 11 ggsn-ingress - -
Post-processing Action Priorities:
Name Type Priority Charging-action Description
================================================================================
Routing Action Priorities:
Ruledef Name Priority Analyzer Description
================================================================================
Groups of Prefixed Urls For Url Preprocessing :
EGCDR Fields:
```

```
Tariff time thresholds (min:hrs):
Interval Threshold : 0 (secs)
Uplink Octets : 0 Downlink Octets : 0
Total Octets : 0
Time Based Metering: Disabled
Content Filtering Group : Not configured
Content Filtering Policy : Not configured
Content Filtering Mode : Not configured
URL-Blacklisting Action : Not Configured
URL-Blacklisting Content ID : Not Configured
UDR Fields:
Interval Threshold : 0 (secs)
Uplink Octets : 0 Downlink Octets : 0
Total Octets : 0
First Hit Content-Id Trigger : Disabled
Tariff time trigger (min:hrs) : Disabled
NEMO-Prefix-Update Trigger : Disabled
CCA Fields:
RADIUS charging context: Not configured
RADIUS charging group : Not configured
RADIUS interim interval: Not configured
DIAMETER Requested Service Unit: Not configured
Quota Retry Time : 60 (secs)
Quota Holding Time (QHT): Not configured
Quota Time Duration Algorithms: Not configured
Flow End Condition : Disabled
Flow Any Error Charging Action: Disabled
Billing records : Disabled
Limit For Total Flows : Disabled
Limit For TCP Flows : Disabled
Limit For Non-TCP Flows : Disabled
FW-and-NAT Default Policy : n/a
PCP Service : n/a
QoS Renegotiation Timeout : Disabled
EDRs on DCCA Failure Handling : Disabled
EDRs on transaction complete : Disabled
Extract host from uri: Disabled
Tethering Detection : Disabled
OS-based Detection : N/A
UA-based Detection : N/A
Tethering Detection (ip-ttl) : Disabled
Max SYN detection in a flow : N/A
Tethering Detection (DNS-Based): Disabled
Tethering Detection (Application): Disabled
Websocket Flow-Detection Configuration:
n/a
Check-point Account Synchronization Timer Configuration:
SR : n/a
ICSR : n/a
EDR Suppress zero byte records : Disabled
EDR Timestamp Rounding : Round Off
EDR Charge Volume (sn-charge-volume)
Retransmissions counted : Enabled
Dropped counted : Disabled
EGCDR Timestamp Rounding : Round Off
RTP Dynamic Routing : Disabled
Ignore port number in application headers: Disabled
RTSP Delayed Charging : Disabled
Delayed Charging : Disabled
No Rating Group Override
No Service Id Override
IP Reassembly-Timeout : 5000 milliseconds
IP Reset ToS field : Disabled
IP Readdress Failure Terminate : Disabled
```

```
TCP Out-of-Order-Timeout : 5000 milliseconds
TCP Out-of-Order-Max-Entries : 1000 packets
TCP 2MSL Timeout : 2 sec Port Reuse: No
HTTP header parse limit : Disabled
RTSP initial bytes limit : Disabled
Xheader Certificate Name :
Xheader Re-encryption Period : 0 min
TCP MSS Modification : Disabled
TCP Check Window Size : Disabled
WTP Out-of-Order-Timeout : 5000 milliseconds
TCP transmit-out-of-order-packets : Immediately
WTP transmit-out-of-order-packets : Immediately
Verify Transport layer checksum : Enabled
ICMP Request Threshold : 20
Default Bandwidth-Policy : n/a
Bandwidth-Policy Fallback : Disabled
P2P Dynamic Routing : Disabled
TCP Proxy Mode Configuration:
TCP Proxy Mode : Disabled
CAE-Readdressing : Disabled
Transactional-Rule-Matching : Disabled
TRM Fastpath : Disabled
Override Control : Disabled
Override-Control-with-name : Disabled
Override-Control-with-grp-info : Disabled
Charging-Action Override : Disabled.
TFT notification to UE for default bearer : Enabled
Ran-Bandwidth Optimization : Disabled
Total rulebase(s) found: 1
```

show user-plane-service rule-base name *rule-base-name*

このコマンドを実行すると、次の出力が表示されます。

```
Service Name: default
Rule Base Name: prepaid
Charging Action Priorities:
Name Type Priority Charging-action Timedef Description
================================================================================
rule-qci8 RD 1 charge-action-qci8 - -
rule-qci7 RD 2 charge-action-qci7 - -
rule-qci6 RD 3 charge-action-qci6 - -
rule-qci5 RD 4 charge-action-qci5 - -
rule-qci4 RD 5 charge-action-qci4 - -
rule-qci3 RD 6 charge-action-qci3 - -
rule-qci2 RD 7 charge-action-qci2 - -
rule-qci1 RD 8 charge-action-qci1 - -
rule-qci9 RD 9 charge-action-qci9 - -
ip-any-rule RS 11 ggsn-ingress - -
Post-processing Action Priorities:
Name Type Priority Charging-action Description
================================================================================
Routing Action Priorities:
Ruledef Name Priority Analyzer Description
================================================================================
Groups of Prefixed Urls For Url Preprocessing :
EGCDR Fields:
Tariff time thresholds (min:hrs):
Interval Threshold : 0 (secs)
Uplink Octets : 0 Downlink Octets : 0
Total Octets : 0
Time Based Metering: Disabled
Content Filtering Group : Not configured
Content Filtering Policy : Not configured
```

```
Content Filtering Mode : Not configured
URL-Blacklisting Action : Not Configured
URL-Blacklisting Content ID : Not Configured
UDR Fields:
Interval Threshold : 0 (secs)
Uplink Octets : 0 Downlink Octets : 0
Total Octets : 0
First Hit Content-Id Trigger : Disabled
Tariff time trigger (min:hrs) : Disabled
NEMO-Prefix-Update Trigger : Disabled
CCA Fields:
RADIUS charging context: Not configured
RADIUS charging group : Not configured
RADIUS interim interval: Not configured
DIAMETER Requested Service Unit: Not configured
Quota Retry Time : 60 (secs)
Quota Holding Time (QHT): Not configured
Quota Time Duration Algorithms: Not configured
Flow End Condition : Disabled
Flow Any Error Charging Action: Disabled
Billing records : Disabled
Limit For Total Flows : Disabled
Limit For TCP Flows : Disabled
Limit For Non-TCP Flows : Disabled
FW-and-NAT Default Policy : n/a
PCP Service : n/a
QoS Renegotiation Timeout : Disabled
EDRs on DCCA Failure Handling : Disabled
EDRs on transaction complete : Disabled
Extract host from uri: Disabled
Tethering Detection : Disabled
OS-based Detection : N/A
UA-based Detection : N/A
Tethering Detection (ip-ttl) : Disabled
Max SYN detection in a flow : N/A
Tethering Detection (DNS-Based): Disabled
Tethering Detection (Application): Disabled
Websocket Flow-Detection Configuration:
n/a
Check-point Account Synchronization Timer Configuration:
SR : n/a
ICSR : n/a
EDR Suppress zero byte records : Disabled
EDR Timestamp Rounding : Round Off
EDR Charge Volume (sn-charge-volume)
Retransmissions counted : Enabled
Dropped counted : Disabled
EGCDR Timestamp Rounding : Round Off
RTP Dynamic Routing : Disabled
Ignore port number in application headers: Disabled
RTSP Delayed Charging : Disabled
Delayed Charging : Disabled
No Rating Group Override
No Service Id Override
IP Reassembly-Timeout : 5000 milliseconds
IP Reset ToS field : Disabled
IP Readdress Failure Terminate : Disabled
TCP Out-of-Order-Timeout : 5000 milliseconds
TCP Out-of-Order-Max-Entries : 1000 packets
TCP 2MSL Timeout : 2 sec Port Reuse: No
HTTP header parse limit : Disabled
RTSP initial bytes limit : Disabled
Xheader Certificate Name :
Xheader Re-encryption Period : 0 min
```

```
TCP MSS Modification : Disabled
TCP Check Window Size : Disabled
WTP Out-of-Order-Timeout : 5000 milliseconds
TCP transmit-out-of-order-packets : Immediately
WTP transmit-out-of-order-packets : Immediately
Verify Transport layer checksum : Enabled
ICMP Request Threshold : 20
Default Bandwidth-Policy : n/a
Bandwidth-Policy Fallback : Disabled
P2P Dynamic Routing : Disabled
TCP Proxy Mode Configuration:
TCP Proxy Mode : Disabled
CAE-Readdressing : Disabled
Transactional-Rule-Matching : Disabled
TRM Fastpath : Disabled
Override Control : Disabled
Override-Control-with-name : Disabled
Override-Control-with-grp-info : Disabled
Charging-Action Override : Disabled.
TFT notification to UE for default bearer : Enabled
Ran-Bandwidth Optimization : Disabled
Total rulebase(s) found: 1
```

show user-plane-service rule-def all

このコマンドを実行すると、次の出力が表示されます。

```
Service Name: default
Ruledef Name: ip-any-rule
ip any-match = TRUE
Rule Application Type: Charging
Copy Packet to Log: Disabled
Tethered Flow Check: Disabled
Multi-line OR: Disabled
Ruledef Name: rule-qci1
ip any-match = TRUE
Rule Application Type: Charging
Copy Packet to Log: Disabled
Tethered Flow Check: Disabled
Multi-line OR: Disabled
Ruledef Name: rule-qci2
ip any-match = TRUE
Rule Application Type: Charging
Copy Packet to Log: Disabled
Tethered Flow Check: Disabled
Multi-line OR: Disabled
Ruledef Name: rule-qci3
ip any-match = TRUE
Rule Application Type: Charging
Copy Packet to Log: Disabled
Tethered Flow Check: Disabled
Multi-line OR: Disabled
Ruledef Name: rule-qci4
ip any-match = TRUE
Rule Application Type: Charging
Copy Packet to Log: Disabled
Tethered Flow Check: Disabled
Multi-line OR: Disabled
Ruledef Name: rule-qci5
ip any-match = TRUE
Rule Application Type: Charging
Copy Packet to Log: Disabled
Tethered Flow Check: Disabled
Multi-line OR: Disabled
```

```
Ruledef Name: rule-qci6
ip any-match = TRUE
Rule Application Type: Charging
Copy Packet to Log: Disabled
Tethered Flow Check: Disabled
Multi-line OR: Disabled
Ruledef Name: rule-qci7
ip any-match = TRUE
Rule Application Type: Charging
Copy Packet to Log: Disabled
Tethered Flow Check: Disabled
Multi-line OR: Disabled
```

show user-plane-service rule-def name *rule-def-name*

```
Service Name: default
Ruledef Name: rule-qci8
ip any-match = TRUE
Rule Application Type: Charging
Copy Packet to Log: Disabled
Tethered Flow Check: Disabled
Multi-line OR: Disabled
Total Ruledef(s) : 1
```

第 67 章

パスワード暗号化の改善

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.27.4

機能説明

CUPS の構成ファイルには、非機密情報からきわめて機密性の高い情報まで、さまざまなレベルの機密情報に関する多くのコマンドが含まれています。管理者またはユーザーによる不正アクセスから機密情報を保護する必要があります。以下に示すように、機密データを保護するさまざまな方法があります。

- 対称暗号化
- 非対称暗号化
- 一方向ハッシュ

機能の仕組み

対称暗号化は、クライアント認証用のリモート TACACS+ パスワード、LI 設定、パスワード、SSH キー、SNMP コミュニティストリングなど、構成ファイルに存在する機密情報を保護するために使用されます。プレーンテキスト形式の機密情報が CUPS のリモートサーバーに転送される場合があります。1 つの例は、CUPS システムが TACACS+ クライアントとして機能し、

リモートTACACS+サーバーにアクセスするためにパスワード認証が必要な場合です。一方向ハッシュプロセス後に機密情報が保存されると、システムはハッシュ値を復号または反転してプレーンテキストを取得できません。CUPS は対称暗号化を使用して、パスワードをランダムなソルトでハッシュできるようにして、この問題に対処します。

次に示されているように、プレーンテキストパスワードは、**PBKDF2**ハッシュアルゴリズムを使用してシステムによってハッシュされます。

- システムが、/dev/urandom デバイスファイルから 16 バイトのランダムなソルトを生成します。
- **PBKDF2** 内の反復回数は、次のように計算されます。
  - 基本値として 10,000 ラウンド。
  - ランダムなソルトに基づく追加のラウンド。
  - 長さ 64 バイトの結果（ハッシュ値）。

ハッシュされたパスワードは、システム設定プロセス中に保存されます。ユーザーが入力したプレーンテキストパスワードは、認証フェーズと比較するために、同じソルトに基づいてハッシュ値に変換されます。

（注） パスワードハッシュ値は、既存の CLI でのさらなる変更を最小限に抑え、回避するように暗号化されます。

対称暗号化の発生

CUPS では、さまざまなタイプのデータに対する対称暗号化が数多く発生します。

小規模な一般機密データの暗号化（512 バイト未満）

CUPS は、長さが 512 バイト未満の小規模な一般機密データの暗号化を処理します。

フラッシュ上の永続性ファイルに対する P2P ライブラリライセンスの有効期限

P2P ライセンス機能では、有効期限によって P2P ライブラリを制御します。P2P ライセンスには、有効な P2P ライブラリのローディングを制御する有効期限があります。P2P ライセンスのライセンス有効期限は、後で参照できるようにファイルに保存されます。

長いデータの暗号化（512 バイトを超える長さ）

サイズの大きいバイナリテキストは、それぞれ512バイトの小さいチャンクに分割されます。これらの小さなチャンクはそれぞれ個別に暗号化され、文字列として連結されます。

CUPS をクライアントとする SSH キー（mgmt インターフェイス）

CUPS は、一部のトランザクションでは SSH クライアントとしても機能します。クライアント SSH キーが生成されると、設定時に暗号化されて保存されます。その後のシステムのリブートでは、この SSH キーを復号して使用します。

CUPS のサーバー SSH キー（コンテキストごと）

CUPS は、管理者から受信するログイン接続要求に対して、SSH サーバーとして機能します。SSH サーバーの SSH キーは一度生成され、設定時に暗号化されて保存されます。その後のシステムのリブートでは、この SSH キーを復号して使用します。

システムの RSA 秘密キー

CUPS は、設定モードで RSA 証明書と秘密キーの設定をサポートします。これらの秘密キーは、設定時に対称暗号化を使用して暗号化されます。

暗号化パスワードの設定

システムレベルおよび管理者パスワードの暗号化

システムレベルおよび管理者パスワードの暗号化について以下で説明します。

保存された設定の管理者パスワード

システム管理者アカウントのパスワードの値は、**show configuration o/p** コマンドでは「**」と表示されます。一方、パスワードは **save configuration o/p** コマンドを使用して暗号化されます。

テクニカル サポート パスワード

サポートおよびデバッグ用のテクニカルサポートパスワードは、CUPS で使用できます。テクニカル サポート パスワードを設定するには、次のコンフィギュレーション コマンドを使用します。

```
configure
   tech-support test-commands [encrypted] password
   end
```

QvPC-SI システムの接続アプリケーション セッション パスワード

セッションパスワードを設定するには、次のコンフィギュレーション コマンドを使用します。

```
sess-passwd encrypted password
```

ACS 課金情報

RADIUSユーザーのパスワードを設定するには、次のコンフィギュレーション コマンドを使用します。

cca radius user-password encrypted password *password*

IMS CSCF NPBD バインド IP システム ID

IMS CSCF NPBD バインド IP システム ID を設定するには、次のコンフィギュレーション コマンドを使用します。

IMS CSCF NPBD Bind IP System-id *sys_id* **id** *id* **encrypted password** *password*

SNMP コミュニティ文字列

SNMP コミュニティ文字列を設定するには、次のコンフィギュレーション コマンドを使用します。

snmp community encrypted *password*

TACACS+ クライアントパスワード

TACACS+ クライアントパスワードを設定するには、次のコンフィギュレーション コマンドを使用します。

server priority ip-address *ip_address* **password** *password*

BFD マルチホップピア認証

BFD マルチホップピア認証を設定するには、次のコンフィギュレーション コマンドを使用します。

bfd multihop-peer *peer_name* **authentication** *authentication* **encrypted password** *password*

第 68 章

PDI 最適化

機能の概要と変更履歴

マニュアルの変更履歴

Note リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

パケット検出情報（PDI）最適化機能を使用すると、コントロールプレーンとユーザープレーン機能の間で、Sx 確立および Sx 変更メッセージを介して PFCP シグナリングを最適化できます。PDI最適化を使用しない場合、次の共通パラメータがすべてのパケット検出ルール（PDR）のPDIで特定のベアラーに対して繰り返されるため、コントロールプレーンとユーザープレーン間のシグナリングが必要以上に増加します。

- ローカル F-TEID
- ネットワークインスタンス

- UE IP アドレス
- PDI最適化は、PDRのPDIの共通パラメータを、トラフィックエンドポイント（トラフィックエンドポイントID）と呼ばれる単一のコンテナに統合することによって実現されます。複数の PDR から統合されたパラメータは、トラフィックエンドポイント参照で使用されます。
- PDI最適化はCLI制御機能であり、Sxa、Sxb、Sxc、Sxab、およびN4インターフェイスでサポートされます。

関係

PDI 最適化機能は、次の機能の前提条件です。

- ユーザープレーンでの GTP-U Error Indication のサポート
- Sx バルク統計情報
- CUPS バルク統計情報のサポート

機能の仕組み

トラフィックエンドポイントIDは、PFCPセッション内で一意です。PDIがトラフィックエンドポイントを参照している場合、そのトラフィックエンドポイントにあるパラメータはPDIで再び提供されません。コントロールプレーン機能は、該当する場合は常にトラフィックエンドポイントを更新します。

トラフィックエンドポイントが更新されると、ユーザープレーン機能でそのトラフィックエンドポイントを参照するすべての PDR で、更新された情報が使用されます。

F-TEID 割り当てがユーザープレーン機能で実行される場合、ユーザープレーン機能により、トラフィックエンドポイントに関連付けられたF-TEIDが割り当てられて、保存されます。ユーザープレーン機能は、PFCP セッション確立応答または PFCP セッション変更応答メッセージで、割り当てられた F-TEID をコントロールプレーン機能に提供する際、受信した F-TEID でコントロールプレーン機能に保存されているトラフィックエンドポイント情報を更新します。

コントロールプレーン機能は、トラフィックエンドポイントIDの作成に関するユーザープレーン機能から確認メッセージを取得して初めて、別の PFCP メッセージで作成されたトラフィックエンドポイント ID を使用します。

コントロールプレーン機能でトラフィックエンドポイントが削除されると、ユーザープレーン機能が、コントロールプレーン機能によって削除されたトラフィックエンドポイントを参照するすべての PDR を削除します。Evolved Packet Core（EPC）の場合、Remove Traffic Endpoint IE は、複数の PDR が存在する（同じトラフィックエンドポイント ID を持つ）ベアラーを削除するために使用されます。

トラフィックエンドポイントは、ユーザープレーン上の特定の Sx セッションのベアラーを一意に識別するメカニズムとして使用されます。識別は、ベアラーの PDR に関連付けられているトラフィックエンドポイント ID を使用して行われます。

コントロールプレーンでの PDI 最適化の変更

トラフィックエンドポイントと呼ばれる新しいコンテナがサポートされているため、特定のベアラーの反復的な PDI 情報を伝送できます。各トラフィックエンドポイントは、トラフィックエンドポイント ID に関連付けられます。この ID は、特定の Sx セッションに対して一意です。

新しい IE である Create Traffic Endpoint IE は、Sx 確立要求の一部としてサポートされます。

Sx 変更要求の一部としてサポートされる新しい IE は次のとおりです。

- Create Traffic Endpoint IE
- Update Traffic Endpoint IE
- Remove Traffic Endpoint IE

PDR の作成では、この PDR が関連付けられているベアラーの入力または出力トラフィック エンドポイントを識別する新しい IE であるトラフィックエンドポイント ID がサポートされています。

新しい IE である Created Traffic Endpoint IE は、Sx 確立応答および の Sx 変更応答メッセージの一部としてサポートされます。

Create Traffic Endpoint IE

Pure-P コールでサポートされている Create Traffic Endpoint IE の IE は次のとおりです。

- トラフィックエンドポイント ID
- ローカル F-TEID
- ネットワークインスタンス
- UE IP アドレス

Pure-S コールでサポートされている Create Traffic Endpoint IE の IE は次のとおりです。

- トラフィックエンドポイント ID
- ローカル F-TEID

注：ネットワークインスタンスおよび UE IP アドレス IE は、現在 Pure-S コールではサポートされていません。

Collapsed コールの場合、Sxa トラフィックエンドポイントには S-GW に関連する IE があり、Sxb トラフィックエンドポイントには P-GW に関連する IE があります。

3GPP 標準で定義された IE に加えて、「Bearer Info IE」と呼ばれるプライベート IE が Create Traffic Endpoint に追加されます。対象には次のものが含まれます。

- 作成されるベアラーの QCI。
- 作成されるベアラーの ARP。
- 作成されるベアラーの課金 ID。

Pure-S コールの場合、その PDN のベアラーごとに作成される 2 つのトラフィックエンドポイントがあります。

1. 入力トラフィックエンドポイントのトラフィックエンドポイントを作成します。これは、入力 F-TEID 用に送信され、ベアラーの入力 S-GW PDR によって参照されます。
2. 出力トラフィックエンドポイントのトラフィックエンドポイントを作成します。これは、出力 F-TEID 用に送信され、ベアラーの出力 S-GW PDR によって参照されます。

Pure-S コールの場合、ベアラーの入力および出力トラフィックエンドポイント ID に基づいて、ユーザープレーンでベアラーは一意に識別されます。トラフィックエンドポイントには、ベアラーの QCI、ARP、および課金 ID も保存されます。

Pure-P コールの場合、その PDN のベアラーごとに 1 つのトラフィックエンドポイントのみが作成されます。入力トラフィックエンドポイントのトラフィックエンドポイントを作成します。これは、入力 F-TEID 用に送信され、ベアラーの入力 PDR によって参照されます。P-GW 出力にはトンネルエンドポイント ID が割り当てられていないため、Pure-P コール用に作成される個別の出力トラフィックエンドポイントはありません。同じトラフィックエンドポイントが、ベアラーの入力と出力の両方の PDR によって参照されます。ベアラーのトラフィックエンドポイント ID に基づいて、ユーザープレーンでベアラーは一意に識別されます。トラフィックエンドポイントには、ベアラーの QCI、ARP、および課金 ID も保存されます。

Collapsed コールの場合、各ベアラーのコールの S-GW レッグ用に作成される 2 つのトラフィックエンドポイントがあります。そのため、2 つの Create Traffic Endpoints が入力と出力に送信されます。Sxa PDR は、方向（入力または出力）に基づいてこれらのトラフィックエンドポイントを参照します。各ベアラーのコールの P-GW レッグに対して 1 つのトラフィックエンドポイントのみが作成されます。同じトラフィックエンドポイント ID が、ベアラーのすべての Sxb PDR によって参照されます。P-GW の場合、Create Traffic Endpoint が入力に対して送信されます。Sxa および Sxb PDR のトラフィックエンドポイント ID によって、ベアラーが識別されます。

Created Traffic Endpoint IE

この IE は、Sx 確立および Sx 変更応答に存在し、作成されたさまざまなトラフィックエンドポイントのユーザープレーンによってローカルに割り当てられた F-TEID についてコントロールプレーンに通知します。

Created Traffic Endpoint IE の IE は次のとおりです。

- トラフィックエンドポイント ID
- ローカル F-TEID

Created Traffic Endpoint IE で受信した情報はコントロールプレーンによって処理され、ユーザープレーンによって割り当てられた F-TEID は、入力と出力のコントロールプレーンに適宜保存されます。

Update Traffic Endpoint IE

この IE は、ユーザープレーンのトラフィックエンドポイント情報を更新するために Sx 変更要求に存在します。

Update Traffic Endpoint IE の IE は次のとおりです。

- トラフィックエンドポイント ID
- ローカル F-TEID
- ネットワークインスタンス
- UE IP アドレス
- 3GPP 標準で定義された IE に加えて、「Bearer Info IE」と呼ばれるプライベート IE が Create Traffic Endpoint に追加されます。対象には次のものが含まれます。
- ベアラーの QCI
- ベアラーの ARP
- ベアラーの課金 ID

注：現在、Update Traffic Endpoint IE は、Bearer Info IE などのプライベート IE 拡張機能の更新のみをサポートしています。ローカル F-TEID、ネットワークインスタンス、UE IP アドレスなどの他の情報の更新が必要な使用例はありません。

特定のベアラー EPS ベアラー ID（EBI）の QCI/ARP が変更されると、変更された QCI/ARP が課金 ID とともに、Update Traffic Endpoint IE を使用してユーザープレーンに伝達されます。特定のトラフィックエンドポイント ID は、ユーザープレーンで正常に作成された場合にのみ更新できます。

Remove Traffic Endpoint IE

この IE は、トラフィックエンドポイントを削除するための Sx 変更要求に存在します。トラフィック エンドポイント ID は、Remove Traffic Endpoint IE に含まれています。特定のトラフィックエンドポイント ID は、ユーザープレーンで正常に作成された場合にのみ削除できます。

Pure-S、Pure-P、および Collapsed コールの場合、ベアラーがコントロールプレーンで削除されると、ベアラーに関連付けられているトラフィックエンドポイントは、トラフィックエンドポイント削除機能によって削除されます。そのベアラーで PDR 削除と FAR 削除を送信するための明示的な要件はありません。

ユーザープレーンでは、Pure-S コールの場合、トラフィックエンドポイント削除機能により、そのベアラーのすべての PDR、FAR、および URR が削除されます。Pure-P コールと Collapsed

コールの場合、トラフィックエンドポイント削除機能により、そのベアラーのすべての PDR、FAR、QER、および URR が削除されます。

PDR 作成での PDI の変更

PDI 最適化が PDN に対して有効になっている場合、トラフィックエンドポイント ID は、PDN のベアラーに関するすべての PDR の PDI フィールドに設定されます。F-TEID、PDN インスタンス、UE IP アドレスなどの PDI フィールドは入力されていないため、これらのフィールドはユーザープレーンで検証され、検証に失敗した場合はエラーメッセージが投稿されます。これは、Sxa、Sxb、Sxab、N4、Sxc などのすべてのインターフェイスに当てはまります。

ユーザープレーンでの PDI 最適化の変更

Create Traffic Endpoint の処理

Create Traffic Endpoint を受信すると、IE の内容の正確さが検証されます。正しくない場合、エラーメッセージがコントロールプレーンに送信されます。

検証は、次の場合に失敗します。

- 基本的な IE 検証が失敗した場合。
- このトラフィックエンドポイント ID のトラフィックエンドポイントが存在する場合。
- トラフィックエンドポイント内の F-TEID IE で CH ビットが設定されていない場合。
- PDN インスタンスが無効な場合。
- UE IP アドレスが無効な場合。

Create Traffic Endpoint が正常に処理されると、ローカル F-TEID がユーザープレーンによって割り当てられて、トラフィックエンドポイントに関連付けられます。Created Traffic Endpoint は、F-TEID 情報とトラフィックエンドポイント ID とともに、このトラフィックエンドポイントのコントロールプレーンに返送されます。

Sx 確立要求のユーザープレーンで Create Traffic Endpoint リストが処理されると、Sx セッションのライフタイムの間、PDI 最適化が有効になり、途中で変更できません。

トラフィックエンドポイントの更新の処理

[Update Traffic Endpoint] を受信すると、この IE の内容が正しいかどうかが検証されます。正しくない場合、エラーメッセージがコントロールプレーンに送信されます。

検証は、次の場合に失敗します。

- 基本的な IE 検証が失敗した場合。
- トラフィックエンドポイント ID に合致するトラフィックエンドポイントが存在しない場合。

注：現在、[Update Traffic Endpoint] で更新されるのは、ユーザープレーンの QCI、ARP、課金 ID などのベアラー情報のみです。その他のトラフィック エンドポイント パラメータの更新は、サポートされていません。

トラフィックエンドポイントの削除の処理

[Remove Traffic Endpoint] を受信すると、この IE の内容が正しいかどうかが検証されます。正しくない場合、エラーメッセージがコントロールプレーンに送信されます。

検証は、次の場合に失敗します。

- 基本的な IE 検証が失敗した場合。
- トラフィックエンドポイント ID に合致するトラフィックエンドポイントが存在しない場合。

[Remove Traffic Endpoint] を受信すると、トラフィック エンドポイントに関連付けられている PDR、PDR に関連付けられている FAR、PDR に関連付けられている QER、および PDR に関連付けられている URR も削除されます。

ベアラーを削除するため、コントロールプレーンは、ベアラーに関連付けられているトラフィックエンドポイントに対して [Remove Traffic Endpoints] を送信します。すると、ユーザープレーン上のベアラー関連データがクリーンアップされます。

コントロールプレーンは、ベアラーの削除にあたり、[Remove PDRs]、[Remove FARS]、[Remove QERS]、[Remove URRs] を明示的に送信しません。ただし、コントロールプレーンから [Remove Traffic Endpoints] とともに [Remove PDRs]、[Remove FARS]、[Remove QERS]、[Remove URRs] が送信されたとしても、メッセージは受け付けられ、正常に処理されます。

PDR 作成の処理

Sx セッションで PDI 最適化が有効になっている場合、トラフィックエンドポイント ID は Create PDR に設定されます。有効になっていない場合は、エラー応答がコントロールプレーンに返されます。Create PDR の検証は、次の場合に失敗します。

- 基本的な IE 検証が失敗した場合。
- Create PDR の PDI IE にトラフィックエンドポイント ID が設定されていない場合。
- Create PDR の PDI IE に有効な F-TEID IE がある場合。
- Create PDR の PDI IE に有効な PDN インスタンス IE がある場合。
- Create PDR の PDI IE に有効な UE IP アドレス IE がある場合。

PDI 最適化が無効になっている Sx セッションの場合、Create PDR は他のさまざまなフィールドに対して検証されます。トラフィックエンドポイント ID が PDI で有効な場合、PDI 最適化が無効になっている Sx セッションにトラフィックエンドポイント ID が存在してはならないため、エラー応答がコントロールプレーンに返されます。

セッションリカバリと ICSR

コントロール プレーン

セッションリカバリと ICSR は、PDN の全ベアラーのトラフィックエンドポイント ID でサポートされます。トラフィックエンドポイント ID は、特定の PDN のすべてのベアラーを対象として回復されます。これは、Pure-S、Pure-P、および Collapsed コールでサポートされます。これにより、PDN の PDI 最適化有効ステータスも回復されます。フルチェックポイントは、ベアラーのトラフィックエンドポイント ID のチェックポインティングとリカバリに使用されます。

ユーザープレーン

セッションリカバリと ICSR は、全ベアラーのユーザープレーンのトラフィックエンドポイントでサポートされます。特定の Sx セッションに関連付けられているすべてのトラフィックエンドポイントが回復されます。特定のトラフィックエンドポイントの関連する PDR リストも回復されます。特定の PDR の関連するトラフィックエンドポイント ID が回復されます。

標準準拠

PDI 最適化機能は、次の標準規格に準拠しています：3GPP TS 29.244 V15.5.0 (Interface between the Control Plane and the User Plane Nodes)

制限事項

PDI 最適化機能には、次の制限事項があります。

- ネットワークインスタンス IE および UE IP アドレス IE は、現在 Pure-S コールではサポートされていません。
- Update Traffic Endpoint IE は、Bearer Info IE などのプライベート IE 拡張機能の更新のみをサポートします。ローカル F-TEID、ネットワークインスタンス、UE IP アドレスなど、その他の情報の更新はサポートされていません。
- Update Traffic Endpoint で更新されるのは、ユーザープレーンの [QCI]、[ARP]、[Charging ID] などのベアラー情報のみです。その他のトラフィックエンドポイントパラメータの更新は、サポートされていません。

PDI 最適化機能の設定

ここでは、PDIX 最適化機能を設定する方法について説明します。

PDI 最適化の有効化

この機能を有効にするには、次の CLI コマンドを使用します。

```
configure
  context context_name
    sx-service service_name
      [ no ] sx-protocol pdi-optimization
      end
```

注：

- **no**：PDI 最適化を無効にします。
- デフォルトでは、この CLI は無効になっています。
- PDI最適化は、PDN レベルで有効化または無効化されます。PDI 最適化は Sx サービス の設定に基づいて各 PDN に対して有効になります。コントロールプレーンでの Sx 確立要求の処理中にこの設定が有効になっている場合、PDN は PDI 最適化に対応します。
- 設定を変更しても、PDN には影響しません。Sx 確立要求の処理中に適用される設定は、PDN のライフタイム全体にわたって維持されます。マルチ PDN コールでは、PDN のセットアップ中に各 PDN に設定が適用されます。
- ユーザープレーンには、PDN で PDI 最適化が有効になっているかどうかを判断するための個別の設定はありません。Create Traffic Endpoint IE が Sx セッションの Sx 確立要求で受信されると、Sx セッションはセッションのライフタイム全体で PDI 最適化が有効になっていると見なされます。これは途中で動的に変更されることはなく、その通りに検証が行われます。検証に失敗した場合は、エラー応答がコントロールプレーンに送り返されます。
- 同じトラフィックエンドポイント ID を持つ複数の Create Traffic Endpoint IE がある場合、最初の Create Traffic Endpoint IE が処理され、残りは無視されます。同じ動作が、Created Traffic Endpoint IE、Update Traffic Endpoint IE、および Remove Traffic Endpoint IE に適用されます。

PDI 最適化機能の設定の検証

PDI 最適化機能が有効か無効かを確認するには、**show sx-service all** CLI コマンドを使用します。この show コマンドの出力が拡張され、次の情報が表示されるようになりました。

- SX PDI Optimisation: [Enabled/Disabled]

PDI 最適化 OAM のサポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

show コマンドのサポート

PDI 最適化機能をサポートする、次の show CLI コマンドを使用できます。

show subscribers user-plane-only callid <call_id> pdr all

この CLI コマンドの出力は、次のフィールドを表示するように拡張されました。Associated Create Traffic Endpoint -ID(s)

show subscribers user-plane-only callid <call_id> pdr full all

この CLI コマンドの出力範囲が拡張され、次のフィールドが表示されるようになりました。

- Create Traffic Endpoint-ID
  - Bearer QOS
    - QCI
    - ARP
    - Charging Id

第 69 章

CUPS の P-GW CDR

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

CUPS アーキテクチャに、custom24 GTPP ディクショナリの P-GW CDR 生成のサポートが追加されました。

P-GW CDR は、次の手順とシナリオに対して生成されます。

- デフォルトベアラー：
  - 音量/時間制限
  - PCRF によって開始されたルールベースの変更
  - S1 ハンドオーバーによる S-GW/PLMN の変更
  - ULI/タイムゾーンの変更
  - QoS の変更
  - UE やネットワークで開始されたセッションの削除

- RAN-NAS 原因コード
- maximum change condition トリガー

- 専用ベアラー：
  - 音量/時間制限
  - QoS の変更
  - ハンドオーバー手順
  - ULI/タイムゾーンの変更
  - PCRF ルールベースの変更
  - UE やネットワークで開始された専用ベアラーの削除手順
  - RAN-NAS 原因コード

（注） Gi のコンテキスト ID と課金コンテキストが CP と UP の両方で一致すると、CDR で正しいボリュームが報告されます。ID が一致しない場合、CDR で報告されるボリュームはゼロになります。

制限事項

aFRecordInformation は、CUPS アーキテクチャではサポートされません。

P-GW CDR のユーザーロケーション情報

P-GW CDR には、次の 2 つの属性フィールドにユーザーロケーション情報（ULI）が含まれています。

- User Location Information (32)
- User Location Information (34-0-20)

現行の動作に従い、上記の 2 つのフィールドに P-GW CDR の「ユーザーロケーション情報」が含まれています。これらのフィールドは、ULI-change trigger が有効になっている場合のみ更新されます。ULI-change trigger が設定されていない場合、P-GW CDR は、[Radio Access Technology] が変更された後でも、初回 CDR で報告されたままのユーザーロケーションを保持します。

この問題を解決するために、この機能が導入され、ULI-change trigger が無効になっている場合でも、すべての CDR に最新の「ユーザーロケーション情報」が含まれるようになります。この機能の機能概要は次のとおりです。

- この機能により、P-GW CDR は、MME および S-GW によって提供される最新のユーザーロケーション情報を使用して、[User Location Information (32)] と [User Location Information (34-0-20)] の属性を更新できます。
- 機能の実装は、機能に固有のさまざまなフィラー関数を介して行われます。
- この機能を使用するには、お客様/ユーザーによるソフトウェアの変更（2か所）が必要になります。1つ目は、新たに実装されたフィラー関数を使用したCDRカスタムディクショナリ/お客様のディクショナリの ULI フィールドの更新です。現在の実装は、要件に従い [custom dictionary 38] にあります。並行して、同じディクショナリのサポートをマクロ「ACS_CHK_DICT_SUPPORT_FOR_LATEST_ULI」に追加する必要があります。

新しいフィラー関数を含むディクショナリを使用すると、次のイベントが発生した場合に最新の ULI がパッキングされます。

サブスクライバの PGW-CDR の一部を送信/生成するイベント：

- QoSの変更回数またはタリフ時間の変更回数が、設定された課金条件の変更回数の上限に達した場合。
- それまでは、変更のたびにサービスコンテナが CDR に追加されます。
- [interval x] を使用して設定された x 秒ごと。
- [volume x]（アップ/ダウン/合計）を使用して設定された x オクテットごと。
- コマンド gtpp interim now active-configured egcdr。
- 新しい S-GW/SGSN へのコンテキストの転送（サービングノードの変更）。
- 同じ P-GW 内のアクセスタイプの変更（RAT の変更）。

サブスクライバの最終的な P-GW CDR を送信または生成するイベント：

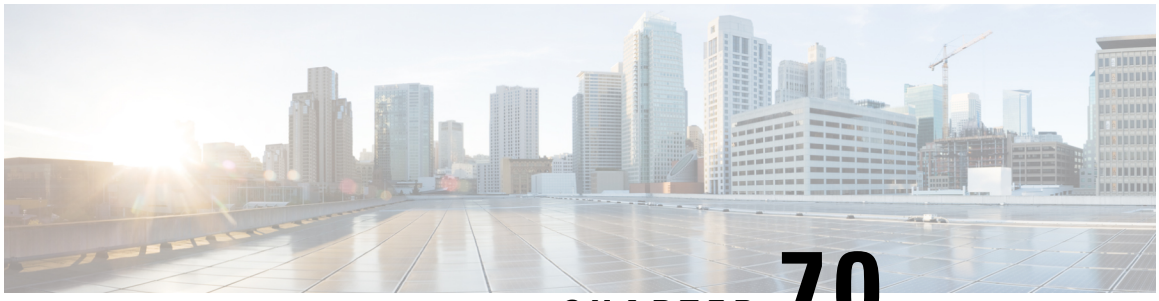
- UE から受信した接続解除要求
- S-GW から受信したベアラーコンテキスト削除要求
- サブスクライバの手動クリア
- パス障害などの異常による解放

設定例

以下に設定例を示します。

```
Customer dictionary: custom38
Customer running configuration:
    gtpp group pgwhdd
      gtpp attribute local-record-sequence-number
      gtpp attribute node-id-suffix PGW11
      no gtpp attribute twanuli
      gtpp dictionary custom38
      no gtpp trigger dcca
      no gtpp trigger service-idle-out
```

```
      no gtpp trigger serving-node-change-limit
      no gtpp trigger inter-plmn-sgsn-change
      no gtpp trigger qos-change
      no gtpp trigger ms-timezone-change
      gtpp trigger egcdr max-losdv
      no gtpp trigger uli-change
      gtpp egcdr lotdv-max-containers 1
      gtpp egcdr losdv-max-containers 1
      gtpp suppress-cdrs zero-volume-and-duration gcdrs egcdrs
      gtpp egcdr service-data-flow threshold interval 43200
     gtpp egcdr service-data-flow threshold volume total 104857600
     gtpp storage-server mode local
gtpp storage-server local file purge-processed-files file-name-pattern

                ACQ* purge-interval 2880
      gtpp storage-server local file format custom3
      gtpp storage-server local file rotation volume mb 30
      gtpp storage-server local file rotation cdr-count 65000
      gtpp storage-server local file rotation time-interval 600
      gtpp storage-server local file name prefix PGW11_Laca
    #exit.
```



CHAPTER 70

P-GW 再起動通知

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

P-GW パス障害時の Sx インターフェイスを介した UP 通信では、P-GW 再起動通知（PRN）手順がサポートされています。P-GW 再起動通知手順で、P-GW の障害が検出されたときに S11/S4 インターフェイスに関連するシグナリングの量を最適化します。

PRN 手順は、P-GW 障害の検出を MME/S4-SGSN に通知するために S-GW でサポートされる標準ベースの手順です。

P-GW の障害検出は、（再起動した P-GW から受信した再起動カウンタに基づき）P-GW が再起動したことを検出した場合、または（パス障害検出に基づき）P-GW に障害が発生したが再起動していないことを検出した場合に S-GW で実行されます。

S-GW は、ピア P-GW が再起動したことを検出すると、障害が発生した P-GW に関連付けられているすべての PDN 接続とベアラーコンテキストをローカルに削除し、P-GW 再起動通知を介して MME に通知します。

S-GW は、S11/S4 インターフェイスのエコー要求/応答で、P-GW 再起動通知手順がサポートされていることを示します。

P-GW 再起動通知手順はオプションの手順であり、MME/S4-SGSN と S-GW の両方のピアでサポートされている場合にのみ呼び出されます。

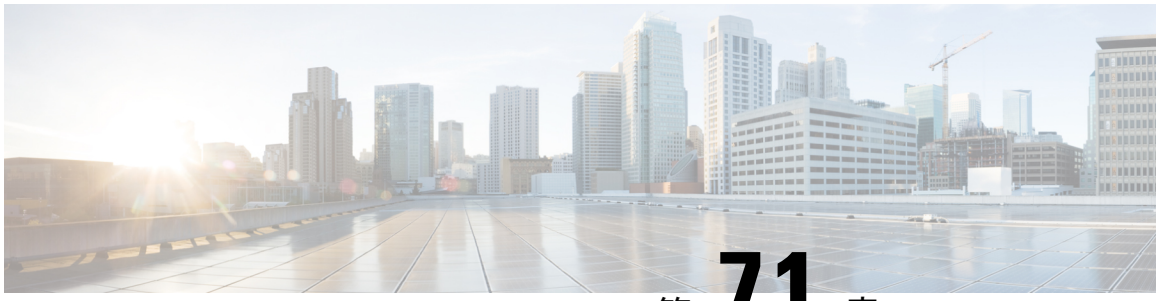
この手順がない場合、S-GW は削除手順を開始して、障害が発生した P-GW にアンカーされているすべての PDN をクリーンアップします。その結果、複数の PDN で S-GW および P-GW が使用されている場合、S11/S4 で GTP メッセージがフラッディングします。

次の図は、パス障害時の PRN フローを示しています。

CUPS では、パス障害が検出されると、次のようになります。

画像はこちら

- S5 パス障害を検出すると、S-GW と MME で PRN 機能がサポートされている場合、S-GW が PRN 処理を開始します。
- パス障害セッションの場合、S-GW は MME に PRN メッセージを送信していない場合、MME ごとに 1 回 PRN メッセージを送信します。
- パス障害セッションの場合、S-GW CP は FAR アクション（DROP）で Sx 変更を送信します。
- S-GW CP は、Sx 変更応答を受信すると、Sx 削除要求を UP に送信します。



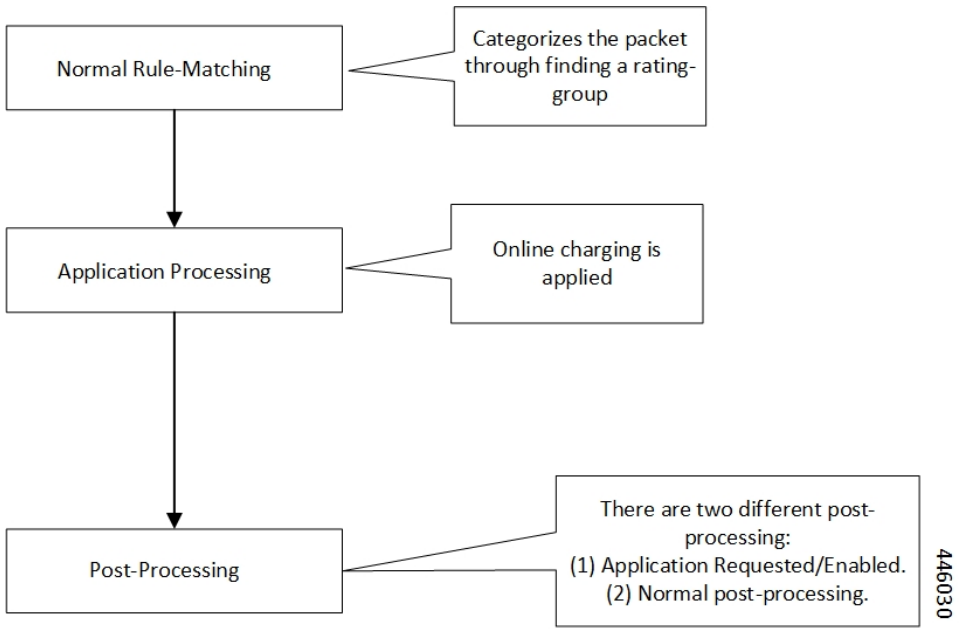
第 71 章

DCCA の後処理のインタラクション

機能説明

次の図は、パケット処理について説明しています。

図 *43 : DCCA* の後処理のインタラクション



通常ルールの照合

このフェーズでは、受信パケットとボックスで設定されたルールとの比較が行われます。このルール照合プロセスでは、パケットの分類のみを行います。ボックスの [Rule Matching] 設定には、次の CLI を使用します。

action priority *<priority-number>* **ruledef** *<ruledef-name>*
charging-action *<charging-action>*

優先順位に基づいて、パケットのルール照合が行われます。一致する最初のルールによってパケットを分類します。

対応する課金アクションがパケットに適用されます。課金アクションの設定に「cca charging credit」が含まれている場合、オンライン課金がトリガーされ、そのパケットが DCCA アプリケーションに移動します。

アプリケーション処理

パケットが DCCA アプリケーションに到達すると、パケットのクォータ（評価グループ/コンテンツ ID）がチェックされ、必要な処理が行われます。その評価グループのクレジットがなくなると、パケットに対して Final-Unit-Action が実行されます。その評価グループに no-credit が存在する場合、DCCA はその評価グループをブラックリストに登録することもできます。アプリケーションがブラックリストに登録されている場合、パケットは破棄またはドロップとしてマークされ、ACS mgr に通知するために disposition-action に入ります。クォータが存在する場合、パケットは転送されます。DCCA アプリケーションは、代わりに、後処理ルールやフィルタリストを入力し、後処理のためにパケットをマークできます。後処理は、OCS が、Final-Unit-Indication AVP とともにフィルタ ID またはフィルタルールの適用を要求したときに発生します。パケットの DCCA アプリケーション処理が完了すると、パケットは ACS mgr に戻ります。

後処理

アプリケーションからパケットが返ると、ACS MGR が DCCA アプリケーションによって設定された廃棄アクション値を確認します。破棄対象としてマークされている場合は、パケットは破棄されます。

- アプリケーションからの要求による後処理：廃棄アクションが PP_RESTRICTION_RULE または PP_FILTER_ID に適用される場合、content-id/rated-group に対応する restrict-rules-list または restrict-filter-id-list の取得を試行し、後処理を適用します。パケットは、下記の後処理（一般的な後処理）を試行しません。
  - ACS_CONTROL_PP_RESTRICTION_RULE：この廃棄アクションは、RFC 4006 に従って、Final-Unit-Indication Grouped-AVP 内で DCCA が OCS から送信された制限フィルタルールをアクティブ化する場合に適用されます。制限フィルタルールは、「fui_restrict_access」内の「restriction_list」に適用されます。
  - ACS_CONTROL_PP_FILTER_ID：この廃棄アクションは、RFC4006 に従って、DCCA が [Filter-Id] をアクティブ化する場合に、Final-Unit-Indication grouped-AVP 内の OCS に適用されます。Filter-Id はルール定義名であり、「fui_restrict_access」内の「filter_id_list」に適用されます。

    DCCA アプリケーションは、どちらの廃棄アクションも設定できます。[Disposition-action] はビットマスクにすぎません。

これらの後処理制限ルールまたは後処理フィルタ ID は、OCS から取得され、DCCA アプリケーションによって有効化/アクティブ化されます。このルールは、評価グループ固有のルールです。ルール照合は、OCS が送信する順序で行われます。

各 acs_sub_sess に、「service_id & rating_group」で指数付けされた「dcca_mscc_fui_restrict_access_t」のリストがあります。この組み合わせごとに、前述のタイプ構造体が存在します。この「dcca_mscc_fui_restrict_access_t」構造体には、「filter_id_list」リストと「fui_restrict_access」リストが含まれています。この構造体は、デフォルトでは空になります。DCCA アプリケーションは、特定のサービス ID と評価グループに対応した後処理のフィルタリングをアクティブ化するときに、この構造体に入力できます。

- 一般的な後処理：転送の場合、後処理が開始されます。後処理において、パケットは、Boxer で設定された後処理ルールと照合されます。

  次の CLI を使用して、Boxer で後処理ルールを設定します。

  Post processing priority *<priority-number> ruledef* **<ruledef-name> charging-action** *<charging-action-name>*

  これらの後処理ルールは、優先順位の番号順にパケットと照合されます.

制限に達した後処理

前述の 2 つのディスポジションアクション値に加えて、制限に達したシナリオにはもう 1 つの値 ACS_CONTROL_PP_LIMIT_REACHED があります。ここでの limit-reached は、ユーザーのクォータ制限が終了したことを示します。ユーザークォータを超えると、パケットはデフォルトでアプリケーションによってドロップされ、後処理は適用されません。この制限に達して後処理の設定が行われるシナリオや、このクォータを使い果たしたシナリオであっても、この機能を使用して制御を追加できます。

制限に達したり、クォータを使い果たしたパケットの後処理を有効にするための設定オプションを使用できます。この設定には、次の CLI を使用します。

```
configure
  active-charging service service_name
    rulebase rulebase_name
      post-processing policy { always | not-for-dynamic-discard }
      end
```

「not-for-dynamic-discard」オプションがデフォルトのオプションです。このオプションは、制限に達した/クォータを使い果たしたシナリオには後処理が適用されないことを示します。

「post processing policy always」CLI の場合、制限に達した/クォータを使い果たしたシナリオに後処理ルールが適用されます。ディスポジションアクションの「ACS_CONTROL_PP_LIMIT_REACHED」値は、この動作について通知するためのものです。後処理で優先順位ベースのルールがある場合は、リダイレクトルールをチェックし、それ以外の場合はデフォルトでパケットを破棄します。これらの制限に達したパケットには、転送、ネクストホップ、X ヘッダー挿入などの他の後処理アクションは適用されません。

後処理の設定

limit-reached ケースを含む後処理 ruledef には、「rule-application post processing」オプションとともに「cca qutoa-state = limit-reached」が設定されています。この設定は、この ruledef が limit-reached シナリオ用であることを示します。

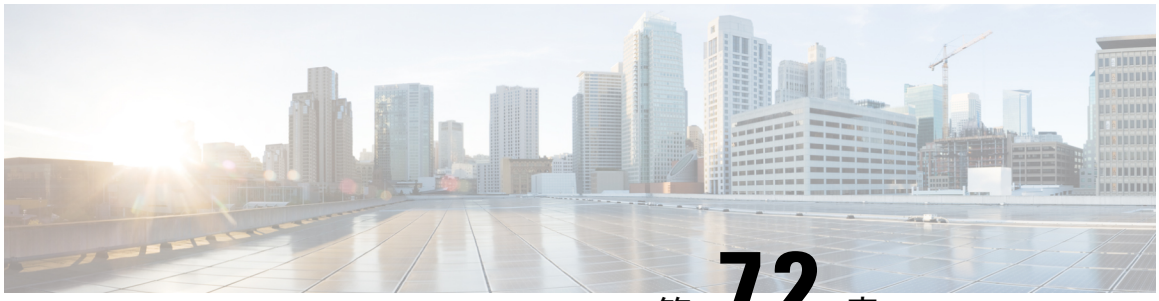
```
ruledef http_low
  http any-match = TRUE
  cca quota-state = limit-reached
  rule-application postprocessing
#exit
```

対応する課金アクションには、「flow action redirect」設定があります。他のフローアクション値は、limit-reached シナリオでは無効です。

```
charging-action redirect
  flow action redirect-url http://webpages/index.html
#exit
```

limit-reached 後処理ルールの優先順位が高くなるように、ルールベースで後処理優先順位ルールを設定するため、パケットは最初に limit-reached ruledef に一致します。

```
rulebase base1
  .................................
  post processing priority 1 ruledef http_low charging-action redirect
#exit
```



第 72 章

VoLTE コールの優先順位リカバリのサポート

機能の概要と変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

この機能により、通常のコールよりも、アクティブおよび非アクティブな VoLTE コールを優先できます。優先されるのは、ユーザープレーンの障害によるコールのリカバリです。

関係

この機能は、*CUPS* における *VoLTE* のサポートに関連しています。

機能の仕組み

ユーザープレーンには、次の 2 種類のセッションがあります。

- 通常セッション
- 優先セッション

優先セッション：Sx セッションの確立または変更要求中にコントロールプレーンから受信した PFCP ヘッダーに設定されている MP（メッセージの優先順位）ビット。リカバリの場合は、優先セッションが優先されます。通常のコールは、優先されたコールのリカバリ完了後に初めて回復されます。

コントロールプレーンでは、MP（最初のオクテットの 2 番目のビット）とともに PFCP ヘッダーでメッセージの優先順位（16番目のオクテットの上位ニブル）を設定します。現在、EMPS コールのメッセージの優先順位は 1 です。同様に、VoLTE アクティブコールのメッセージの優先順位は 2、VoLTE 非アクティブコールのメッセージの優先順位は 3 です。次の図は、さまざまなコールの PFCP ヘッダー形式のメッセージの優先順位を示しています。

	ビット							
オクテット	8	7	6	5	4	3	2	1
1	Version			予備	予備	予備	MP = 1	S = 1
2	メッセージ タイプ							
3	メッセージ長（第 1 オクテット）							
4	メッセージ長（第 2 オクテット）							
5	セッションエンドポイント識別子（第 1 オクテット）							
6	セッションエンドポイント識別子（第 2 オクテット）							
7	セッションエンドポイント識別子（第 3 オクテット）							
8	セッションエンドポイント識別子（第 4 オクテット）							
9	セッションエンドポイント識別子（第 5 オクテット）							
10	セッションエンドポイント識別子（第 6 オクテット）							
11	セッションエンドポイント識別子（第 7 オクテット）							
12	セッションエンドポイント識別子（第 8 オクテット）							
13	シーケンス番号（第 1 オクテット）							
14	シーケンス番号（第 2 オクテット）							
15	シーケンス番号（第 3 オクテット）							

16	メッセージの優先順位 = 1：EMPS/緊急 = 2：VoLTE アクティブコール = 3：VoLTE 非アクティブ	予備

SX セッションの確立または変更要求を受信すると、ユーザープレーンで Sx セッションが優先セッションとしてマークされます。優先順位は、PFCP ヘッダーに入力されたメッセージの優先順位に関するゼロ以外の値（EMPS = 1、VoLTE アクティブ = 2、VoLTE 非アクティブ = 3）に基づいています。

この機能は、VoLTE コールの優先順位リカバリに関する次の側面をサポートします。

コントロールプレーン上：（P-GW、S-GW、SAE-GW、GGSN）

- APN での VoLTE コールの設定
- SX セッション確立要求の PFCP ヘッダーに MP 優先順位ビットとメッセージの優先順位を設定します。
- SX セッション変更要求の PFCP ヘッダーに MP 優先順位ビットとメッセージの優先順位を設定します。

ユーザープレーン上：

- 以前のメッセージに関する PFCP ヘッダーのメッセージの優先順位を確認します。
- メッセージの優先順位が 0 以外の場合は、セッションを優先セッションとしてマークします。
- 優先順位付けされたセッションは、SR/ICSR の後、優先順位付けされていないセッションの前に回復されます。

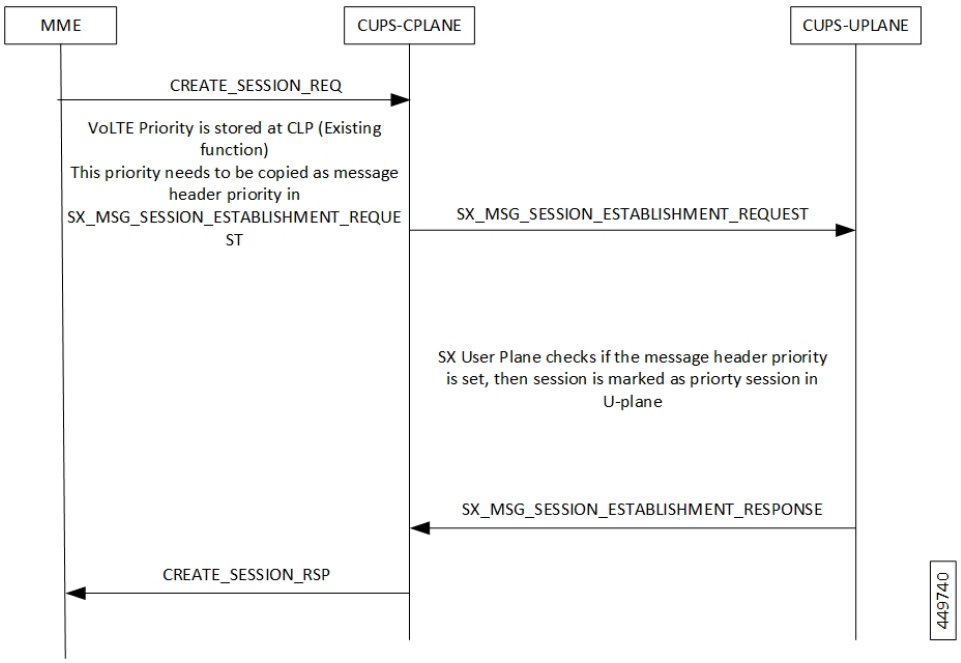
コール フロー

次のコールフローでは、以下の点について説明します。

- セッション確立処理
- セッション変更処理

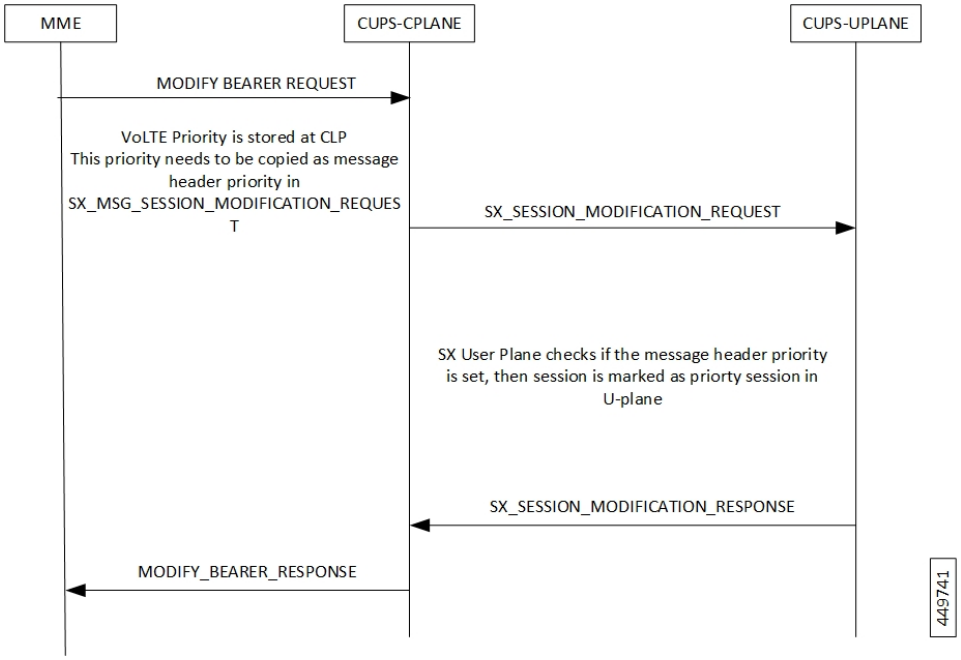
セッション確立処理コールフロー

次のコールフローでは、セッションの確立について説明します。



セッション変更処理コールフロー

次のコールフローでは、セッションの変更について説明します。



設定

Pure-P/Collapsed コールと Pure-S コールの設定は次のとおりです。

Pure-P コールまたは Collapsed コールの設定

Pure-P/Collapsed コールについて、コントロールプレーンでコールを VoLTE としてマークするための設定を次に示します。

```
configure
          context ingress
             apn vrf.com
             qci1 ims-media
             end
```

Pure-S コールの設定

Pure-S/Collapsed コールについて、コントロールプレーンでコールを VoLTE としてマークするための設定を次に示します。

```
configure
          apn profile apn_1
          qci1 ims-media
configure
   operator-policy name intershat
   apn default-apn-profile apn_1
   end
configure
   lte-policy
   subscriber-map map_name
      precedence 1 match-criteria all operator-policy-name intershat
   end
configure
   context ingress
   sgw-service sa_sgw_service
   associate subscriber-map map_name
   end
```

モニタリングおよびトラブルシューティング

この項では、VoLTE コールの優先順位リカバリのモニタリングと障害対応に使用できる CLI コマンドについて説明します。

show コマンドと出力

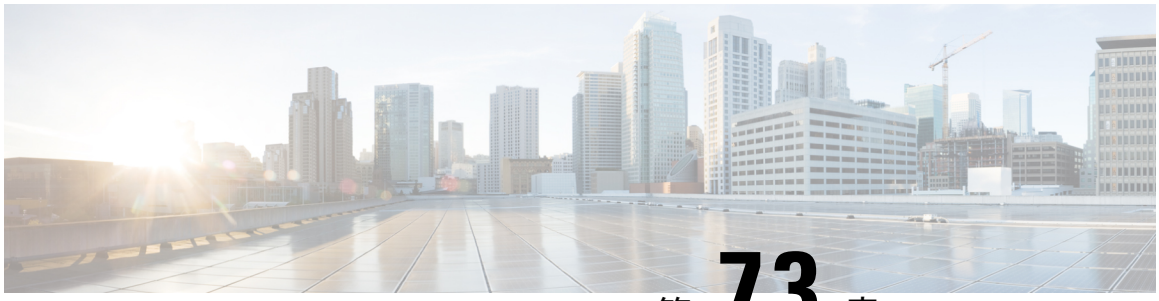
ここでは、ユーザープレーンにおける VoLTE コールの優先順位リカバリをサポートするために使用できる show CLI コマンドについて説明します。

show session subsystem facility sessmgr instance 1 debug-info

```
AAA TCP Connect Succeeded with   : 0    Retries
fetched_from_aaamgr                 : 1    pror_to_audit                  : 1

passed_audit                        : 1    calls_recovered                : 1

calls_recovered_by_tmr              : 1    calls_recovered_by_med         : 0

priority_calls_recoverd_by_med      : 0    non_priority_calls_ignored_by_med: 0
```

show session subsystem facility aaamgr instance 1 debug-info

```
1 Current recovery archives 1 Current valid recovery records
1 Current valid priority recovery records
```



第 73 章

Ruledefs の QoS グループのサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

Ruledef の QoS グループは、QGR または SGQ とも呼ばれます。この機能は、サブスクライバの公正使用ポリシングを有効にします。

機能の仕組み

次の設定では、主にフローステータスと帯域幅制限が階層的に実行されます。最初に一致した課金アクションで実行され、次に QoS グループレベルで実行されます。

```
conf
active-charging service acs
  qos-group-of-ruledefs QGR1
      add-group-of-ruledef group
      add-ruledef http
    #exit
```

```
rulebase cisco
action priority 2 ruledef http charging-action standard
action priority 5 ruledef catchall charging-action standard
route priority 1 ruledef http-rule analyzer http
end
```

PCRF を介して受信した QoS グループ QGR1。

```
qos-group-rule-install
qgr-name QGR2
qgr-mon-key 1
qgr-flow-status 3
qgr-precedence 1
qgr-eqos-information
qgr-eqos-mbr 1000 2000
qgr-eqos-mbr-burst-size 1000 2000
qgr-eqos-mbr-limit-conform-action 1 -1 1 -1
qgr-eqos-mbr-limit-exceed-action 2 7 2 8
```

データパスの適用

1. パケットは ruledef「http」と一致します。
2. 一致した ruledef/group を持つ QGR の有無を確認するために、QGR の照合が実行されます。優先順位が一番高い QGR が返されます。ruledef/group は、静的または定義済みにできます。
3. QGR が一致した場合、フローアクションの適用は最初に課金アクションレベルで実行されてから QGR レベルで実行され、課金アクションでパケットが許可されたと見なされます。パケットがドロップされた場合、QGR レベルフローアクションの適用はスキップされます。
4. QGR のフローアクションでパケットが許可されると、QER の制限がパケットに適用されます。QGR でパケットがドロップされた場合、QER の制限はスキップされます。
5. 同様に、QER の制限は段階的に実行され、最初に課金アクションレベルで実行され、次に QGR でパケット対象が課金アクションで許可されます。

ユーザープレーンへの静的設定のプッシュ

- ECS 要素 ruledef/Charging-action/group-of-ruledefs と同様に、静的設定は PFD メカニズムを介して CP から UP にプッシュされます。
- 「show user-plane-service qos-group-of-ruledefs all/name」の show CLI コマンドにより、ユーザープレーンの静的設定が表示されます。

UPlane への QGR パラメータのプッシュ

QGR は、Session Establishment Request および Session Modification Request とともにプッシュされます。

QGR の名前と優先順位は、プライベート IE で送信されます。フローアクション、帯域幅パラメータ、モニタリングキーにより、新しい FAR、新しい QER、新しい URR がそれぞれ作成されます。

QGR の動的パラメータを変更すると、FAR/QER/URR の更新がトリガーされます。

これは、Session Establishment Request または Session Modification Requestで送信されます。

プライベート IE

```
Qos-Group-Of-Ruledef:
Name:
Operation:  (0 - Add  1 - Modify 2 - Delete)
Precedence:
FAR ID:
URR ID:
QER ID:
```

表 *46 : FAR* 形式

FAR ID	固有 ID
拡張適用アクション	プライベート IE には、Flow-Action Allow、Discard、Uplink、Discard Downlink、Terminate Flow が含まれます。

表 *47 : QER* 形式

QER ID	固有 ID
最大ビットレート:	QGR の MBR（Kbps）： UL MBR： DL MBR：
バースト サイズ	バーストサイズを指定するプライベート IE： UL Burst DL Burst:
適合アクション	適合アクションを設定するプライベート IE： Uplink Action: Uplink ToS: Downlink Action: Downlink ToS:

QER ID	固有 ID
超過アクション	超過アクションを設定するプライベート IE： Uplink Action: Uplink ToS: Downlink Action: Downlink ToS:

「show subscribers user-plane-only callid <> far|qer full all」コマンドを実行すると、FAR、PDR、QER、および URR が表示されます。

UPlane での QGR の処理

- IE「Qos-Group-Of-Ruledef」の受信時に、静的設定で QGR を検索します。QGR の ruledef/group-of-ruledef ごとに、対応する PDR を検索し、受信した QGR FAR/URR/QER ID で FAR/QER リストを更新します。
- UPlane の ruledef/group-of-ruledef PDR ごとに、優先順位の高い QGR の FAR-ID、QER-ID を関連付けます。
- コントロールプレーンと UPlane の両方で QGR マップが維持されます。マップは、QGR 名、優先順位、QER-ID、および FAR-ID で構成されます。必要に応じて、リカバリとルックアップに QGR マップを使用します。

データパスの QGR ヒット

- パケット一致ルール PDR の場合、最も優先順位の高い QGR FAR および QER を検索し、パラメータを適用します。
- flow-status と flow-rate を想定どおりに適用します。
- オフロードされたフローの QGR マッチングが処理されます。
- QGR ヒット統計情報が増加します。

制限事項

QoS Group of Ruledefs（QGR）サポート機能には、次の制限があります。

- URR の作成および適用はサポートされません。
- ダイナミックルールを含む静的 QGR 定義はサポートされません。
- フロー ステータス リダイレクトとフローの強制終了はサポートされません。

- QoS グループ確認アクションを [Drop] 、かつ超過アクションを [ALLOW] または [MARK_DSCP] にすることはサポートされません。
- CP は、PCRF を介して受信した最大 20 の QGR を UP に伝達できます。

モニタリングおよびトラブルシューティング

ここでは、機能のモニタリングと障害対応に使用できる CLI コマンドについて説明します。

show コマンドと出力

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show subscribers user-plane-only full all

この show コマンドの出力範囲が拡張され、この機能をサポートするために導入された次のフィールドが表示されるようになりました。

- Total QoS-Group Active
- QoS-Group Statistics
  - QGR Name
  - Pkts-Down
  - Bytes-Down
  - Pkts-Up
  - Bytes-Up
  - Hits
  - Match-Bypassed
  - FP-Down(Pkts/Bytes)
  - FP-Up(Pkts/Bytes)

show user-plane-service qos-group-of-ruledefs all name

この show コマンドの出力範囲が拡張され、この機能をサポートするために導入された次のフィールドが表示されるようになりました。

QGR 情報リスト

- 値
- QGR の数
- QGR 情報

- NAME
- PRECEDENCE
- OPERATION
- FAR ID
- QER ID

- QGR 情報
  - NAME
  - PRECEDENCE
  - OPERATION
  - FAR ID
  - QER ID

show subscribers user-plane-only callid 00004e21 qos-group all

この show コマンドの出力範囲が拡張され、この機能をサポートするために導入された次のフィールドが表示されるようになりました。

```
Callid: 00004e21
           Interface Type: Sxb
         QGR-Name:      Priority:       FAR-ID:         QER-ID:         URR-ID:
         ---------      ---------       -------         -------         ------


        Total Number of QGRs found:
```

show subscribers user-plane-only callid 00004e21 far full all

この show コマンドの出力範囲が拡張され、この機能をサポートするために導入された次のフィールドが表示されるようになりました。

- QGR との関連付け
  - Extended Apply Action

show subscribers user-plane-only callid 00004e21 qer full all

この show コマンドの出力範囲が拡張され、この機能をサポートするために導入された次のフィールドが表示されるようになりました。

- UL Burst
- UL Conform Action
  - UL DSCP Value
- UL Exceed Action

- UL DSCP Value

- DL バースト
- DL Conform Action
  - DL DSCP Value
- DL Exceed Action
  - DL DSCP Value

show subscribers user-plane-only callid 00004e21 qos-group statistics all name

この show コマンドとその出力は、この機能をサポートするために導入されました。

- フローステータス統計
  - Total Uplink Packets
  - Total Uplink Bytes
  - Uplink Packets Redirected
  - Uplink Bytes Redirected
  - Uplink Packets Dropped
  - Uplink Bytes Dropped
  - Uplink Packets Term-Flow
  - Uplink Bytess Term-Flow
  - Total Downlink Packets
  - Total Downlink Bytes
  - Downlink Packets Redirected
  - Downlink Bytes Redirected
  - Downlink Packets Dropped
  - Downlink Bytes Dropped
  - Downlink Packets Term-Flow
  - Downlink Bytes Term-Flow
- 帯域幅制御の統計
  - Total Uplink Packets
  - Total Uplink Bytes
  - Uplink Packets QoS-Exceed
  - Uplink Bytes QoS-Exceed

- Uplink Packets QoS-Conform
- Uplink Bytes QoS-Conform
- Uplink Packets Dropped
- Uplink Bytes Dropped
- Uplink Packets Marked
- Uplink Bytes Marked
- Total Downlink Packets
- Total Downlink Bytes
- Downlink Packets QoS-Exceed
- Downlink Bytes QoS-Exceed
- Downlink Packets QoS-Conform
- Downlink Bytes QoS-Conform
- Downlink Packets Dropped
- Downlink Bytes Dropped
- Downlink Packets Marked
- Downlink Bytes Marked

- Total qos-group-of-ruledefs matched
- Total subscribers matching specified criteria

show user-plane-service statistics qos-group sessmgr all

Sessmgr Instance

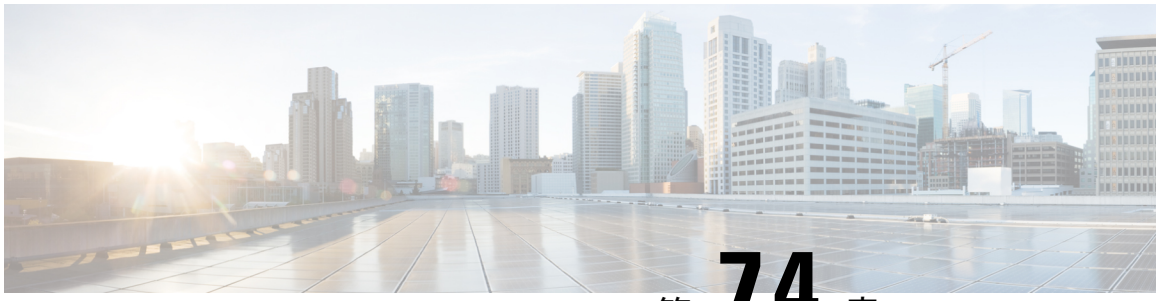
- Total Uplink Pkt
- Total Uplink Bytes
- Uplink FP Pkts
- Uplink FP Bytes
- Total Dnlink Pkts
- Total Dnlink Bytes
- Dnlink FP Pkts
- Dnlink FP Bytes

- フローステータス統計
  - Total Uplink Packets
  - Total Uplink Bytes

- Uplink Packets Redirected
- Uplink Bytes Redirected
- Uplink Packets Dropped
- Uplink Bytes Dropped
- Uplink Packets Term-Flow
- Uplink Bytess Term-Flow
- Total Downlink Packets
- Total Downlink Bytes
- Downlink Packets Redirected
- Downlink Bytes Redirected
- Downlink Packets Dropped
- Downlink Bytes Dropped
- Downlink Packets Term-Flow
- Downlink Bytes Term-Flow

- 帯域幅制御の統計
  - Total Uplink Packets
  - Total Uplink Bytes
  - Uplink Packets QoS-Exceed
  - Uplink Bytes QoS-Exceed
  - Uplink Packets QoS-Conform
  - Uplink Bytes QoS-Conform
  - Uplink Packets Dropped
  - Uplink Bytes Dropped
  - Uplink Packets Marked
  - Uplink Bytes Marked
  - Total Downlink Packets
  - Total Downlink Bytes
  - Downlink Packets QoS-Exceed
  - Downlink Bytes QoS-Exceed
  - Downlink Packets QoS-Conform
  - Downlink Bytes QoS-Conform

- Downlink Packets Dropped
- Downlink Bytes Dropped
- Downlink Packets Marked
- Downlink Bytes Marked



第 74 章

レート制限機能（RLF）

この章は、次の内容で構成されています。

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

RLF機能はさまざまなインターフェイスや製品で使用できる汎用フレームワークを実装し、Gx の Diameter メッセージや PCRF への Gy インターフェイスをはじめとする発信メッセージのレート制限やスロットリングを実現します。

重要 CUPS アーキテクチャにおける CLI コマンドなどの RLF 機能の動作は、CUPS 以外の環境での動作と似ています。

アプリケーションが高いレートでピアにメッセージを送信する場合（多数のセッションが同時にダウンする場合など）、すべてのセッションのアカウンティング停止メッセージが同時に生成されるため、ピアはこのような高レートでメッセージを処理できない可能性があります。この状況を克服するために、レート制限機能（RLF）フレームワークが開発されました。アプリ

ケーションは最適なレートでメッセージを送信するため、ピアはすべてのメッセージを受信でき、過負荷状態になることがありません。

この機能を有効にするには、グローバル コンフィギュレーション モードで **rlf-template** コマンドを使用します。ユーザーは、このテンプレート内でレート制限の設定を定義できます。コマンドの詳細については、『*Command Line Interface Reference*』[英語] を参照してください。

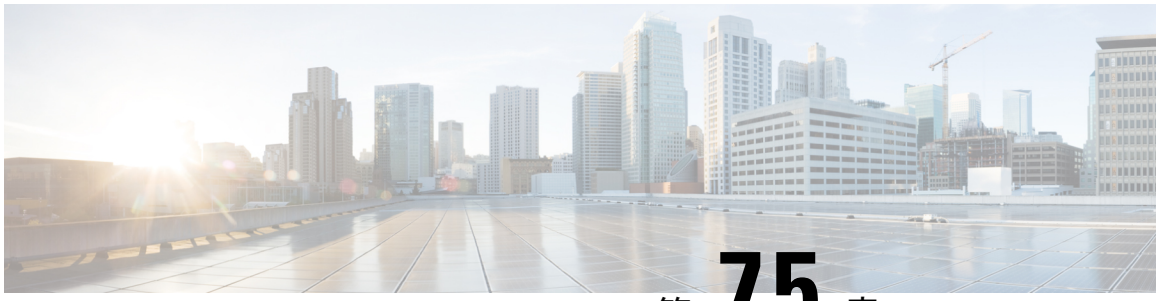
重要 RLF テンプレートが任意のアプリケーション（ピア/エンドポイント）にバインドされている場合は削除できません。

RLF機能が有効になっている場合、アプリケーションから送られたすべてのメッセージは、スロットリングとレートコントロールを行うために RLF モジュールにプッシュされます。設定されたメッセージ レートに応じて、RLF モジュールはピアにメッセージを送信します。レートまたはしきい値に達すると、RLFモジュールはアプリケーションに対して、メッセージの送信速度を下げるか停止するように通知します。ピアに送られるメッセージをさらに受け入れることが可能になった場合にも、RLFモジュールはアプリケーションに通知します。RLFモジュールは通常、トークン バケット アルゴリズムを使用してレート制限を実現します。

現在、Diameter アプリケーション（Gx、Gy など）環境において、多くのオペレータが発信制御トラフィックのレート制限を実現する手段として **max-outstanding** *number* CLI コマンドを使用しています。RLFはすべてのケースでレート制限の処理を行っているため、RLF が設定されている場合は、このコマンドを使用する必要はありません。RLF と **max-outstanding** の両方を使用すると、望ましくない結果が生じる可能性があります。

重要 RLF が **diameter endpoint** とともに使用されると、ピアの **max-outstanding** 値が 255 に設定されます。

テンプレートを使用するには、Diameterまたはその他のアプリケーションをテンプレートに関連付ける必要があります。RLF は、設定された 1 秒あたりのトランザクション数（TPS）でレート制限を実行するためのフレームワークのみを提供します。アプリケーション（Diameter など）は、各アプリケーションに固有の設定を実行する必要があります。



第 75 章

S2a インターフェイスのサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

この参照ポイントは、信頼できる非 3GPP アクセスポイント（信頼できる W-iFi ゲートウェイ（TWAN）/コンバージドアクセス ゲートウェイ（CGW））と PDN ゲートウェイ（P-GW）間のシグナリングとモビリティのサポートを提供することで、ベアラーインターフェイスをサポートします。これは GTP ベースのインターフェイスサポートであり、信頼できる非 3GPP IP アクセスポイントへの接続を可能にします。S2a インターフェイスは、制御とデータの両方に IPv4 と IPv6 を使用します。

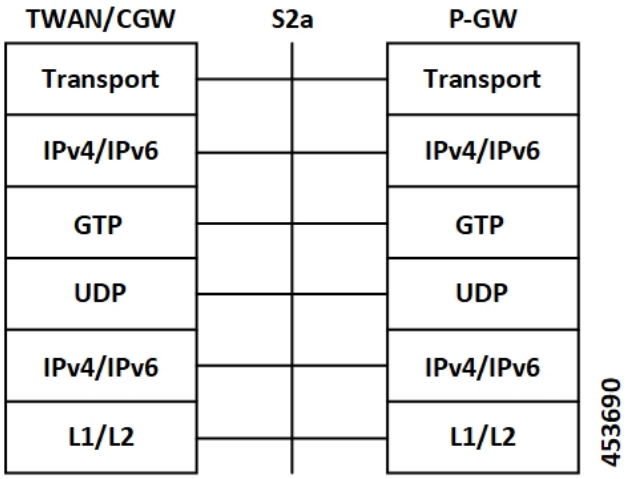
サポートされているプロトコル

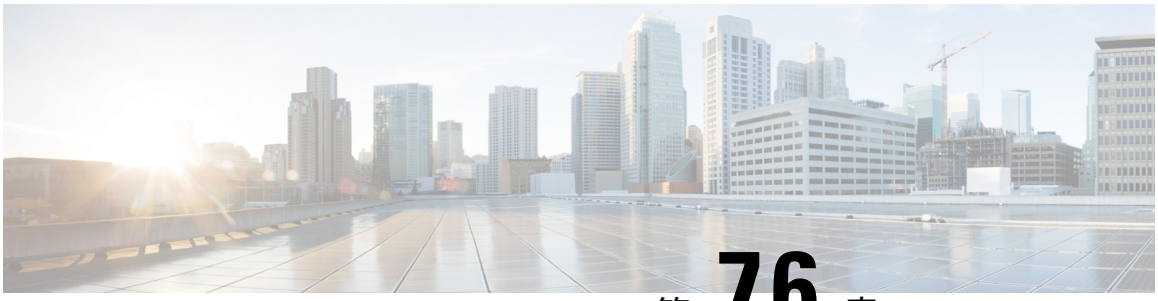
S2a インターフェイスは、次のプロトコルをサポートしています。

- トランスポート層：UDP、TCP
- トンネリング：GTP 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

図 *44 : S2a* インターフェイスでサポートされるプロトコル





第 76 章

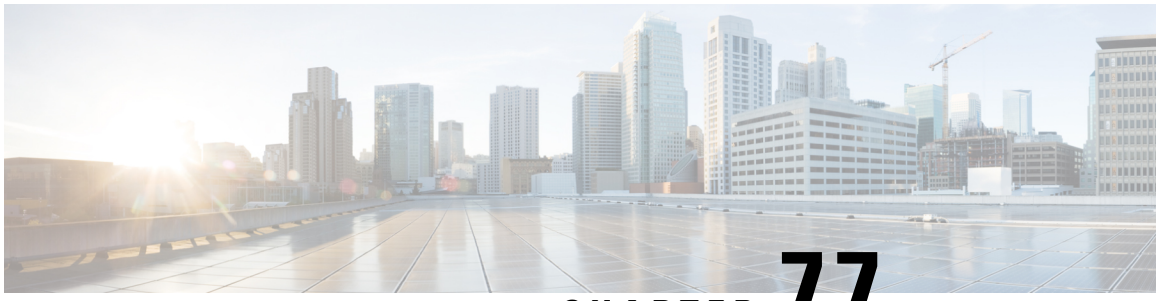
S2b インターフェイスのサポート

機能説明

CUPS アーキテクチャでは、ePDG からの信頼できない Wi-Fi コールが SAEGW（Pure-P）に接続するケースの S2b インターフェイスに対するサポートが追加されました。

現在、次の手順がサポートされています。

- セッション確立のサポート手順：
  - ローミング、非ローミング、および LBO 用の GTP ベースの S2b（3GPP TS 23.402 [4] clause 7.2.4）。
  - GTP ベースの S2b を介した緊急サービス（3GPP TS 23.402 [4] clause 7.2.5）。
  - GTP を使用した信頼できない非 3GPP IP アクセスから追加の PDN への UE 開始接続（3GPP TS 23.402 [4] clause 7.6.3）。
- セッション解放のサポート手順：
  - S2b での GTP を使用した UE/ePDG 開始の切断手順（TS 23.402 [4] clause 7.4.3.1）。
  - S2b での GTP を使用した HSS/AAA 開始の切断手順（TS 23.402 [4] clause 7.4.4.1）。
- ベアラー非アクティブ化のサポート手順：
  - S2b での GTP を使用した P-GW 開始のベアラーの非アクティブ化（TS 23.402 [4] clause 7.9.2）。



CHAPTER 77

CUPS の S-GW CDR

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

CDR 生成は、Cisco UPC CUPS アーキテクチャの S-GW でサポートされています。

CUPS の CDR は、S-GW の UE ベアラーの課金情報を収集するために生成されます。課金トリガーを受信すると、CUPS のコントロールプレーンノードが対応するユーザープレーンノードから情報をプルし、収集されたボリュームカウントが S-GW CDR に追加されます。

S-GW CDR は、デフォルトベアラーと専用ベアラーの両方でサポートされています。

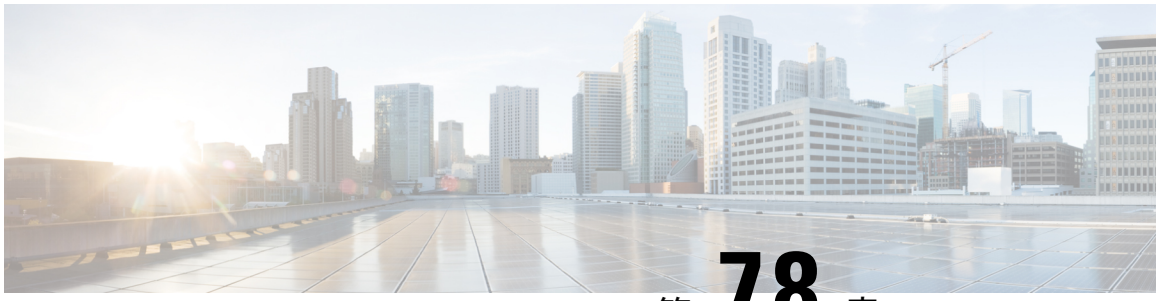
（注） 現在、S-GW CDR は custom24 ディクショナリでサポートされています。

課金データは、次のトリガーに基づいて収集されます。

- アクセス側トリガー：
  - ULI の変更

- RAT の変更
- 管理者による介入（暫定 CDR はサポートされていません）
- 正常/異常コールの解放

- ネットワーク側のトリガー：
  - QCI の変更
  - APN AMBR の変更



第 78 章

S-GW の新規コール拒否

機能説明

この CLI 制御による機能により、サブスクライバタイプ（Roamer、Homer、Visitor）または APN に基づいて Pure-S コールを拒否できます。

（注） この機能は、[CUPS] が有効になっている場合にのみ適用されます。

機能の仕組み

新しいコールが S-GW に届いたときに、この機能の CLI が有効になっており、かつコールの APN が CLI で設定された APN と一致している場合、コールは拒否されます。この機能は、サブスクライバのタイプ（ホーム、ビジター、ローミング）を識別して動作します。この識別は、次の方法で行われます。

- S-GW の PLMN ID が PGW および International Mobile Subscriber Identity（IMSI）の PLMN ID と同じである場合、ホームサブスクライバとして識別されます。
- IMSI に関係なく、S-GW の PLMN ID が PGW の PLMN ID と異なる場合、ローミングサブスクライバとして識別されます。たとえば、MS-1 が PLMN1 に登録されていて、PLMN2 の SGW に接続されています。次に、MS-1 は PLMN2 から PLMN1 の PGW とのセッションを開始します。このシナリオでは、MS-1 はローミングです。
- IMSI に外部の PLMN ID が含まれているサブスクライバは、ビジターとして識別されます。

S-GWは、ホーム、ビジター、ローミングサブスクライバ用に設定されたAPNのすべてのセッションを拒否します。最初の接続CS要求とUEが要求した追加のPDN接続のPure-Sコールに対するCS要求も拒否の対象と見なされます。CS要求は*No Resource Available*というGTPV2の理由で拒否されます。このような場合、MMEがこの原因コードに基づいて接続を再試行し、ブラックリストアルゴリズムの実装に基づいてこのS-GWをブラックリストに登録することが予想されます。

ホームおよびローミングサブスクライバ用の一連の APN（最大 10）が S-GW によって拒否されるように設定する必要があります。

SAEGW 展開の場合、Pure-S コールのみが拒否されます。SAEGW が Collapsed コールの CS 要求を受信した場合、対応する APN が拒否リストで設定されていても、このコールは拒否されません。

次の場合、IMS APNで新しいコールが拒否対象に設定されていても、緊急コールやeMPSコールは拒否されません。

- S-GW が IMS APN および未認証の imsi フラグが設定された CS 要求を受信した場合。
- S-GW が IMS APN を含む CS 要求を受信し、eARP 値が S-GW サービスの eMPS eARP として設定されている場合。

（注） CS要求では、eARPはeMPS eARPとして設定されていないS-GWによって受信されます。CS応答中に、S-GWは、eMPSセッションとしてマークできる新しい承認済みeARPを受信できます。ただし、CS応答でこの機能が有効になっている場合、CS要求の処理中のみセッションが拒否されます。

制限事項

Pure S コールが新規コール拒否ポリシーによって拒否されると、**show saegw-service statistics all function sgw** CLI コマンドの [New Call Policy Rejection Stats] セクションに拒否統計が収集されます。拒否されたコールに関して、その他の SGW 関連の統計は収集されません。

S-GW の新規コール拒否の設定

この項では、新しいコールを拒否するためのS-GWのサポートを有効または無効にする設定コマンドについて説明します。

新規コール拒否の有効化

次の設定コマンドを使用して、ローミングサブスクライバ、ホームサブスクライバ、ビジターサブスクライバ、およびAPNサブスクライバのS-GWでのコールを拒否します。

```
configure
   context context_name
      sgw-service sgw-service_name
         [ default | no ] newcall reject { roamer  | home [ apn apn_name
] | visitor [ apn apn_name }
         end
```

注：

- **default**：コマンドをデフォルト設定の [Disabled] にリセットします。
- **no**：指定したサブスクライバのすべてのコールで拒否を無効にします。
- **newcall**：設定された S-GW サービスの新しいコールを設定します。
- **reject**：設定された S-GW サービスの [Home]、[Visitor]、または [Roamer] サブスクライバを対象に newcall reject-policy を設定します。
- **roamer**：Roamer サブスクライバを対象に、設定された S-GW サービスの newcall reject-policy を設定します。
- **home**：Home サブスクライバを対象に、設定された S-GW サービスの newcall reject-policy を設定します。
- **visitor**：Vistor サブスクライバを対象に、設定された S-GW サービスの newcall reject-policy を設定します。
- **apn-name** *apn_name*：Home または Visitor サブスクライバを対象に、設定された S-GW サービスのコールを拒否するための APN 名（最大 10 個の APN プロファイル）を設定します。

モニタリングおよびトラブルシューティング

ここでは、S-GW で新しいコールや APN セッションが拒否された際に、モニタリングと障害対応に使用できるコマンドについて説明します。

コマンドや出力の表示

ここでは、S-GW での新しいコールと APN セッションの拒否をサポートするために導入された show コマンドとフィールドについて説明します。

show saegw-service statistics all function sgw

この show コマンドの出力は、新規コールを拒否するために sgw-service で設定された apn-profiles を表示するように変更されました。次のフィールドが導入されました。

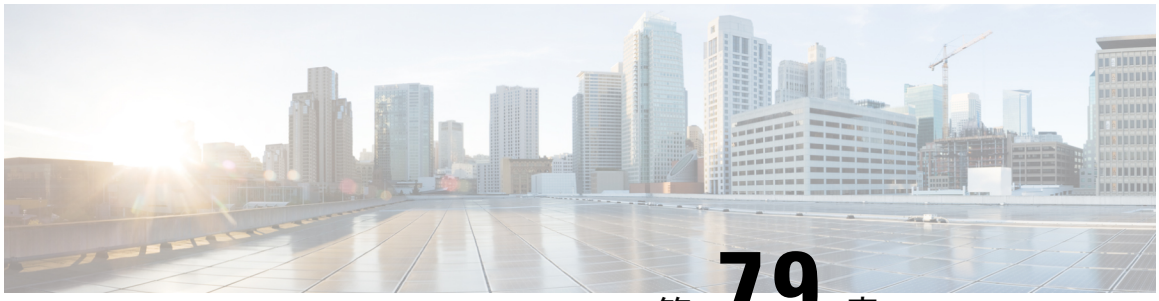
- 新しいコールポリシー拒否統計
- 新しいコール（New Calls）
  - 訪問サブスクライバ

- ホームサブスクライバ
- ローミングサブスクライバ

show sgw-service name

この show コマンドの出力は、新規コールを拒否するために sgw-service で設定された apn-profiles を表示するように変更されました。次のフィールドが導入されました。

- SGW Reject Calls Visitor Subs
- SGW Reject Calls Roamer Subs
- SGW Reject Calls Home Subs



第 79 章

S-GW セッションのアイドルタイムアウト

マニュアルの変更履歴

Note リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

この章では、S-GWセッションのアイドルタイムアウト処理機能について説明します。ASR5500プラットフォームでは、サブスクライバセッションはコールラインで表されます。S-GW 製品のコールラインは、S11/S4 の MME/S4-SGSN および S5/S8 の P-GW を介してピアに接続します。一部のシナリオでは、ピアセッションはそれぞれのピアによって削除されます。S-GW は削除メッセージを受信も除外もしないため、その結果、S-GW セッションはアイドル状態のままになります。このようなアイドル状態のセッションや古いセッションは、リソースを消費して、キャパシティを減らすため、システム内の有効なコールラインにカウントされます。このような場合、S-GWは新しいサブスクライバセッションの取得をトリガーします。その結果、同じサブスクライバの古いセッションが削除されます。アイドルタイムアウト処理のサポートにより、このようなセッションの識別が可能になり、リソースを解放するために削除が開始されます。

次に、S-GW セッションのアイドルタイムアウト処理について説明します。

- サブスクライバのデータ トラフィック アクティビティがない場合、サブスクライバセッションはアイドル状態です。セッションマネージャは、コールラインの状態を追跡します。コールラインのデータトラフィックが記録されていない場合、そのようなセッションはアイドル状態に遷移します。
- アイドルタイムアウトと呼ばれる定義されたタイムフレームの間アイドル状態にあるセッションは、アイドルタイムアウト処理の対象と見なされます。アイドル タイムアウトセッションでは、S-GW はピアへのセッションの削除を開始します。
- アイドルタイムアウトは、ネットワーク要件に応じて秒単位で設定されます。タイムアウトの範囲は 1 ～ 4294967295 秒です。
- アイドルタイムアウトの設定は、S-GW サービスレベルで適用され、そのサービスによって処理される一連のサブスクライバのアイドル タイムアウト処理を有効にします。

セッション アイドル タイムアウトの設定

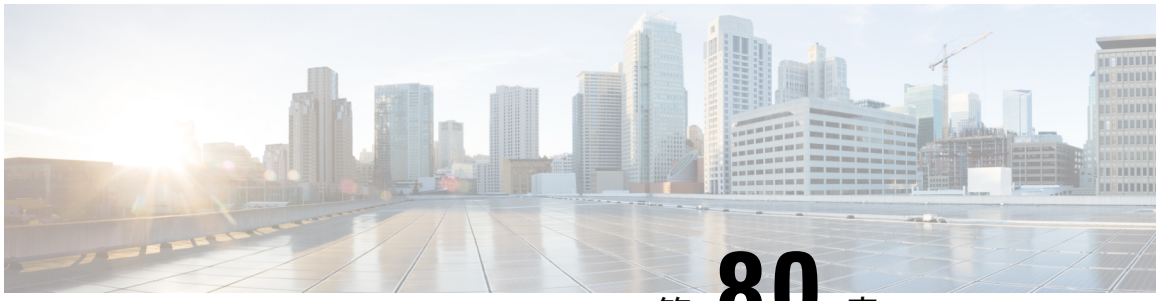
S-GW セッションのセッションアイドルタイマーは、S-GW サービスから設定できます。

S-GW のセッション アイドル タイムアウトを設定するには、次の設定を使用します。

```
configure
   context context_name
      sgw-service service_name
         [ no | default] timeout idle timeout_duration
         end
```

注：

- **timeout idle** *timeout_duration*：システムがセッションを自動的に終了する前に、セッションがアイドル状態を維持できる最大時間を秒単位で指定します。*timeout_duration* は 1 ～ 4294967295 の範囲の整数である必要があります。0 を指定すると、この機能が無効になります。デフォルトでは、この機能は S-GW サービスで無効になっています。



第 80 章

DDN 遅延および DDN スロットリングを使用した SAEGW アイドルバッファリング

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
このリリースでは、UP の FAR ごとにバッファされるパケット数を設定できます。FAR ごとにバッファされるパケットを設定するには、ACS コンフィギュレーション モードで **buffering-limit far-max-packets** *far_max_packets* CLI コマンドを使用します。 より多くの FAR バッファパケットを設定して、パケットドロップの少ない QoS を実現できます。	21.28.m23
最初の導入。	21.24 より前

機能説明

CUPS アーキテクチャでは、UE がアイドル状態の場合、DDN 遅延と DDN スロットリング、および SAEGW でのバッファリングをサポートするダウンリンクデータ通知（DDN）メッセージがサポートされます。

機能の仕組み

この項では、この機能の仕組みを紹介します。

- バッファリングは SAEGW-U でサポートされています。
- Release Access Beare によって UE がアイドル状態に遷移すると、バッファリングのサポートが開始されます。
- アクティブ状態からアイドル状態への遷移：
  - SAEGW はバッファリング機能をサポートし、セッションの SAEGW-U でバッファリングをアクティブ化することを決定するため、UE が ECM-IDLE 状態に遷移すると、SAEGW-C は Sx セッション変更を介して SAEGW-U に通知します。
  - バッファリングが開始された後、最初のダウンリンクパケットがいずれかのベアラーに到着すると、SAEGW-U は SAEGW-C に通知します。 SAEGW-U は、特に指定されていない限り、Sx レポートメッセージを SAEGW-C に送信し、ダウンリンクパケットの受信先の S5/S8 ベアラーを識別します。
  - SAEGW-C は、レポートメッセージを受信すると、3GPP TS 23.401 [2] での定義に従って、DDN メッセージを MME に送信するかどうかを決定します。DDN 通知は、Sx 使用状況レポートとともに送信されます。
- アイドル状態からアクティブ状態への遷移：
  - UE が ECM-CONNECTED 状態に遷移すると、SAEGW-C は eNodeB/RNC/SGSN の F-TEIDu を使用して Sxa インターフェイスを介して SAEGW-U を更新します。バッファリングされたデータパケットがある場合は、SAEGW-U によって eNodeB/RNC/SGSN に転送されます。
- Apply Action が BUFFER で、SGW-U が回復した場合、SGW-U はダウンリンクデータパケットの到着時に Sx レポート（Report Type：DLDR）を開始します。
- SGW-U には、各 Sx レポート（Report Type：DLDR）が送信された後に開始するタイマーが実装されています。Apply Action が変更されていない場合、タイマーの期限が切れると、Sx レポート（Report Type：DLDR）が再度開始されます。
- ベアラーの ARP は DDN メッセージに含まれます。
- マルチ PDN セッションでは、ある PDN に対して DDN が開始され、ベアラーの優先順位が高い別の PDN でデータが受信された場合、DDN は優先順位がより高い ARP 値で再度開始されます。

ダウンリンクデータ通知：遅延（DDN-D）のサポート

特定の条件下では、UE がサービス要求をトリガーすると、アップリンクおよびダウンリンクデータがトリガーされ、ベアラー変更要求（MBR）を受信する前に SGW-C で受信され、不要なダウンリンクパケット通知メッセージが送信されて、MME の負荷が増加します。

このような場合、MMEはこれらのイベントの発生レートをモニターします。レートがオペレータの設定値より大きくなり、MME の負荷がオペレータの設定値を超えた場合、MME はパラメータ D を使用して「Delay Downlink Packet Notification Request」を Serving Gateway に表示します。D は要求された遅延で、50 ミリ秒の倍数の整数、または 0 で指定します。S-GW では、ダウンリンクデータを受信してからダウンリンクデータ通知メッセージを送信するまでの間、この遅延が使用されます。

ダウンリンクデータ通知は、Collapsed コールと Pure-S コールの両方でサポートされています。

システムの分散型の性質により、特定の MME からのセッションは異なるセッションマネージャにオフロードされるため、セッションがオフロードされると、すべてのセッションマネージャに通知されます。また、この機能は、すべてのセッションマネージャから DEMUX マネージャにメッセージを送信できないように設計されています。

- DDN 遅延機能では、DDN 遅延タイマーのサポートはコントロールプレーンで行われます。
- 最初のデータパケットが到着すると、Sx レポートメッセージが開始されますが、DDN メッセージは遅延タイマーの満了後にコントロールプレーンから開始されます。
- DDN 遅延機能はピアレベルの機能であるため、DDN 遅延値の受信元であるピアのすべてのセッションに適用されます。
- 以前にピアから遅延値を受信していて、現在のメッセージに含まれていない場合、遅延値は 0 と見なされます。

DDN のセッションリカバリと ICSR がサポートされています。

DDN スロットリングのサポート

SGW-C から MME への DDN 要求が多すぎると、MME での処理が過負荷になる可能性があります。この負荷を軽減するために、MME は SGW-C に対して、所定の期間に送信される DDN メッセージを一定の割合で減らすよう動的に要求します。

DDN スロットリングの場合、S-GW は、所定の期間に一定の割合の DDN をドロップする必要があります。S-GW は、各セッションマネージャで確率的アルゴリズムを使用することで、この機能を実装します。

一方、DDN スロットリングの従来の実装では、各セッションマネージャが、低優先ベアラーの保留中の DDN リストを中央エンティティと共有する必要があります。中央エンティティは保留中の DDN の正味負荷を計算し、各セッションマネージャがドロップする必要がある DDN の数を決定します。この実装では、セッションマネージャでの DDN メッセージのバッファリングが必要になります。また、シャーシ内におけるソフトウェアサブシステムの分散処理の性

質上、セッションマネージャと中央エンティティ（Boxer の場合は demuxmgr）間で定期的に大量のメッセージングが必要になります。

確率的アルゴリズムを実装すると、セッションマネージャでのバッファリングと、demuxmgr とのメッセージングの必要性がなくなります。セッションマネージャでの ARP 優先順位が低いページング負荷が増加すると、確率的アルゴリズムの精度が向上します。ページング負荷が低くても、指定されたスロットリング係数にかなり近い精度となります。

リリース 10 に準拠していない MME の場合、SGW_C には CLI を使用してスロットリングを有効にするオプションがあります。

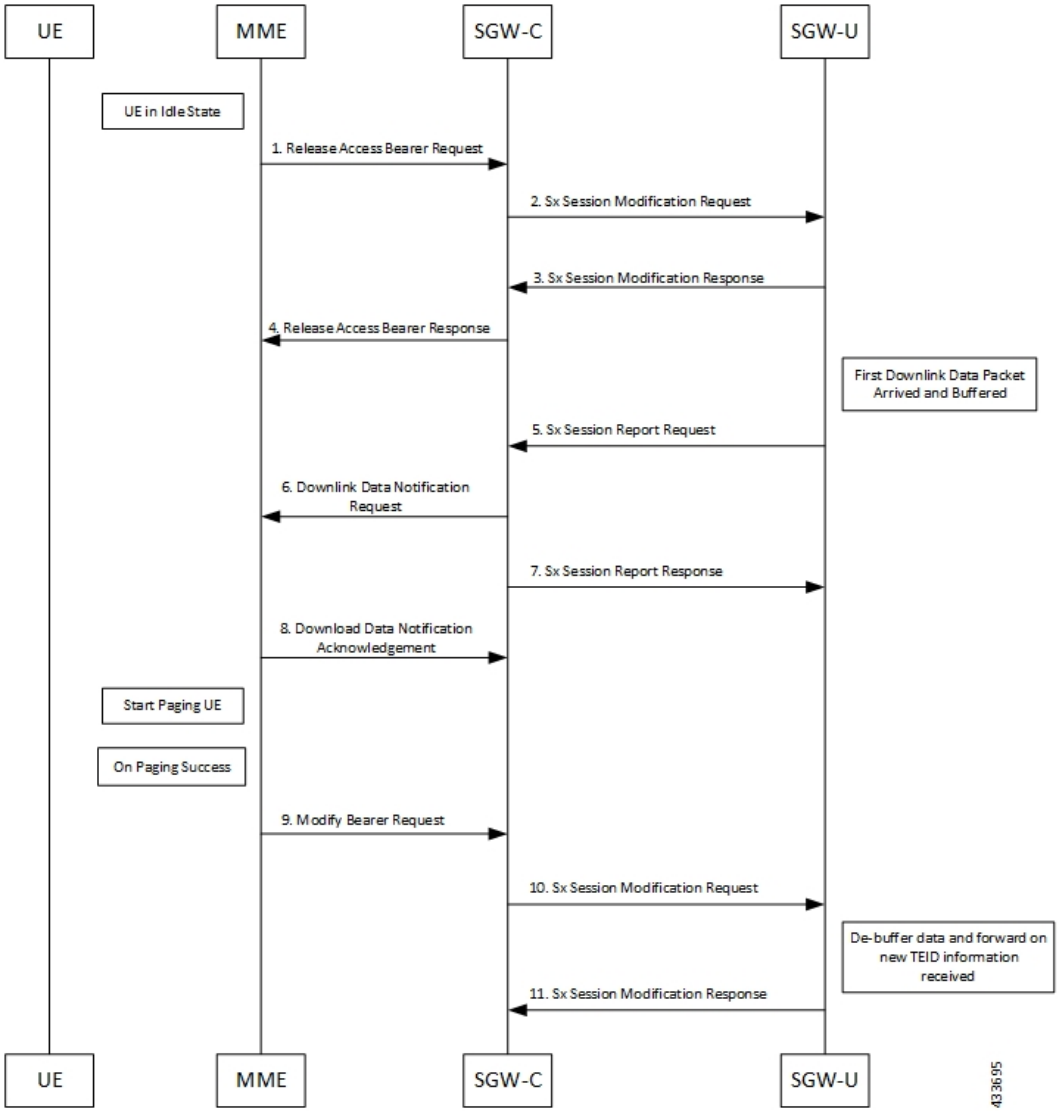
低優先ベアラーの ARP しきい値は、S-GW サービス設定を使用して設定する必要があります。たとえば、設定された ARP 値が「9」の場合、ARP が 9 を超えるベアラーはすべて、低優先ベアラーと見なされます。DDN スロットリングは、この設定によって有効になります。SGW サービス設定を通じて DDN スロットリングが有効になっている場合、MME への各 DDN メッセージには ARP IE が含まれます。

ユーザー接続タイマーのサポートなし

- 肯定的なダウンリンクデータ通知の確認応答後にベアラー変更要求を受信しない場合、タイマーが設定されます。
- タイマーは、DDN 確認応答を受信したときに SGW-C で開始されます。
- ベアラー変更要求の到着時に、SGW-C はこのタイマーを停止します。
- タイマーの期限が切れると、SGW-C はバッファリングされたパケットをドロップするように SGW-U に通知します。

DDN コールフロー

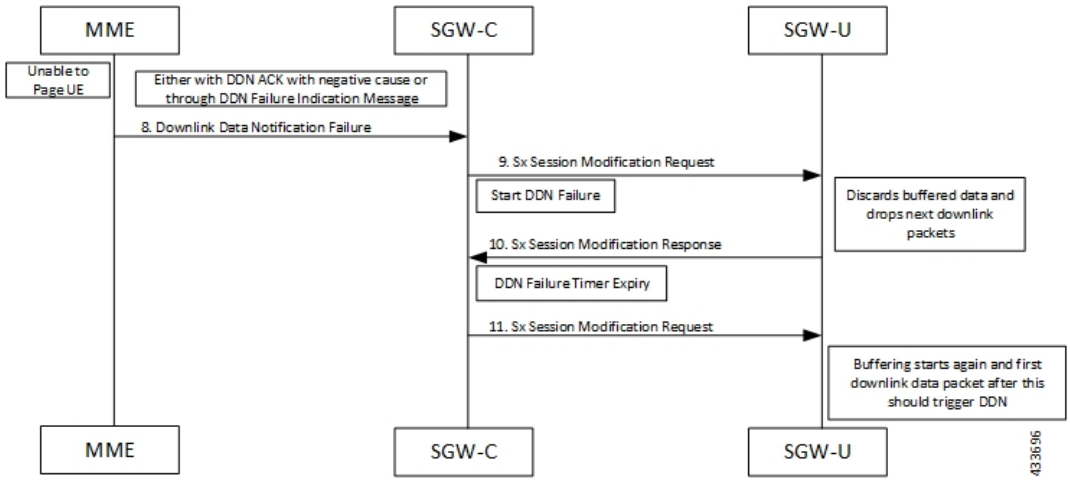
DDN の成功シナリオ



1. 該当する UE の全ベアラーのダウンリンクリモート TEID を解放するため、MME が SGW-C にアクセスベアラー解放要求を送信します。
2. アクセスベアラー解放要求を受信すると、SGW-C はすべての PDN への Sx 変更要求の [Apply Action] を「BUFFER」にして FAR を更新することで、同じ情報を SGW-U に通知します。
3. SGW-U が、対応する PDN に対して SGW-U でバッファリングを適用後、Sx 変更応答を送信します。
4. SGW-C が MME にアクセスベアラー解放応答を送信します。

5. SGW-U が受信する最初のダウンリンクデータにより、SGW-C に対する Sx レポート要求（[Report Type] が「Downlink Data Report」）がトリガーされます。
6. Sx レポート要求メッセージを受信すると、SGW-C が MME へのダウンリンクデータ通知要求メッセージを開始します。
7. SGW-C が、SGW-U に向けて Sx レポート応答メッセージを送信します。
8. MME は、UE にページング要求を送信できる場合、ダウンリンクデータ通知確認応答メッセージで [Cause] を「Request Accepted」に設定して、SGW-C に送信します。
9. ページングが成功すると、SGW で S1-U 接続を設定する eNodeB TEID を使用して、MME が S-GW にベアラー変更要求を送信します。
10. SGW-C が、新しい TEID 情報に関する更新された FAR を含む Sx 変更要求を SGW-U に送信します。SGW-U は、バッファされたすべてのデータを eNodeB を介して UE に転送できるようになりました。
11. SGW-U が、SGW-C に Sx 変更応答を送信します。

DDN の失敗シナリオ



1. MME が、その UE に対するすべてのベアラーのダウンリンクリモート TEID を解放するために、SGW-C にアクセスベアラー解放要求を送信します。
2. アクセスベアラー解放要求を受信すると、SGW-C はすべての PDN への Sx 変更要求の Apply Action を BUFFER にして FAR を更新することで、同じ情報を SGW-U に通知します。
3. SGW-U が、対応する PDN に対して SGW-U でバッファリングを適用後、Sx 変更応答を送信します。
4. SGW-C は MME にアクセスベアラー解放応答を送信します。

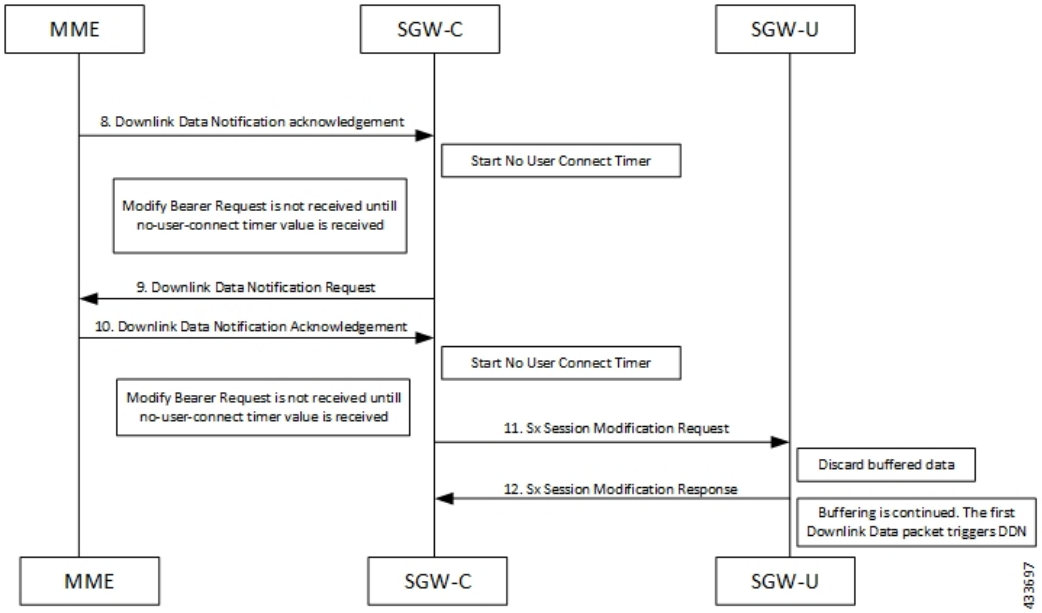
5. SGW-U が受信する最初のダウンリンクデータにより、SGW-C に対する Sx レポート要求（Report Type：Downlink Data Report）がトリガーされます。
6. Sx レポート要求メッセージを受信すると、SGW-C が MME へのダウンリンクデータ通知要求メッセージを開始します。
7. SGW-C が、SGW-U に向けて Sx レポート応答メッセージを送信します。
8. MME が UE をページングできない場合、関連する原因でダウンリンクデータ通知要求を拒否できます。

   または

   MME がダウンリンクデータ通知要求を受け入れた場合、UE がページングに応答しなかったことを SGW-C に示すために、後でダウンリンクデータ通知の失敗通知を送信します。
9. SGW-C が DDN の失敗を受信すると、次の DDN 送信をただちに停止するために、DDN 失敗タイマーを開始します。SGW-C はバッファされたパケットを破棄するために DROBU フラグを付け、後続のパケットをドロップするために Apply Action を DROP に してから、Sx 変更要求を送信します。
10. SGW-U が、SGW-C に Sx 変更応答を送信します。
11. DDN 失敗タイマーの期限が切れると、SGW-C はバッファリングを再開するために、Apply Action を BUFFER にして Sx 変更を開始します。

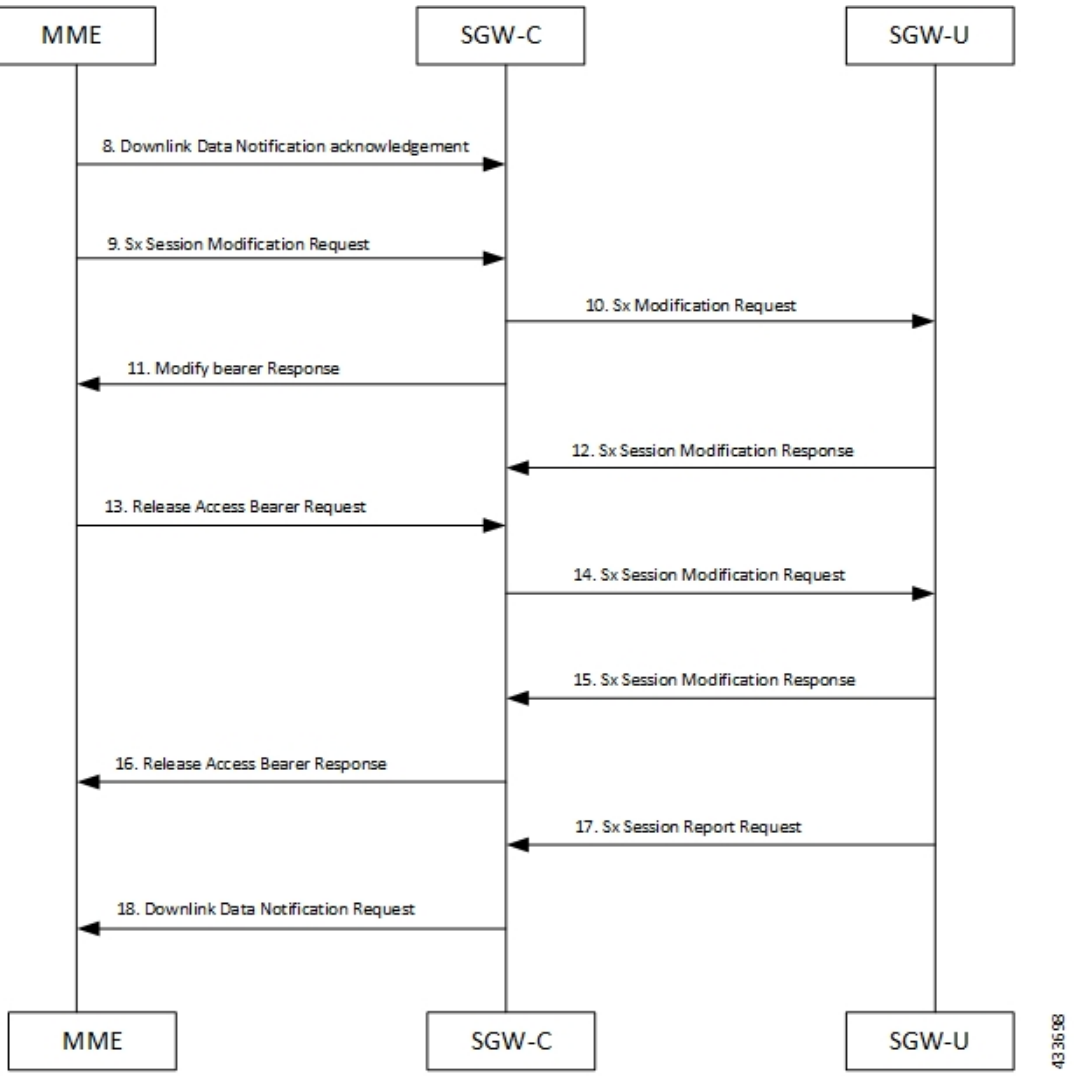
DDN の成功シナリオ （785 ページ）のコールフローのステップ 3 以降の手順が続きます。

ユーザーの接続なしタイマーのサポート



1. MME が、その UE に対するすべてのベアラーのダウンリンクリモート TEID を解放するために、SGW-C にアクセスベアラー解放要求を送信します。
2. アクセスベアラー解放要求を受信すると、SGW-C はすべての PDN への Sx 変更要求の Apply Action を BUFFER にして FAR を更新することで、同じ情報を SGW-U に通知します。
3. SGW-U が、対応する PDN に対して SGW-U でバッファリングを適用後、Sx 変更応答を送信します。
4. SGW-C は MME にアクセスベアラー解放応答を送信します。
5. SGW-U が受信する最初のダウンリンクデータにより、SGW-C に対する Sx レポート要求（Report Type：Downlink Data Report）がトリガーされます。
6. Sx レポート要求メッセージを受信すると、SGW-C が MME へのダウンリンクデータ通知要求メッセージを開始します。
7. SGW-C が、SGW-U に向けて Sx レポート応答メッセージを送信します。
8. ダウンリンクデータ通知確認応答が MME から受信されます。SGW-C が no-user-connect を開始します。
9. eNodeB TEID 情報を含むベアラー変更要求が受信されず、no-user-connect タイマーが期限切れになった場合、SGW-C はダウンリンク データ通知を再度送信します。
10. MME からダウンリンクデータ通知確認応答を受信します。SGW-C は、no-user-connect タイマーを再度開始します。
11. SGW-C はメッセージに DROBU フラグを付けて、SGW-U への Sx セッション変更要求を開始します。SGW-U はこのフラグを受信すると、バッファされたデータをドロップします。新しいデータはバッファリングされ、後続の最初のパケットは、ダウンリンクデータ通知メッセージを開始するための Sx レポートメッセージを開始します。
12. SGW-U が Sx 変更応答を送信します。

DDN 遅延タイマー



1. MME が、その UE に対するすべてのベアラーのダウンリンクリモート TEID を解放するために、SGW-C に Release Access Bearer 要求を送信します。
2. Release Access Bearer 要求の到着時に、SGW-C がすべての PDN の Sx 変更要求の Apply Action として BUFFER を使用して FAR を更新することで、同じ情報を SGW-U に通知します。
3. SGW-U が、対応する PDN に対して SGW-U でバッファリングを適用後、Sx 変更応答を送信します。
4. SGW-C が MME に Release Access Bearer 応答を送信します。
5. SGW-U に到着した最初のダウンリンクデータにより、SGW-C に対する Sx レポート要求（レポートタイプはダウンリンクデータレポート）がトリガーされます。

6. Sx レポート要求メッセージが到着すると、SGW-C が MME へのダウンリンクデータ通知要求メッセージを開始します。
7. SGW-C が、SGW-U に向けて Sx レポート応答メッセージを送信します。
8. DDN 遅延タイマー値に従い、MME からダウンリンクデータ通知確認応答を受信します。この遅延タイマー値はこのピア用に保存されるため、その後、このピアに対するすべてのダウンリンクデータ通知は、この遅延の後に開始する必要があります。
9. ページングが成功すると、SGW で S1-U 接続を設定する eNodeB TEID を使用して、MME が SGW にベアラー変更要求を送信します。
10. SGW-C が、新しい TEID 情報に関する更新された FAR を含む Sx 変更要求を SGW-U に送信します。 SGW-U は、バッファされたすべてのデータを eNodeB を介して UE に転送できるようになりました。
11. SGW-C が、ベアラー変更応答を MME に送信します。
12. SGW-U が、SGW-C に Sx 変更応答を送信します。
13. MME が、その UE に対するすべてのベアラーのダウンリンクリモート TEID を解放するために、SGW-C に Release Access Bearer 要求を送信します。
14. Release Access Bearer 要求の到着時に、SGW-C がすべての PDN の Sx 変更要求の Apply Action として BUFFER を使用して FAR を更新することで、同じ情報を SGW-U に通知します。
15. SGW-U が、対応する PDN に対して SGW-U でバッファリングを適用後、Sx 変更応答を送信します。
16. SGW-C が MME に Release Access Bearer 応答を送信します。
17. SGW-U に到着した最初のダウンリンクデータにより、SGW-C に対する Sx レポート要求（レポートタイプはダウンリンクデータレポート）がトリガーされます。
18. Sx レポート要求メッセージの到着時に、SGW-C が DDN 遅延タイマーを開始します。DDN 遅延タイマーが期限切れになると、SGW-C が MME へのダウンリンクデータ通知メッセージを開始します。

Sx インターフェイス

Sx セッションレベルのレポート手順

アイドルモード UE の最初のダウンリンクデータの検出（SAEGW-U が実行）：

SAEGW-U はダウンリンクパケットを受信するが、送信用の S1 ベアラーを受信せず、バッファリングが SAEGW-U によって実行される場合、UE をページングするために、最初のダウンリンクデータの検出を SAEGW-C に報告します。

PFCP セッションレポート要求

PFCPセッションレポート要求は、PFCPセッションに関連する情報をコントロールプレーン機能に報告するために、ユーザープレーン機能によって Sxab インターフェイスを介して送信されます。

情報要素	P	条件/コメント	アプリケーション				IE タイプ
			Sxa	Sxb	Sxc	N4	
レポートタイプ	M	この IE は、レポートのタイプを示します。	X	X	X	X	レポートタイプ
Downlink Data Report	C	この IE は、Report Type が Downlink Data Report を示している場合に存在します。	×	-	-	×	Downlink Data Report

PFCP セッションレポート要求内の Downlink Data Report IE

Downlink Data Report のグループ化された IE は、次の表に示すようにエンコードされます。

オクテット 1 および 2		Downlink Data Report IE タイプ = 83（10 進数）					
オクテット 3 および 4		長さ = n					
情報要素	P	条件/コメント	アプリケーション				IE タイプ
			Sxa	Sxb	Sxc	N4	

PDR ID	M	この IE は、UP 機能で受信されたダウンリンクデータパケットの PDR を識別します。 ダウンリンクデータパケットを受信した複数の PDR を表すために、このタイプの IE を複数含めることができます。	×	-	-	×	PDR ID

ユーザープレーン機能への DDN 障害に関する通知

コントロールプレーン機能はユーザープレーン機能に障害を通知します。これにより、バッファリングされたパケットがドロップされ、PFCP Sx 変更メッセージの DROBU フラグを介して DDN 関連フラグをリセットできます。

PFCPSMReq フラグ	C	DROBU（Drop Buffered Packets）：この PFCP セッションで現在バッファリングされているパケットをドロップするように UP 機能が要求された場合、CP 機能はこのフラグを設定します（注 1 を参照）。

制限事項

この機能には次の既知の制限事項があります。

- フローアイドルタイムアウトまたはその他のケースが原因で削除されるバッファ データ（データパケットストリーム）のサポートはありません。

DDN遅延およびDDNスロットリングサポート設定を使用したSAEGWアイドルバッファリング

リリース10準拠MMEのDDNスロットリング

DDN スロットリングは、ARP 値を指定することで、コール制御プロファイルを介して有効になります。たとえば、指定された ARP 値が 10 の場合、ARP 値が 10 ～ 15 であるベアラーはすべて優先順位が低いベアラーとして扱われ、スロットリング処理が行われます。S-GW サービス設定で ARP 値が指定されていない場合、スロットリングは有効になりません。また、DDN スロットリングが S-GW サービスを使用して設定されていない限り、MME への DDN メッセージに ARP IE は含まれません。MME がリリース 10 に準拠している場合、DDN 確認応答にスロットリング IE があるため、ユーザーが期間値を設定する必要はありません。準拠していない場合は、期間値を設定することで、S-GW でスロットリングを有効にできます。0 に設定されている場合、S-GW はスロットリングを繰り返し適用します。特定の期間のみスロットリングを有効にするには（リリース 10 非準拠の MME）、ユーザーが時間と分で値を設定する必要があります。設定時から、タイマーの期間が終了するまでスロットリングが S-GW で適用されます。たとえば、ユーザーが時間を 10、分を 30 と設定した場合、S-GW は次の 10 時間 30 分後にスロットリングを適用します。

再設定時に、すべてのパラメータが新しい値で設定されますが、ポーリング時間と時間係数を除き、次の再キャリブレーションからのみ適用されます。

リリース 10 MME の DDN スロットリングを設定するには、次の設定を使用します。

```
configure
  context context_name
    sgw-service service_name
      [ no ] ddn throttle arp-watermark arp_value
      end
```

注：

- **arp-value**：1 ～ 15 の有効な ARP 値。設定された値よりも大きい ARP を持つパケットはすべて、スロットリング係数に従ってスロットリングされます。

リリース10非準拠MMEのDDNスロットリング

リリース 10 以外の MME の DDN スロットリングを設定するには、次の設定を使用します。

```
configure
  context context_name
    sgw-service service_name
      ddn throttle arp-watermark arp_value [ rate-limit limit time-factor
 seconds throttle-factor percent increment-factor percent [ poll-interval
seconds ] throttle-time-sec seconds [ throttle-time-min minutes ] [
throttle-time-hour hour ] stab-time-sec seconds [ stab-time-min minutes ]
```

```
[ stab-time-hour hour ]
       no ddn throttle
       end
```

注：

- **rate-limit**：1 秒あたりに許可される DDN。
- **time-factor**：SGW がスロットリングを決定する期間（秒単位）（有効範囲：1 ～ 300 秒）。
- **arp-value**：1 ～ 15 の有効な ARP 値。設定された値よりも大きな ARP 値を持つすべてのパケットは、スロットリング係数に従ってスロットリングされます。
- **throttling-factor**：DDN サージの検出時にドロップされる DDN のパーセンテージ（有効範囲：1 ～ 100）。
- **throttling-time-sec**：SGW で DDN がスロットリングされる期間（秒単位）（有効範囲：0 ～ 59 秒）。
- **throttling-time-min**：SGW で DDN がスロットリングされる時間（分単位）（有効範囲：0 ～ 59 分）。
- **throttling-time-hour**：SGW で DDN がスロットリングされる期間（時間単位）（有効範囲：0 ～ 310 時間）。
- **increment-factor**：既存のスロットリング係数では DDN の急増を抑制するには不十分な場合に、スロットリング係数を動的に増加させるパーセンテージ値。
- **poll-interval**：秒単位の時間（オプションの引数、デフォルト値：1 秒、poll interval < time-factor）
- **stab-time-sec/min/hours**：安定化時間係数。DDN レートが正常に戻った場合に、スロットリング期間全体でスロットリングを適用する必要がない期間。

リリース 10 に準拠していない MME の DDN スロットリングは、SGW での既存のリリース 10 スロットリング実装を利用します。SGW サービスの設定メカニズムを提供することで、オペレータは DDN スロットリングを適用する際に MME からのフィードバックを必要としません。この機能の重要なポイントを以下に説明します。

1. CLI 設定は、MME/S4-SGSN ごとに適用されます。スロットリングパラメータは、MME/S4-SGSN ごとに個別に追跡されます。
2. CLI を使用してこの機能を設定すると、demuxmgr は送信された DDN の数について各 sessmgr をポーリングします。デフォルトでは、ポーリングは毎秒実行されます。この時間間隔は、poll-interval 時間を設定することで変更できます。ポーリング間隔を長くすると、シャーシ内の内部メッセージの数が少なくなります。ただし、DDN サージの検出には時間がかかります。
3. 時間係数を設定することで、オペレータは必要に応じて S-GW がスロットリングを適用する時間間隔を指定できます。実質的な DDN レートが時間係数の時間間隔で指定された制限内にある場合、DDN のサージがある程度許容されます。たとえば、time-factor = 10 秒、ddn rate = 1000、poll interval = 2 秒の場合について説明します。Demux は 2 秒ごとに各

sessmgr をポーリングします。許容される DDN レート制限は、1000*10＝10 秒ごとに 10000 DDN です。2 秒後に 4000 DDN が送信されたとします。この場合、10000 DDN のレート制限を 10 秒以内に超えるまで、S-GW はスロットリングを適用しません。これにより、DDN の断続的なバーストが可能になります。

4. DDN レート制限は CLI を使用して設定します。たとえば、DDN レート制限が 1000 で、ポーリング間隔が 1 秒、時間係数が 5 秒の場合、許容可能なレート制限は 5 秒間で 5000 DDN です。S-GW によって送信された DDN の数が 5 秒後に 5000 を超えた場合、demuxmgr はすべての sessmgr にスロットリングを開始するように要求します。
5. スロットリングされる DDN の割合は、スロットリング係数を使用して設定されます。
6. 既存のスロットリング係数では DDN の急増を抑制するには不十分な場合、オペレータは増分係数を指定してスロットリング係数を増やすことができます。たとえば、スロットリング係数＝10%、DDN レート＝1000、増分係数＝10% の場合について説明します。スロットリングが適用されると、S-GW は最大 10% の DDN をドロップします。ただし、DDN レートがさらに 1000 を超える場合、S-GW はスロットリング係数を 20% に増やします。それでも十分でない場合は、30% に増加します。スロットリング係数を増やした後、ドロップされた DDN の数が予想よりも多い場合、スロットリング係数は増分係数によって下げまれます。たとえば、このケースでスロットリング係数を 30% に増やした後、送信される DDN が 1 秒あたり 1000 未満になった場合（時間係数とポーリング間隔を考慮）、スロットリング係数は 20 に低下します。スロットリング係数低下の下限値は、設定された値（この場合は 10%）になります。
7. オペレータは、S-GW でスロットリングが適用される期間を設定できます。これは、日数の指定順序によっては大きな値になる場合があります（例：10 日または 240 時間）。オペレータは、 DDN レートが十分に制御されている場合に、安定化時間係数を設定することでスロットリングを停止できます。スロットリングを停止すると、DDN は不必要にドロップされません。たとえば、スロットリング時間＝10 日、スタブ時間＝8 時間の場合について説明します。S-GW が DDN スロットリングを開始した後、8 時間で送信された DDN＋ドロップされた DDN が DDN レート * 8 時間未満の場合、スロットリングは停止されます。

バッファリング制限の設定

パケットバッファリング制限を設定するには、次の設定を使用します。

```
configure
  active-charging service service_name
    buffering-limit { far-max-packets far_max_packets | flow-max-packets
 flow_max_packets | subscriber-max-packets subscriber_max_packets }
      { default | no } buffering-limit { far-max-packets |
flow-max-packets | subscriber-max-packets }
      end
```

注：

- **far-max-packets** *Far_max_packets*：FAR あたりの、バッファリングされるパケットの最大数を指定します。*Far_max_packets* は 1 ～ 128 までの整数で指定する必要があります。

デフォルト値：5 パケット

- **flow-max-packets** *flow_max_packets*：フローあたりの、バッファリングされるパケットの最大数を指定します。*flow_max_packets* は 1 ～ 255 までの整数で指定する必要があります。
- **subscriber-max-packets** *subscriber_max_packets*：サブスクライバあたりの、バッファリングされるパケットの最大数を指定します。*subscriber_max_packets* は、1 ～ 255 までの整数で指定する必要があります。

show コマンドの入力と出力

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show subscribers user-plane-only-full all

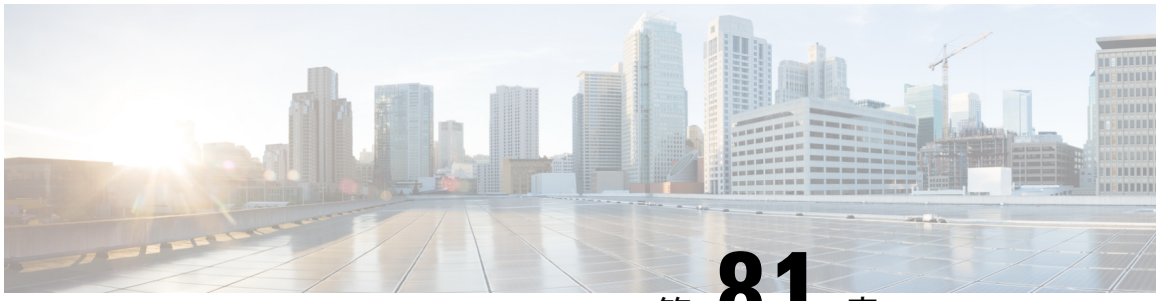
このコマンドの出力には、この機能をサポートする次のフィールドが表示されます。

- buffered pkts
- buffered bytes
- buffer overflow drop pkts
- buffer overflow drop bytes

show user-plane-service statistics all

以下に、バッファリングに関連する統計情報を表示するこのコマンドの出力例を示します。

```
[local]qvpc-si# show user-plane-service statistics all
…
  Data Statistics Related To Buffering:
    Packets Buffered:                  0    Bytes Buffered:                     0
    Packets Discarded:                 0    Bytes Discarded:                    0
    Packets Dropped per FAR (<=9)      0    Packets Dropped per FAR (10-19)     0
    Packets Dropped per FAR (20-29)    0    Packets Dropped per FAR (30-39)     0
    Packets Dropped per FAR (40-49)    0    Packets Dropped per FAR (>=50)      0
…
```



第 81 章

CDR レコードのセカンダリ RAT 使用状況レポート

マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、「CDR レコードのセカンダリ RAT 使用状況レポート」機能のサポートも追加されました。	21.20.31
このリリースでは、「CDR レコードのセカンダリ RAT 使用状況レポート」機能のサポートも追加されました。	21.26
初版	21.23.14

機能説明

5G **RANSecondaryRATUsageReport** に関連するレポートの問題は、以下の不足によって発生します。

- **RANSecondaryRATUsageReport** を CDR で処理する必要があるかどうかの識別に関する制御。この制御により、S-GW、P-GW、および SAEGW は、当該レポートを SGW-CDR や PGW-CDR に含めたり、単に無視したりできます。
- 制御がアクティブな場合に、CDR 内で使用可能なレポートの数。

- ゼロボリュームレポートを CDR 内で作成する必要があるかどうかの識別に関する制御。

この結果、課金情報データが失われます。これらのレポートの問題を解決するには、GTPP グループ構成を使用して CLI 制御をトリガーし、次の手順を実行します。

- S-GW、P-GW、および SAEGW が、SGW-CDR や PGW-CDR に RANSecondary RAT 使用状況レポートを含めたり、単に無視したりできるようにします。
- SGW-CDR や PGW-CDR 内で使用可能なセカンダリ RAT 使用状況レポートの数を特定します。

（注） この制限は、システム機能に準拠する必要があるため、CDR のファイル形式を考慮する必要があります。設定された制限を超えると、適切な変更条件を使用して SGW-CDR または PGW-CDR が閉じられます。たとえば、**max-change-condition** CDR は、以降のレポートに再利用されます。

- CDR 内のゼロボリュームレポートを追加または無視します。
- CLI **gtpp limit-secondary-rat-usage** またはハードコードされた制限は削除され、CLI **gtpp limit-secondary-rat-usage** は 1 ～ 100 の範囲内のレコード数を制御するために再利用されます。
- CDR サイズが最大サイズに達したときにロギングを提供します。CDR がサイズ制限を超えた回数は、PGW-CDR カウンタでモニターできます。

動作マトリックス

次の表では、この機能の P-GW と S-GW の新しい動作について説明します。

CLI	P-GW 新しい動作	S-GW 新しい動作
gtpp attribute secondary-rat-usage デフォルトでは、この CLI コマンドは GTPP グループで有効になっています。	P-GW は、ゼロボリュームレコードを含むセカンダリ RAT 使用状況レコードを CDR で送信します。	S-GW は、ゼロボリュームレコードを含むセカンダリ RAT 使用状況レコードを CDR で送信します。
[no] gtpp attribute secondary-rat-usage	P-GW は、CDR でセカンダリ RAT 使用状況レコードを送信しません。	S-GW は、CDR でセカンダリ RAT 使用状況レコードを送信しません。

CLI	P-GW 新しい動作	S-GW 新しい動作
gtpp suppress-secondary-rat-usage zero-volume デフォルトでは、このCLIコマンドはGTPPグループで無効になっています。	P-GW は、CDR にゼロボリュームセカンダリ RAT レコードを含めず、送信しません。P-GW は、ゼロ以外のボリュームを含むセカンダリ RAT レコードのみを送信します。	S-GW は、CDR にゼロボリュームセカンダリ RAT レコードを含めず、送信しません。S-GW は、ゼロ以外のボリュームを含むセカンダリ RAT レコードのみを送信します。
[no] gtpp suppress-secondary-rat-usage zero-volume	P-GW は、ゼロボリュームレコードを含むセカンダリ RAT 使用状況レコードをCDRで送信します。	S-GW は、ゼロボリュームレコードを含むセカンダリ RAT 使用状況レコードをCDRで送信します。
gtpp limit-secondary-rat-usage *range_1–100*。設定されていない場合、デフォルト値は 32 です。デフォルトでは、このCLIコマンドはGTPPグループで有効になっています。 例：**gtpp limit-secondary-rat-usage 32** （注） このCLIは、1 ～ 100 の範囲を指定して既存の CLI コマンド **gtpp limit-secondary-rat-usage** を変更したものです。	PGWは、受信したセカンダリ RAT レコードの総数が 32 を超え、報告された原因値が *maximum change condition* の場合、ただちにCDRを生成します。 受信したセカンダリ RAT レコードの合計が32の倍数の場合、P-GWは複数のCDRを生成します。 例：P-GW が 2 回のトリガーの間に 100 の RAT レコードを受信した場合、PGWは3つのCDRを生成し、残りの4つの RAT レコードを次の CDR トリガー用に保持します。	S-GW は、受信したセカンダリ RAT レコードの総数が 32 を超え、報告された原因値が *maximum change condition* の場合、ただちにCDRを生成します。 受信したセカンダリ RAT レコードの合計が32の倍数の場合、S-GWは複数のCDRを生成します。 例：S-GW が 2 回のトリガーの間に 100 の RAT レコードを受信した場合、S-GW は 3 つのCDRを生成し、残りの4つの RAT レコードを次の CDR トリガー用に保持します。

CLI	P-GW 新しい動作	S-GW 新しい動作
例：**gtpp limit-secondary-rat-usage 40**	P-GW は、受信したセカンダリ RAT レコードの合計が 40 を超え、原因値が *maximum change condition* の場合、ただちに CDR を生成します。 受信したセカンダリ RAT レコードの合計が 40 の倍数の場合、P-GW は複数の CDR を生成します。 **例**：2 回のトリガーの間に 100 の RAT レコードを受信した場合、P-GW は 2 つの CDR を生成し、残りの 20 の RAT レコードを次の CDR トリガー用に保持します。	設定された値が 32 より大きく、すべての CDR で 32 のセカンダリ RAT レコードを送信する場合、**gtpp limit-secondary-rat-usage 40** CLI コマンドを無視します。
例：**gtpp limit-secondary-rat-usage 20**	P-GW は、受信したセカンダリ RAT レコードの合計が 20 を超え、原因値が *maximum change condition* の場合、ただちに CDR を生成します。 受信したセカンダリ RAT レコードの合計が 20 の倍数の場合、P-GW は複数の CDR を生成します。 **例**：P-GW が 2 回のトリガーの間に 100 の RAT レコードを受信した場合、P-GW は 2 つの CDR を生成し、残りの 20 の RAT レコードを次の CDR トリガー用に保存します。	S-GW は、受信したセカンダリ RAT レコードの合計が 20 を超え、原因値が *maximum change condition* の場合、ただちに CDR を生成します。 受信したセカンダリ RAT レコードの合計が 20 の倍数の場合、S-GW は複数の CDR を生成します。 **例**：S-GW が 2 回のトリガーの間に 100 の RAT レコードを受信した場合、5 つの CDR が生成されます。

CLI	P-GW 新しい動作	S-GW 新しい動作
[no] gtpp limit-secondary-rat-usage	受信したセカンダリ RAT レコードの合計が 255 を超え、原因値が *maximum change condition* の場合、ただちに CDR を生成します。 受信したセカンダリ RAT レコードの合計が 255 の倍数の場合、複数の CDR を生成します。 **例**：2 回のトリガーの間に 1,000 の RAT レコードを受信した場合、3 つの CDR が生成されます。残りの 235 の RAT レコードは、次の CDR トリガー用に保存されます。	**[no] gtpp limit-secondary-rat-usage** CLI を無視し、すべての CDR で 32 のセカンダリ RAT レコードを送信します。 この動作は **gtpp limit-secondary-rat-usage** *32* CLI の実装に似ています。 カウンタログとデバッグログは、CDR サイズの 64k を超えることはないため、必要ありません。
	サービス固有のユニット制限を **serviceConditionChange** ファイルで送信します。	レコードクロージャ

他の機能との関係性

- 『*P-GW Administration Guide*』の「Sessmgr Restart While Processing Secondary RAT Usage CDR Records」[英語] を参照してください。
- GnGp ハンドオーバー時の Secondary RAT Usage IE、S-GW、および Gz CDR でのセカンダリ RAT データ使用状況レポートの P-GW サポートについては、『*P-GW Administration Guide*』の「*5G Non-Standalone*」の章 [英語] を参照してください。
- Rf CDR でのセカンダリ RAT データ使用状況レポートの P-GW サポートについては、『*P-GW Administration Guide*』の「*5G Non-Standalone*」の章 [英語] を参照してください。

制限事項

この機能には、次の制限事項があります。

- セッションリカバリ中に、ベアラーごとに 16 のセカンダリ RAT レコードのみが S-GW に対して回復されます。S-GW では、ベアラーごとに最大 16 のセカンダリ RAT レコードのチェックポイントを設定できます。

- セッションリカバリ中に、すべてのベアラーで最大 142 のセカンダリ RAT レコードが P-GW に対して回復されます。P-GW では、すべてのベアラーに対して最大 142 のセカンダリ RAT レコードのチェックポイントを設定できます。
- 最大数を超えた場合、セッションリカバリ中にレコードが失われます。

GTPP を介したセカンダリ RAT 使用状況レポートの設定

バッファサイズを超える前にセカンダリ RAT 使用状況の CDR レコードを閉じるには、次の GTPP 設定を使用します。

セカンダリ RAT 使用状況レポートの有効化または無効化

セカンダリ RAT 使用状況レポートを有効または無効にするには、次の設定を使用します。

```
configure
  context context_name
    gtpp group group_name
      gtpp attribute secondary-rat-usage
      default gtpp attribute secondary-rat-usage
      no gtpp attribute secondary-rat-usage
      end
```

注：

- **gtpp attribute secondary-rat-usage**：オプション属性のセカンダリ RAT 使用状況レコードを送信します。
- **default gtpp attribute secondary-rat-usage**：デフォルトで、オプション属性のセカンダリ RAT 使用状況レコードを送信します。
- **no gtpp attribute secondary-rat-usage**：オプション属性のセカンダリ RAT 使用状況レコードを送信しません。

エントリの最大数の制御

セカンダリ RAT の使用状況レコードが CDR 内で設定されている最大値に達すると、CDR 終了原因が発生し、**maxChangeCond** を使用します。**gtpp limit-secondary-RAT-usage** CLI コマンドは、P-GW および S-GW CDR のセカンダリ RAT 使用状況レコードエントリの最大数を制御します。32 を超える制限値が設定されている場合、S-GW CDR で部分的な CDR が最大 32 個生成されます。

（注） S-GW の既存の動作には、32 のセカンダリ RAT 使用状況レコードの制限があります。

次の表では、セカンダリ RAT レコードと CDR の動作、および上限数について説明します。

シリアル番号	CDR タイプ	Configured limit-secondary-rat-usage	有効な上限数	UE によって送られるセカンダリ RAT レコード数	セカンダリ RAT レコードと CDR の動作
1	P-GW	32 未満 例：20	20	35	部分的な CDR が 20 個のセカンダリ RAT レコードで生成されます。
					残りの 15 個のセカンダリ RAT レコードは次のトリガーで送信されます。
	S-GW	32 未満 例：20	20	35	部分的な CDR が 20 個のセカンダリ RAT レコードで生成されます。
					残りの 15 個のセカンダリ RAT レコードは次のトリガーで送信されます。

シリアル番号	CDR タイプ	Configured limit-secondary-rat-usage	有効な上限数	UE によって送られるセカンダリ RAT レコード数	セカンダリ RAT レコードと CDR の動作
2	P-GW	32	32	35	部分的な CDR が 32 個のセカンダリ RAT レコードで生成されます。
					残りの 3 個のセカンダリ RAT レコードは次のトリガーで送信されます。
	S-GW	32	32	35	部分的な CDR が 32 個のセカンダリ RAT レコードで生成されます。
					残りの 3 個のセカンダリ RAT レコードは次のトリガーで送信されます。

シリアル番号	CDR タイプ	Configured limit-secondary-rat-usage	有効な上限数	UE によって送られるセカンダリ RAT レコード数	セカンダリ RAT レコードと CDR の動作
3	P-GW	32 超 例：100	100	100	部分的な CDR が 100 個のセカンダリ RAT レコードで生成されます。
	S-GW	32 超 例：100	32	100	それぞれ 32 個のセカンダリ RAT レコードを含む 3 つの部分的な CDR が生成されます。
					残りの 4 個のセカンダリ RAT レコードは次のトリガーで送信されます。

シリアル番号	CDR タイプ	Configured limit-secondary-rat-usage	有効な上限数	UE によって送られるセカンダリ RAT レコード数	セカンダリ RAT レコードと CDR の動作
4	P-GW	設定なし	255	1000	それぞれ 255 個のセカンダリ RAT レコードを含む 3 つの部分的な CDR が生成されます。
					報告された残りのセカンダリ RAT レコードは、次のトリガーで CDR の一部になります。
	S-GW	設定なし	32	1000	部分的な CDR は生成されません。
					32 個のセカンダリ RAT レコードは、次のトリガーで CDR の一部になります。

エントリの上限数を制御するには、次の設定を使用します。

```
configure
   context context_name
      gtpp group group_name
         gtpp limit-secondary-rat-usage usage_limit
         default gtpp limit-secondary-rat-usage
         no gtpp limit-secondary-rat-usage
         end
```

注：

- **gtpp limit-secondary-rat-usage** *usage_limit*：セカンダリ RAT レポートの最大数を入力します。 *usage_limit* は、1 ～ 100 の範囲の整数にする必要があります。S-GW CDR の推奨値は 32 です。

たとえば、上限が 10 に設定されている場合、設定された値に達すると CDR が生成されます。

- **default gtpp limit-secondary-rat-usage**：32 のデフォルト値を指定します。
- **no gtpp limit-secondary-rat-usage**：限られた数のセカンダリ RAT 使用状況情報の CDR 生成を無効にします。

ゼロボリュームのセカンダリ RAT 使用状況レポートの抑制

ゼロボリュームのセカンダリ RAT 使用状況レポートを抑制するには、次の設定を使用します。

```
configure
  context context_name
    gtpp group group_name
      gtpp suppress-secondary-rat-usage zero-volume
      default gtpp suppress-secondary-rat-usage zero-volume
      no gtpp suppress-secondary-rat-usage zero-volume
      end
```

注：

- **gtpp suppress-secondary-rat-usage zero-volume**：セカンダリ RAT レコードまたはゼロボリュームのセカンダリ RAT レコードを抑制します。
- **default gtpp suppress-secondary-rat-usage zero-volume**：ゼロボリュームのセカンダリ RAT 使用状況レコードを抑制しません。
- **no gtpp suppress-secondary-rat-usage zero-volume**：ゼロボリュームのセカンダリ RAT 使用状況レコードを抑制しません。

モニタリングおよびトラブルシューティング

ここでは、この機能をサポートする show コマンドを使ったモニタリングと障害対応の方法について説明します。

show コマンドと出力

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show config

この CLI コマンドの出力には、次のパラメータが表示されます。

フィールド	説明
gtpp attribute secondary-rat-usage	CDR に [Secondary RAT reports] フィールドを含めるには、このオプションを指定します。

フィールド	説明
gtpp suppress-secondary-rat-usage zero-volume	ボリュームが 0 のセカンダリ RAT レポートの CDR からの除外を有効にします。
gtpp limit-secondary-rat-usage	設定された値による、CDR のセカンダリ RAT 使用状況レポート数の制限を有効にします。

show config verbose

この CLI コマンドの出力には、次のパラメータが表示されます。

フィールド	説明
gtpp attribute secondary-rat-usage	セカンダリ RAT 使用状況レコードが表示されます。
gtpp suppress-secondary-rat-usage zero-volume	P-GW および S-GW からのゼロ以外のボリュームを含むセカンダリ RAT レコードのみ表示されます。
gtpp limit-secondary-rat-usage	受信したセカンダリ RAT レコードの合計が 10 の倍数である場合、P-GW および S-GW によって生成された複数の CDR が表示されます。報告された原因値は、maximum change condition になります。
no gtpp limit-secondary-rat-usage	未設定の原因に関するセカンダリ RAT レコードが表示されます。

show gtpp group

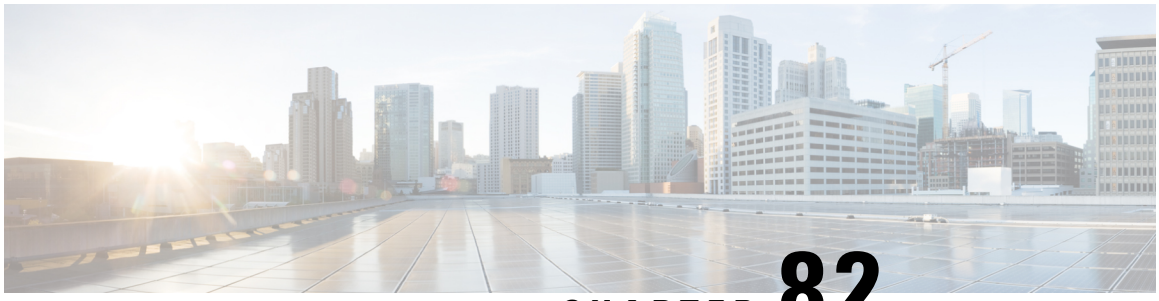
この CLI コマンドの出力には、次のパラメータが表示されます。

フィールド	説明
Secondary RAT records present	セカンダリ RAT レコードが存在するかどうかを指定します。次のオプションを使用できます。 • なし • あり
Limit-secondary-rat-usage	セカンダリ RAT 使用状況レポートの制限を指定します。

show gtpp statistics group

この CLI コマンドの出力には、次のパラメータが表示されます。

フィールド	説明
Total PGW-CDR exceed size limit	P-GW のサイズ制限を超えた CDR の総数を表示します。



CHAPTER 82

UP での Sx の自己過負荷検出とアドミッションコントロール

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

ユーザープレーン（UP）での過負荷の検出および制御は、eMPS 機能を使用して実装されます。Sx での過負荷シナリオでは、すべての非 eMPS サブスクライバを対象に、Sx（UP）で受信したセッション確立要求およびセッション変更要求が拒否されます。

現在、過負荷制御は Sx コントロールプレーン（CP）でサポートされています。UP で eMPS をサポートするため、CP は PFCP ヘッダーの Message Priority IE に eMPS 値を追加し、UP にメッセージを送信します。

UP は、Sx セッション確立/変更要求を受信すると、過負荷チェックを実行します。検出されたシステム負荷が正常であれば、セッションの確立/変更が許可され、セッションは PFCP ヘッダーに設定された MP フラグに基づいて優先セッションとしてマークされます。

検出されたシステム負荷が過負荷状態であれば、すべての eMPS サブスクライバを対象に、Sx セッションの確立/変更が拒否されます。

システムの負荷レベルは、次の要因によって決まります。

- システム使用率（CPU、メモリ、およびライセンス）
- セッションマネージャの使用率（CPU およびメモリ）
- VPP-CPU 使用率

制限事項

この機能には次の既知の制限事項があります。

- データスロットリングはサポートされません。
- アラームはサポートされません。
- バルク統計はサポートされません。
- Pure-S シナリオでの APN ベースの緊急コールの処理はサポートされません。IMSI ベースや IMEI の有効性ベースなど、その他の緊急コールは処理されます。
- このリリースでは、自己過負荷保護のみがサポートされます。
- ユーザープレーン ICSR は、このリリースではサポートされません。
- 既存のコールへの影響：**userplane-overload-control-profile** が設定され、ユーザープレーンサービスに関連付けられている状態で、システムが過負荷状態に移行し、ユーザープレーンサービスが SX セッション確立および SX セッション変更メッセージを拒否した場合、SX セッション変更メッセージをトリガーする関連コールのコールクリーンアップ/ドロップが発生します。この動作は、システムが通常の負荷状態に戻るまで続きます。

ユーザープレーンでの過負荷制御の設定

コントロールプレーンの S-GW および P-GW サービスに対する eMPS プロファイルの作成および関連付け

重要 この設定は、UP で過負荷制御プロファイルを設定する前に行う必要があります。

```
configure
  emps-profile profile_name
    earp earp_value
    end
```

```
configure
  context context_name
    sgw-service service_name
      associate emps-profile profile_name
      exit
    pgw-service service_name
      associate emps-profile profile_name
      end
```

UP での過負荷制御プロファイルの設定

過負荷制御プロファイルを設定するには、次のコマンドを使用します。

```
configure
  userplane-overload-control-profile profile_name
  end
```

過負荷しきい値パラメータの設定

過負荷しきい値パラメータを設定するには、次のコマンドを使用します。

```
configure
  userplane-overload-control-profile profile_name
    overload-threshold system lower-limit limit_value upper-limit
limit_value sessmgr lower-limit limit_value upper-limit limit_value vpp-cpu
lower-limit limit_value upper-limit limit_value
    end
```

注：

- **overload-threshold**：system、sessmgr、および vpp-cpu の過負荷しきい値制限を設定します。
- **system**：ノードが自己保護モードに移行するまでの過負荷システムしきい値を設定します。
- **vpp-cpu**：ノードが自己保護モードに移行するまでの過負荷 vpp-cpu しきい値を設定します。
- **sessmgr**：ノードが自己保護モードに移行するまでのセッションマネージャの過負荷しきい値を設定します。
- **upper-limit** *limit_value*：ノードが自己保護モードに移行するまでの過負荷 vpp-cpu しきい値 L2 を設定します。デフォルトの制限値は 60% です。
- **lower-limit** *limit_value*：ノードが自己保護モードに移行するまでの過負荷 vpp-cpu しきい値 L1 を設定します。デフォルトの制限値は 50% です。

システム重み付けパラメータの設定

セッションマネージャの重みパラメータを設定するには、次のコマンドを使用します。

```
configure
  userplane-overload-control-profile profile_name
    system-weightage system-cpu-utilization utilization_value
system-memory-utilization utilization_value license-session-utilization
utilization_value
    end
```

注：

- **system-weightage**：さまざまな過負荷制御パラメータのシステムの重みを設定します。全パラメータの重みの合計は 100 である必要があります。デフォルト値は、system-cpu-utilization に対する重みが 40%、system-memory-utilization に対する重みが 30%、license-session-utilization に対する重みが 30% です。
- **system-cpu-utilization**：システムの CPU 使用率の重みをパーセンテージで設定します。過負荷係数のデフォルトの重みは 40% です。
- **system-memory-utilization**：システムメモリ使用率の重みをパーセンテージで設定します。過負荷係数のデフォルトの重みは 30% です。
- **license-session-utilization**：ユーザープレーンサービスのライセンスセッション使用率の重みをパーセンテージで設定します。過負荷係数のデフォルトの重みは 30% です。

セッションマネージャの重みパラメータの設定

セッションマネージャの重みパラメータを設定するには、次のコマンドを使用します。

```
configure
  userplane-overload-control-profile profile_name
    sessmgr-weightage sessmgr-cpu-utilization utilization_value
sessmgr-memory-utilization utilization_value
    end
```

注：

- **sessmgr-weightage**：さまざまな負荷制御パラメータに対するセッションマネージャの重みを設定します。全パラメータの重みの合計は 100 である必要があります。デフォルト値は、sessmgr-cpu-utilization に対して 35% の重み、sessmgr-memory-utilization に対して 65% の重みです。
- **sessmgr-cpu-utilization**：セッションマネージャの CPU 使用率の重みをパーセンテージで設定します。過負荷係数のデフォルトの重みは 35% です。
- **sessmgr-memory-utilization**：セッションマネージャのメモリ使用率の重みをパーセンテージで設定します。過負荷係数のデフォルトの重みは 65% です。

過負荷制御プロファイルとユーザープレーンサービスの関連付け

次のコマンドを使用して、過負荷制御プロファイルをユーザープレーンサービスに関連付けます。

```
configure
  context context_name
    user-plane-service service_name
    [ no ] associate userplane-overload-control-profile profile_name
```

注：

- **associate**：このコマンドは、ユーザープレーン過負荷制御プロファイルをユーザープレーンサービスに関連付けます。

モニタリングおよびトラブルシューティング

show コマンドの入力と出力

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show user-plane-service name *name*

この機能をサポートするために、次のフィールドが表示されます。

- Service name
  - Service-Id
  - Context
  - Status
  - PGW Ingress GTPU Service
  - SGW Ingress GTPU Service
  - SGW Egress GTPU Service
  - Control Plane Tunnel GTPU Service
  - Sx Service
  - Control Plane Group
  - Userplane Overload Control Profile
  - Fast-Path service

show user-plane-service statistics name *user_plane_service_name*

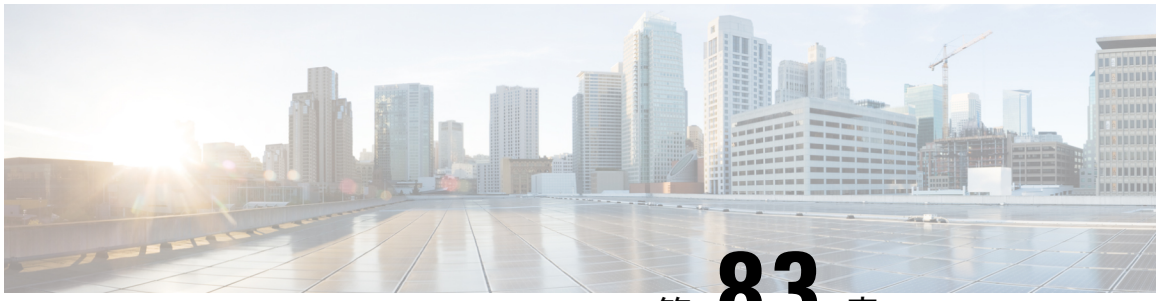
この機能をサポートするために、次のフィールドが表示されます。

- 過負荷制御情報
  - 現在の過負荷率（System）：すべてのユーザープレーンサービス値の平均
  - 現在の過負荷率（SessMgr）
  - 現在の過負荷率（VPP-CPU）
  - 過負荷しきい値に達した回数
  - 過負荷中に拒否されたセッション確立要求の数
  - 過負荷中に拒否されたセッション変更要求の数
  - 過負荷中に許可された eMPS セッション確立要求の数
  - 過負荷中に許可された eMPS セッション変更要求の数

show userplane-overload-control-profile name *name*

この機能をサポートするために、次のフィールドが表示されます。

- ユーザープレーン過負荷制御プロファイル
- ユーザープレーン過負荷制御プロファイル名
- システムの重みとしきい値：
  - CPU Utilization Weightage
  - Memory Utilization Weightage
  - License Session Utilization Weightage
  - System Threshold Lower Limit
  - System Threshold Upper Limit
- Sessmgr の重みとしきい値：
  - CPU Utilization Weightage
  - Memory Utilization Weightage
  - Sessmgr Threshold Lower Limit
  - Sessmgr Threshold Upper Limit
- VPP の重みとしきい値：
  - VPP Utilization Weightage
  - vpp-cpu Threshold Lower Limit
  - vpp-cpu Threshold Upper Limit



第 83 章

スマートライセンス

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

概要

Ultra Packet Core CUPS はスマートライセンスをサポートしています。スマートライセンシングは、シスコのソフトウェア資産の購入、展開、管理をシンプル化するクラウドベースのライセンシングのアプローチです。権限付与は Cisco Commerce Workspace（CCW）を介したシスコアカウントを通じて購入され、使用できるようにバーチャルアカウントにすぐに取り込まれます。これにより、あらゆるデバイスにライセンスファイルをインストールする必要がなくなります。スマートライセンシングが有効化されている製品では、使用状況のレポートがシスコに直接通知されます。シスコのソフトウェアライセンス (Cisco Smart Software Manager (CSSM)) を管理するために、お客様が 1 つの場所を使用できます。ライセンスの所有権と使用状況に関する情報をすぐに利用でき、使用状況やビジネスニーズに基づいて的確な購入判断ができます。

シスコ スマート ライセンシングの詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html を参照してください。

従来のライセンシングとスマートライセンシングの比較

シスコでは、従来のライセンシングとスマート ソフトウェア ライセンシングの 2 種類のライセンスモデルを採用しています。**従来のライセンシング**は、製品アクティベーションキー（PAK） をシスコ製品にインストールすることによって、ソフトウェア アクティベーションで構成されます。製品アクティベーションキーは、他のシスコ機器と同様の方法で発注し、シスコ製品の機能セットのライセンスファイルを取得するために使用する購入可能品目です。**スマート ソフトウェア ライセンシング**は、ライセンスレポートを承認および提供するいくつかのツールを利用した、エンドツーエンドプラットフォームのクラウドベースのライセンシングです。StarOS に組み込まれたスマート ソフトウェア ライセンシング機能により、製品登録と承認が完了し、エンドカスタマーがレポートサービスを利用できるようになります。

評価期間

使用中のすべてのライセンスに対して 90 日間の評価期間が付与されます。この期間中、機能ライセンスは制限なく使用でき、カウントライセンスを 1 つまで使用できます。評価期間は、システムが CSSM または Cisco.com に正常に登録されると終了します。この 90 日の期間が満了すると、ライセンス供与された機能がブロックされます。

CUPS は、オン/オフ機能ライセンスに対してライセンスの強制停止を行います。各オン/オフ機能ライセンスは、それらのオン/オフ機能を使用する可能性があるサービスライセンスに関連付けられています。オン/オフライセンスのコンプライアンス違反（OOC）が検出された場合、次の条件に従って、対応するサービスの新しいコールがドロップされます。

- 各オン/オフ機能ライセンスには、90 日の猶予（評価）期間が与えられます。この間、システムは有効なライセンスが利用できないことを通知する SNMP トラップを生成します。OOC を解決するには、この機能のライセンスの購入と登録、または機能の無効化などの是正措置が必要です。
- 90 日の猶予期間後もこの機能が OOC である場合、CUPS は各ライセンスの事前定義されたポリシーに基づいて OOC 状態を強制的に停止します。強制が必要な場合は、オン/オフライセンスに対応するサービスの新しいコールがドロップされます。

次の CLI コマンドを使用して、使用中のスマートライセンスの強制終了に関する詳細を表示できます。

```
show license enforcement policy
show license enforcement status [ allowed | blocked ] [ feature | service
 ]
```

Cisco Smart Software Manager

Cisco Smart Software Manager（CSSM）を使用すると、ソフトウェア ライセンスとスマートアカウントを単一のポータルから管理できます。このインターフェイスでは、製品の有効化、権限付与の管理、ソフトウェアの更新やアップグレードが可能です。登録プロセスを完了するには、機能しているスマートアカウントが必要です。Cisco Smart Software Manager にアクセスするには、こちら https://software.cisco.com をご覧ください。

スマートアカウントおよびバーチャルアカウント

スマートアカウントでは、スマート対応のすべての製品と権限付与を 1 つの場所で管理します。これにより、シスコソフトウェアの調達、展開、およびメンテナンスを迅速に行うことができます。スマートアカウントを作成するには、要求元の組織を代表する権限が必要です。送信後、要求は簡単な承認プロセスを経由します。

バーチャルアカウントは、スマートアカウント内のサブアカウントとして存在します。バーチャルアカウントは、組織の配置、ビジネス機能、地域、または定義された階層に基づくお客様定義の構造体です。これらはスマートアカウント管理者によって作成および管理されます。

スマートアカウントの詳細、設定、または管理については、https://software.cisco.comを参照してください。

スマートライセンスモード

スマートライセンスモードは次のように分類されます。

- **Reporting Licenses (Parent Licenses)**：親ライセンスはバックエンド ライセンス サーバー（CSSM）に報告され、ライセンスの使用状況に計上されます。親ライセンスごとに権限付与タグが作成され、この権限付与タグがサービスまたは機能のタイプの識別に使用されます。
- **Non-Reporting Licenses (Child Licenses)**：子ライセンスはバックエンド ライセンス サーバー（CSSM）に報告されず、これらのライセンスは親ライセンスとともにデフォルトで有効になっています。子ライセンスの権限付与タグは作成されません。

つまり、スマートライセンスは、設定されている製品タイプに基づいてすべての親ライセンスと子ライセンスを有効にします。ただし、報告が行われるのは親ライセンスのみです。

スマート ライセンス エージェントの状態は、リブートやクラッシュ後も維持されます。

Cisco スマートアカウントの要求

Cisco スマートアカウントは、スマートライセンスが有効になっているすべての製品が保管されているアカウントです。Cisco スマートアカウントを使用すると、デバイスのライセンスの管理とアクティブ化し、ライセンス使用状況のモニター、シスコライセンスの購入の追跡を行えます。透過的なアクセスにより、スマートライセンス製品をリアルタイムで表示できます。IT 管理者は、Smart Software Manager を使用して、組織のスマートアカウント内のライセンスとアカウントユーザーを管理できます。

手順

ステップ 1 ブラウザのウィンドウに次の URL を入力します。

```
https://software.cisco.com
```

ステップ 2 クレデンシャルを使用してログインし、[Administration] 領域で [Request a Smart Account] をクリックします。

[Smart Account Request] ウィンドウが表示されます。

ステップ 3 [Create Account] で、次のいずれかのオプションを選択します。

- [Yes, I have authority to represent my company and want to create the Smart Account]：このオプションを選択した場合は、組織を代表して製品とサービスの資格、ユーザー、およびロールを作成し、管理する権限に同意したことになります。
- [No, the person specified below will create the account]：このオプションを選択した場合は、スマートアカウントを作成する担当者の電子メールアドレスを入力する必要があります。

ステップ 4 [Account Information] で次の手順を実行します。

a) [Account Domain Identifier] の横にある [Edit] をクリックします。

b) [Edit Account Identifier] ダイアログボックスで、ドメインを入力し、[OK] をクリックします。デフォルトでは、ドメインはアカウントを作成する担当者の電子メールアドレスに基づいており、このアカウントを所有する企業に帰属している必要があります。

c) [Account Name] に入力します（通常は会社名）。

ステップ 5 [Continue] をクリックします。
スマートアカウント要求は、アカウントドメイン識別子によって承認されるまで保留中の状態になります。承認後、設定プロセスを実行するための手順を含む電子メールの確認が送信されます。

ソフトウェアタグと権限付与タグ

ライセンスを識別、レポート、および強制するために、次のソフトウェアおよび権限付与のタグが作成されています。

ソフトウェアタグ

ソフトウェアタグは、デバイス上の各ライセンス可能なソフトウェア製品または製品スイートを一意に識別します。CUPS には、次のソフトウェアタグがあります。

製品タイプの説明	ソフトウェアタグ
CUPS_CP 4G CUPS：コントロールプレーン	regid.2020-08.com.cisco.CUPS_CP、 1.0_7afd7a3c-38dd-4a04-aecc-26df25029649
CUPS_UP 4G CUPS：ユーザープレーン	regid.2020-08.com.cisco.CUPS_UP、 1.0_fd28551c-a541-4902-87af-bba2d6b33cf1

CUPS_CP のレポート（親）権限付与タグ

次の権限付与タグは、各製品タイプで使用されているライセンスを識別します。

ライセンスの表示名と説明	権限付与タグ	ライセンスのタイプ	レポートスラブ	タグ名
4G CUPS CP 1K 4G CUPS コントロールプレーン 1K セッション	regid.2020-08.com.cisco. L_CUPS_CP_SAE_1K、 1.0_a84e70b6-d3f9-41c9 -8449-4b7bb7426b30	カウント	1K	L_CUPS_CP _ SAE_1K

CUPS_UP のレポート（親）権限付与タグ

次の権限付与タグは、各製品タイプで使用されているライセンスを識別します。

ライセンスの表示名と説明	権限付与タグ	ライセンスのタイプ	レポートスラブ	タグ名
4G CUPS UP 1K 4G CUPS ユーザープレーン 1K セッション	regid.2020-08.com.cisco. L_CUPS_UP_SAE_1K、 1.0_41005ab7-1ad0-46ac -905b-c3c5ed402981	カウント	1K	L_CUPS_UP _SAE_1K
4G CUPS UP インスタンス 4G CUPS ユーザープレーンインスタンス	regid.2020-08.com.cisco. F_CUPS_UP_INS、 1.0_897c46a0-04b5-4fdb -bedd-9d5fb75bdb76	On/Off	1/0	F_CUPS_UP_INS

非レポート（子）ライセンスリスト

このリリースでは、親ライセンスが有効になっている場合、次の子ライセンスがデフォルトで有効になります。

ライセンスの説明	ライセンスのタイプ
PGW 1k セッション	カウント
SGW 1k セッション	カウント
GGSN 1k セッション	カウント
サブスクライバごとのステートフルファイアウォール 1k セッション	カウント
ENAT 1k セッション	カウント
拡張課金バンドル 1	カウント
拡張課金バンドル 2	On/Off

ライセンスの説明	ライセンスのタイプ
動的ポリシーインターフェイス	On/Off
拡張 LI サービス	On/Off
合法的傍受	On/Off
セッションリカバリ	On/Off
RADIUS AAA サーバーグループ	On/Off
IPv6	On/Off
インテリジェント トラフィック制御	On/Off
Diameter クローズドループ課金インターフェイス	On/Off
サブスクライバ単位のトラフィックポリシングまたはシェーピング	On/Off
ダイナミック RADIUS 拡張（CoA および PoD）	On/Off
プロキシ MIP	On/Off
FA	On/Off
IPSec	On/Off
シャーシ間セッションリカバリ	On/Off
ICSR/SR のパフォーマンスの向上	On/Off
データとコントロールプレーンの ICSR 拡張リカバリ、1K セッション	On/Off
MPLS	On/Off
TACACS+	On/Off
DPI を備えた NAT/PAT	On/Off
レート制限機能（スロットリング）	On/Off
EPC-GW の過課金保護	On/Off
EPC-GW の過課金保護のアップグレード	On/Off
Gx を介した ADC トリガー、1K セッション	On/Off
Gx ベースの仮想 APN 選択、1K セッション	On/Off
Wi-Fi 統合に対する EPC-GW サポート、1K セッション	On/Off
EPC-GW 非標準 QCI サポート、1K セッション	On/Off
ローカルポリシー意思決定エンジン	On/Off
ヘッダーの機能拡張	On/Off
HTTP ヘッダーの暗号化	On/Off

ライセンスの説明	ライセンスのタイプ
HTTP ヘッダーの機能拡張と暗号化	On/Off
ブロードキャストおよびマルチキャストサービス	On/Off
統合コンテンツ フィルタリング プロビジョニング済みサービス	On/Off
アプリケーション検出と制御 1k セッション	カウント
5G NSA 機能セット 100K セッション VPCSW アクティブ 1k セッション	カウント
5G NSA 導入料金、ネットワーク全体	On/Off
マルチメディア優先順位サービス機能セット、1K セッション	On/Off
EPC Gw VoLTE の機能拡張	On/Off
DNS スヌーピング	On/Off

スマート ライセンスの設定

作業を開始する前に、次を確認してください。

- https://software.cisco.com でスマート ライセンス アカウントを作成した。
- スマートアカウント/バーチャルアカウントの一部として作成した製品インスタンス登録トークンを使用して製品を https://software.cisco.com で登録した。
- StarOS システムと CSSM サーバーまたは Cisco.com 間の通信パスを有効にした。

スマートライセンスの有効化

CUPS のスマートライセンスは、デフォルトでは無効になっています。スマートライセンスを有効にするには、次のコンフィギュレーション モード コマンドを入力します。

```
configure
   license smart product { cups-cp | cups-up }
   license smart enable
   end
```

注：スマートライセンスを有効にする前に、[Product Type] を設定し、製品タイプに応じたデフォルトライセンスを有効にする必要があります。

次のコマンドを入力して設定を確認します。

```
show configuration | grep license
```

シスコへのデバイスの登録

https://software.cisco.com で製品を登録したときに提供された製品インスタンス登録トークンIDを使用し、次の Exec モードコマンドでシステムを登録します。

license smart register idtoken *token*

これで、システムは権限付与の使用数をCSSMサーバーに自動的に報告し、また、コンプライアンスステータスを受信するようになります。これにより、システムは「評価モード」からも削除されます。

コンプライアンスステータスを表示するには、次の Exec モードコマンドのいずれかを入力します。

```
show license status
show license summary
show license statistics
```

システムの登録が 180 日ごとに自動的に更新されます。必要に応じて、次の Exec モードコマンドを使用して、登録情報を手動で更新します。

license smart renew id

システムのライセンス承認は 30 日ごとに自動で更新されます。必要に応じて、次の Exec モードコマンドを使用して、ライセンス承認を手動で更新します。

license smart renew auth

デバイスの登録を解除するには、次の Exec モードコマンドを入力します。

license smart deregister

スマートトランスポート URL の変更

スマートエージェントは、Smart Transportを使用してCisco CSSMサーバーと通信します。Smart Transport は、設定済みの URL を使用して、CSSM が到達可能な接続先 URL を識別します。これにより、シスコとの通信が開始されることはありません。必要に応じて、次の [Configuration] モードコマンドを入力します。

```
configure
  license smart transport smart
  license smart url https_link
```

コンプライアンス違反の処理

特定の SKU のバーチャルアカウントに十分なライセンスがない場合、CSSM はコンプライアンス違反（OOC）メッセージをデバイスに送信します。システムは OOC 状態がクリアされるまで、追加のセッション許可を停止します。デバイスが承認済み応答を受信すると、OOC 状態がクリアされます。

スマートライセンシングのモニタリングとトラブルシューティング

次の Exec モードコマンドを入力して、スマートライセンスの設定を確認します。

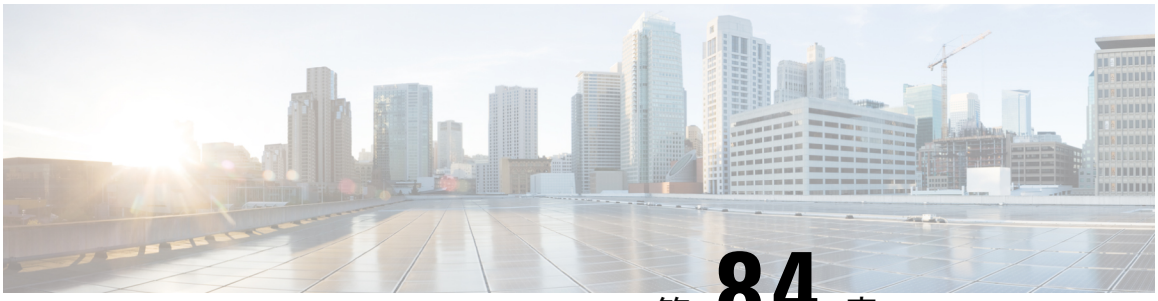
show configuration | grep license

次の Exec モードコマンドは、スマートライセンスに関する情報を表示します。

show license { all | enforcement | smart-tags | statistics | status | summary | tech-support | udi | usage }

注：

- **all**：ステータスの表示、使用状況の表示、UDI の表示、および スマート ライセンス エージェントのバージョンを含む情報のスーパーセットを表示します。
- **enforcement { policy | status [allowed | blocked] [feature | service] }**：適用された実施ポリシー、またはスマートライセンスの現在の適用ステータスを表示します。ステータス情報をフィルタリングして、現在許可またはブロックされているライセンスのみ、またはタイプ（機能ライセンスまたはサービスライセンス）ごとに表示できます。
- **smart-tags [feature | service]**：現在サポートされている機能とサービス、および対応するスマート権限付与タグを表示します。
- **statistics [verbose]**：個々の機能ライセンスのステータスを表示します。
- **status**：スマート ライセンスのステータス情報を表示します。
- **summary**：スマートライセンスのステータスの概要を表示します。
- **tech-support**：スマートライセンスの問題のデバッグに役立つ情報を表示します。
- **udi**：すべての一意のデバイス ID（UDI）の詳細を表示します。
- **usage**：現在使用されているすべての権限付与の使用状況情報を表示します。



第 84 章

ソフトウェア管理の運用

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
ソフトウェアリリースのN-4下位互換性のためにサポートを拡張。	21.26
ソフトウェアリリースのN-3下位互換性のためにサポートを拡張。	21.25
ソフトウェアリリースのN-2下位互換性のためにサポートを拡張。	21.24.1
最初の導入。	21.24 より前

概要

CUPS は、コントロールプレーン（CP）およびユーザープレーン（UP）でのソフトウェアリリースの下位互換性をサポートしています。この機能により、1つ前のリリース（N-1）、2つ前のリリース（N-2）、3 つ前のリリース（N-3）、4 つ前のリリース（N-4）の間で、ソフトウェアをシームレスにアップグレードまたはダウングレードできます。この機能には、次のサポートが含まれます。

- ICSR モードの 2 つの CP におけるソフトウェアリリースの N-1/N-2/N-3 /N-4 互換性：CP 1:1 冗長性シナリオで、CP をバージョン間でシームレスにアップグレードできます。

- ICSR モードの 2 つの UP におけるソフトウェアリリースの N-1/N-2/N-3 /N-4 互換性：UP 1:1 冗長性シナリオで、UP をバージョン間でシームレスにアップグレードできます。
- CP と UP 間のソフトウェアリリースの N-1/N-2/N-3/N-4 互換性：関連付けられた CP または UP をバージョン間でシームレスにアップグレードできます。
- マルチ Sx を使用した CP と UP 間のソフトウェアリリースの N-1/N-2/N-3/N-4 互換性：マルチ Sx シナリオで、関連付けられた CP または UP をバージョン間でシームレスにアップグレードできます。

重要 ソフトウェアバージョンをアップグレードまたはダウングレードする前に、シスコのアカウント担当者に連絡して、手順に関するサポートを受けてください。

CP と UP 間のバージョン交換

CP と UP がペアになると、バージョンまたはリリース情報が交換されます。リリース情報は、アクティブとスタンバイの間で交換されるハートビートメッセージを介して、CP がスタンバイ CP とペアになったり、UP がスタンバイ UP とペアになったりする場合（1:1 冗長シナリオ）にも交換されます。

互換性のないリリースがペアリングされると、アラーム（SNMP トラップ）が発生します。詳細については、「SNMP トラップ」の項を参照してください。

リリース情報の交換中にピアバージョンを示すために、関連付け要求およびハートビート要求メッセージに次の新しい IE が含まれています。

情報要素	P	条件/コメント								IE の長さ	IE ID
ピアバージョン	O	ピア GR/PFCP バージョンと StarOS バージョンを指定するために使用されます。								4 バイト	245
		ビット									
	オクテット	8	7	6	5	4	3	2	1		
	1 ～ 2	ピアバージョン IE タイプ = 245（10 進数）									
	3 ～ 4	長さ = n バイト									
	5 ～ 8	ピア GR/PFCP バージョン									
	9 ～ 12	StarOS GR バージョン									
	13 ～ 13	StarOS バージョン文字列長									
	可変長	StarOS バージョン文字列値									

SNMP トラップ

互換性のないリリースとのペアリングが行われると、次の SNMP トラップが発生します。

SNMP トラップ	説明
SRPPeerUnsupportedVersion	上位バージョンのアクティブ/スタンバイ CP/UP は、ピアのバージョンが N-4 よりも下位の場合に SNMP トラップを発生させます。
SRPPeerUnsupportedVersionClear	上位バージョンのアクティブ/スタンバイ CP/UP は、SNMP トラップを発生させて SRPPeerUnsupportedVersion をクリアします。
SxPeerUnsupportedVersion	上位バージョンの CP/UP は、ピアのバージョンが N-4 よりも下位の場合に SNMP トラップを発生させます。
SxPeerUnsupportedVersionClear	上位バージョンの CP/UP は、SNMP トラップを発生させて SxPeerUnsupportedVersion をクリアします。

制限事項

この機能には次の既知の制限事項があります。

- ピアバージョンがサポートされている N-4 バージョンよりも低いと判断された場合、関連付けとペアリングが許可されますが、同じ機能の側面は保証されません。

⚠

注意 互換性のないバージョンからはアップグレードしないでください。アップグレードパスや手順については、シスコのアカウント担当者にお問い合わせください。

SNMP トラップは、StarOS バージョンに関しては最新バージョンのノードによって発生します。詳細については、この章の「*SNMP* トラップ」の項を参照してください。

- リリース 21.24.1 以降、RCM はチェックポイントに依存せず、将来の UP リリースのサポートを可能にします。現在、RCM は N-4 互換性をサポートしておらず、N-1 互換性のみをサポートしています。

CP および UP のアップグレードまたはダウングレード

次のメンテナンス操作手順（MOP）では、コントロールプレーンとユーザープレーンを以前のリリース（N-1）/（N-2）/（N-3）/（N-4）から最新の N リリースにアップグレードするか、または逆にダウングレードするために必要な手順の概要を示します。

重要 ソフトウェアバージョンをアップグレードまたはダウングレードする前に、シスコのアカウント担当者に連絡して、手順に関するサポートを受けてください。

アップグレードオプションは次のとおりです。

- [Only CP Upgrade]：CP のみをアップグレードし、UP はそのままにする必要がある場合。
- [Only UP Upgrade]：UP のみをアップグレードし、CP はそのままにする必要がある場合。
- [Both CP and UP Upgrade]：CP と UP の両方をアップグレードする必要がある場合。この場合、最初に CP をアップグレードしてから UP をアップグレードするか、その逆を行います。

正常性チェック

シャーシのアップグレード、ダウングレード、またはリロードの各操作の後に、次の正常性チェックを実行します。

1. アクティブシャーシのサービス冗長性プロトコル（SRP）情報を確認して、SRP スイッチオーバー中の問題を回避し、SRP スイッチオーバーの前にプロアクティブな分析の実施が必要かどうかを判断します。次の CLI コマンドを使用します。
   - **srp validate-configuration srp validate-switchover**
   - **show srp info**

   次に、出力例を示します。

   ```
   Peer Configuration Validation: Complete
   Last Peer Configuration Error: None
   Last Peer Configuration Event: Wed Mar 18 15:34:02 2019  (1602 seconds ago)
   Last Validate Switchover Status: None
   Connection State: Connected
   ```

   次のパラメータを確認します。

   - **Peer Configuration Validation: Complete**：[In Progress] と表示されている場合は、15 秒ほど待ってから **show srp info** を再度実行する必要があります。
   - **Last Peer Configuration Error: None**：[Peer Checksum Validation Failure] と表示された場合は、アクティブシャーシとスタンバイシャーシ間で設定に相違があり、修正が必要であることを示しています。
   - **Last Validate Switchover Status: None**：出力に [None] と表示される必要があります。また、**srp validate-configuration** および **srp validate-switchover** CLI コマンドがトリガーされると、出力は [Remote Chassis - Ready for Switchover (XX seconds before)] になります。
   - **Connection State: Connected**：出力に [Connected] と表示される必要があります。

2. アクティブシャーシとスタンバイシャーシの両方のサブスクライバ数を確認します。

   セッションが起動したら、アクティブシャーシで **show subscribers summary | grep Total** CLI コマンドを実行します。次に、出力例を示します。

```
show subscribers summary | grep Total
   Total Subscribers:  100
```

   スタンバイシャーシで、**show srp checkpoint statistics | grep allocated** CLI コマンドを実行します。次に、出力例を示します。

```
show srp checkpoint statistics | grep allocated
   Current pre-allocated calls:  100
```

3. **show license information** CLI コマンドを実行して、ライセンスのステータスを確認します。ステータスは [Expired] ではなく、[Good (Redundant)] である必要があります。

4. **show session recovery status verbose** CLI コマンドを実行して、セッション リカバリ ステータスを確認します。次に、出力例を示します。

```
Session Recovery Status:
  Overall Status        : Ready For Recovery
  Last Status Update    : 7 seconds ago

              ----sessmgr---  ----aaamgr----  demux
 cpu state    active standby  active standby  active  status
1/0  Active     8      1        8      1        17     Good
```

5. **show srp checkpoint statistics | grep Sessmgrs** CLI コマンドを実行して、スタンバイシャーシのすべての SessMgr が [Standby-Connected] 状態であることを確認します。次に、出力例を示します。

```
Number of Sessmgrs:        1
Sessmgrs in Active-Connected state:  0
Sessmgrs in Standby-Connected state: 8
Sessmgrs in Pending-Active state:    0
```

6. すべてのカードのステータスを確認して、[Active] 状態か [Standby] 状態かを確認します。次に、出力例を示します。

```
show card table

Slot          Card Type              Oper State  SPOF  Attach
------------ ------------------------ ----------- ----- ------
1: VC        5-Port Virtual Card     Active        -
```

7. **show task resources | grep -v good** CLI コマンドを実行します。出力には SessMgr とセッションの合計数のみが表示される必要があります。

8. **show crash list** CLI コマンドを実行して、新しいクラッシュがあったかどうかを確認します。

9. **show service all** CLI コマンドを実行して、状態が [Initialized] ではなく [Started] と表示されていることを確認します。

ビルドアップグレード

Backup Configuration

1. 現在の設定をバックアップし、現在の設定を保存します。バックアップは、ダウングレード時に使用されます。ダウングレードには、現在までのすべての機能と設定が含まれている可能性があります。
2. 変更またはアップグレードを実行する前に、アクティブシャーシとスタンバイシャーシの両方で **show support details** を収集します。
3. ヘルスチェックを実行します。

アップグレード手順

1. 両方のノードでシャーシのヘルスチェックを実行します。
2. スタンバイ状態のセカンダリシャーシ（ICSR）で、起動優先順位を N ビルドに変更します。
3. 最新の 21.xx.xx ビルドにリロードします。
4. スタンバイシャーシで新しい設定の変更を行います（たとえば、新しいCLI、ライセンス、または設定の変更）。
5. リロードされたシャーシでヘルスチェックを実行します。クラッシュやエラーを確認します。

スイッチオーバーの実行

1. 両方のシャーシでSRPをアクティブからスタンバイに切り替える前に、以下の点を確認します。
   1. アクティブシャーシ：**show subscriber summary | grep Total**
   2. スタンバイシャーシ：**show srp checkpoint statistics | grep allocated**

（注） カウントは両方で同じである必要があります。

   3. アクティブおよびスタンバイシャーシ：**show sx peer**

      次に例を示します。

```
|||||  Sx Service                                                    No of
|||||  ID                                                                Restart
|||||  |                                                 Recovery              |
   Current    Max        Peer
vvvvv  v     Group Name    Node ID         Peer ID     Timestamp             v
   Sessions   Sessions   State
----- ---- ----------------- ------------------------ ------------------- ------
 --------- --------- --------
```

```
CAAXD  22     CPGROUP21   209.165.200.225   50331649    2021-03-17:02:33:55    0
        0           0       NONE

Total Peers:    1
```

（注） ピアの状態はアクティブであり、関連付けられている必要があります。ピアIDは両方のシャーシで一致する必要があります。

4. スタンバイシャーシ：**show srp checkpoint statistics | grep Sessmgrs**

（注） 「Number of Sessmgrs」は「Sessmgrs in Standby-Connected state」と同じである必要があります。

5. アクティブシャーシ：
   1. **srp validate-configuration**：この CLI コマンドは、アクティブシャーシから設定検証チェックを開始するコマンドです。エラーがない場合、この CLI コマンドの出力は空白になります。
   2. **srp validate-switchover**：アクティブシャーシとスタンバイシャーシの両方で計画した SRP スイッチオーバーの準備ができていることを検証します。スイッチオーバーの準備ができている場合、この CLI コマンドの出力は空白になります。
   3. **show srp info | grep "Last Validate Switchover Status"** ：この CLI コマンドの出力は次のようになります。

      ```
      Last Validate Switchover Status: Remote Chassis - Ready for Switchover
      ```

   4. **show srp info debug**：アクティブシャーシとスタンバイシャーシの出力は同じである必要があります。

2. アクティブシャーシ：**srp initiate-switchover**
   1. 両方のノードでシャーシのヘルスチェックを実行します。また、「スイッチオーバーの実行」の項のステップ 1a とステップ 1c を確認します。5% の差が生じる場合があります。
   2. 新しいセッションは新しいアクティブシャーシで処理されるため、コールテストを実行します。
   3. 「アップグレード手順」の項のステップ 2 からステップ 5 で説明されているように、古いアクティブシャーシをアップグレードします。

CP のアップグレード

ここでは、CP のみを対象にアップグレード手順を説明します。

1. 正常性チェック （830ページ）の項の説明に従って、両方のCPノードで正常性チェック手順を実行します。
2. ビルドアップグレード （832ページ）の項の説明に従って、スタンバイCPでアップグレードを実行します。

（注） CPとUPのコンテキスト名が異なる場合は、アップグレードされたCPで**debug pgw pfd-mgmt** CLIコマンドを実行してからアクティブにします。

3. 両方のシャーシで正常性チェックを実行し、アップグレードされたシャーシにCPスイッチオーバーを実行します。
4. 新しいシャーシが新しいセッションを取得していること、新しいクラッシュがないこと、またはエラーシナリオによるセッションのドロップがないことを確認します。CPとUPの両方で正常性チェックを実行します。
5. ビルドアップグレード （832ページ）の項の説明に従って、新しいスタンバイCPをアップグレードします。

UP のアップグレード

ここでは、UP のみを対象にアップグレード手順を説明します。

1. 正常性チェック （830 ページ）の項の説明に従って、両方の UP ノードで正常性チェック手順を実行します。
2. ビルドアップグレード （832ページ）の項の説明に従って、スタンバイUPでアップグレードを実行します。
3. アップグレードされたスタンバイシャーシで「sx-peer configuration」を実行します。
4. 両方のUPノードで正常性チェックを実行してから、UPスイッチオーバーを実行します。
5. ビルドアップグレード （832 ページ）の項の説明に従って、新しいスタンバイ UP をアップグレードします。

CP および UP のアップグレード

ここでは、最初に CP をアップグレードしてから UP をアップグレードする手順、またはその逆の手順について説明します。

CP を最初にアップグレードする場合

1. 正常性チェック （830ページ）の項の説明に従って、CPとUPの両方で正常性チェック手順を実行します。

2. ビルドアップグレード（832 ページ）の項の説明に従って、スタンバイ CP でアップグレードを実行します。

（注） CP と UP のコンテキスト名が異なる場合は、アップグレードされた CP で **debug pgw pfd-mgmt** CLI コマンドを実行してからアクティブにします。

3. ビルドアップグレード（832 ページ）の項の説明に従って、スタンバイ UP でアップグレードを実行します。
4. スタンバイ CP と UP の両方を N ビルドにアップグレードします。
5. 両方のシャーシで正常性チェックを実行し、アップグレードされたシャーシへの CP スイッチオーバーを実行します。
6. 新しいシャーシが新しいセッションを取得していること、新しいクラッシュがないこと、またはエラーシナリオによるセッションのドロップがないことを確認します。
7. 両方の UP ノードで正常性チェックを実行してから、UP スイッチオーバーを実行します。
8. 新しくアクティブになった UP で正常性チェックを実行します。コールのドロップがなく、データが新しいシャーシを通過していることを確認します。
9. ビルドアップグレード（832 ページ）の項の説明に従って、新しいスタンバイ CP と UP をアップグレードします。

UP を最初にアップグレードする場合

1. CP と UP の両方で正常性チェックとビルド転送手順を実行します。
2. ビルドアップグレード（832 ページ）の項の説明に従って、スタンバイ UP でアップグレードを実行します。
3. アップグレードされたスタンバイシャーシで「sx-peer configuration」を実行します。
4. 両方の UP ノードで正常性チェックを実行してから、UP スイッチオーバーを実行します。
5. ビルドアップグレード（832 ページ）の項の説明に従って、新しいスタンバイ UP でアップグレードを実行します。
6. ビルドアップグレード（832 ページ）の項の説明に従って、スタンバイ CP でアップグレードを実行します。
7. 両方の CP ノードで正常性チェックを実行してから、CP スイッチオーバーを実行します。

（注） CP と UP のコンテキスト名が異なる場合は、CP で **debug pgw pfd-mgmt** CLI コマンドを実行します。

8. 新しいスタンバイ CP シャーシをアップグレードします。正常性チェックを実行します。
9. アクティブ UP とスタンバイ UP の両方で正常性チェックを実行します。
10. すべてが想定どおりに機能している場合は、最初にスタンバイ CP で設定の変更を行います。次に、アクティブ CP で同様の変更を行い、**push config-to-up all** CLI コマンドを実行します。新しい変更内容は、新しいアクティブ UP にプッシュされます。

ダウングレード手順

ダウングレード：CP と UP の両方

アップグレードの一環として CP で新しい設定や設定変更が必要な場合は、まず UP のアップグレード手順に従います。

1. CP と UP の両方で正常性チェックを実行します。
2. スタンバイ UP でブートの優先順位を N-1/N-2/N-3/N-4 ビルドに変更します。スタンバイ UP をリロードします。
3. ダウングレードされたスタンバイ UP で「sx-peer configuration」を実行します。
4. 両方の UP ノードで正常性チェックを実行してから、UP スイッチオーバーを実行します。
5. 新しいスタンバイ UP でステップ 1 ～ 3 を実行します。
6. スタンバイ CP でブートの優先順位を N-1/N-2/N-3/N-4 ビルドに変更します。スタンバイ CP をリロードします。

（注） CP と UP のコンテキスト名が異なる場合は、CP で **debug pgw pfd-mgmt..** CLI コマンドを実行します。

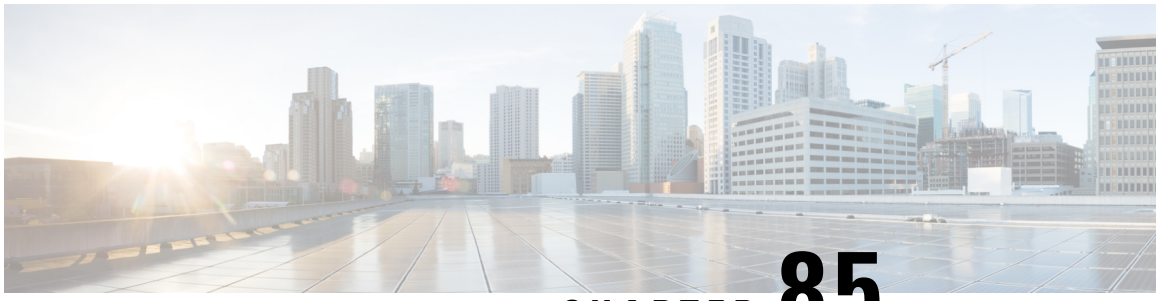
7. ビルドアップグレード （832 ページ）の「バックアップの設定」の項に記載されているステップ 1 で保存した設定をロードします。
8. 両方の CP ノードで正常性チェックを実行してから、CP スイッチオーバーを実行します。
9. ステップ 6 と 7 を実行して古いアクティブノードをダウングレードします。
10. アクティブ CP で、**push config-to-up all** CLI コマンドを実行して、設定の変更が UP にプッシュされるようにします。

ダウングレード：**CP** のみ

「ダウングレード：*CP* と *UP* の両方」の項に記載されているステップ 6 ～ 10 を実行します。

ダウングレード：**UP** のみ

「ダウングレード：*CP* と *UP* の両方」の項に記載されているステップ 1 ～ 5 を実行します。



CHAPTER 85

標準 QCI のサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
最初の導入。	21.24 より前

機能説明

重要 標準 QCI は、CUPS アーキテクチャではサポートおよび認定されていません。

標準化された QCI 値（65、66、69、および 70）は、ミッションクリティカルおよびプッシュツートーク（MC/PTT）アプリケーションをサポートします。標準 QCI は 3GPP TS 23.203 リリース 12 に基づいています。

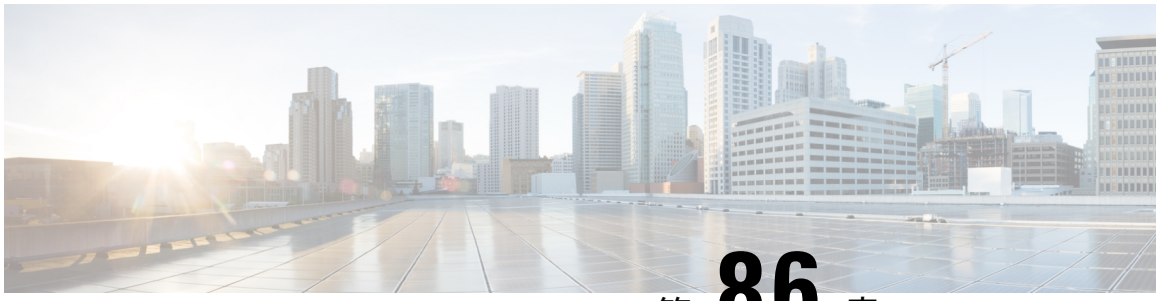
この機能は、次の機能をサポートしています。

- デフォルトベアラーおよび専用ベアラーを作成、削除、および更新します。
- 対象となるすべての課金レコードに標準 QCI 値が含まれます。
- QCI に関連するすべての機能が標準 QCI 値と連動します。

制限事項

この機能には次の既知の制限事項があります。

- S2a/S2b/GGSN はサポートされません。
- eMPS 機能全体はサポートされていません。
- **require ecs credit-control session-mode per-subscriber** が設定されている場合、URR はセカンダリベアラーを含むサブスクライバセッション全体で処理されるため、一部のアプリケーションで問題が発生する可能性があります。CUPS では、APN レベルで **credit-control-client override session-mode per-sub-session** コマンドを使用して、セッションモードの設定を上書きします。



第 86 章

シャロー パケット インスペクションの静的ルールと事前定義ルールの照合のサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

この機能により、CUPS 展開内のノードまたは進行中のセッションに関連するさまざまなデータ統計情報を確認するためのサポートが追加されます。

この機能をサポートするために、新しいキーワード「real-time」が次の CLI コマンドに追加されました。

- show apn statistics real-time：このコントロールプレーンに接続されている全ユーザープレーンのすべての APN に関する集約データと制御統計情報を表示します。

- show apn statistics real-time all：このコントロールプレーンに接続されている全ユーザープレーンのデータおよび制御統計情報を APN ごとに表示します。
- show apn statistics real-time name：特定の APN に対するすべてのユーザープレーンからデータを取得して、データおよび制御統計情報を表示します。

重要 このリリースでは、次の 8 つのカウンタのみサポートされています。

- アップリンクバイト数
- ダウンリンクバイト数
- アップリンクパケット数
- ダウンリンクパケット数
- ドロップされたアップリンクバイト数
- ドロップされたダウンリンクバイト数
- ドロップされたアップリンクパケット数
- ドロップされたダウンリンクパケット数

機能の仕組み

以下に、SPI 機能の仕組みについて簡単に説明します。

- コントロールプレーンで使用可能な静的ルールポリシーおよび事前定義ルールポリシーは、サブスクライバに関連付けられている rulebase に基づいてユーザープレーンにパーコレートされます。この情報は、コントロールプレーンで PDR フォーマットに変換されます。

  コントロールプレーン上の静的ルールおよび事前定義ルールは、PDR に変換され、静的ルールを rulebase PDR に変換するために送信されます。同時に事前定義ルールは、PDR ID に変換され、個々の PDR ID がユーザープレーンに送信されアクティブ化されます。この方法によって、一連のサブスクライバポリシーがユーザープレーンで定義されます。

  セッションの確立により、サブスクライバが使用可能な事前定義された静的ルールが関連付けられます。これにより、サブスクライバに関連付けられているポリシーの実装に対応します。

- PDR 照合では、該当する PDR の PDI フィールドで指定されたフィルタに対してデータパケットをマッピングします。すべてのフィルタ条件が一致すると、パケットが PDR に一致します。FAR ID に基づいて、パケットに対して実行するアクションが認識されます。それに応じてサービスチェーンが更新され、実行されます。

- 静的ルールと事前定義ルールの場合、QCI、サービスID、および評価グループの組み合わせに基づいて一意のURRが生成され、コントロールプレーンで設定されます。このURRはユーザープレーンに渡され、転送アクションが実装されます。

  この情報に基づいて、URRの更新やQERの適用など、パケットに対するポリシングおよび課金アクションが実装されます。

  PDRに一致した場合、転送アクションによってパケットが「許可」または「破棄」されます。

モニタリングおよびトラブルシューティング

この項では、この機能のサポートにおけるshowコマンドまたはその出力について説明します。

コマンドや出力の表示

この項では、この機能のサポートにおけるshowコマンドまたはその出力について説明します。

show subscribers user-plane-only full all

このコマンドの出力範囲が拡張されて、この機能をサポートする次の新しいフィールドと値が追加されました。

- 静的ルールと事前定義ルール一致の統計情報
  - Rule Name
  - Pkts-Down
  - Bytes-Down
  - Bytes-Up
  - Hits
  - Match-Bypassed
- ダイナミックルール一致の統計情報
  - PDR Id
  - Pkts-Down
  - Bytes-Down
  - Pkts-Up
  - Bytes-Up
  - Hits
  - Match-Bypassed

show subscribers user-plane-only callid <callid> pdr full all

このコマンドの出力が拡張され、この機能をサポートする次のフィールドが追加されました。

ルール名

このフィールドは、事前定義されたルールに対してのみ表示されます。

show subscribers user-plane-only seid <seid> pdr full all

このコマンドの出力が拡張され、この機能をサポートする次のフィールドが追加されました。

ルール名

このフィールドは、事前定義されたルールの場合にのみ表示されます。

show subscribers user-plane-only callid <callid> pdr id <id>

このコマンドの出力が拡張され、この機能のサポートに次のフィールドが含まれています。

ルール名

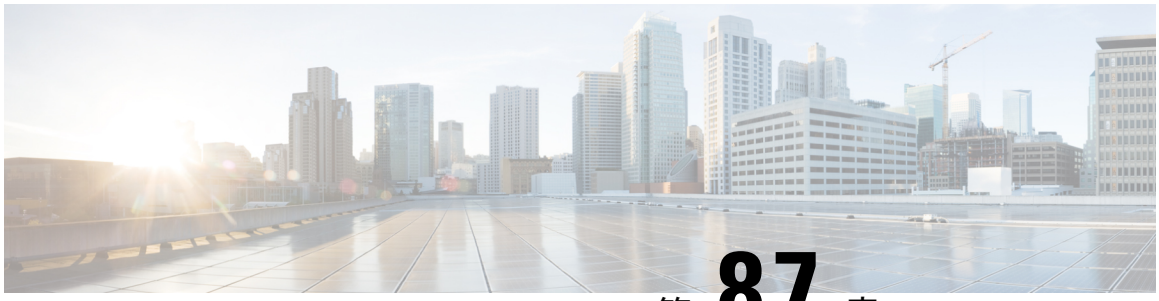
このフィールドは、事前定義されたルールに対してのみ表示されます。

show subscribers user-plane-only seid <seid> pdr id <id>

このコマンドの出力が拡張され、この機能のサポートに次のフィールドが含まれています。

ルール名

このフィールドは、事前定義されたルールに対してのみ表示されます。



第 87 章

RADIUS からの静的 IP の割り当て

機能説明

この機能では、サブスクライバの静的 IP アドレスは、初回の認証手順において RADIUS サーバーから割り当てられます。この機能は、CUPS で使用可能な静的 IP アドレス（UE からの要求による）機能を活用します。

機能の仕組み

RADIUS サーバーがセッションに静的 IP アドレスを割り当てた後、静的セッションのユーザープレーンの選択は、APN に関連付けられているユーザープレーングループからユーザープレーンへのチャンクの割り当てに従って固定されます。

複数の APN で同じ静的 IP アドレスの範囲が使用されている場合は、それらの APN で同じユーザープレーングループを使用することを推奨します。

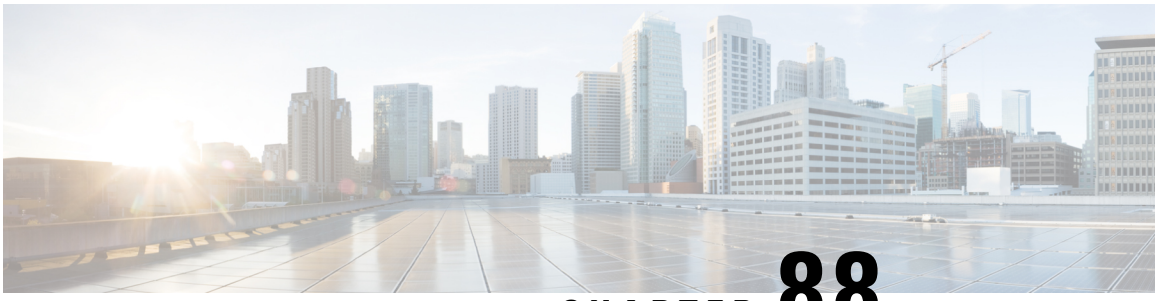
静的 IP プール管理の詳細については、『*Ultra Packet Core CUPS User Plane Administration Guide*』*[英語]* または『*Ultra Packet Core CUPS Control Plane Administration Guide*』[英語] の IP プール管理に関する章を参照してください。

制限事項

この機能には次の既知の制限事項があります。

- RADIUS からの静的 IP アドレスプールの割り当ては、この機能ではサポートされません。
- SAEGW-C は、IP アドレスの 1 つ（IPv4 または IPv6、またはその両方）が静的アドレスであっても、RADIUS から受信した静的アドレスを使用した IPv4v6 PDN タイプのコールをサポートしません。
- SAEGW-C は、[allow-static] タイプのプール設定をサポートしていません。

- 静的 IP アドレス割り当てを使用したマルチ PDN コールはサポートされません。



CHAPTER 88

Pure-S コールの一時停止および再開通知

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

Pure-S コールの一時停止および再開通知が CUPS アーキテクチャでサポートされるようになりました。ユーザープレーン（UP）とコントロールプレーン（CP）は、一時停止/再開通知を受信すると、Sx 確立/変更要求を介して通信します。

進行中のストリームは UP で維持されます。CP は一時停止/再開通知を受信すると、Sx 変更要求メッセージを介して UP の FAR アクションを変更します。UP は応答として適切な FAR アクションを設定します。

一時停止通知後にベアラー変更要求を受信すると、eNodeB TEID が MBReq に存在する場合、FAR でモードが転送に設定されます。eNodeB TEID が存在しない場合、モードはバッファに設定されます。

機能の仕組み

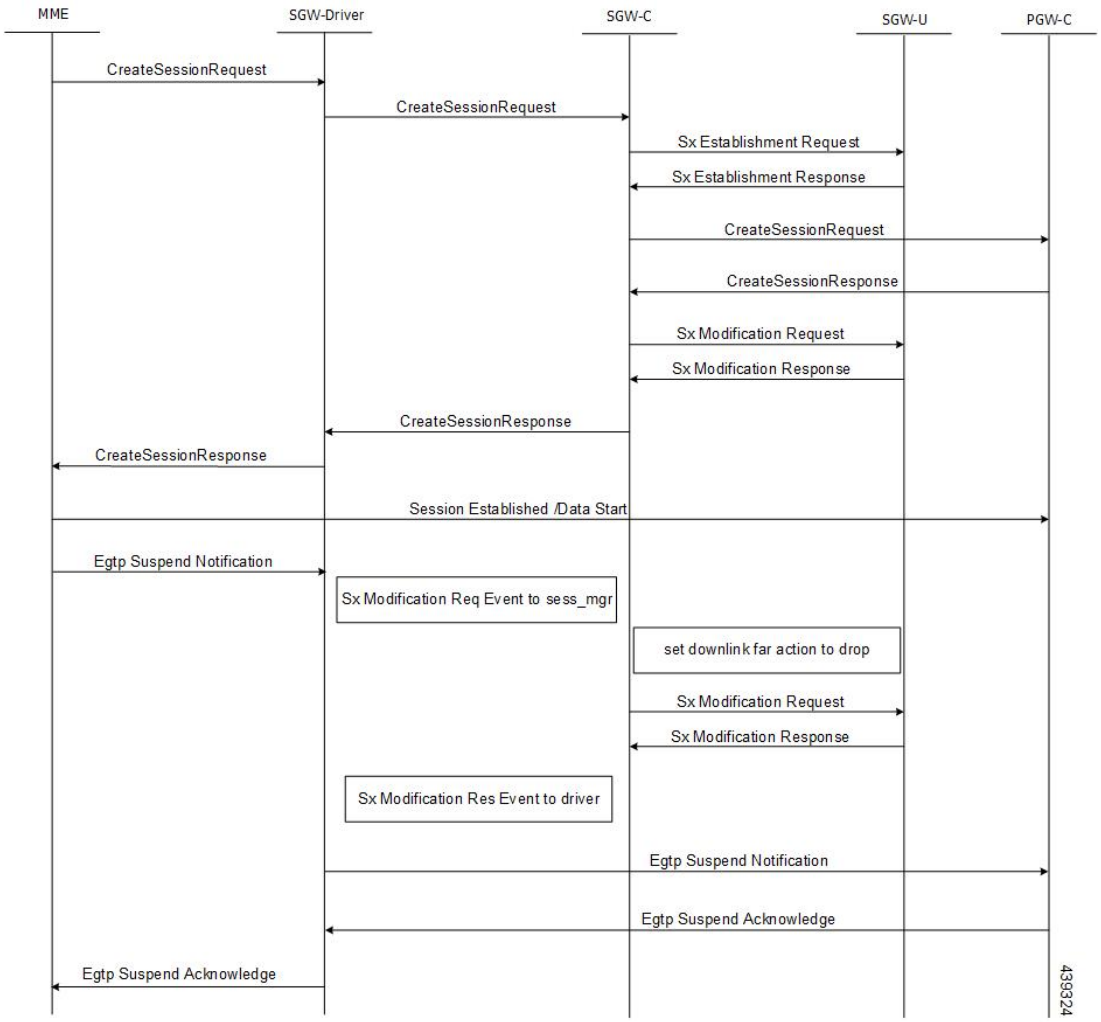
一時停止通知では、ダウンリンク方向の FAR アクションを DROP に設定することで、ダウンリンクデータが一時停止されます。再開通知では、ダウンリンク方向の FAR アクションを BUFFER に設定することで、ダウンリンクデータがバッファリングされます。

コール フロー

一時停止通知

Pure-S コールで一時停止通知を受信すると、SGW-C は FAR アクションを DROP に設定して Sx セッション変更要求を SGW-U に送信することで、FAR のダウンロードアクションを更新します。

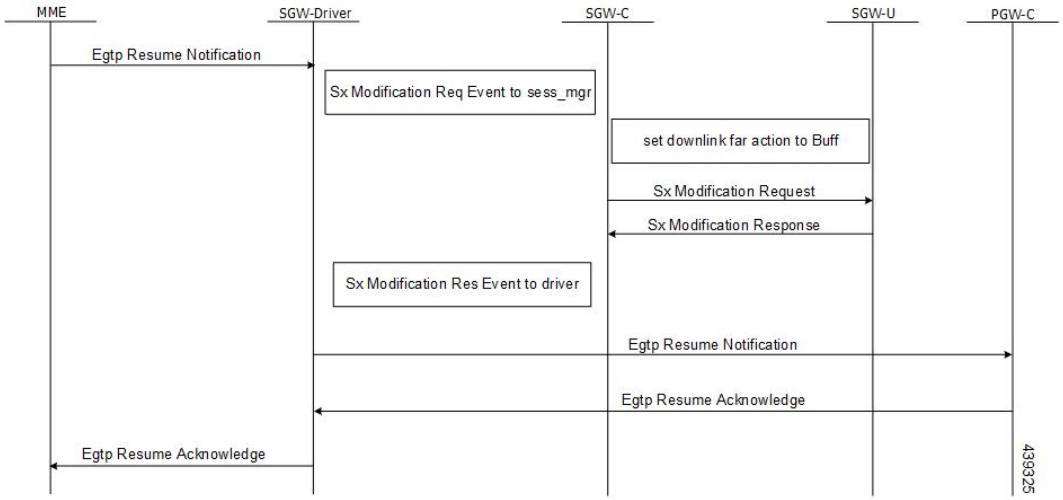
次のコールフローの概要は、Pure-S コールの一時停止通知を示しています。

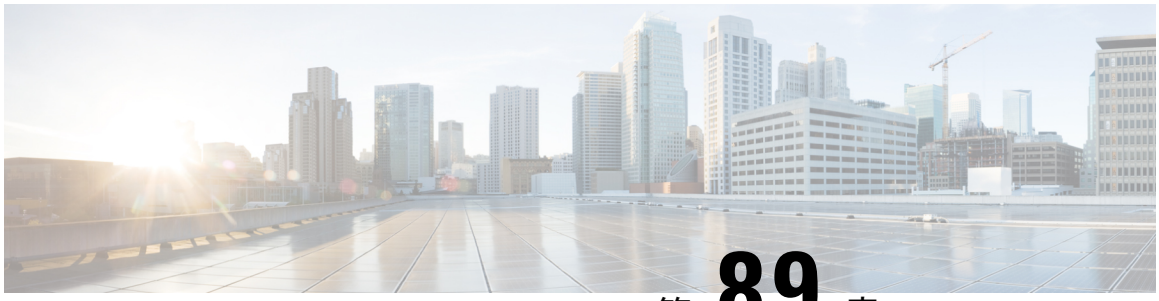


再開通知

Pure-S コールで再開通知を受信すると、SGW-C は FAR アクションを [BUFFER] に設定した Sx セッション変更要求を SGW-U に送信することで、FAR のダウンロードアクションを更新します。

次のコールフローは、Pure-S コールの再開通知の概要を示しています。





第 89 章

TACACS+ Over IPSec

マニュアルの変更履歴

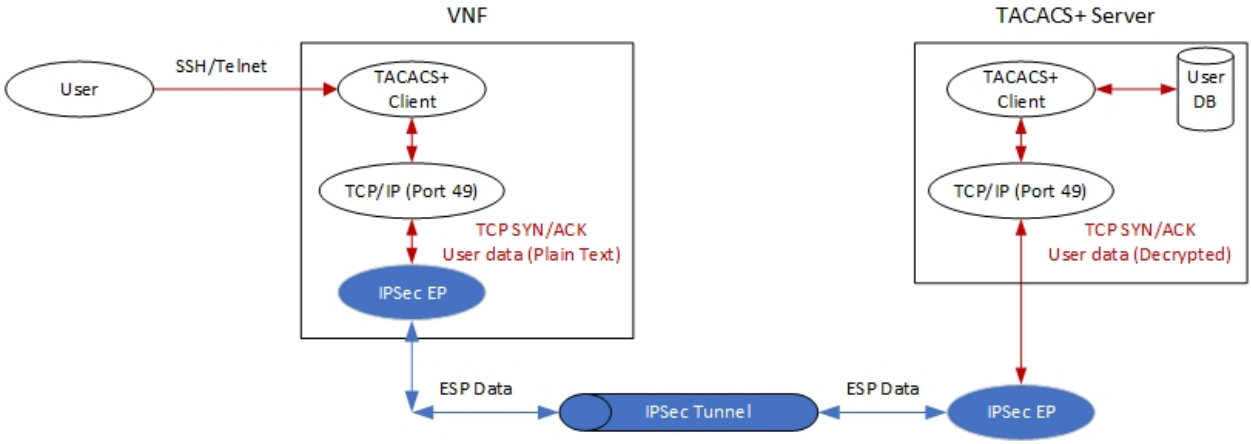
改訂の詳細	リリース
初版	21.24

機能説明

Terminal Access Controller Access Control Server Plus（TACACS+）は、StarOS でのユーザーアクセス権限の認証に使用されるセキュリティプロトコルです。TACACS+クライアントおよびサーバーを介して送信される認証データを保護するために、CUPS VNF は認証データの暗号化に関して TACACS+ over IPSec をサポートしています。

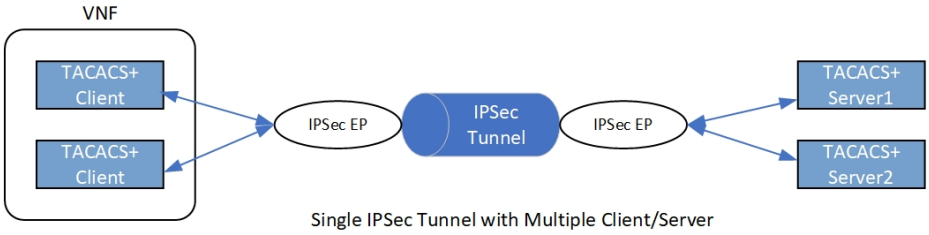
アーキテクチャ

次の図は、セキュアな TACACS+ アーキテクチャを示しています。

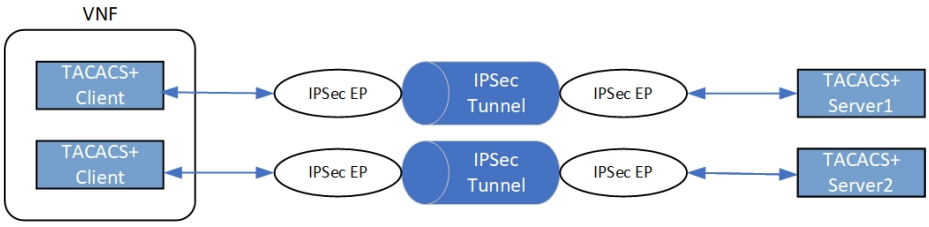


導入アーキテクチャ

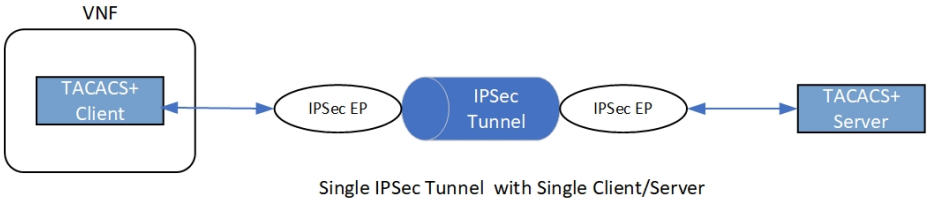
TACACS+クライアント/サーバーをセキュアな方法で使用する方法は複数あります。単一または複数の TACACS+ サーバーを使用できます。単一の VNF で単一または複数のクライアントをホストできます。TACACS+ over IPSec ソリューションは、単一の VNF で複数のクライアントを処理できます。



Single IPSec Tunnel with Multiple Client/Server



Multiple IPSec Tunnel with Multiple Client/Server



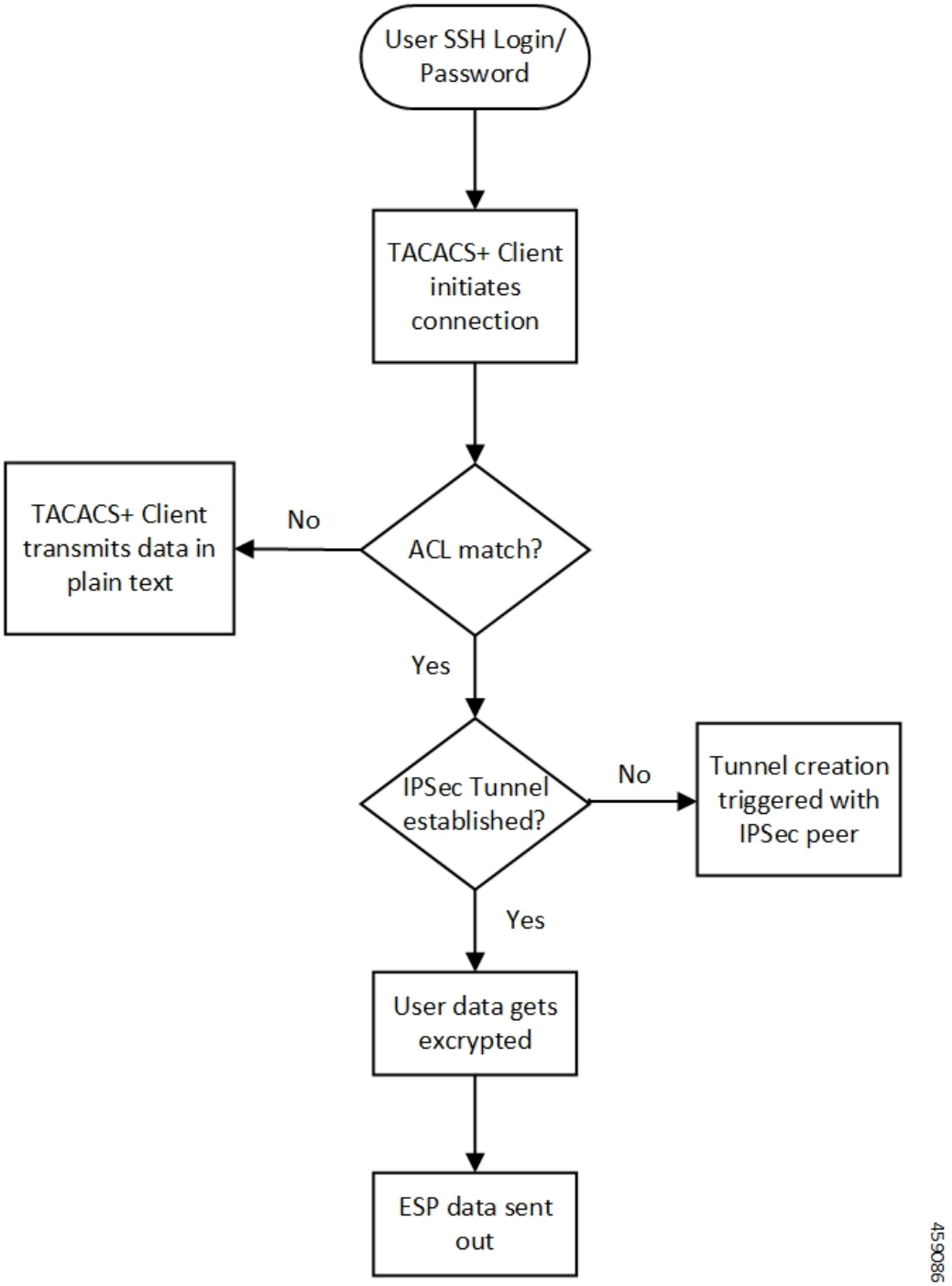
Single IPSec Tunnel with Single Client/Server

機能の仕組み

展開要件に応じて、保護する必要がある複数のアプリケーションには、独立した ACL ルールがあります。これらの ACL ルールは、単一の暗号マップまたは個別の暗号マップの一部として設定されます。どちらの場合も、複数の TUN インターフェイスが作成され、暗号化を必要とする各アプリケーションに接続されます。

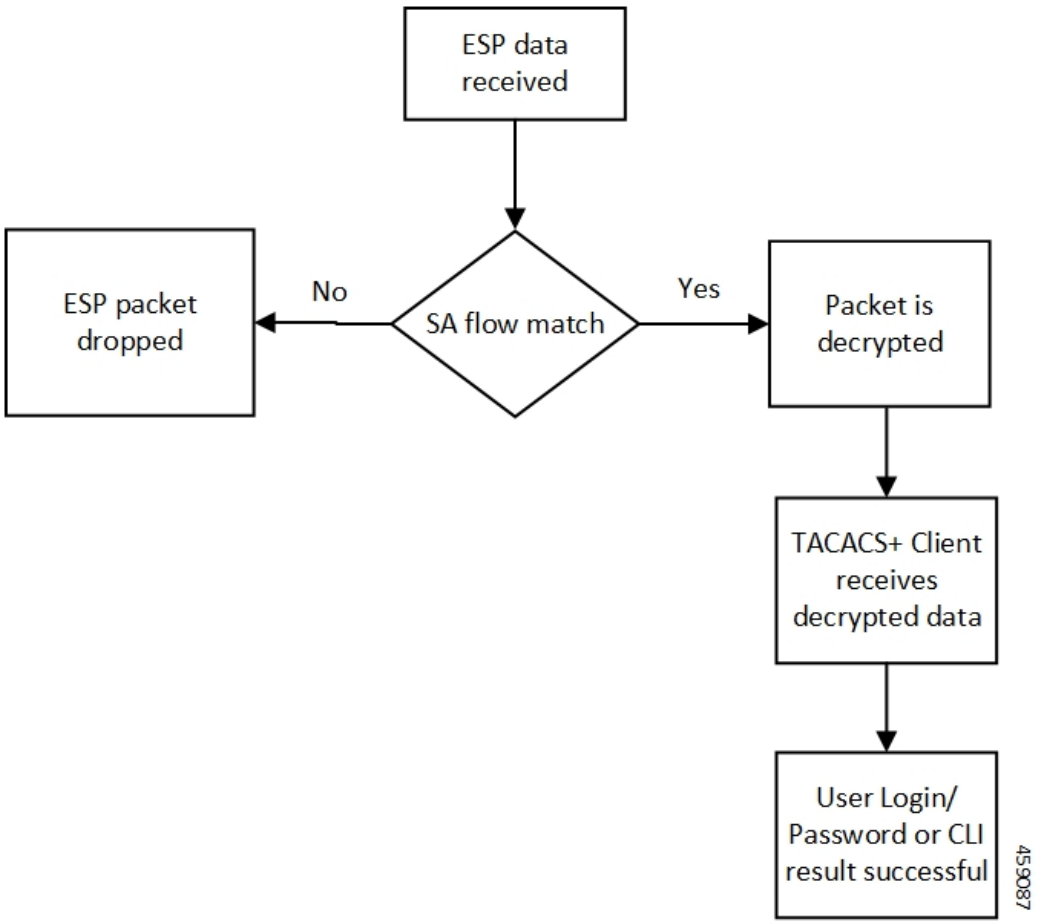
TACACS+ クライアントデータの暗号化

次の図は、トンネルの確立とパケット暗号化を表したものです。



TACACS+ サーバーデータの復号

次の図は、パケットの復号について説明したものです。



次の手順では、IPSec を介して TACACS+データセキュリティを実現するためのパケットフローについて説明します。

1. TACACS+/アプリケーションは、最初の TCP-SYN パケットの形式で TACACS+ サーバーとの TCP 接続を開始します。
2. SYN パケットは TUN インターフェイスにルーティングされ、ローカルコンテキストで IpsecMgr によって直接読み取られます。
3. IpsecMgr は、ACL と照合するために TCP-SYN パケットを NPUSIM の最初のインスタンスに送信します。
    1. ACL エントリが TCP-SYN パケットと一致する場合、パケットを IpsecMgr またはローカルに送り返します。
    2. パケットが ACL エントリと一致しない場合、NPUSIM はパケットの暗号化を回避して、ローカル管理インターフェイスにパケットを送信します。
4. IpsecMgr またはローカルコンテキストは、ACL との照合の後に NPUSIM からパケットを受信します。ローカルコンテキストで作成されたローカル raw ソケットを使用して IKE-INIT/IKE-AUTH パケットを交換することで、ピアとの IPSec トンネルの形成をトリガーします。

5. 最初の TCP-SYN パケットは、IPSec トンネルの作成をトリガーした後、IpsecMgr またはローカルでドロップされます。
6. TACACS+ やアプリケーションが別の TCP-SYN パケットを送信し、ステップ 2 ～ 3b が繰り返されます。
7. IpsecMgr は ACL との照合の後に NPUSIM から 2 番目の TCP-SYN パケットを受信すると、トンネルはすでに確立されているため、TCP-SYN パケットを暗号化し、IpsecMgr やローカルによってローカルコンテキストで作成された ESP raw ソケットを介してパケットを送信します。
8. IpsecMgr は、管理ポートを介してローカルコンテキストの ESP raw ソケットから送られてきた ESP パケットもリッスンします。
9. IpsecMgr やローカルで ESP パケットを受信すると、SA フロー処理のために ESP パケットを NPUSIM に送信します。
10. SA フローが NPUSIM で一致する場合、ESP パケットはパケットの復号を行う IpsecMgr またはローカルに送信されます。
11. このパケットは、TACACS+ クライアントから TACACS+ サーバーに送信された 2 番目の TCP-SYN パケットの応答である TCP-SYN-ACK の可能性があります。
12. 復号されたパケットは、TACACS+ またはアプリケーションに返送されたときの送信元の TUN インターフェイスに返送されます。
13. 双方向通信は、TCP-ACK パケットを送信する TACACS+ またはアプリケーションによって確立されます。上記の手順は、後続のすべてのパケットのデータセキュリティを実現するために繰り返されます。

リカバリ

IPsec トンネルは、アクティブの TACACS+ クライアントと TACACS+ サーバーアプリケーションの間で確立されます。スタンバイと TACACS+ サーバー間には IPsec トンネルは確立されません。通常のシナリオでは、IPsec エンドポイントが情報（ハートビート）メッセージを交換して、IPsec トンネルの正常性を確認します。アクティブ VNF がダウンした場合、TACACS+ サーバーの IPSec エンドポイントは、アクティブ VNF の IPSec エンドポイントのデッドピア検出（DPD）によりそれを検出します。DPD タイムアウトも設定可能です。DPD は、TACACS+ サーバー側でトンネルのクリアをトリガーします。スタンバイ VNF がアクティブに戻り、TACACS+ アプリケーションが TACACS+ サーバーアプリケーションとのデータ交換を開始すると、新しいアクティブ VNF と TACACS+ サーバー間に新しい IPsec トンネルが確立されます。

制限事項

この機能には次の既知の制限事項があります。

- IPv6 を使用する TACACS+ は、IPv6 トンネルエンドポイントを使用する IPSec ではサポートされません。ただし、IPSec を使用しない場合は、IPv6 を使用する TACACS+ がサポートされます。また、IPv4 を使用する TACACS+ は、IPv4 トンネルエンドポイントを使用する IPSec の有無にかかわらずサポートされます。
- ローカルコンテキストの暗号マップは、Day-0/Day-1 設定の一部として事前設定する必要があります。つまり、ローカルコンテキストの暗号マップがある場合は、他のコンテキストで暗号マップを設定する前に、ローカルコンテキストで暗号マップを設定する必要があります。

TACACS+ over IPSec の設定

ここでは、TACACS+ over IPSec 機能の設定方法について説明します。

この設定には、次の手順が含まれます。

1. TACACS+ コンフィギュレーション モードの設定。
2. IPSec を使用した TACACS+ のプロビジョニング。
3. トンネルモードでの IPSec を使用した TACACS+ のプロビジョニング。
4. トランスポートモードでの IPSec を使用した TACACS+ のプロビジョニング

TACACS+ コンフィギュレーション モードの設定

StarOS/VNF で TACACS+ をプロビジョニングするための設定は、非 CUPS アーキテクチャでの設定と同じです。ただし、「IPSec トンネルモード」でトンネルを確立するには、**src-ip** をプロビジョニングする必要があります。TACACS+通信用に追加の送信元IPアドレス（*src_ip*）を 1 つ予約し、その通信を保護する必要があります。

「IPSec トランスポートモード」でトンネルを確立する場合、追加の **src-ip** をプロビジョニングする必要はありません。管理インターフェイス IP アドレスは **src-ip** として選択されます。

以下に設定例を示します。

```
configure
  context context_name
    tacacs mode
      server priority priority_number ip-address server_ip_address password
text_password src_ip
      accounting command
      authorization prompt
    #exit
  aaa tacacs+
end
```

IPSec を使用した TACACS+ のプロビジョニング

次の設定により、すべての IKE/ESP パケットがユーザースペースの IPSec マネージャまたはローカルで処理されます。非ローカルコンテキストや VPP、IFtask、NPU などの基盤となるデータプレーンの IPSec マネージャでは処理されません。

```
configure
  require crypto ikev1-acl software context context
  require crypto ikev2-acl software context context
end
```

トンネルモードでの IPSec を使用した TACACS+ のプロビジョニング

次の設定例では、トンネルモードのローカルコンテキストでクリプトマップを作成します。**209.165.201.1** と **209.165.200.225** は、それぞれ TACACS+ サーバーとクラアントの IP アドレスと見なされます。

（注） 現在、トンネルモードは IKEv2 でのみサポートされています。

```
configure
  context local
    ip access-list foo
      permit ip 209.165.200.225 1 0.0.0.0 209.165.201.1 0.0.0.0
    #exit
    ipsec transform-set B-foo
      group 14
    #exit
    ikev2-ikesa transform-set ikesa-foo
      group 14
    #exit
    crypto map foo ikev2-ipv4
      match address foo
      authentication local pre-shared-key encrypted key EncryptedKey1
      authentication remote pre-shared-key encrypted key EncryptedKey2
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 2000
      ikev2-ikesa transform-set list ikesa-foo
      ikev2-ikesa rekey
      payload foo-sa0 match ipv4
        ipsec transform-set list B-foo
        rekey keepalive
      #exit
      peer 209.165.200.226
      ikev2-ikesa policy error-notification
    #exit
    interface local1
      ip address 209.165.200.227 255.255.255.224
      ipv6 address 2001:420:2c7f:f620::83/64 secondary
      crypto-map foo
    #exit
```

トランスポートモードでの IPSec を使用した TACACS+ のプロビジョニング

次の設定例では、**209.165.200.229** が TACACS+ サーバーの IP アドレスと見なされるトランスポートモードのローカルコンテキストでクリプトマップを作成します。

（注） 現在、トランスポートモードは IKEv1 でのみサポートされています。

```
configure
  context local
    ip access-list foo
      permit tcp 209.165.200.228 0.0.0.0 209.165.200.229 0.0.0.0
    #exit
    ip routing shared-subnet
    ikev1 keepalive dpd interval 3600 timeout 10 num-retry 3
    crypto ipsec transform-set A-foo esp hmac sha1-96 cipher aes-cbc-128
      mode transport
    #exit
    ikev1 policy 1
    #exit
    crypto map foo ipsec-ikev1
      match address foo
      set peer 209.165.200.229
      set ikev1 encrypted preshared-key EncryptedKey1
      set pfs group2
      set transform-set A-foo
    #exit
    interface local1
      ip address 209.165.200.228 255.255.255.224
      ipv6 address 2001:420:2c7f:f620::84/64 secondary
      crypto-map foo
    #exit
```

モニタリングおよびトラブルシューティング

show コマンドと出力

この機能をサポートするために、次の show CLI コマンドを使用できます。

- **show crypto map**
- **show crypto ikev2-ikesa security-associations** *summary*
- **show crypto ikev1 security-associations** *summary*
- **show crypto statistics**
- **show crypto ipsec security-associations** *summary*

第 90 章

タリフ時間のサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

タリフ切り替え時間機能は、サブスクライバがあるタリフプランから別のタリフプランに切り替わるときに適用されます。

Tariff-Time-Change AVP はタリフ切り替え時間を決定するために使用され、Monitoring-Time IE はタリフ時間サポート機能をサポートするために使用されます。

タリフタイマーが終了すると、ゲートウェイは別途、使用量を課金バケットに累積し、引き続き元のクォータ値から消費します。次回のレポート時（クォータの枯渇またはその他の制御イベント発生時）に、ゲートウェイはこの課金バケットの 2 つの使用量（タリフ時間変更の前後）をレポートします。

この課金バケットの 1 つ目のレポートには [Reporting-Reason] として Tariff-Time-Change が含まれ、2 つ目のバケットには前回のレポート理由と、タリフタイマー終了後のクォータの使用状況が含まれます。

データトラフィックの使用状況は、タリフ切り替え前のリソース使用量とタリフ切り替え後のリソース使用量に分けられます。Tariff-Change-Usage AVP は、Used-Service-Units AVP 内で使用され、レポートされた使用状況をタリフ時間変更の前と後で区別します。

制限事項

この機能には次の既知の制限事項があります。

- RG/サービス ID の各組み合わせに対してサポートされるタリフ時間は 1 つのみです。
- タリフ時間の変更の前後で異なるクォータの割り当てはサポートされません。この機能は、3GPP 標準規格に準拠していません。

第 91 章

UP コール概要ログ

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.24.1

機能説明

ユーザープレーンコール概要ログ（CSL）は、次のパラメータを外部ログ収集サーバーに報告するメカニズムです。

- セッションの確立
- セッションの変更
- セッションの削除
- 使用状況レポート

システムは CSL レコードを使用して、サブスクライバコールを分析およびデバッグします。

この機能は、次の機能をサポートしています。

- Sxb および Sxab インターフェイスの UP CSL のサポート（Pure-P、および Collapsed コール用）

- CSL レコードは CSV 形式でのみ保存されます。
- Sessmgr_u は、定義された時間間隔（最大 30 秒）で CSL レコードをバッファリングします。

機能の仕組み

UP とログ収集サーバー間のインターフェイスは SFTP に基づいています。各レコードは、カンマ区切りの ASCII 値（CSV レコード）の形式です。UP は、行ごとに 1 つの ASCII 形式の CSV レコードを送信します。システムは CSV レコードをファイルに保存し、外部収集サーバーに送信する前にファイルを圧縮します。15 分経過した CSV レコードは保存できないため、少なくとも 15 分に 1 回は外部収集サーバーにファイルを SFT する必要があります。UP と収集サーバー間の CSV レコードファイルの転送は、PULL または PUSH モデルで実行されます。PULL モデルの場合、外部収集サーバーは UP を使用して SFTP を処理します。PUSH モデルの場合、UP は CSV レコードファイルを外部収集サーバーに送信します。ファイル転送は、設定された PUSH タイマー間隔に基づいて行われます。

次のイベントで CSL レコードがトリガーされます。

イベント	説明
1	セッション確立要求/応答
2	セッション変更要求/応答
3	セッション削除要求/応答
4	使用状況レポートの要求/応答

CSL レコードには、CSV 形式の次の情報が含まれます。

ケース	説明	書式例
1	UP CSL レコード番号	整数 <proclet-type>|<instance-id>|<RTT-record-#>
2	UP バージョン番号	整数 v21.24.0 のバージョン 1
3	手順番号	PFCP IE 29.244（表 7.3-1：メッセージタイプ）
4	UP 名	シャーシのホスト名
5	手順開始時刻	UTC の時刻（ミリ秒の精度で表示）
6	手順終了時刻	UTC の時刻（ミリ秒の精度で表示）

ケース	説明	書式例
7	ASR5K CallID	Internal CallID 376efb10
8	Sx-PFCP リモート SEID	
9	インターフェイス タイプ	
10	予約済み	
11	IMSI	整数（15 桁） 例：[311480076488840]
12	[MSISDN]	整数の例：[19728256305]
13	IMEISV	整数（16 桁）の例：[9900028823793406]
14	RAT	IPv6 Address
15	SGW TEID（FARID、RTEID）	ピアのトンネル識別子 例：1,0x084BC005|2,0x084BC01|3,0x084BC010|
16	PGW TEID（PDR ID、F-TEID）	UP のトンネル識別子 例：1,0x084BC005|2,0x084BC010|3,0x084BC010|
17	APN	文字列 例：[vzwims.mnc311.mcc480.3gppnetwork.org]
18	IPv4 アドレス	IPv4 アドレス UE が割り当てた IPv4 アドレス
19	IPv6 Address	IPv6 アドレス UE が割り当てた IPv6プレフィックス/アドレス
24	アップリンク AMBR	整数（0 ～ 40 億） Kbps 単位の例：[0 ～ 4,294,967,295]
25	ダウンリンク AMBR	整数（0 ～ 40 億） Kbps 単位の例：[0 ～ 4,294,967,295]
26	アップリンク MBR	整数（0 ～ 40 億） Gbps 単位。MBR （QER ID、MBR） 例：1,1234 | 2,3456 |3,567
27	ダウンリンク MBR	整数（0 ～ 40 億） Gbps 単位。MBR （QER ID、MBR）

ケース	説明	書式例
	アップリンク GBR	整数（0 ～ 40 億） （QER ID、GBR）
	ダウンリンク GBR	整数（0 ～ 40 億）
	Sx 応答値	（原因、問題のある IE）1、0 または 64、44 Request/Acceptance/Rejection Cause、例：[1-255] 1 ～ 6
	PFCP セッション確立要求/応答	Create PDR 1|2|3|4 Create FAR 1|2 Create QER 1|2 Create URR 1|2|3|4 Create TE 1|2
	PFCP セッション変更要求/応答	Create PDR 5|6 Update PDR 3|4 Remove PDR 1|2 Create FAR 1|2 Update FAR （RTEIDxxxx、アクションの適用） Create QER 1|2 Create URR 1|2|3|4 Create TE 1|2 Update TE 1|2
	PFCP セッション削除要求/応答	Remove PDR 5|6 Remove FAR 7|8 Remove URR 1|2 Remove QER Remove TE
	PFCP セッションレポート要求/応答	レポートタイプ（DLDR|USAR....|UISR）

障害および障害レポート

sessmgr は、 cdrmod への CSL のポストに失敗した場合、またはメモリ割り当てが原因でバッファリングの問題が発生した場合に、警告メッセージを表示します。Sessmgr によって障害を

報告するために定義された SNMP トラップはありません。Cdrmod は、UP CSL レコードファイルを RAM に保存する際に問題が発生した場合、障害の問題を個別に報告します。

冗長性

セッションリカバリと ICSR の両方が UP CSL でサポートされています。UP CSL がサブスクライバに対して有効になっている場合は、Sessmgr のリカバリ後も UP CSL が続行されます。同様に、ICSR コールについては、UP CSL がサブスクライバに対して有効になっている場合、UP CSL が続行されます。セッションリカバリおよび ICSR 中に、ローカルにバッファされた Sessmgr CSL レコードが失われます。

CSL レコードファイルは RAMFS またはハードディスクを使用して保存され、リカバリ全体で使用できるため、CDRMOD でのセッションリカバリには最小限のサポートが必要です。ICSR の場合、UP CSL レコードファイルを古いアクティブシャーシから新しいアクティブシャーシに転送する必要があります。

相互依存性

この機能をサポートするには、次の CDRMOD 機能が必要です。

- UP CSL レコードをサポートする新しい CDR モジュールタイプ
- RAMFS を使用した UP CSL レコードの保存
- UP CSL レコードファイルの圧縮
- 障害レポート
- SNMP トラップ生成
- 統計/一括統計のサポート
- セッションリカバリと ICSR

制限事項と制約事項

この機能を有効にするには、CDRMOD、UP サービス設定、および SFTP 設定が必須です。CDRMOD 設定は、CDRMOD モジュールタイプ、圧縮方式、保存方式などの必要な設定パラメータを使用した CDRMOD のセットアップに必要です。UP サービス設定は、UP CSL のレポートを有効にするのに必要です。SFTP 設定は、UP CSL レコードファイルをシャーシから外部収集サーバーに転送するために必要です。

UP でのコール概要ログの設定

CSL の有効化/無効化

ログに記録する UP イベントレコードのレポートを有効または無効にするには、次の設定を使用します。

```
configure
  context context_name
    apn apn_name
      [ no | default ] reporting-action up-event-record
      end
```

注：

- **reporting-action:**：イベントレポートを設定します。
- **up-event-record:**：イベントレコードのレポートを有効にします。デフォルトでは、イベントレコードのレポートは無効になっています。

UP サービスの設定

UP サービスを設定するには、以下を使用します。

```
session-event-module
 file name evt-repo rotation volume 2097152 rotation time 30 compression gzip
 event use-harddisk
 event remove-file-after-transfer
 event transfer-mode push primary url  sftp://xxxxxxxx@xx.xx.xxx.xxx/tmp/  via local-
 context
 event push-interval 30
```

モニタリングおよびトラブルシューティング

セッションマネージャレベルで **show subs sgw-only full** CLI コマンドを使用して、UP の CSL が有効になっているかどうかを確認します。また、セッションマネージャの警告メッセージを有効にして、セッションマネージャでのイベント報告に問題がある場合に通知することもできます。

CDRMOD は、個別の CLI、SNMP トラップ、警告/デバッグメッセージを使用して、UP の CSL に関連した CDRMOD 問題の障害対応を支援します。

統計情報

次の CLI コマンドは、この機能をサポートするために使用できます。

show up-event-record statistics interface-type [sxb | sxab | n4]

注：

- **up-event-record**：イベントレコードの数を表示します。
- **statistics**：イベントレコードの統計情報を表示します。
- **interface-type**：インターフェイスタイプのイベントレコードを表示します。

show コマンドの出力

show up-event-record statistics interface-type sxb CLI の出力例を以下に示します。

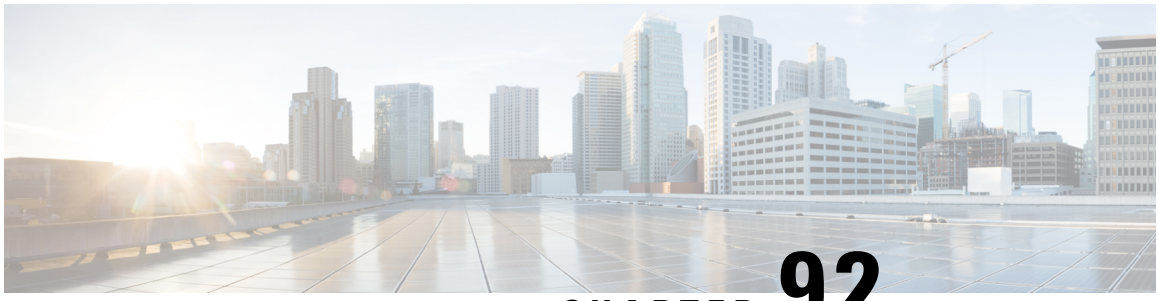
```
Number of event records: 80
Number of event records for sx procedures: 50
   PFCP Session Establishment procedure: 10
   PFCP Session Modification procedure: 20
   PFCP Session Deletion procedure: 10
   PFCP Session Report procedure: 100
```

イベントレコードのレポートが有効になっている場合の **show config** または **show config verbose** の出力例を以下に示します。

```
config
  context <>
    apn <>
      …
      reporting-action up-event-record
```

イベントレコードのレポートが無効になっている場合の **show config verbose** の出力例を以下に示します。

```
config
  context <>
    apn <>
      …
      no reporting-action up-event-record
```



CHAPTER 92

URL のブロックリスト登録

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

URL ブロックリスト機能は、URL または URI がブロックリストに登録されている Web サイトからコンテンツを表示またはダウンロードするためのサブスクライバのアクセスを規制します。この機能では、検出された URL がブロック対象として分類されているかどうかを示す URL のリストを記録するデータベースが使用されます。

機能の仕組み

ユーザープレーン（UP）で URL のブロックリスト登録機能を有効にするには、フラッシュ、SFTP、またはそのサブディレクトリ内に「optblk.bin」という名前の URL ブロックリストデータベースがある必要があります。このデータベースディレクトリのパスは、ユーザープレーンのサービス起動後に、ユーザープレーンで設定する必要があります。

HTTP アナライザの URL ブロックリスト登録を有効にする必要があります。HTTP アナライザは、受信した HTTP リクエストデータパケットから URL 情報を抽出します。抽出された URL コンテンツが、URL ブロックリストデータベースと比較されます。受信した HTTP データパケットの URL がデータベースの URL エントリと一致すると、その URL はブロックリスト登録された URL として扱われ、該当する HTTP パケットに対して次のいずれかのアクションが実行されます。

- フローの終了
- パケットの破棄

URL のブロックリスト登録設定は、コントロールプレーン（CP）のアクティブ課金サービスの Rulebase 設定で設定する必要があります。さらに、CP のアクティブ課金サービスレベルの設定では、URL のブロックリスト登録方式として、[Exact] と [Generic] の 2 種類がサポートされています。これらの CLI 設定は、PFD メカニズムを介して UP にプッシュされ、Sx 関連付け手順において CP にプッシュされます。

重要 ブロックリストデータベースは、IWF（Internet Watch Foundation）および NCMEC（National Center for Missing and Exploited children）によって提供されます。ASR5500、CUPS UP は常に、最適化されたフォーマット（最適化されたブロックリスト DB フォーマット）でブロックリスト DB を受信します。

URL ブロックリストデータベースのアップグレード

次の 2 つの方法による URL データベースのアップグレードがサポートされます。

- タイマーベースのアップグレードまたは自動アップグレード
- CLI ベースのアップグレードまたは手動アップグレード

タイマーベースのアップグレードまたは自動アップグレード

データベースがシャーシに初めてロードされると、5 分間のタイマーが開始されます。このプロセスは、データベースを自動アップグレードするために開始されるものです。

タイマー終了時に、ディレクトリパスに有効なデータベースのより上位のバージョンがある場合には、データベースのアップグレード手順が開始され、新しいバージョンのデータベースが UP シャーシにロードされます。

URL ブロックリストデータベースをアップグレードするには、「optblk_f.bin」という名前の有効な URL ブロックリストデータベースの上位バージョンが、現在のデータベース「optblk.bin」と同じディレクトリ内にある必要があります。

データベースが正常にアップグレードされると、以前の「optblk.bin」ファイルの名前が「optblk_0.bin」に変更され、「optblk_f.bin」ファイルの名前が「optblk.bin」に変更されます。すると、「optblk_0.bin」ファイルは、古いデータベースのバックアップファイルとして扱われます。

もう一度アップグレードが実行されると、「optblk_0.bin」ファイルの名前は「optblk_1.bin」に変更され、現在の「optblk.bin」ファイルの名前は「optblk_0.bin」に変更されます。

データベースに保存されるバックアップファイルの数は、**max-versions** CLI を使用して UP で設定できます。

CLI ベースのアップグレードまたは手動アップグレード

このアップグレード方法では、CLI コマンド **upgrade url-blacklisting database** を使用して、現在のデータベースを新しいバージョンにアップグレードします。

制限事項

このリリースでは、セッションリカバリおよびユーザープレーンの冗長性のサポートは完全には認定されていません。

URL のブロックリスト登録の設定

UP での URL ブロックリストデータベースのロード

UP で URL ブロックリストデータベースをロードするには、次の設定を使用します。

StarOS 21.26 より前のリリース：

```
configure
   url-blacklisting database directory path database_directory_path
   url-blacklisting database max-versions max_version_value
   end
```

StarOS 21.26 以降のリリース：

```
configure
   url-blockedlisting database directory path database_directory_path
   url-blockedlisting database max-versions max_version_value
   end
```

注：

- **database directory path**：データベースのディレクトリパスを設定します。

  database_directory_path は、1 ～ 255 文字の文字列です。

- **max-versions**：データベースの最大アップグレードバージョンを設定します。

  max_version_value は 0 ～ 3 の整数です。

URL ブロックリストを有効にするための設定

コントロールプレーンでURLブロックリスト機能を有効にするには、次の設定を使用します。

CUPS 21.26 より前のリリース：

```
configure
  require active-charging service_name
    url-blacklisting match-method [ exact | generic ]
    rulebase rulebase_name
      url-blacklisting action [ discard | terminate-flow ]
      end
```

CUPS 21.26 以降のリリース：

```
configure
  require active-charging service_name
    url-blockedlisting match-method [ exact | generic ]
    rulebase rulebase_name
      url-blockedlisting action [ discard | terminate-flow ]
      end
```

注：

- **match-method [exact | generic]**：URL ブロックリストに使用する一致メソッドを指定します。

  exact：URL ブロックリストで、URL の完全一致を実行します。

  generic：URL ブロックリストで、URL の汎用一致を実行します。

- **url-blockedlisting action [discard | terminate-flow]**

  discard：受信した HTTP パケットを破棄します。

  terminate-flow：受信した HTTP パケットのフローを終了します。

URL ブロックリストデータベースのアップグレード

URL ブロックリストデータベースをアップグレードするには、次のコマンドを使用します。

CUPS 21.26 より前のリリース：

```
upgrade url-blacklisting database
```

CUPS 21.26 以降のリリース：

```
upgrade url-blockedlisting database
```

（注） このCLIは、URLブロックリストデータベースの手動アップグレードに使用されます。ブロックリストデータベースを更新するには、ファイルoptblk_f.binが存在している必要があります。

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングとトラブルシューティングのサポートに使用できるCLIコマンドに関する情報を提供します。

コマンドや出力の表示

この項では、この機能のサポートにおけるshowコマンドまたはその出力について説明します。

show user-plane-service url-blacklisting database

この機能をサポートするために、次のフィールドが表示されます。

- URL ブラックリスト静的評価データベース：
  - 前回のアップグレードステータス
  - パス
    - データベースステータス
    - DB 内の URL の数
    - タイプ
    - バージョン
    - 作成時間
    - ホスト名
    - コメント
    - 最終アクセス時刻
    - 最終変更時刻
    - ステータスの最終変更時刻

show user-plane-service url-blacklisting database url *database_directory_path*

この機能をサポートするために、次のフィールドが表示されます。

- URL ブラックリスト静的評価データベース：
  - 前回のアップグレードステータス
  - パス
    - [データベースステータス（Database Status）]
    - DB 内の URL の数

- タイプ（Type）
- バージョン
- Creation Time
- ホストネーム（Hostname）
- コメント
- Last Access Time
- 最終変更時刻
- ステータスの最終変更時刻

show user-plane-service url-blacklisting database facility sessmgr all

この機能をサポートするために、次のフィールドが表示されます。

- URL-Blacklisting SessMgr Instance Based Database Configuration
  - SessMgr Instance
  - BL DB Load Status
  - BL DB Version
  - Number of URLs
  - Checksum

show user-plane-service inline-services info

この機能をサポートするために、次のフィールドが表示されます。

- URL ブラックリスト：有効
  - URL ブラックリストの照合方法：汎用

show user-plane-service rulebase name *rulebase_name*

この機能をサポートするために、次のフィールドが表示されます。

- URL-Blacklisting Action
- URL-Blacklisting Content ID

show user-plane-service inline-services url-blockedlisting statistics

この機能をサポートするために、次の情報が表示されます。

- 累積 URL ブロックリストの統計

- ブロックリストの URL ヒット数
- ブロックリストの URL 欠落数
- 一致したルールベースの総数

show user-plane-service inline-services url-blacklisting statistics rulebase name *rulebase_name*

この機能をサポートするために、次のフィールドが表示されます。

- ルールベース名
  - URL ブラックリストの統計情報
  - ブラックリストに登録された URL のヒット数
  - ブラックリストに登録された URL の欠落数
- 一致したルールベースの総数

バルク統計情報

URLブラックリスト機能をサポートするために、次のバルク統計情報がシステムスキーマに追加されました。

- **url-blacklisting-hits**：ブラックリストに登録された URL の総数を示します。
- **url-blacklisting-misses**：ブラックリストに登録されていない URL の総数を示します。

SNMP トラップ

この機能をサポートするために、次の SNMP トラップが追加されました。

- **BLDBError**：表示される OPTBLDB ファイルエラーをエラーコードとともにブラックリストに登録します。
- **BLDBErrorClear**：OPTBLDB ファイルエラーのブラックリスト登録を解除します。
- **BLDBUpgradeError**：表示される OPTBLDB ファイルエラーをエラーコードとともにブラックリストに登録します。
- **BLDBUpgradeErrorClear**：OPTBLDB ファイルエラーのブラックリスト登録を解除します。

第 93 章

ユーザープレーンの選択

APN および APN プロファイルベースのユーザープレーンの選択

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
最初の導入。	21.24 より前

機能説明

CUPS アーキテクチャでは、SAEGW-C は、接続が最も少ないユーザープレーンを選択するアルゴリズムを使用してユーザープレーンを選択します。また、ユーザープレーンのフラットリストからユーザープレーンを選択します。

この機能により、オペレータは、APN または APN プロファイルに関連付けられている特定の UP グループからユーザープレーンを選択できます。

S-GW では、UP グループはアクセスポイント名（APN）プロファイルに関連付けられます。APN プロファイルは、1 つ以上の APN に適用可能な一連の APN 固有のパラメータをグループ化します。1 つの APN プロファイルを複数のオペレータポリシーと関連付けられます。

機能の仕組み

Cisco CUPS ソリューションは、UP の静的選択をサポートします。これは、アクティブで使用可能な SAEGW-U の静的選択に基づいています。UP の静的選択では、UP グループの概念が使用されます。UP グループは UP SAEGW-U のグループです。各 APN は 1 つの UP グループに関連付けられます。APN は関連付けられた UP グループによってサービスを提供されます。UP の選択では、その特定のグループで使用可能な接続数が最も少ない UP を選択するアルゴリズムが使用されます。

UP グループ

UP は 1 つの UP グループにのみ属することができます。UP グループでは、すべての UP のキャパシティと機能が同じである必要があります。異なるタイプの UP は、異なる UP グループに含める必要があります。

CUPS は、次のタイプの UP グループをサポートします。

- 特定の UP グループ：明示的に設定された UP のセットです。特定のグループを使用すると、特定のタイプの UP を柔軟にグループ化できます。これは、特定の UP セットを特定の目的で予約するのに役立ちます。特定のグループは複数設定できます。
- デフォルト UP グループ：これは、登録済みで、特定の UP グループに含めるよう明示的に設定されていないすべての UP をグループ化するデフォルトグループです。デフォルトグループには、CP で UP を明示的に設定することなく、ゼロタッチ方式で UP を登録できるという利点があります。このタイプのグループは、同じキャパシティと機能を持つすべての UP が同じデータセンターにあるような、コロケーション CUPS に適しています。デフォルトグループは、CP の UP 設定を最適化します。

APN は UP グループに関連付けることができます。APN に関連付けられているグループがない場合は、デフォルトの UP グループがその APN にサービスを提供するために使用されます。同様に、Pure-S コールに対して UP を選択する場合は、UP グループを APN プロファイルに関連付けることができます。APN プロファイルやオペレータポリシーが定義されていない場合、または APN プロファイルに関連付けられているグループがない場合、SAEGW-C は選択の際に「デフォルト」の UP グループを使用します。

オペレータは、特定のアプリケーション用に特定の UP を予約できます。たとえば、IMS、インターネット、および IoT は異なる UP グループを持つことができます。

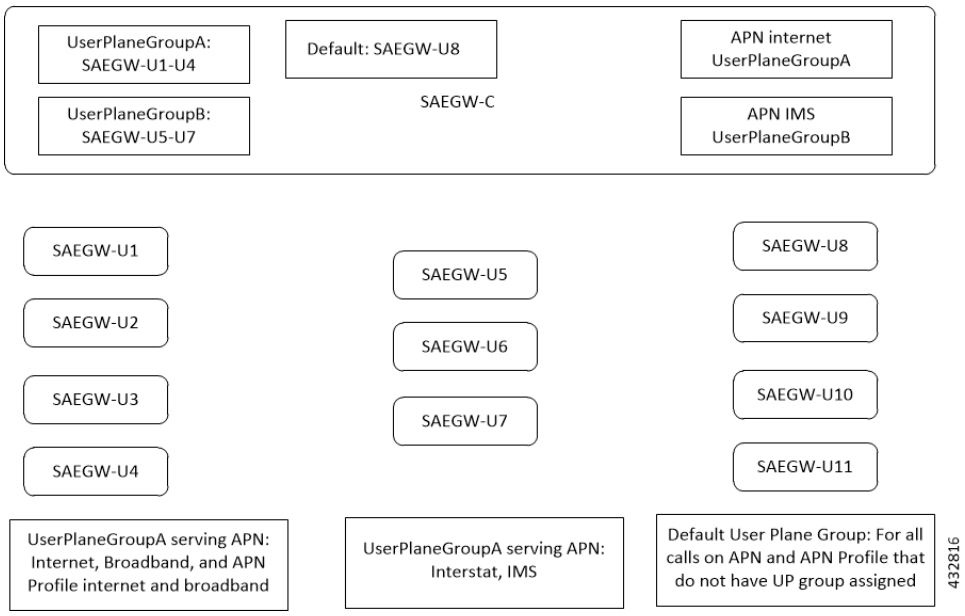
この機能の目的は次のとおりです。

- SAEGW-C には、常に「default」という名前のユーザープレーングループが 1 つあります。
- SAEGW-C は、最大 100 のユーザープレーンをサポートします。
- ユーザープレーンは、さまざまなグループに編成できます。

- 現在、100 のユーザープレーングループを設定でき、1 つのグループに最大 100 のユーザープレーンを設定できます。
- 1 つのユーザープレーンは、1 つのユーザープレーングループのみに属することができます。
- 特定のユーザープレーングループおよびデフォルトグループには複数のユーザープレーンを設定できます。
- SAEGW-C に関連付けられているが、どのユーザープレーングループにも定義されていないユーザープレーンは、デフォルトグループに追加されます。
- オペレータは、ユーザープレーングループを APN および APN プロファイルに関連付けることができます。
- Pure-P コールや Collapsed コールの APN に関連付けられているユーザープレーングループがない場合、SAEGW-C はデフォルトグループを使用してそのセッションのユーザープレーンを選択します。
- APN プロファイルに関連付けられたユーザープレーングループがない場合、または APN プロファイルが定義されていない場合、SAEGW-C は Pure-S コールに「デフォルト」ユーザープレーングループを使用します。
- 同じ APN を使用したマルチ PDN コールの場合、同じユーザープレーンが選択されます。異なる APN を使用したマルチ PDN コールの場合、別のユーザープレーングループの別のユーザープレーンが選択されます。
- APN に関連付けられたユーザープレーングループは、IP プールチャンクをユーザープレーンに送信するときにも使用されます。APN に関連付けられた IP プールはチャンクに分割され、APN に関連付けられたグループからすべての UP に配布できます。
- APN に関連付けられていないユーザープレーングループの場合、SAEGW-C はこれらのグループに属する UP に IP プールチャンクを送信しません。これは、デフォルトグループにも当てはまります。
- 静的 IP アドレス（IPv4 または IPv6）を使用したセッションがサポートされています。静的セッションのユーザープレーンの選択は、APN に関連付けられたユーザープレーングループからユーザープレーンへのチャンクの割り当てに従って固定されます。
- 複数の APN で同じ静的 IP アドレス範囲が使用されている場合は、それらの APN で同じユーザープレーングループを使用することを推奨します。

アーキテクチャ

次の図は、この機能のアーキテクチャの概要を示しています。



セッションリカバリと ICSR

Sx-Demux リカバリ、ICSR、Sessmgr、および VPNmgr リカバリがサポートされています。

制限事項

CUPS アーキテクチャでは、この機能には次の既知の制限事項があります。

- SAEGW-C では、IP アドレスの一方（IPv4 または IPv6、またはその両方）が静的アドレスであっても、UE から受信した静的アドレスを使用した IPv4v6 PDN タイプのコールはサポートされていません。
- SAEGW-C では、「allow-static」タイプのプール設定はサポートされていません。
- 静的 IP アドレス割り当てを使用したマルチ PDN コールはサポートされていません。

ライセンス

この機能はライセンスによって制御されます。ライセンスの詳細については、シスコのアカウント担当者にお問い合わせください。

APN ベースの UP のグループ化の設定

ここでは、この機能をサポートするために使用可能な設定について説明します。

前提条件：

- コントロールプレーンとユーザープレーンに同じ IP コンテキストが存在する必要があります。

- APN 設定で指定された IP コンテキスト名は、コントロールプレーンとユーザープレーンで同じである必要があります。

コントロールプレーンでのユーザープレーングループの設定

新しいユーザープレーングループは、ユーザー プレーン エンドポイントをリストする [Global Configuration] モードで定義されます。

1. ユーザープレーングループ名「default」がデフォルトで作成されます。オペレータは、デフォルトグループの peer-node-id を追加および削除できます。ただし、ユーザープレーングループ「default」は削除できません。
2. 定義済みのユーザープレーングループのいずれにも属さないユーザープレーンノード ID の Sx 関連付けセットアップ要求を受信した場合、そのユーザープレーンノード ID はデフォルト ユーザー プレーン グループの一部となります。

ユーザープレーングループの設定

コントロールプレーンでユーザープレーンのエンドポイントグループを設定するには、次の CLI コマンドを使用します。

```
configure
  [ no ] user-plane-group group_name
  end
```

注：

- ユーザープレーングループを削除すると、そのグループにある個々のピア ID のコントロールプレーンから Sx-Association Release がトリガーされます。

ピアノード ID とユーザープレーンノード IP アドレスの設定

時間ベースの PCC ルールを設定するには、次のコンフィギュレーション コマンドを使用します。

```
configure
  user-plane-group group_name
    [ no ] peer-node-id { ipv4-address | ipv6-address }
    end
```

注：

- peer-node-id を削除すると、そのピア ID のコントロールプレーンからの Sx 関連付けの解除がトリガーされます。

ユーザープレーングループの確認

検証には、次の CLI コマンドを使用します。

```
show user-plane-group { all | name group_name }
```

ユーザープレーングループと APN の関連付け

特定の APN へのコールは、事前定義された選択基準に基づいて特定のグループのユーザープレーンに関連付けることが推奨されます。オペレータは、ユーザープレーングループを APN 設定に関連付けることができます。

APN に設定されたユーザープレーングループは、IP プールチャンクをユーザープレーンに送信するときにも使用されます。APN に関連付けられた IP プールがある場合のみ、そのプールからのチャンクがこのグループ内のすべてのユーザープレーンに送信されます。

APN のユーザープレーングループ設定は、P-GW の Pure-P および Collapsed コールでユーザープレーンを選択するために使用されます。

APN で特定のグループが設定されていない場合は、「デフォルト」グループが使用されます。

APN でのユーザープレーングループの設定

次の CLI コマンドを使用して、APN でユーザープレーングループを設定します。

```
configure
  context context_name
    apn apn_name
      [ no ] user-plane-group group_name
      end
```

注：この EFT リリースでは、APN からのユーザープレーングループの削除や変更はサポートされていません。

APN でのユーザープレーングループの確認

検証には、次の CLI コマンドを使用します。

```
show apn name apn_name }
```

ユーザープレーングループと APN プロファイルの関連付け

S-GW Pure-S コールのユーザープレーンを選択するために、SAEGW-C は、オペレータポリシーで APN プロファイルに関連付けられたユーザープレーングループを使用します。APN プロファイルにユーザープレーングループが関連付けられていないか、APN プロファイルが使用されていない場合、SAEGW-C はデフォルトのユーザープレーングループからユーザープレーンを選択します。

APN プロファイルでのユーザープレーングループの設定

次の CLI コマンドを使用して、APN でユーザープレーングループを設定します。

```
configure
  apn-profile profile_name
    [ no ] user-plane-group group_name
    end
```

ユーザープレーングループを APN から削除する、または変更するための Method of Procedure（MOP）

明示的なユーザープレーングループが設定されている場合、または暗黙的なデフォルトグループが使用されている場合、SAEGW-Cは、設定されているプール（またはAPNに明示的なプール設定がない場合はグローバルプール）からの IP プールチャンクをグループ内のユーザープレーンに送信します。

現在、ユーザープレーンが SAEGW-C に関連付けられた後は、APN 内のユーザープレーングループのランタイム設定変更がサポートされていないため、APNに関連付けられたユーザープレーングループを変更または削除する場合は、この MOP に従うことを推奨します。

APN でユーザープレーングループを変更する前に、次の CLI コマンドを使用して、最初にその APN に関連付けられたユーザープレーングループに属する既存のコールをすべて、正常にクリアすることを推奨します。

clear subscribers saegw-only user-plane-group *group_name* **no-select-up**

この CLI コマンドを実行すると、指定されたユーザープレーングループに属するユーザープレーンからすべてのセッションが正常に解放され、そのユーザープレーンが「セッション選択に使用不可」としてマークされます。そのユーザープレーンは関連付けられた状態のままですが、セッションの選択には使用できません。

（注） **clear subscribers** コマンドが UP で実行されると、CP には通知されず、セッションは実行中であると CP で見なされます。

セッションをクリア後、ユーザープレーンで次のいずれかの CLI コマンドを実行してコントロールプレーンから関連付けを削除し、UP の関連付けが解放された後に必要な変更を行います。

no user-plane-service *service_name*

または：

no peer-node-id { ipv4-address *ipv4_address* **| ipv6-address** *ipv6_address***}**

APN ベースの UP のグループ化のモニタリングと障害対応

この機能は、次の CLI コマンドをサポートしています。

- **show sx peers**
  - このコマンドの出力の [Group Name] 列には、コントロールプレーンでピアが属する user-plane-group の名前が表示されます。
  - どのグループにも属していないピアは、「default」ユーザープレーングループに追加されます。
  - user-plane-group がどの「apn」にも関連付けられていない場合、SAEGW-C はこのグループからユーザープレーンに IP プールを送信しません。したがって、このコマン

ドの出力では、「apn」に関連付けられていないグループ名の IP プールのステータスは「N – Not Applicable」になります。また、このグループのユーザープレーンについては、**show sx peers** を UP で実行すると、ピア ID が「0」と表示されます。

- **show ip user-plane**
- **show ip pool-chunks up-id** *up_id* **user-plane-group name** *up_group_name*

ダイナミック ユーザー プレーンの選択

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
最初の導入。	21.24 より前

機能説明

マルチアクセス エッジ コンピューティング（MEC）アーキテクチャでは、エッジユーザープレーン（UP）を選択することで、低遅延と最大限の帯域幅効率が実現します。ユーザー機器（UE）のロケーション情報を使用して、UP が選択されます。

エッジ UP を選択では、次の詳細度が考慮されます。

- 詳細度が最も低いのが、E-UTRAN セルグローバル識別子（ECGI）またはセルグローバル識別子（CGI）です。
- 次に詳細度が低いのが、トラッキングエリア識別子（TAI）、回送エリア識別子（RAI）、またはサービスエリア識別子（SAI）です。
- TAI-SAI-RAI-ECGI では、TAI、SAI、RAI、および ECGI には固定優先順位があり、複数の ULI タイプを受信した場合には ULI タイプを照合します。

アーキテクチャ

次回のセッションの場所パラメータに基づいて UP を選択するために、TAI/RAI /SAI または ECGI/CGI を含む DNS 命名機関ポインタ （NAPTR）クエリが DNS サーバーに送信されます。DNS（NAPTR）応答には、UP IP のリストが含まれています。このリストから UP を選択するために、負荷制御情報（LCI）とセッション数がショートリストに適用されます。

この機能により、仮想 APN の選択と動的な UP の選択が可能になります。その結果、APN は指定された基準に基づいて選択されます。仮想 APN の選択基準は、無線のアドミッションコントロール（RAC）範囲などのロケーションにも基づきます。

動的 UP の選択は、**configure fqdn postfix** CLI コマンドと選択した APN のタイプに基づきます。選択したタイプが ECGI または CGI の場合は、セル ID に基づいて DNS ストレート NAPTR（S-NAPTR）クエリが送信されます。選択したタイプがトラッキングエリアまたはルーティングエリアとして設定されている場合、TAI、RAI、または SAI が DNS（S-NAPTR）クエリに使用されます。

関連付けられた Sx ピアのリストを取得するために、選択した APN の UP グループが使用されます。DNS（S-NAPTR）応答の UP IP は、グループ内の Sx ピアのリストと照合されます。このリストから、負荷が最も低いピア、またはセッション数が最も少ないピアが選択されます。

ULI にサポートされていないロケーション データが含まれている場合、動的 UP 選択は、ULI 外の RAI IE に基づいて行われます。

機能の仕組み

この項では、一連の操作について説明します。

1. P-GW、GGSN、または SAEGW の場合、**fqdn-postfix** と FQDN タイプ（EGCI/CGI または TAI/RAI/SAI）を含む UP の完全修飾ドメイン名（FQDN）が APN レベルで設定されます。
2. S6b インターフェイス プロトコルベースの認証では、認証応答の **fqdn-postfix** 値が使用されます（P-GW、GGSN、または SAEGW サービスにのみ適用可能）。
3. DNS（S-NAPTR）クエリが DNS サーバーに送信されます。

（注） DNS（S-NAPTR）は、GGSN の APN レベルのユーザープレーン FQDN で設定されたタイプ（E-CGI | RAI-TAI-SAI | TAI-SAI-RAI-ECGI）に基づいて生成されます。

4. DNS サーバーから受信した応答は、P-GW/GGSN/SAEGW（Collapsed）のサービス **x-3gpp-upf:x-sxb** および S-GW の **x-3gpp-upf:x-sxa** に一致します。
5. 一致する DNS（S-NAPTR）応答は、UP IP に対して再帰的に処理されます。
   - 有効になっている場合、処理された IP は、LCI ベースの UP の選択に関する候補リストに表示されます。
   - 有効になっていない場合、処理された IP は、セッション数ベースの UP の選択（LCI の有無にかかわらず）に関する候補リストに表示されます。
6. 応答に存在するいずれの UP IP も、関連付けられた Sx ピアと一致しない場合、セッションの作成が失敗します。

7. S-GW 動的 UP の選択の場合、DNS クライアントコンテキストは **sgw-service** コンテキストと同じである必要があります。
8. S-GW 動的 UP の選択に対する DNS 応答が成功すると、UP アドレスの DNS 動的リストから UP が選択されます。DNS 障害が発生した場合（UP アドレスまたは DNS タイムアウトなしで DNS 応答が空になった場合）、UP の選択は、静的に設定された APN プロファイルベースのユーザープレーングループ機能にフォールバックします。

（注）
- Pure S-GW マルチ PDN は、独立した DNS ベースの UP の選択で動作します。
- S-GW の再配置の使用例は、ハンドオーバー時に独立した DNS ベースの UP の選択で機能します。ユーザープレーングループが APN プロファイルで設定されている場合、動的 UP の選択が優先されます。
- DNS（NAPTR）クエリが送信されてから、応答を受信するまでに数秒の遅延（tx＋rx に相当）があります。
- DNS サーバーに到達できない場合は、セッションの確立が最大 30 秒遅延してから、従来のメソッドを使用して UP が選択される場合があります。

次の項では、動的 UP の選択機能に関連するさまざまなシナリオについて説明します。

関連付けられた IP プールがある仮想 APN を持つ P-GW 動的 UP の選択

この項では、P-GW が、関連付けられた IP プールがある仮想 APN を持つ UP を動的に選択するための一連の動作について説明します。

1. 作成セッション処理の一環として、PGW-C が TAC 範囲に基づいて仮想 APN を選択します。
2. DNS（S-NAPTR）クエリが、選択した APN の設定に基づいて DNS サーバーに送信されます。
3. DNS サーバーから受信した応答がサービスと照合され、サービスフィールドが一致するレコードが選択対象と見なされます。
4. 設定された IP プールの一部であり、応答に存在する UP IP は、選択された APN の UP グループに基づいて、関連付けられた Sx ピアと照合されます。
5. 一致リストから、P-GW が最も負荷の少ない UP を選択します。

関連付けられた IP プールがない仮想 APN を持つ P-GW 動的 UP の選択

この項では、P-GW が、関連付けられた IP プールがない仮想 APN を持つ UP を動的に選択するための一連の動作について説明します。

1. 作成セッション処理の一環として、PGW-C が TAC 範囲に基づいて仮想 APN を選択します。

2. DNS（S-NAPTR）クエリが、選択した APN の設定に基づいて DNS サーバーに送信されます。
3. DNS サーバーから受信した応答がサービスと照合され、サービスフィールドが一致するレコードが選択対象と見なされます。
4. パブリック IP プールの一部であり、応答に存在する UP IP は、選択された APN の UP グループに基づいて、関連付けられた Sx ピアと照合されます。
5. 一致リストから、P-GW が最も負荷の少ない UP を選択します。

正常な DNS 応答に対する S-GW 動的 UP の選択

この項では、DNS サーバーから正常な応答を受信した後に、S-GW が動的に UP を選択する一連の動作について説明します。

1. トラッキングエリア（またはセル ID）内の UE がダイナミック ECGI を使用して S-GW に接続要求を送信すると、RAI-TAI-SAI | TAI-SAI-RAI-ECGI ベースの UP の選択機能が有効になり、DNS（S-NAPTR）クエリが DNS サーバーに送信されます。
2. S-GW が、UP IP のリストを含むクエリ応答を DNS サーバーから受信します。
3. UP IP のリストから、S-GW が負荷が最も少ない UP を選択します。

DNS 応答タイムアウトに対する S-GW 動的 UP の選択

この項では、DNS サーバーがタイムアウトした後、またはサーバーが否定応答を送信した後に、S-GW が動的に UP を選択するための一連の動作について説明します。

1. S-GW が DNS（S-NAPTR）クエリを DNS サーバーに送信します。
2. DNS サーバーがタイムアウトするか、DNS（S-NAPTR）クエリが DNS サーバーに送信された後にサーバーが否定応答を送信する場合、S-GW が静的 IP で設定された APN プロファイル UP グループから UP を選択します。
3. UP IP のリストから、S-GW が負荷が最も少ない UP を選択します。

コール フロー

ここでは、次のコールフローについて説明します。

DNS クエリの生成と応答処理のコールフロー

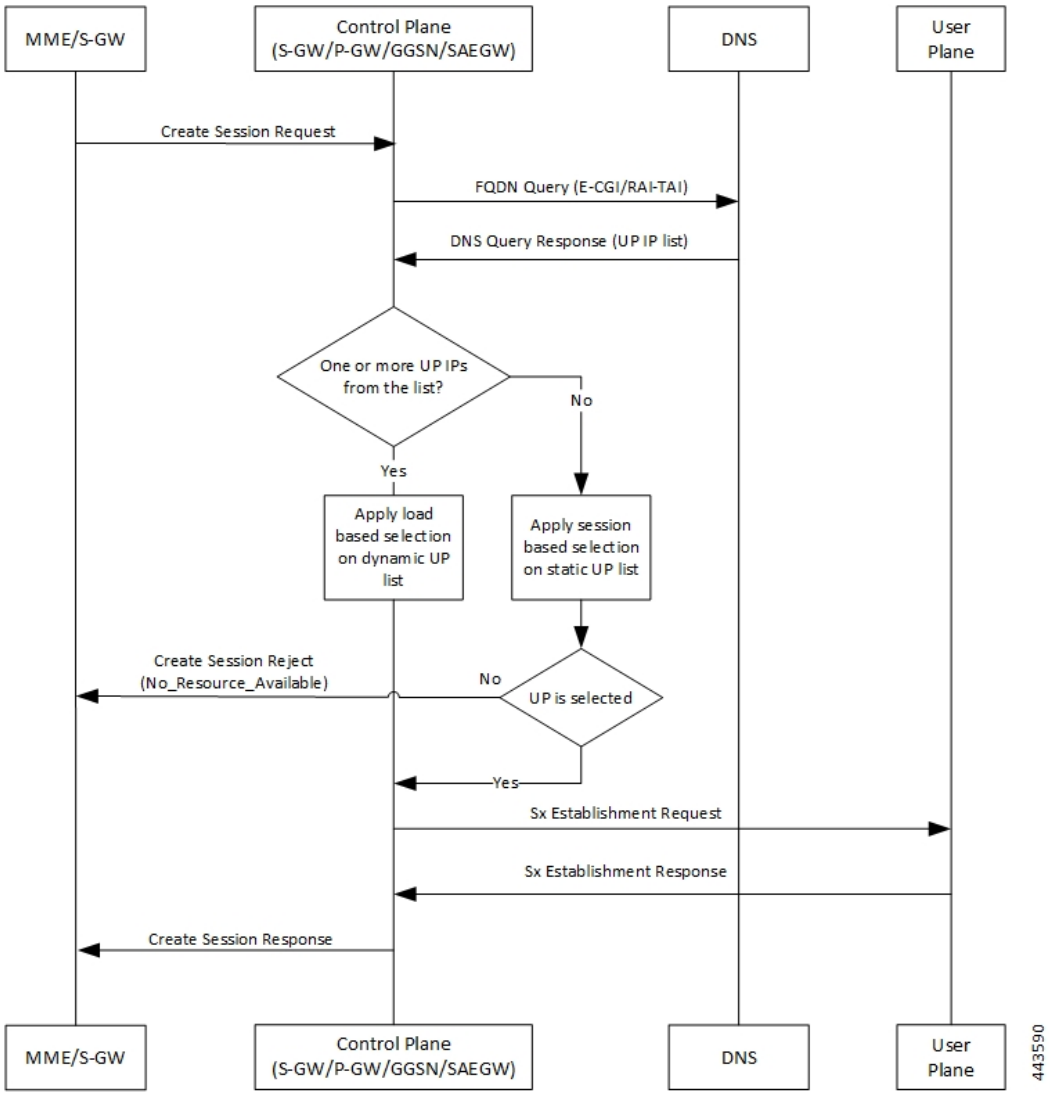


表 *48 : DNS* クエリの生成と応答処理のコールフローの説明

ステップ	説明
1	MME または S-GW が、セッション作成要求メッセージをコントロールプレー（S-GW、P-GW、GGSN、または SAEGW）に送信します。
2	コントロールプレーン（CP）は、FQDN クエリ（E-CGI または TAI-RAI- SAI TAI-SAI-RAI-ECGI）を DNS サーバーに送信します。
3	CP は、UP IP のリストを含む FQDN クエリへの応答を受信します。

ステップ	説明
4	• 受信したリストに UP IP が 1 つ以上含まれる場合、CP はダイナミック トに LCI を適用して UP IP を選択します。 • UP IP が含まれない場合は、CP は静的 IP リストにセッション数を適用 IP を選択します。
5	• UP が選択された場合、CP は UP に Sx 確立要求メッセージを送信しま テップ 6 に進みます）。 • UPが選択されない場合は、セッション作成拒否メッセージがMMEまた に送信されます。
6	UP は応答し、Sx 確立応答メッセージを CP に送信します。
7	CP は、セッション作成応答メッセージを MME または S-GW に送信します

プライマリ DNS の DNS クエリ タイムアウト コール フロー

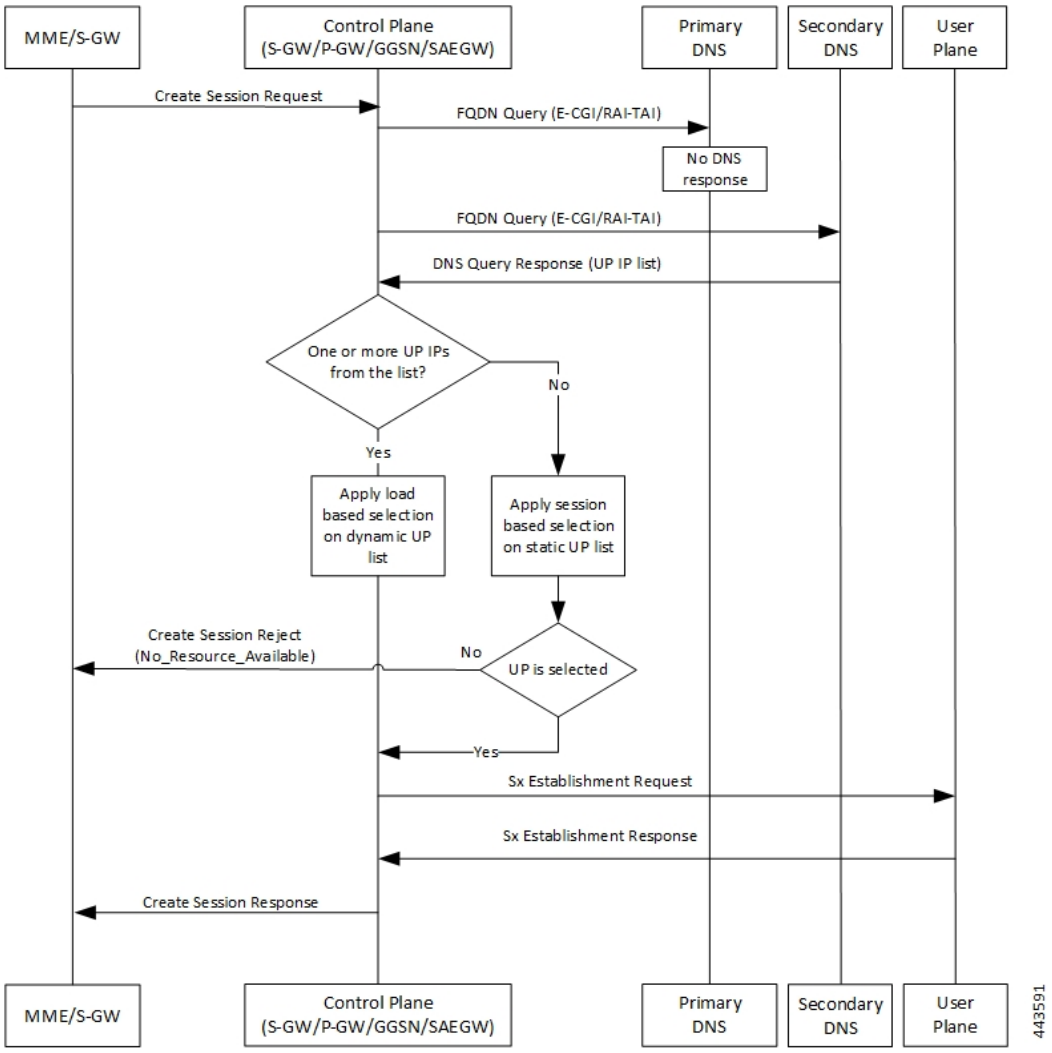


表 *49 :* プライマリ *DNS* の *DNS* クエリ タイムアウト コール フローの説明

ステップ	説明
1	MME または S-GW が、セッション作成要求メッセージをコントロールプレーン P-GW、GGSN、または SAEGW）に送信します。
2	コントロールプレーン（CP）は、FQDN クエリ（E-CGI または TAI-RAI- SAI また TAI-SAI-RAI-ECGI）をプライマリ DNS サーバーに送信します。
3	タイムアウトが原因でプライマリ DNS サーバーからクエリに対する応答がない場 今度はセカンダリ DNS サーバーに FQDN クエリを送信します。
4	CP は、セカンダリ DNS サーバーから UP IP のリストを含む FQDN クエリへの応答 ます。

ステップ	説明
5	• 受信したリストに UP IP が 1 つ以上含まれる場合、CP はダイナミック IP を適用して UP IP を選択します。 • UP IP が含まれない場合は、CP は静的 IP リストにセッション数を適用し択します。
6	• UP が選択された場合、CP は UP に Sx 確立要求メッセージを送信します に進みます）。 • UP が選択されない場合は、セッション作成拒否メッセージが MME また信されます。
7	UP は応答し、Sx 確立応答メッセージを CP に送信します。
8	CP は、セッション作成応答メッセージを MME または S-GW に送信します。

プライマリおよびセカンダリ **DNS** の **DNS** クエリ タイムアウト コール フロー

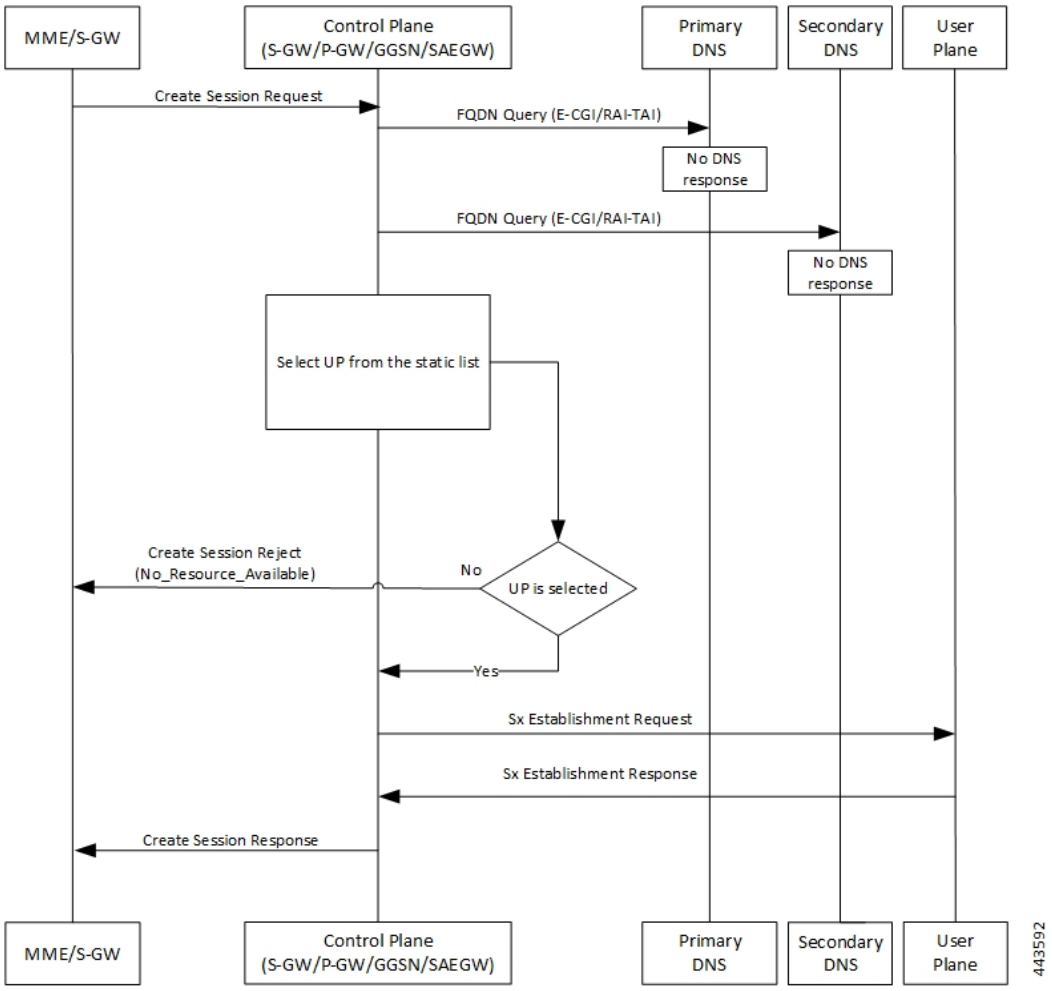


表 ***50*** *:* プライマリおよびセカンダリ ***DNS*** の ***DNS*** クエリ タイムアウト コール フローの説明

ステップ	説明
1	MME または S-GW が、セッション作成要求メッセージをコントロールプレ（S-GW、P-GW、GGSN、または SAEGW）に送信します。
2	コントロールプレーン（CP）は、FQDN クエリ（E-CGI または TAI-RAI- SA TAI-SAI-RAI-ECGI）をプライマリ DNS サーバーに送信します。
3	タイムアウトが原因でプライマリ DNS サーバーからクエリに対する応答がな CP は今度はセカンダリ DNS サーバーに FQDN クエリを送信します。
4	セカンダリ DNS サーバーからもクエリに対する応答がない場合、CP は静的 から UP IP を選択します。

ステップ	説明
5	• UP が選択された場合、CP は UP に Sx 確立要求メッセージを送信しま プ 6 に進みます）。 • UP が選択されない場合は、セッション作成拒否メッセージが MME に送信されます。
6	UP は応答し、Sx 確立応答メッセージを CP に送信します。
7	CP は、セッション作成応答メッセージを MME または S-GW に送信しま

制限事項

ダイナミック UP 選択機能には、次の制限事項があります。

- P-GW、S-GW、および SAEGW にのみ適用されます。
- SR および ICSR の場合、特定のパラメータは保存されません。**smgr** がリセットされると、設定された値が **sessctrl** から再度プッシュされます。
- DNS サーバーへの変更は考慮されません。
- UP で処理される IP 数の上限は 6 です。これらの IP は、IPv4 アドレスと IPv6 アドレスの組み合わせです。

ダイナミック ユーザー プレーン選択機能の設定

ここでは、ダイナミック ユーザー プレーン選択機能を設定する方法について説明します。

P-GW または GGSN の FQDN の設定

P-GW または GGSN（Pure-P コールおよび Collapsed コール）の FQDN を設定するには、次の設定を使用します。

```
configure
   context context_name
      apn apn_name
         user-plane-fqdn
         user-plane-fqdn fqdn_postfix_string type [ E-CGI | RAI-TAI -SAI |
TAI-SAI-RAI-ECGI ]
         end
```

注：

- **user-plane-fqdn**：ダイナミック UP 選択（DNS ベース）用にローカルに設定された FQDN ポストフィックスを有効にします。
- **E-CGI**：UP 選択の FQDN クエリタイプを E-CGI に設定します。
- **RAI-TAI-SAI**：UP 選択の FQDN クエリタイプを RAI-TAI-SAI に設定します。

- **TAI-SAI-RAI-ECGI**：UP 選択の FQDN クエリタイプを TAI-SAI-RAI-ECGI に設定します。

S-GW の FQDN の設定

S-GW（Pure-S コール）の FQDN を設定するには、次の設定を使用します。

```
configure
  context context_name
    sgw-service sgw-service_name
      user-plane-fqdn
      user-plane-fqdn fqdn_postfix_string type [ E-CGI | RAI-TAI -SAI |
TAI-SAI-RAI-ECGI ]
      end
```

注：

- **user-plane-fqdn**：ダイナミック UP 選択（DNS ベース）用にローカルに設定された FQDN ポストフィックスを有効にします。
- **E-CGI**：UP 選択の FQDN クエリタイプを E-CGI に設定します。
- **RAI-TAI-SAI**：UP 選択の FQDN クエリタイプを RAI-TAI-SAI に設定します。
- **TAI-SAI-RAI-ECGI**：UP 選択の FQDN クエリタイプを TAI-SAI-RAI-ECGI に設定します。

Boxer の設定

ここでは、次の Boxer の設定と制限事項について説明します。

1. DNS クライアントを設定し、P-GW および GGSN サービスに関連付ける必要があります。
2. UP FQDN は APN で設定する必要があります。
3. プライマリおよびセカンダリ DNS サーバーの IP アドレスは、ISP コンテキストで設定する必要があります。
4. S-GW のダイナミック UP 選択を可能にするため、UP FQDN を S-GW サービスで設定する必要があります。

DNS サーバーの設定

ここでは、外部 DNS サーバーの設定に関する、次のガイドラインと制約事項について説明します。

1. NAPTR に ECFI/CGI/TAI/RAI/SAI を記録させる場合には、DNS を設定する必要があります。
2. NAPTR レコードのサービスフィールドは、P-GW/SAEGW（Collapsed）および GGSN サービスの場合は「**x-3gpp-upf:x-sxb**」、S-GW の場合は「**x-3gpp-upf:x-sxa**」に設定されている必要があります。

3. NAPTR レコードでは、置換文字列が A レコードまたは AAAA レコードの FQDN であることを示すフラグが「**a**」に設定されている必要があります。

次の CLI コマンドは、DNS サーバーの設定例を示しています。

```
$ORIGIN 3gppnetwork.org.

$TTL 60              ; Put the Default
        TTL in seconds here (Its 1 day currently)

3gppnetwork.org.     IN SOA  nsbng.3gppnetwork.org. root.3gppnetwork.org.

273 ; serial

7200 ; refresh (2 hours)

3600 ; retry (1 hour)

86400 ; expire (1 day)

43200 ; minimum (12 hours)

)

 NS    nsbng.3gppnetwork.org.

ns AAAA 3001::41

;CUPS NAPTR Records Start From Here

;TAI NAPTR Records

tac-lb89.tac-hb67.tac.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  "a"
"x-3gpp-upf:x-sxb" ""
        uplane-address1-v4.3gppnetwork.org.

tac-lb89.tac-hb67.tac.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  "a"
"x-3gpp-upf:x-sxb" ""
        uplane-address1-v6.3gppnetwork.org.

tac-lb89.tac-hb67.tac.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  "a"
"x-3gpp-upf:x-sxa" ""
        uplane-address1-v4.3gppnetwork.org.

tac-lb89.tac-hb67.tac.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  "a"
"x-3gpp-upf:x-sxa" ""
        uplane-address1-v6.3gppnetwork.org.

;RAI NAPTR Records

rac34.lac-lb34.lac-hb12.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  "a"
"x-3gpp-upf:x-sxb" ""
          uplane-address1-v4.3gppnetwork.org

。

rac34.lac-lb34.lac-hb12.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  2  "a"
"x-3gpp-upf:x-sxb" ""
        uplane-address1-v6.3gppnetwork.org.

;SAI NAPTR Records

sac1234.lac-lb34.lac-hb12.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  1  'a'
'x-3gpp-upf:x-sxb' ''
           uplane-address1-v4.3gppnetwork.org.

sac1234.lac-lb34.lac-hb12.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1  2  'a'
'x-3gpp-upf:x-sxb' ''
         uplane-address1-v6.3gppnetwork.org.
```

```
;ECGI NAPTR Records

eci-b167.eci-b245.eci-b323.eci-b401.eci.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1
1  "a"   "x-3gpp-upf:x-sxb" ""
        uplane-address1-v4.3gppnetwork.org.

eci-b167.eci-b245.eci-b323.eci-b401.eci.epc.mnc365.mcc214.3gppnetwork.org. IN NAPTR 1
1  "a"   "x-3gpp-upf:x-sxb" ""
        uplane-address1-v6.3gppnetwork.org.

;CGI NAPTR Records

ci-lb34.ci-hb12.ci.lac-lb34.lac-hb12.lac.ggsn.mnc365.mcc214.3gppnetwork.org. IN NAPTR
          1  1
          "a"   "x-3gpp-upf:x-sxb" ""
        uplane-address1-v4.3gppnetwork.org.

ci-lb34.ci-hb12.ci.lac-lb34.lac-hb12.lac.ggsn.mnc365.mcc214.3gppnetwork.org. IN NAPTR
          1  1
          "a"   "x-3gpp-upf:x-sxb" ""s
        uplane-address1-v6.3gppnetwork.org.

;A Records

uplane-address1-v4   100     IN
          A    209.165.200.225

;uplane-address1-v4   100     IN      A
      209.165.200.225

uplane-address1-v4   100     IN
          A    209.165.200.225

;uplane-address2-v4   100     IN
          A    209.165.200.225

;AAAA Records

uplane-address1-v6   100     IN
          AAAA    1::1:111

uplane-address1-v6   100     IN
          AAAA    1111::1:111

;uplane-address2-v6   100     IN
          AAAA    1111::1:111
```

S6b の設定（オプション）

ここでは、カスタム属性 **aaa-uplane-fqdn** および **fqdn_post_fix_string** をサポートするための外部 S6b の設定に関するガイドラインを説明します。

```
AA-Answer
   apn-config
      uplane-fqdn
```

インターフェイス

以下の項では、DNS クエリと応答のフォーマットについて説明します。

DNS（S-NAPTR）クエリフォーマット

ここでは、DNS（S-NAPTR）クエリメッセージのフォーマットについて説明します。

重要 SAI ベースの FQDN は独自のフォーマットになっており、3GPP TS 23.003 19.4.2 完全修飾ドメイン名のようには指定しません。

ネットワークノード	クエリのフォーマット
SGW-C	**ECGI ベース** eci b1<ECI byte-1>.eci b2<ECI-byte-2>. Eci b3<ECI byte-3> .eci b4<ECI-byte-4>.eci.epc.mnc <MNC.mcc<MCC>.3gppnetwork.org **TAI ベース** tac lb<TAC low byte>.tac hb<TAC-high-byte> .tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
PGW-C	**ECGI ベース** eci-b1<TAC-byte-1>.eci-b2 <ECI-byte-2.Eci-b3<TAC-byte-3> .eci-b4<ECI-byte-4>.eci.epc.mnc<MNC> .mcc<MCC>.3gppnetwork.org **TAI ベース** tac-lb<TAC-low-byte> .tac-hb<TAC-high-byte> .tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
GGSN-C	**CGI ベース** ci-lb<CI-low-byte>.ci-hb<CI-high-byte> .eci.lac-lb<LAC-low-byte>.lac-hb<LAC-high-byte> .lac.ggsn.mnc<MNC>.mcc<MCC>. 3gppnetwork.org **RAI ベース** rac<RAC>.lac-lb<LAC-low-byte> .lac-hb<LAC-high-byte>.lac.ggsn.mnc<MNC> .mcc<MCC>.3gppnetwork.org **SAI ベース** sac<SAC>.lac-lb<LAC-low-byte>. lac-hb<LAC-high-byte>.lac.ggsn mnc<MNC>.mcc<MCC>.3gppnetwork.org

ネットワークノード	クエリのフォーマット
SAEGW-C（Collapsed）	**ECGI ベース** eci-b1<TAC-byte-1>.eci-b2<ECI-byte-2> . Eci-b3<TAC-byte-3>.eci-b4<ECI-byte-4> .eci.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org **TAI ベース** tac-lb<TAC-low-byte> .tac-hb<TAC-high-byte>.tac.epc.mnc <MNC>.mcc<MCC>.3gppnetwork.org **SAI ベース** sac<SAC>.lac lb<LAC low byte> .lac hb<LAC-high-byte>.lac.epc. mnc<MNC>.mcc<MCC>.3gppnetwork.org

DNS（S-NAPTR）応答フォーマット

ここでは、DNS（S-NAPTR）応答メッセージのフォーマットの例を紹介します。

```
Query ID              : 22290
Type                  : Response
Question              : NAPTR ?
          ci-lb34.ci-hb12.ci.lac-lb34.lac-hb12.lac.ggsn.mnc365.mcc214.3gppnetwork.org.
Answer                :
  Name                :
          ci-lb34.ci-hb12.ci.lac-lb34.lac-hb12.lac.ggsn.mnc365.mcc214.3gppnetwork.org.
  TTL                 : 60
  Type                : NAPTR
  Order               : 1
Preference : 1
  Flags               : a
  Service             : x-3gpp-upf:x-sxb
  Regexp              :
Replacement : uplane-address2.3gppnetwork.org.
  Name                :
        ci-lb34.ci-hb12.ci.lac-lb34.lac-hb12.lac.ggsn.mnc365.mcc214.3gppnetwork.org.
  TTL                 : 60
  Type                : NAPTR
  Order               : 1
  Preference          : 1
  Flags               : a
```

```
  Service             : x-3gpp-upf:x-sxb
  Regexp              :
Replacement : uplane-address1.3gppnetwork.org.
Query ID              : 44640
Type : Query
Question              : A?
        uplane-address2.3gppnetwork.org.
Query ID : 55480
Type                  : Query
Question              : A?
        uplane-address1.3gppnetwork.org.
Query ID : 55480
Type                  : Response
Question              : A?
         uplane-address1.3gppnetwork.org.
Answer                :
Name : uplane-address1.3gppnetwork.org.
  TTL                 : 100
  Type                : A
Address : 20.20.20.108
Query ID              : 44640
Type                  : Response
Question              : A?
         uplane-address2.3gppnetwork.org.
Answer                :
  Name                : uplane-address2.3gppnetwork.org.
  TTL                 : 100
  Type                : A
Address : 209.165.200.225
```

コマンドの表示

ここでは、ダイナミック UP 選択機能でサポートされるコマンドについて説明します。

show apn name *apn_name*

このコマンドは、Pure-P コールと Collapsed コールの DNS 関連情報を表示します。

このコマンドの出力を使用して、次の値を確認できます。

- APN の FQDN
- FQDN のタイプ

show sgw-service name *sgw_service_name*

このコマンドは、Pure-S コールの DNS 関連情報を表示します。

このコマンドの出力を使用して、次の値を確認できます。

- APN の FQDN
- FQDN のタイプ

show saegw-service statistics

show saegw-service statistics CLI コマンドを使用して、統計情報を収集します。

以下に、**show saegw-service statistics all** および **show saegw-service statistics name** *SAEGW21* CLI コマンドの出力例の一部を示します。

```
Dynamic Uplane Selection Statistics:
   Attempted              :             x
   Successful             :             x
   Failure                :             x
   Peer not Found         :             x
   Negative DNS response  :             x
   DNS timed out          :             x
   Unsolicited UP Selection Response:   x
   DNS Query Response post DNS timeout: x
```

以下に、**show saegw-service statistics all function sgw** CLI コマンドの出力例の一部を示します。

```
Dynamic Uplane Selection Statistics:
  Attempted:                            7
  Successful                            4
  Failure:                              3
    Mismatch DNS response:              1
    Negative DNS response:              1
    DNS timed out:                      1
    Unsolicited UP Selection Response:  1
    DNS Query Response post DNS timeout: 1
```

バルク統計情報

SAEGW Schema

このスキーマを使用して、動的ユーザープレーン選択機能に関連する次のバルク統計情報を収集します。

- saegw-dyn-up-attempt
- saegw-dyn-up-attempt
- saegw-dyn-up-success
- saegw-dyn-up-success
- saegw-dyn-up-failure
- saegw-dyn-up-failure
- saegw-dyn-up-peer-not-found

- saegw-dyn-up-peer-not-found
- saegw-dyn-up-dns-timeout
- saegw-dyn-up-dns-timeout
- saegw-dyn-up-neg-resp
- saegw-dyn-up-neg-resp

マルチ UP グループのサポート

マニュアルの変更履歴

表 *51* : マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.25

機能説明

リモートCUPSを使用すると、オペレータネットワークでプログレッシブ設定をロールアウトできます。特定の CP または UP プールでパイロットまたはカナリアバージョン N+1 を展開してアクティブ化できますが、バージョン N の設定は、モニタリング期間後に、この N+1 設定をすべての CP または UP プールにロールアウトするとオペレータが決めるまで、他の CP または UP プールでアクティブなままです。

この機能の使用例は次のとおりです。

- ECS または ADC 設定の更新のロールアウト：一方の CP または UP で古い設定を使用している間に、もう一方の CP または UP パイロットを使用して設定をテストする機能。
- 新しい APN 設定の更新：別のコンポーネントで古い設定を使用している間に、一連の CP または UP パイロットを使用して新しい APN 設定をテストする機能。
- IP プールの設定の更新を追加または削除します。

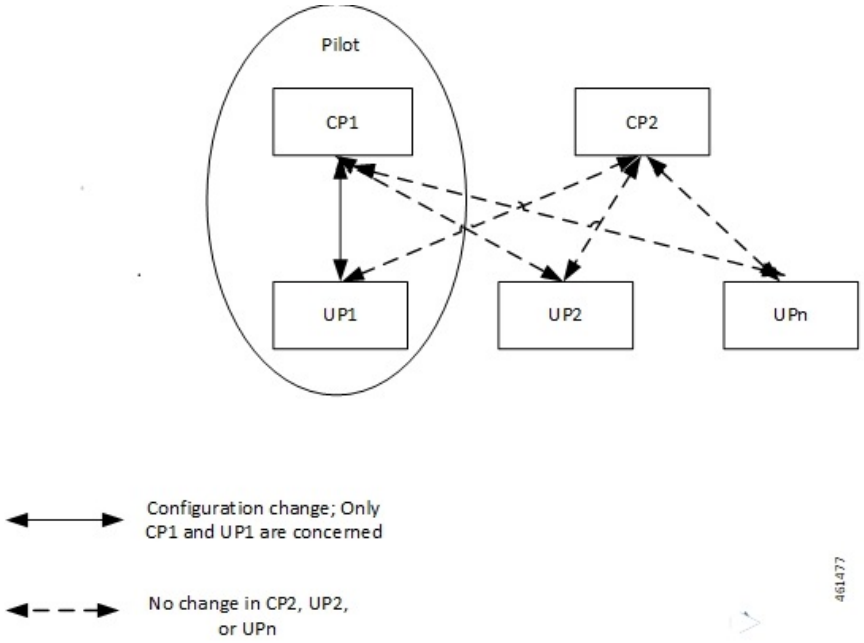
関係

TAC RAC プロファイルサポート機能は、テスト用仮想 APN の選択に使用される複数 UP グループサポート機能に関連するものです。

アーキテクチャ

次の図は、プログレッシブな設定の運用開始アーキテクチャを示しています。

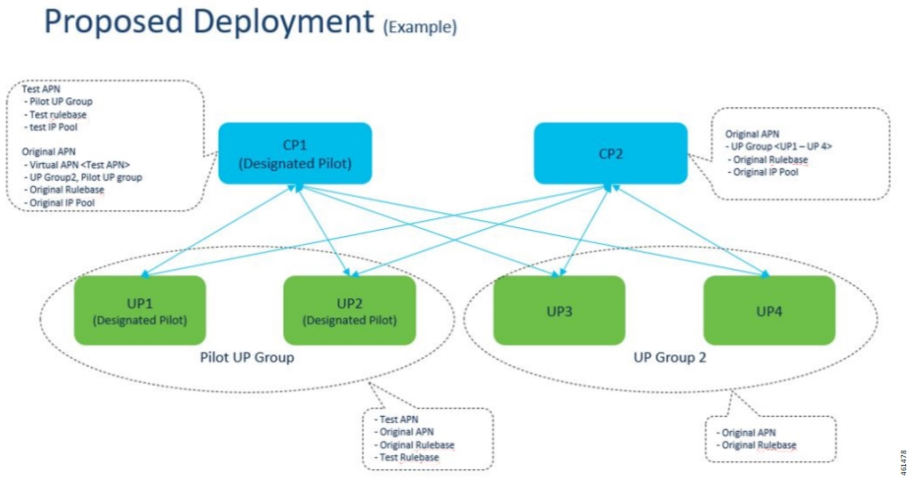
図 *45 :* プログレッシブな設定の運用開始



コンポーネント

次の図は、提案される導入コンポーネントを示しています。

図 *46 :* 導入案



機能の仕組み

パイロット CP は、着信テストパイロットコールをパイロット UP グループにルーティングします。

パイロット CP は、通常のビジネスコールも元の展開に従って任意の UP にルーティングするため、この機能は 1 つの APN にある複数の UP グループをサポートします。最初の UP グループにパイロット UP が含まれ、2 番目の UP グループに他のすべての非パイロット UP が含まれます。1 つの UP が 2 つの UP グループに同時に存在することはできません。UP と UP グループ間には厳密な 1:1 マッピングがあります。

制限事項と制約事項

複数 UP グループのサポート機能には次の制限事項と制約事項があります。

- パイロット設定は、UP グループレベルでのみ適用できます。
- CP と UP は個別に設定します。
- ruledef、課金アクションなどの下位レベルで発生する ECS 設定の変更は、パイロット UP から分離できません。ルールベースレベルで区別する必要があります。
- パイロット CP と UP は、展開時に指定する必要があります。展開後の指定では、既存のセッションをクリアする必要があります。
- ユーザーグループがいずれの APN にも接続されていない場合は、対応する UP ノードを登録解除し、CP 設定から削除する必要があります。
- 静的 IP プールはサポートされていません。

複数 UP グループのサポート機能の設定

ここでは、 複数 UP グループのサポート機能の設定方法を説明します。

複数 UP グループのサポート機能を設定するには、次の手順を実行します。

シリアル番号	設定	パイロット設定の場合
1	ECS または ADC の設定 （ruledef、rulebase、課金アクションなど）	パイロット CP の場合：設定の差別化は rulebase レベルで実施する行必要があります。ruledef、課金アクションなどの設定エンティティを変更する場合は、重複が必要となります。 パイロット CP の場合：対応する設定変更を 1 つまたは複数のパイロット UP で直接実行する必要があります。

シリアル番号	設定	パイロット設定の場合
2	APN 設定	• 必要な設定を変更して新しい APN を作成します。 • 必要なリダイレクトルールを設定して、既存の APN でテスト用 APN を仮想 APN として設定します。または、MME を使用してコールをテスト用 APN にリダイレクトします。
3	UP グループ設定	• 展開時にパイロット CP と UP を選択します。 • APN に設定する必要がある複数の UP グループを有効にします。
4	IP プール設定	新規 IP プール： • 新しい IP プールを作成し、テスト用 APN に関連付けます。 既存の IP プールの更新： • 直接 IP プールの設定を変更します。 **注**：変更を 1 つまたは複数のパイロット UP のみにローカライズすることはできません。

UP 管理ポリシーの設定

UP 管理ポリシーを設定するには、次の設定を使用します。

```
configure
   up-mgmt-policy policy_name
      user-plane-group group_name
      end
```

注：

- **up-mgmt-policy** *policy_name*：UP 管理ポリシーを 1 ～ 31 文字の文字列で指定します。
- **user-plane-group** *group_name*：ユーザープレーングループの名前を指定します。

Pure-P コールおよび Collapsed コールの UP 選択

Pure-P および Collapsed コールタイプの UP 選択を設定するには、次の設定を使用します。

```
configure
   context context_name
```

```
apn apn_name
  up-mgmt-policy policy_name
  end
```

Pure-S コールの UP 選択

Pure-S コールタイプの UP 選択を設定するには、次の設定を使用します。

```
configure
  context context_name
    apn-profile profile_name
      up-mgmt-policy policy_name
      end
```

注：

- **up-mgmt-policy** *policy_name* は、1 ～ 31 文字の文字列である必要があります。
- APN プロファイルレベルの UP グループまたは UP 管理ポリシーのいずれかを設定できます。
- APN プロファイルの場合、設定できる UP 管理ポリシーは 1 つだけです。
- IP アドレス割り当てのプール名を割り当てます。

UP グループ間の優先順位

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	21.27.2

機能説明

CUPS では、同じ CP に関連付けられた異なる UP 間での IP プールの重複がサポートされます。同じ CP に関連付けられた UP グループはすべて、同じ IP プール範囲を取得します。分離 IP プールは、異なる CP で設定されるもので、異なるロケーションにある UE に同じ IP を割り当てることができます。プールでは Virtual Routing and Forwarding（VRF）を使用して、2 つの UE のトラフィックを区別します。

機能の仕組み

ユーザープレーンは、共通の特性、つまり地理的ロケーションに基づいて UP グループへとクラスタ化されます。CP は、これらの UP グループを特定の IP プールに関連付けます。このとき、同じ地理的ロケーションの UP が同じ IP プール範囲を持つことはできず、異なる地理的ロ

ケーションの UP は同じ IP プール範囲を取得できます。この動作は、IP プール管理ポリシーと呼ばれる新しいポリシーを導入することによって実現されます。IP プール管理ポリシーは APN で適用されます。

UP 選択では、IP プール管理ポリシーの UP グループに DNS ベースの UP 選択アルゴリズムが使用されます。DNS クエリ応答は、DNS クエリ要求で送信される TAC/RAC 値に基づいて、対象となる UP IP アドレスをリストします。その後、対象となる UP IP アドレスに最小負荷アルゴリズムが使用され、最終的に UP が選択されます。

モバイル IP プールの重複をサポートするため、次の要件が満たされます。

- UP グループ固有の IP プールのサポート
- プールが任意の UP グループの固有プールに設定されている場合の UP への IP プールチャンクの割り当て
- 複数の UP グループでの DNS ベースの UP 選択アルゴリズム

以下に、DNS ベースの UP 選択機能に関する考慮事項のリストを示します。

- UP グループに特定の IP プール/グループ名が設定されていない場合、APN に IP プール管理ポリシーが設定されていると、パブリックプールからチャンクを取得します。
- UP 選択は、そのグループ内の他の UP の負荷が少ない場合でも、最小セッション数 UP 選択アルゴリズムと UP 可用性ステータスに基づいて、返された UP IP アドレスの中から行われます。
- DNS クエリ応答では、上限である最大 6 つの UP IP アドレスに対して受信された UP のリストは、IP プール管理ポリシーの設定によっては異なる UP グループに属し、その中で最もセッション数の少ない UP が選択されます。
- UP の選択完了後に、Sx 確立要求が UP から拒否された場合、再試行は行われません。
- IP プールまたはグループ名が複数の UP グループ間で共有されている場合、IP チャンクの割り当ては、UP 登録時に先着順で行われます。このため、IP プールのチャンクが均等に配分されない可能性があります。
- APN で UP グループと IP プール管理ポリシーを同時に設定することはできません。
- UP が選択された後、その UP に十分な IP アドレスがない場合、使用可能なリソースが不足しているため、コールは拒否されます。
- 設定中に RCM で必要な変更はありません。
- CP インスタンス間で分離 IP プールを設定する必要があります。

ダイナミック APN IP プール更新

ダイナミック APN IP プール更新は、UP 関連付けを解除することなく、UP で IP プールチャンクを割り当てまたは解放する必要がある場合に実行されます。IP プール関連の設定変更後に、次の CLI コマンドを実行する必要があります。この CLI は、これまで UP グループと IP プー

ルで APN レベルでサポートされていたものです。それが拡張され、UP グループと IP プールで IP プール管理ポリシーレベルでサポートされるようになりました。

```
update ip-pool apn all
```

詳細については、「ダイナミック *APN* および *IP* プールのサポート」 の章を参照してください。

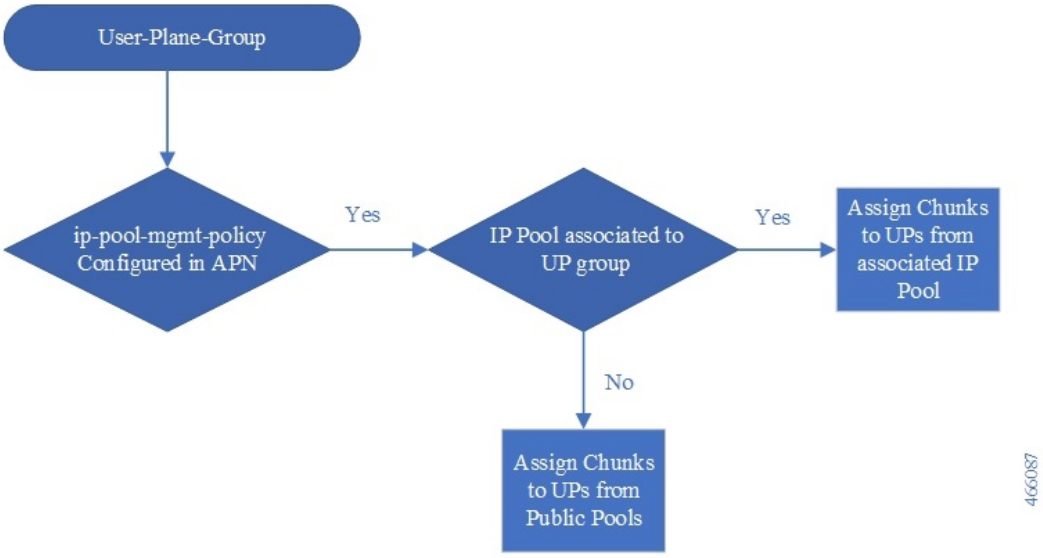
UP グループ固有の IP プールのサポート

APN の複数の UP グループおよび UP グループ固有の IP プールを設定するには、IP プール管理ポリシーを使用します。UP がすでに関連付けられている場合、IP プールに関する APN の変更については、このガイドの「ダイナミック *APN* および *IP* プールのサポート」の章で説明しているダイナミック IP プール手順を実行する必要があります。この手順によって、IP プールのチャンクが UP グループに再割り当てされます。

UP への IP プールチャンクの割り当て

UP を関連付けると、UP 登録要求が VPN に送信されます。要求メッセージには、チャンクが UP に割り当てられる IP プールのリストが含まれます。IP プールのリストは、次の図に示されている動作に従って作成されます。

図 *47*: *IP* プール管理ポリシーを介した *APN* に関連付けられた *UP* グループに対するチャンクの割り当て



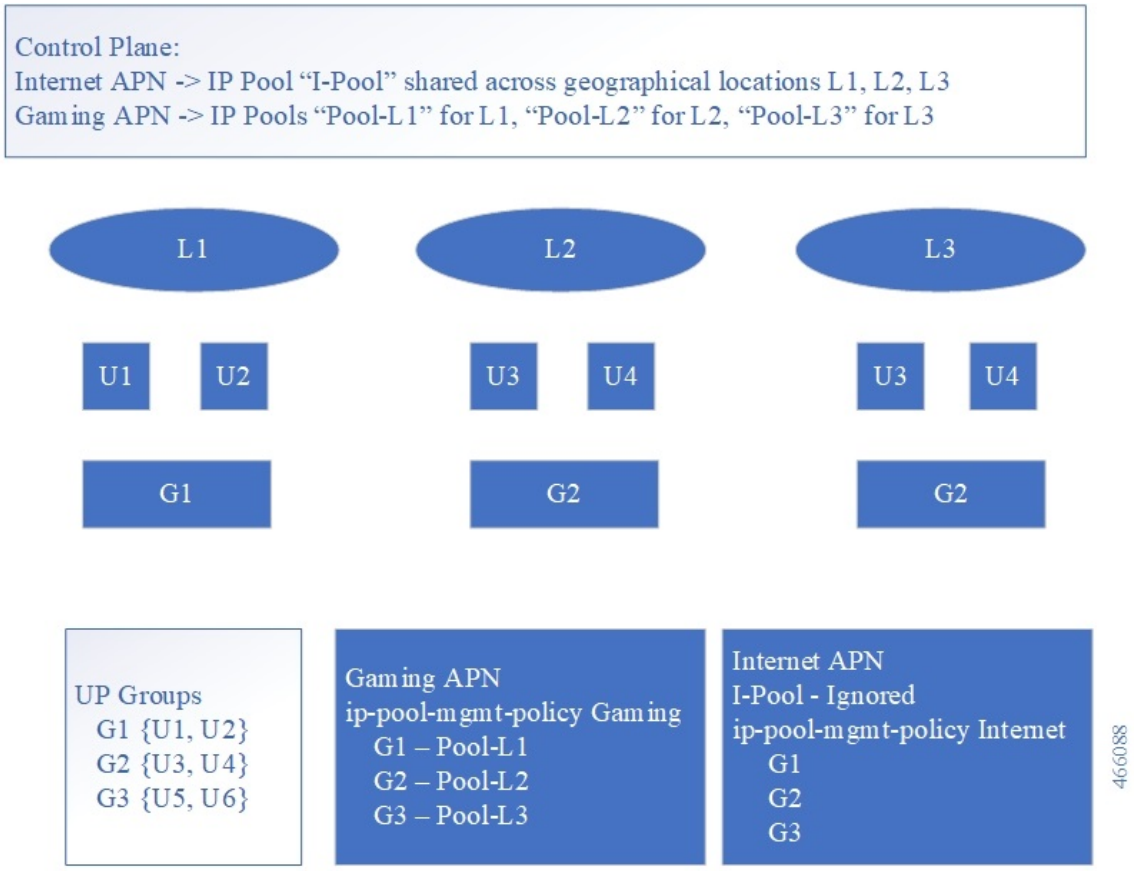
次の表は、G4/G6 がグローバル/パブリック IPv4/IPv6 プール、U4/U6 が UP グループレベルの IPv4/IPv6 プールの場合に予想される動作の例です。

UP グループレベルの IPv4 プール（U-4）	UP グループレベルの IPv6 プール（U-6）	予想される動作
F	F	G4+G6
F	T	U6+G4

T	F	U4+G6
T	T	U4+U6

次の図は、UP グループレベルの IP プールを使用した APN レベルの IP プールの設定を示しています。

図 *48 : UP* グループレベルの *IP* プールを使用した *APN* レベルの *IP* プールの設定



関連付けられた IP プールは、**ip-pool-mgmt-policy** で設定された **user-plane-group** で更新され、UP は再度関連付けられません。これは、IP プール管理ポリシーのダイナミック IP プール更新機能のサポートが有効になっているために可能です。UP は、APN 設定のステータスに基づいて IP プールのチャンクを取得します。

また、コールの確立時に、APN で設定されている現在の IP プール名が、選択した UP グループ名の対応する IP プール名とともに使用されます。

UP を再度関連付けずに、「ip-pool-mgmt-policy」で設定された「user-plane-group」の関連付けられた IP プールを更新できます。これは、IP プール管理ポリシーのダイナミック IP プール更新機能（「ダイナミック APN および IP プールのサポート」の章を参照）のサポートを拡張することで可能になります。UP は、APN 設定の最新のスナップショットに基づいて IP プールのチャンクを取得します。

また、コールの確立時に、APN で設定された IP プール名が、選択した UP グループ名の対応する IP プール名とともに使用されます。

複数の UP グループでの DNS ベースの UP 選択アルゴリズム

DNS は、ロケーション（TAC/RAC）情報を使用してクエリされます。UP 選択アルゴリズムは、DNS から受信した UP（UP IP アドレス）のリストに基づいて、設定された UP グループの UP をフィルタ処理し、結果の一連の UP に対して UP 選択アルゴリズム（LCI/OCI またはセッションカウント）を実行します。この機能は「ip-pool-mgmt-policy」用に拡張されています。フィルタリングは、「ip-pool-mgmt-policy」の一部であるすべての UP グループに適用されるようになりました。

次の図は、DNS ベースの UP の選択に関するイベントとデータの一般的なフローを示しています。

図 *49 : DNS* ベースの *UP* の選択に関するイベントとデータのフロー

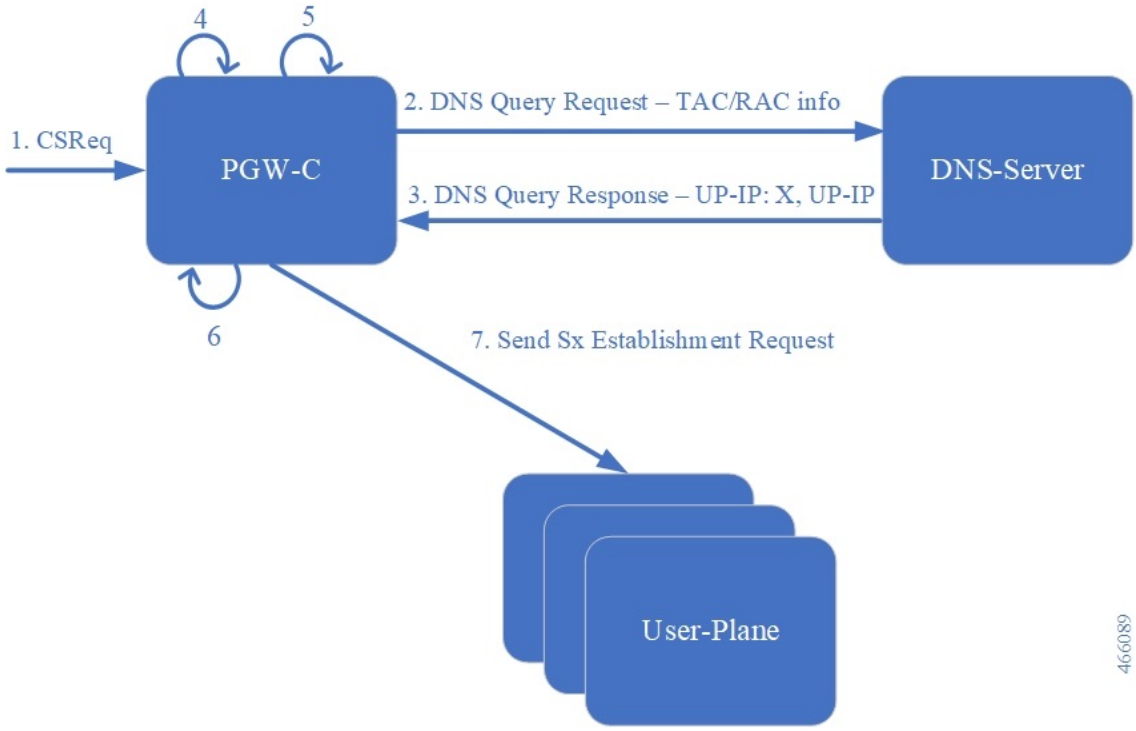


表 *52 : DNS* ベースの *UP* の選択に関するイベントとデータの一般的なフロー

手順	説明
1.	CS 要求メッセージが PGW-C に送信されます。
2 に送信します。	TAC/RAC 情報を含む DNS クエリ要求が、PGW-C によって DNS サーバーに送信されます。

手順	説明
3.	DNS クエリ応答が、DNS サーバーから PGW-C に返送されます。
4.	PGW-C が、DNS 応答と UP グループまたは「ip-pool-mgmt-policy」から一連の UP の共通部分を検出します。
5.	PGW-C が、結果のセットから UP および UP グループを選択します。
6.	PGW-C が、UP グループとプール名に基づいて IP アドレスを選択します。
7.	PGW-C が、Sx 確立要求をユーザープレーンに送信します。

制限事項

この機能には次の既知の制限事項があります。

- UP オーバーライド機能は、IP プール管理ポリシーではサポートされません。
- DNS ベースの UP 選択プロセスで処理される、TAC/RAC ロケーションごとに許可される UP の最大数は 6 です。
- DNS ベースの UP 選択では、UP 間でコールが不均一に配分され、IP プールが枯渇する可能性があります。これは、DNS サーバーが UP のセッション数を認識しないため、TTL が原因で発生します。
- デフォルト UP グループの場合のような、デフォルト IP プール管理ポリシーはありません。
- 静的コールは、IP プール管理ポリシーではサポートされません。
- 1 つの IP プール管理ポリシーに対し、分離した複数の UP グループを設定できます。または、2 つの IP プール管理ポリシーが共通する 1 つの UP グループを共有する場合には、2 つのポリシーの他の UP グループも同じにする必要があります。そうしないと、ロードバランシングが不均一になり、IP プールが枯渇する可能性があります。
- 20 の UP グループを対象とする IP プール管理ポリシーあたり、最大 20 の IP プール管理ポリシーを含むことができます。
- CP システム全体で許可される UP グループの最大数は 100 です。
- 1 つの UP グループで許可される UP の最大数は 100 です。
- 1 つの CP で許可される UP の最大数は 100 です。

特定の IP プールを使用した IP プール管理ポリシーと UP グループの設定

IP プール管理ポリシーを設定するには、次の設定を使用します。

```
configure
   context context_name
      apn apn_name
         ip-pool-mgmt-policy policy_name
         end
```

注：

- **ip-pool-mgmt-policy** *policy_name*：IP プール管理ポリシー名を 1 ～ 32 文字の文字列で指定します。

特定の IP プールを使用して UP グループを設定するには、次の設定を使用します。

```
configure
   ip-pool-mgmt-policy policy_name
      user-plane-group group_name { ip-address-pool-name ipv4_pool_name |
ipv6-address-pool-name ipv6_pool_name } [ secondary ]
      end
```

注：

- **ip-pool-mgmt-policy** *policy_name*：IP プール管理ポリシー名を 1 ～ 31 文字の文字列で指定します。
- **user-plane-group** *group_name*：UP グループ名を 1 ～ 31 文字の文字列で指定します。
- **ip-address-pool-name** *ipv4_pool_name*：IPv4 アドレスプール名を 1 ～ 31 文字の文字列で指定します。
- **ipv6-address-pool-name** *ipv6_pool_name*：IPv6 アドレスプール名を 1 ～ 31 文字の文字列で指定します。

UP および UP グループを追加および削除するための MOP

UP を削除するための MOP

1. CP でコマンドを実行して、その UP に配置されている新しいセッションをブロックし、任意で、up-ip-address を使用してサブスクライバをクリアします。詳細については、「ユーザープレーンノードの停止手順」の章を参照してください。

（注） **clear subscribers** コマンドが UP で実行されると、CP には通知されず、セッションは実行中であると見なされます。

2. すべてのサブスクライバが正常に解放されているか、UP で強制的に切断されていることを確認します。また、すべてのセッションが切断されていることを確認します。
3. UP で、 コマンドを実行して CP との関連付けを解除します。CP から UP の関連付けが解除され、CP では以降のセッションにこの UP が選択されません。
4. CP で、UP グループから UP を削除するコマンドを実行します（UP の BFD モニタリングも登録解除されます）。
5. **no monitor-group** コマンドを使用して、UP および CP でのモニタリングの BFD 設定を無効にします。

UP グループを削除するための MOP

1. 「UP を削除するための MOP」を使用して、UP グループから UP を削除します。
2. 設定から UP グループを削除します。UP グループが APN 範囲または IP プール管理ポリシーに関連付けられているか確認します。
   - APN レベル
     - APN からの UP グループの関連付け解除
   - IP プール管理ポリシー
     - IP プール管理ポリシーからの UP グループの関連付け解除

UP グループを追加するための MOP

1. UP IP アドレスと新しい UP グループを設定に追加します。
2. UP グループは、APN 範囲または IP プール管理ポリシーに追加できます。
   - APN レベル
     - APN での UP グループと IP プールの関連付け
   - IP プール管理ポリシー
     - IP プール管理ポリシーでの UP グループと IP プールの関連付け

APN で IP プール管理ポリシーを削除および変更するための MOP

変更は、削除、追加の順で実行します。

1. 「UP を削除するための MOP」を使用して、UP グループから UP を削除します。
2. 設定から UP グループを削除します。
   - IP プール管理ポリシーからの UP グループの関連付け解除

3. APN の IP プール管理ポリシーを変更または削除できます。

UP グループでの追加操作

IP プールを UP グループに関連付ける方法を以下に示します。

UP グループに IPv4 プールと IPv6 プールの両方を追加

IPv4 と IPv6 の両方のプールを UP グループに追加するには、次の設定を使用します。

```
configure
   ip-pool-mgmt-policy policy_name
      user-plane-group group_name ip-address-pool-name ipv4_pool_name
ipv6-address-pool-name ipv6_pool_name
      end
```

UP グループに IPv4 プールのみを追加

IPv4 プールのみを UP グループに追加するには、次の設定を使用します。

```
configure
   ip-pool-mgmt-policy policy_name
      user-plane-group group_name ip-address-pool-name ipv4_pool_name
      end
```

（注） APN のタイプが IPv4v6 の場合、IPv6 プレフィックスを意味し、この場合はパブリックプールが使用されます。

UP グループに IPv6 プールのみを追加

IPv6 プールのみを UP グループに追加するには、次の設定を使用します。

```
configure
   ip-pool-mgmt-policy policy_name
      user-plane-group group_name  ipv6-address-pool-name ipv6_pool_name
      end
```

（注） APN のタイプが IPv4v6 の場合、IPv4 アドレスを意味し、この場合はパブリックプールが使用されます。

UP グループでの削除操作

次に、UP グループから IP プールの関連付けを解除する方法を示します。

UP グループの削除

UP グループ自体を削除するには、次の設定を使用します。

```
configure
  ip-pool-mgmt-policy policy_name
    no user-plane-group group_name
    end
```

UP グループからの IPv4 プールと IPv6 プールの両方の削除

UP グループから IPv4 と IPv6 の両方のプールを削除するには、IP プールを指定せずに UP グループを再設定します。

設定例：

```
configure
  ip-pool-mgmt-policy xyz
    user-plane-group G1 ip-address-pool-name v4-pool
ipv6-address-pool-name v6-pool
    end
```

次の CLI コマンドを使用して、UP グループを再設定します。

```
configure
  ip-pool-mgmt-policy xyz
    user-plane-group G1
    end
```

（注） APN が IPv4v6 タイプの場合、パブリックプールは IPv4 および IPv6 アドレスに使用されます。

UP グループからの IPv4 または IPv6 プールのみの削除

IPv4 または IPv6 プールを削除するには、削除する UP グループを再設定します。

設定例：

```
configure
  ip-pool-mgmt-policy xyz
    user-plane-group G1 ip-address-pool-name v4-pool
ipv6-address-pool-name v6-pool
    end
```

次の CLI コマンドを使用して、UP グループを再設定します。

```
configure
  ip-pool-mgmt-policy xyz
    user-plane-group G1 ipv6-address-pool-name v6-pool
    end
```

（注） APN が IPv4v6 タイプで、IPv6 プールのみが UP グループに関連付けられている場合、パブリックプールが IPv4 アドレスに使用されます。IPv4 プールが UP グループに関連付けられている場合、パブリックプールが IPv6 アドレスに使用されます。

設定例

コントロールプレーン：1

```
config
   context egress
      ip pool PRIVATE-1 192.168.0.0/16 private chunk-size 1024 vrf-name vf-name-1
      ip pool PRIVATE-2 192.168.0.0/16 private chunk-size 1024 vrf-name vf-name-2
      ip pool PRIVATE-3 192.168.0.0/16 private chunk-size 1024 vrf-name vf-name-3
   exit
#exit
user-plane-group UP-Grp-1
   peer-node-id ipv4-address 192.168.0.1
exit
user-plane-group UP-Grp-2
   peer-node-id ipv4-address 192.168.0.2
exit
user-plane-group UP-Grp-3
   peer-node-id ipv4-address 192.168.0.3
exit
ip-pool-mgmt-policy xyz
   user-plane-group UP-Grp-1 ip-pool name PRIVATE-1
   user-plane-group UP-Grp-2 ip-pool name PRIVATE-2
   user-plane-group UP-Grp-3 ip-pool name PRIVATE-3
end

config
   context ingress
      apn intershat
         ip context-name egress
         ip-pool-mgmt-policy xyz
      exit
  #exit
end

UP-Grp-1 ===> Region 1 (192.168.0.0/16)
UP-Grp-2 ===> Region 2 (192.168.0.0/16)
UP-Grp-3 ===> Region 3 (192.168.0.0/16)
```

コントロールプレーン：2

```
config
   context egress
      ip pool PRIVATE-1 172.16.0.0/12 private chunk-size 1024 vrf-name vf-name-1
      ip pool PRIVATE-2 172.16.0.0/12 private chunk-size 1024 vrf-name vf-name-2
      ip pool PRIVATE-3 172.16.0.0/12 private chunk-size 1024 vrf-name vf-name-3
   exit
#exit
user-plane-group UP-Grp-1
   peer-node-id ipv4-address 192.168.0.1
exit
user-plane-group UP-Grp-2
   peer-node-id ipv4-address 192.168.0.2
exit
user-plane-group UP-Grp-3
   peer-node-id ipv4-address 192.168.0.3
exit
ip-pool-mgmt-policy xyz
   user-plane-group UP-Grp-1 ip-pool name PRIVATE-1
   user-plane-group UP-Grp-2 ip-pool name PRIVATE-2
   user-plane-group UP-Grp-3 ip-pool name PRIVATE-3
end
```

```
config
   context ingress
      apn intershat
         ip context-name egress
         ip-pool-mgmt-policy xyz
      exit
  #exit
end

UP-Grp-1 ===> Region 1 (172.16.0.0/12)
UP-Grp-2 ===> Region 2 (172.16.0.0/12)
UP-Grp-3 ===> Region 3 (172.16.0.0/12)
```

IP プール管理ポリシーの設定の確認

IP プール管理ポリシーを確認するには、次の CLI コマンドを使用します。

show ip-pool-mgmt-policy all

特定の UP グループの IP プール管理ポリシーを確認するには、次の CLI コマンドを使用します。

show ip-pool-mgmt-policy user-plane-group-name *group_name*

プール名の使用済み IP チャンクと空き IP チャンクを確認するには、次の CLI コマンドを使用します。

show ip pool-chunks pool-name

TAC 範囲に基づくユーザープレーンの選択

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
このリリースでは、TAC/RACプロファイル設定がサポートされるようになりました。	21.25
初版	21.24 より前

機能説明

この機能を使用すると、アクセスポイント名（APN）に基づいてユーザープレーングループを選択できます。仮想 APN 選択のルールの組み合わせでトラッキングエリアコード（TAC）範

囲を設定する機能は、エッジコンピューティングやその他のサービス用のロケーションベースのユーザープレーン選択用の柔軟なネットワーク設計に役立ちます。

21.25 以降のリリースでは、コントロールプレーンノードで TAC およびルーティングエリアコード（RAC）プロファイルを設定するためのサポートが追加されています。この機能を使用すると、範囲ではなく、TAC/RAC プロファイルの離散値に基づいて APN を選択できるようになりました。

機能の仕組み

非 CUPS アーキテクチャでは、仮想 APN の選択は次のパラメータに基づきます。

- サブスクライバ IP
- Access-gw-address
- Bearer-access
- cc-behavior
- cc-profile
- ドメイン
- mcc
- msisdn-range
- pdp-type
- rat-type
- roaming-mode
- serv-gw-plmnid

CUPS アーキテクチャでは、仮想 APN の選択はトラッキングエリアコードの範囲に基づいて行われ、その他にも cc-profile や mcc/mnc などのオプションが考慮されます。

この機能をサポートするため、次の点が変更になります。

- 新しいパラメータに対応するため、新しい CLI キーワードを導入します。
- コール処理中に、受信したトラッキングエリアコードが設定済みのトラッキングエリアコードの範囲と比較され、仮想 APN が決定されます。

トラッキングエリアコードに基づく仮想 APN の選択：

- 仮想 APN に対し、30 以上の tracking-area-code-range の設定をサポートします。
- 重複する範囲（サブセットまたはスーパーセット）をサポートします。優先順位が異なる場合は、tracking-area-code-range の重複は許可されません。
- CLI 設定に基づいて仮想 APN を選択し、ユーザープレーンは新しいコールの仮想 APN に応じて、その UE の tracking-area-code に基づいて選択されます。

- 優先順位が同じ tracking-area-code-range と cc-profile の組み合わせをサポートします。

仮想 APN 機能には、リアル/Gn APN ごとのすべての仮想 APN 選択ルールの保存機能が含まれます。すべてのルールには複数の条件があります。ルールはプリファレンス番号によって識別されます。APN のリストが保存され、APN 内でルールはプリファレンス番号によって識別されます。

CSReq（TAI）で受信したトラッキングエリアコードを渡すための新しいパラメータが導入されました。

制限事項

この機能の既知の制限事項と制約事項は次のとおりです。

- 仮想 APN 選択では、複数の選択基準がある新しい設定は、古いビルドやリリースでは機能しません。ユーザーは、古いビルドやリリースの設定に関する個別のコピーを用意する必要があります。
- 仮想 APN ルールの変更操作はサポートされていません。変更操作を実行するには、既存のルールを削除し、新しいルールを追加する必要があります。
- 同じルールで同じオプションが複数回指定されている場合、後で指定したオプションの値が選択対象と見なされます。
- すべての APN に追加される仮想 APN ルールの総数は 2,048 に制限されています。この制限は、非 CUPS アーキテクチャの制限です。
- 最大 1,000 の TAC/RAC プロファイルを設定できます。メモリ使用量は、設定されたプロファイルの数に基づきます。
- プロファイルでサポートされる TAC/RAC の離散値の最大数は 100 です。メモリ使用量はプロファイルごとに固定されます。
- TAC/RAC の範囲または離散値は、既存のプロファイルの分割などのメンテナンスアクティビティをサポートするために、プロファイル間で重複できます。
- これは Day-0 および Day-1 の設定です。
- 複数のプロファイルを 1 つの APN に関連付けられます。
- 既存の IP プール機能に変更はありません。
- ICSR またはマルチ Sx 設定に対する具体的な影響はありません。
- サービスエリアコード（SAC）はサポートされていません。
- Pure-S コールはサポートされていません。
- UP の選択要件は、複数 UP グループのサポート機能で処理されます。

TAC 範囲に基づいたユーザープレーンの選択の設定

この項では、この機能をサポートするために使用可能な CLI コマンドについて説明します。

トラッキングエリアコード範囲の設定

次の CLI コマンドを使用して、コントロールプレーンノードでトラッキングエリアコード範囲の APN を設定します。

```
configure
  context context_name
    apn apn_name
      virtual-apn preference preference apn apn_name
tracking-area-code-range tac_range
      end
```

注：

- **tracking-area-code-range** *tac_range*：トラッキングエリアコード範囲の APN を設定します。*tac_range* は、0 ～ 65,535 の範囲の整数値です。

トラッキングエリアコード範囲の設定の確認

次の CLI コマンドを使用して、機能が有効になっているかどうか、およびトラッキングエリアコードの範囲が設定されているかどうかを確認します。

- **show configuration apn** *apn_name*
- **show apn name** *apn_name*

トラッキング エリア コード プロファイルの設定

21.25 以降のリリースから、トラッキングエリア コードプロファイルはコントロールプレーンノードで設定できます。この機能を使用することで、TAC の範囲のみではなく、個別の値に基づいて APN を選択できるようになります。

次の CLI コマンドを使用して、個別の値と範囲を使ってトラッキング エリア コード プロファイルを設定します。

```
configure
  context context_name
    tac-profile tac_profile_name
      tac range X to Y
      tac value
```

注：

- **tac-profile** *tac_profile*：トラッキング エリア コード プロファイルの APN を設定します。*tac_profile* は、0 ～ 65535 までの任意の範囲または個別の整数値です。
- CLI コマンド 1 回あたりにサポートされる個別の TAC 値の数は 16 です。

TAC プロファイルと APN の関連付け

TAC プロファイルを APN に関連付けるには、次の設定を使用します。

```
configure
  context context_name
    apn apn_name
     virtual-apn preference preference apn apn_name tac-profile tac_profile

      end
```

トラッキング エリア コード プロファイルの設定の確認

次の CLI コマンドを使用して、機能が有効になっているかどうか、およびトラッキング エリア コード プロファイルの範囲が設定されているかどうかを確認します。

- **show configuration apn** *apn_name*
- **show apn name** *apn_name*
- **show rule definition** *tac_profile*

ルーティング エリア コード プロファイルの設定

21.25以降のリリースから、ルーティングエリアコードプロファイルはコントロールプレーンノードで設定できます。この機能を使用することで、範囲ではなく、RAC プロファイルの個別の値に基づいて APN を選択できるようになりました。

次の CLI コマンドを使用して、個別の値を指定してルーティング エリア コード プロファイルを設定します。

```
configure
  context context_name
    rac-profile rac_profile_name
      rac range X to Y
      rac value
```

注：

- **routing-area-code-profile** *rac_profile*：ルーティング エリア コード プロファイルの APN を設定します。 *rac_profile* は、0 ～ 255 の任意の範囲または個別の整数値です。
- 最大 16 個の RAC プロファイル値を設定できます。

RAC プロファイルと APN の関連付け

TAC プロファイルを APN に関連付けるには、次の設定を使用します。

```
configure
  context context_name
    apn apn_name
      virtual-apn preference preference apn apn_name
```

```
routing-area-code-profile rac_profile
        end
```

ルーティング エリア コード プロファイルの設定の確認

次の CLI コマンドを使用して、機能が有効になっているか、およびルーティング エリア コード プロファイルの範囲が設定されているかを確認します。

- **show configuration apn** *apn_name*
- **show apn name** *apn_name*
- **show rule definition** *rac_profile*

第 94 章

ユーザープレーンノードの停止手順

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

ユーザープレーンノードの停止手順は、メンテナンス操作のために特定のユーザープレーン（UP）ノードを停止する手順を示すメンテナンス操作手順（MoP）です。この手順の目的は、新たに受信するセッションに対するノードの選択が行われる際に、コントロールプレーン（CP）ノードで特定の UP ノードを無効にすることです。

この機能により、次のような機能が提供されます。

- 特定の UP を新しいセッションで使用不可としてマークする設定
- アイドル状態のサブスクライバを削除するオプション

前提条件

メンテナンス操作のために UP ノードを停止するにあたっての前提条件は、次のとおりです。

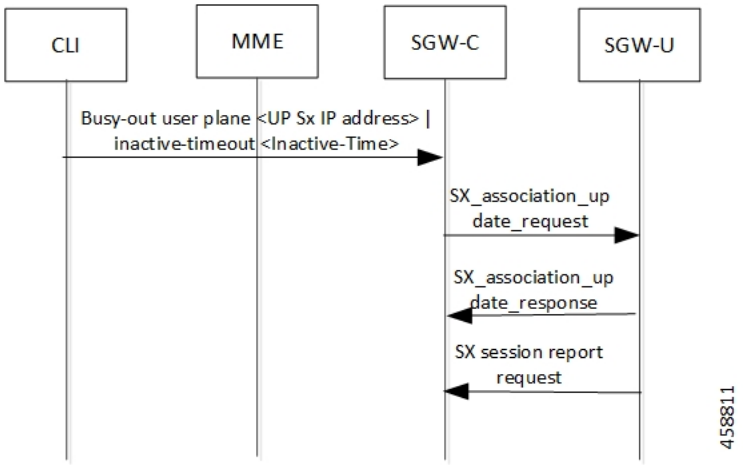
- UP ノードと CP ノードが相互に関連付けられ、コールが特定の UP に到達する必要がある。
- メンテナンスのために特定の UP ノードを無効にし、新たに着信するコールに対して選択されないようにし、その UP ノード上でアイドル状態にある既存のユーザーをクリアしようとしている。
- コールの損失を回避するため、同じ CP グループ内に別の UP ノードがプロビジョニングされている。グループ内に UP が 1 つだけあり、メンテナンスのためにこの UP を無効にした場合、CP は「user-plane-info-not-available」という接続解除理由で新しい着信セッションを拒否する。

機能の仕組み

通話フロー

UP がビジーアウトとマークされた場合の UP の選択

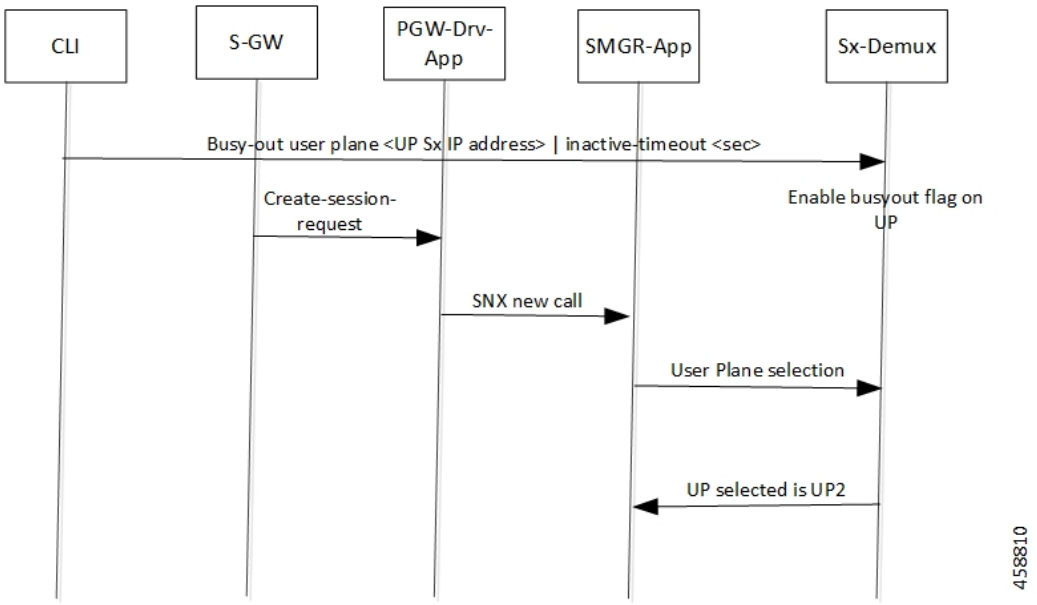
次のコールフローでは、一部の UP が CLI コマンドによって「ビジーアウト」とマークされている場合の Pure-P コールと Collapse コールの UP 選択について説明します。同様に、Pure-S コールの UP 選択も行われます。



手順	説明
1.	ユーザーは、特定の UP を「ビジーアウト」にするために、CP からビジーアウト設定を行います。非アクティブ時間の値は、この設定ではオプションになります。
2.	UP の関連付けの状態は「B」と表示されます。非アクティブ時間値が設定されている場合、「ビジーアウト」の非アクティブ時間値とともに関連付け更新要求メッセージがユーザープレーンに送信されます。

ビジーアウトによる非アクティブタイムアウトに基づく UP でのアイドル状態のサブスクライバのクリア

次のコールフローは、「busy-out」CLI で inactive-time が設定されている場合に、非アクティブセッション（Pure-S コール）が UP でどのようにクリアされるかを示しています。他のコールタイプも同様に機能します。



前のコールフローの続きとして、このコールフローでは、ビジーアウトの非アクティブタイムアウトに基づくアイドルサブスクライバのクリアについて説明します。

ステップ	説明
1.	非アクティブ時間の値に相当する期間アイドル状態が続くと、コールはクリアされます。同じCLIコマンドの「no」形式を設定することで、関連付けられた状態にUPを戻すことができます。

制限事項と考慮事項

この機能には次の既知の制限事項があります。

- 同じ UE のマルチ PDN コールは、異なる UP に分かれる可能性があります。
- 「busy-out」設定は、すべてのアクティブ CP とスタンバイ CP で行われます。
- 現在、新しい IP プールは指定された UP やそれが属する UP グループに追加されていないため、一部の IP チャンクがこの UP に割り当てられず、キャパシティが失われます。
- すべての CP は、「busy-out」に対して同じ設定である必要があります。そうでない場合、UP はいずれかの CP からトリガーされた最新の設定値を使用します。同様に、いずれかの CP で「no busy-out」を実行すると、「busy-out」から UP が起動します。
- UP を完全にブロックするには、2 つの個別の CLI を使用して、IPv4 アドレスと IPv6 アドレスの両方を「busy-out」にします。
- 現在、大量のコールに対してアイドルタイムアウトがトリガーされると、CPU使用率が急増します。すべてのコールがクリアされると、最終的に CPU 使用率は低下します。

UP ノードの停止手順の設定

MOP は、CP と UP のソフトウェアバージョンが同じで、次の「ビジーアウト」CLI のサポートが利用可能な場合にのみ適用されます。

```
configure
  busy-out user-plane { ipv4-address ipv4_address | ipv6-address ipv6_address
} [ inactive-timeout inactive_time ]
  end
```

CP の設定を有効にして、新しいセッションで UP を使用できないようにし、「inactive-timeout」で設定された時間を経過したアイドルセッションをクリアする必要があります。*ipv4_address*/*ipv6_address* は、UP の IPv4 または IPv6 アドレスです。「Inactive-Time」は秒単位で設定されます。

inactive-timeout を設定しない場合、アイドルセッションの動作は変更されません。

注：

- 既存の **clear subscribers saegw-only uplane-address** *ip_address* **no-select-up** CLI コマンドは、セッションリカバリのシナリオに適合しない EXEC レベルの CLI であるため、「ビジーアウト」ロジックのために拡張または再利用されません。また、この CLI を使用して UP を再関連付けせずに、UP の選択ロジックをロールバックする他の方法はありません。

（注） **clear subscribers** コマンドが UP で実行されると、CP には通知されず、セッションは実行中であると見なされます。

- 「busy-out」CLI コマンドを実行すると、当該 UP が UP の選択から削除されます。既存のコールは引き続き通常どおり機能します。割り当てられた IP プールチャンクに対して追加の操作は実行されません。
- アップグレード後に新しいコールを処理するために同じ UP を使用する場合は、**no busy-out user-plane** { **ipv4-address** *ipv4_address* | **ipv6-address** *ipv6_address* } CLI コマンドを実行して、設定を元に戻す必要があります。
- 「busy-out」CLI で UP に対して「inactive-timeout」が設定された後、同じ IP プールを共有する他の UP が、割り当てられたチャンクのしきい値の約 70% に達すると、コールがクリアされ、この UP に割り当てられたプールチャンクの一部が再利用されます。

モニタリングおよびトラブルシューティング

次の CLI コマンドは、この機能をサポートするために使用できます。

コマンドと出力の表示

show sx peers

この CLI コマンドの出力範囲が拡張され、次の新しい関連付けの状態が追加されました。

- Busy-Out：特定の UP が「ビジーアウト」操作中であり、新しいコールには使用できないことを示します。

show sx peers wide

この CLI コマンドの出力範囲が拡張され、次の新しいフィールドが追加されました。

- Last Busy-Out Time：UP が最後に「ビジーアウト」状態であった時刻を示します。
- Last Busy-Out Clear Time：UP の「ビジーアウト」状態が最後にクリアされた時刻を示します。

show sx peers CLI コマンドの出力例を以下に示します。

```
+---Node Type:    (C) - CPLANE       (U) - UPLANE

|

|+--Peer Mode:    (A) - Active       (S) - Standby

|

||+-Association   (i) - Idle         (I) - Initiated

||| State:        (A) - Associated   (R) - Releasing

|||               (X) - Released     (B) - Busy Out

|||
```

```
|||+Configuration (C) - Configured   (N) - Not Configured    (X) - Not Applicable

||||State:

||||

||||+IP Pool:     (E) -  Enable      (D) - Disable           (N) - Not Applicable

|||||

|||||

|||||

|||||  Sx Service
      No of
|||||  ID
     Restart
|||||  |                                                                    Recovery
        |    Current    Max       Peer
vvvvv  v       Group Name               Node ID                Peer ID       Timestamp
        v   Sessions  Sessions    State  LCI  OCI
----- ---- -------------------- ------------------------------ -----------
------------------- ---- --------- --------- -------- ---- ----
UABCE 20   default             209.165.200.225                   33554433
2021-04-14:01:25:32 0    0         1         NONE       X   X

Total Peers:    1

[local]qvpc-si# show sx peers wide

+---Node Type:    (C) - CPLANE       (U) - UPLANE

|

|+--Peer Mode:    (A) - Active       (S) - Standby

|

||+-Association   (i) - Idle         (I) - Initiated

||| State:        (A) - Associated   (R) - Releasing

|||               (X) - Released     (B) - Busy Out

|||

|||+Configuration (C) - Configured   (N) - Not Configured  (X) - Not Applicable

||||State:

||||

||||+IP Pool:     (E) -  Enable      (D) - Disable         (N) - Not Applicable

|||||

|||||+Push Config Status: (C) - Push Complete (P) - Push in Progress (X) - Not Applicable

||||||                    (E) - Push Error

||||||
```

```
||||||+Monitor State:    (U) - UP   (D) - DOWN  (N) - Not Applicable

|||||||

|||||||  ID
       Restart
|||||||  |                                                                                  Recovery
         |    Current    Max   Peer     Config    Auto-Config Config Push         Config
 Push                    Last Busy-Out       Last Busy-Out
vvvvvvv  v       Group Name               Node ID                Peer ID       Timestamp
         v   Sessions  Session State    Failures  Success     Start Time          End
Time             LCI OCI   Time                Clear Time
------ ---- -------------------- ------------------------------ ----------
------------------- ---- --------- -------- -------  -------  ---------
------------------- ------------------- ---- ----  ------------------  --------------------
UAACECN 20   UP-Grp-1             209.165.200.225                   33554435
2021-05-10:12:41:03 0    1         1         NONE     0        0
2021-05-10:12:41:21 2021-05-10:12:41:22   X   X   2021-05-10:12:42:50  2021-05-10:12:43:09

Total Peers:    1
```

show sx peers wide

第 95 章

CUPS の仮想 APN

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
プリファレンスに基づく仮想 APN 選択のサポートを追加。	21.24.1
最初の導入。	21.24 より前

機能説明

アクセスポイント名（APN）は、外部パケットデータネットワークやサブスクライバが利用する特定接続サービスを指す論理名です。

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とともに P-GW によって評価されます。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 でのセッションを全面的に制御します。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

特定の APN で受信されたコールは、特定の基準に基づいて、仮想 APN を介して別の APN にリダイレクトできます。

セッション作成要求で受信された APN は Gn APN と呼ばれ、仮想 APN 選択の一部として選択された APN は Gi APN と呼ばれます。

現在、GGSN、P-GW、SAEGW 非 CUPS 製品は、次のモードをベースとした仮想 APN の選択をサポートしています。

- ローカル設定ベース
- Gx ベース
- RADIUS ベース
- ロケーションベース（GGSN コール用）

CUPS モードで展開された P-GW/SAEGW は、ネットワーク展開で使用する同様の機能もサポートしています。

機能の仕組み

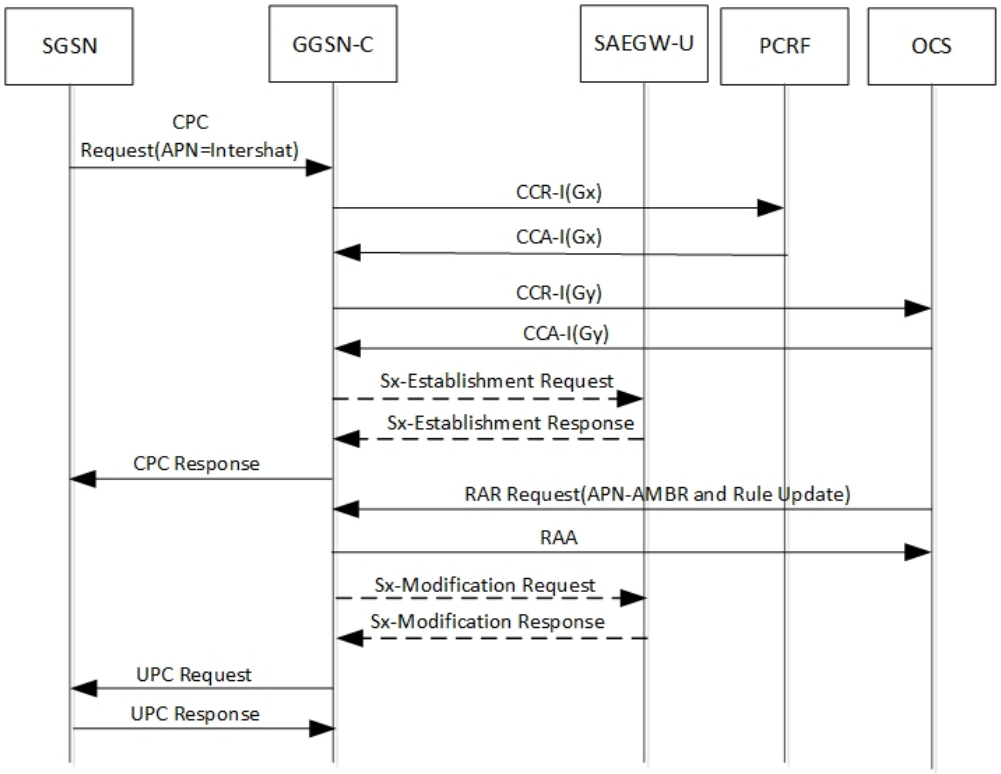
仮想 APN 機能は、CUPS アーキテクチャベースの P-GW/SAEGW ノードとの上位互換としてサポートされます。この機能は段階的にサポートされているため、次の方法を使用して CUPS ベースのゲートウェイノードの仮想 APN を選択できます。

- ローカル設定ベース
- Gx ベース
- ロケーションベース（GGSN コール用）

通話フロー

次のコールフローは、VAPN の選択のさまざまな手順を示しています。

図 *50 : VAPN* の選択



新しいコールが発生した場合は、次の手順が実行されます。

表 *53 : VAPN* の選択コールフロー

手順	説明
1.	新しいセッション作成要求（または PDP コンテキスト作成要求）から、roaming-mode、bearer-access、serv-gw-plmnid、pdp-type を他の必要なすべての基準とともに抽出します。
2 に送信します。	このコールを処理しているサービス名を抽出します。
3.	コールを送信しているピアアドレスを抽出します。
4.	すべてのパラメータを仮想APN選択コードまたはアルゴリズムに渡します。
5.	複数の仮想 APN を選択するか、GnAPN を続行する必要があります。

制限事項

この機能の既知の制限事項と制約事項は次のとおりです。

- 同じオプションが同じルールで複数回指定されている場合、後のオプション値が選択対象と見なされます。
- 新しい設定で仮想 APN 選択のために複数のオプションを指定すると、この機能がサポートされていない古い StarOS ビルドには設定を適用できません。したがって、古いビルド用に（複数のオプションを選択せずに）古い設定のコピーを別に保持する必要があります。
- 仮想 APN ルールの変更操作はサポートされていません。変更操作を実行するには、既存のルールを削除し、新しいルールを追加する必要があります。
- すべての APN で最大 2048 個の仮想 APN ルールを追加できます。

CUPS での仮想 APN の設定

重要 非 CUPS 仮想 APN 機能で使用可能な CLI コマンドは、CUPS 環境に適用できます。

次に設定例を示します。

1. **コントロールプレーンノード**：

```
configure
  context context_name
    apn apn_name
      pdp-type ip_address
      bearer-control-mode mixed
      selection-mode sent-by-ms
      ims-auth-service service_name
        exit
      ip access-group acl_group_name in
      ip access-group acl_group_name out
      authentication pap preference chap preference allow-noauth
      ip context-name context_name
      virtual-apn preference preference apn apn_name
      bearer-access-service  service_name
      cc-profile  cc_profile_index
      [ pdp-type { ipv4 | ipv6 | ipv4v6 } ]
      [ roaming-mode { home | roaming | visiting } ]
      [ serv-gw-plmnid mccmcc_number mnc mnc_number ]
      end
```

（注） **bearer-access-service** *service_name*：ベアラーアクセスサービス（GGSN/P-GW/Other）名を指定します。このサービス名は、コンテキスト全体で一意です。*service_name* は、1 ～ 63 文字の英数字文字列で指定する必要があります。

cc-profile *cc_profile_index*：課金特性（CC）プロファイルインデックスを指定します。*cc_profile_index* は 1 ～ 15 の整数で指定する必要があります。

[pdp-type { ipv4 | ipv6 | ipv4v6 }]：pdp-type ルールを設定します。利用可能なオプションは下記の通りです。

- **ipv4**：IPv4 の VAPN ルールを設定します。
- **ipv4v6**：IPv4v6 の VAPN ルールを設定します。
- **ipv6**：IPv6 の VAPN ルールを設定します。

[roaming-mode { home | roaming | visiting }]：ローミング、訪問、およびホームサブスクライバに対して個別の PDP コンテキストまたは PDN 接続処理をサポートします。

serv-gw-plmnid：Serving Gateway の PLMN ID を指定します。

```
configure
  context context_name
    apn apn_name
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode sent-by-ms
      ims-auth-service service_name
        exit
      ip access-group acl_group_name in
      ip access-group acl_group_name out
      authentication pap preference chap preference allow-noauth
      ip context-name context_name
      end
```

- **Gx ベースの仮想 APN の選択の場合**：

```
configure
  context context_name
    ims-auth-service service_name
      policy-control
      diameter encode-supported-features virtual-apn
      end
```

- **GGSN コールのロケーションベースの仮想 APN 選択の場合**：

```
configure
  context context_name
    apn apn_name
      virtual-apn preference priority apn vapn_name
```

```
routing-area-code-range from start_value to end_value
        end
```

2. ユーザープレーンノード：

```
configure
  context context_name
    apn apn_name
      ip context-name context_name
      end
```

```
configure
  context context_name
    apn apn_name
      ip context-name context_name
      end
```

第 96 章

CUPS での VoLTE のサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

VoLTE は、UPC CUPS アーキテクチャの P-GW（Pure-P）および SAE-GW（Collapsed）コールでサポートされるようになりました。

このリリースでは、VoLTE の次の機能がサポートされます。

- VoLTE の SRVCC/CSFB のサポート
- サポートの一時停止通知手順
- サポートの再開通知手順
- P-CSCF アドレスの選択
- P-CSCF の復元
- AF-Charging-ID のサポート

- インテリジェントなグレースフルシャットダウンのサポート
- IMS PDN の PDN 再アクティブ化のサポート
- 非標準 QCI のサポート

関係

この機能は、「*VoLTE* コールの優先順位リカバリのサポート」に関連しています。

機能の仕組み

CUPS における VoLTE の機能は、このリリースでは最低限の水準で実装されています。

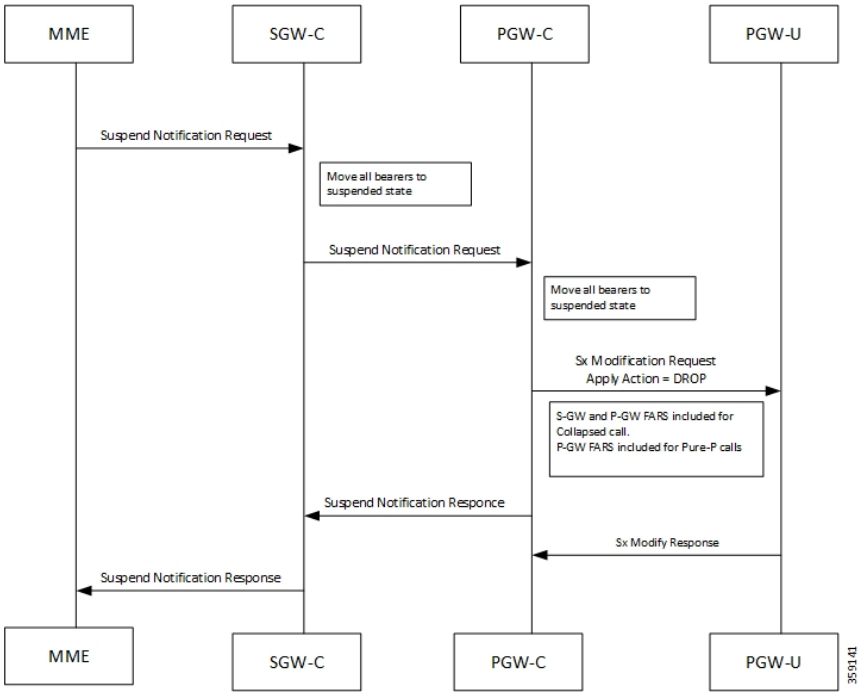
- Pure-P コールと Collapsed コールの一時停止通知
- Pure-P コールと Collapsed コールの再開通知

コールフロー VoLTE のサポート

次の項では、VoLTE 機能をサポートするコールフローについて説明します。

一時停止通知の処理

次のコールフローは、Pure-P コールと Collapsed コールの一時停止通知を示しています。



PGW-Cは、一時停止通知メッセージを受信すると、対応するPFCPセッションのFARのApply Action IEにDROPフラグを設定して、一時停止されたPDN接続で受信したパケットを破棄するようにPGW-Uに要求します。

一時停止通知の一部として、アップリンクおよびダウンリンクデータに対して次のアクションが送信されます。

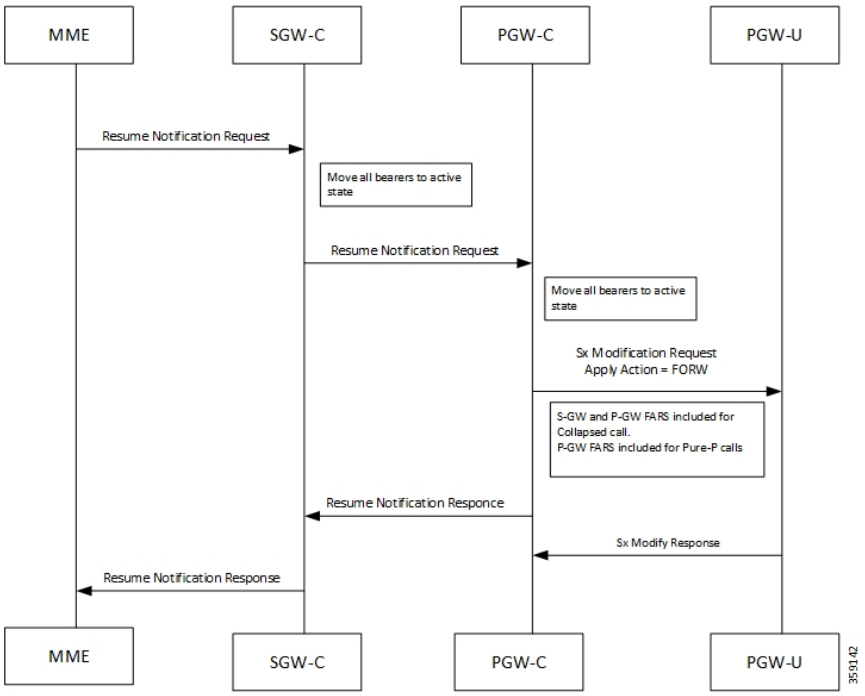
- S-GW アップリンク FARS：転送アクション
- S-GW ダウンリンク FARS：ドロップアクション
- P-GW アップリンク FARS：ドロップアクション
- P-GW ダウンリンク FARS：ドロップアクション

次の条件も導入されます。

- SGW が中断状態で ULI/RAT/TZ レポート MBR を受信すると、すべてのベアラーがアクティブ状態に移行し、MBR が PGW に転送されます。
- PGW が中断状態で ULI/RAT/TZ レポート MBR を受信すると、すべてのベアラーがアクティブ状態に移行します。
- 一時停止通知を受信中、セッションのアイドルタイムアウトは停止します。PGW が中断状態で空の MBR を受信すると、すべてのベアラーがアクティブ状態に移行します。

再開通知の処理

次のコールフローは、Pure-P コールと Collapsed コールの再開通知を示しています。



PDN 接続の再開要求を受信すると、次の手順を実行することで、PGW-C は PGW-U が PDN 接続のパケットを転送することを再度許可します。

- 対応する PFCP セッションの FAR の Apply Action IE で FORW フラグを設定する。
- QER のゲートステータス IE のゲートフィールドの値を OPEN に設定する。

再開通知の一部として、アップリンクおよびダウンリンクデータに対して次のアクションが送信されます。

- P-GW アップリンク FARS：転送アクション
- P-GW ダウンリンク FARS：転送アクション
- S-GW アップリンク FARS：転送アクション
- S-GW ダウンリンク FARS：転送アクション

（注） 再開通知を受信すると、セッションのアイドルタイムアウトが再開されます。

制限事項

CUPS における VoLTE のサポートには、次の制限事項があります。

- VoLTE コールの識別のサポート
- VoLTE のセッションリカバリの機能拡張
- VoLTE 統計
- マルチメディア優先サービスのサポート

第 97 章

Gx を介したボリュームレポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
CUPS で、3G のトリガーベースの使用状況レポートをサポート。	21.25
初版	21.24 より前

機能説明

Volume Reporting over Gx（VoGx）機能により、PCRF はサブスクライバのデータ使用量に基づいてリアルタイムの決定ができます。

この機能は、コントロールプレーンの既存の非 CUPS アーキテクチャを使用して実装されます。実装は、既存の VoGx フレームワークと FAR、PDR、URR などの CUPS データ構造をマッピングすることで行われます。

重要 Volume Reporting over Gx は、ボリュームクォータにのみ適用されます。

機能の仕組み

次の手順を通じて、Gx を介したボリュームレポートの仕組みについて説明します。

1. PCEF は、PCRF からメッセージを受信した後、使用状況モニタリング関連の AVP を解析し、その情報を IMSA に送信します。
2. IMSA はこの情報で ECS を更新します。
3. PCRF からの使用状況モニタリング情報で ECS が更新されると、PCEF（ECS）はデータ使用状況の追跡を開始します。
4. セッションレベルのモニタリングの場合、ECS がデータ使用状況を保持します。
5. PCC ルールモニタリングの場合、モニタリングキーを一意の識別子として使用状況がモニタリングされます。各ノードがモニタリングキーごとの使用状況情報を保持します。データトラフィックが通過すると、使用状況がチェックされ、使用状況のしきい値に照らしてレポートされます。

（注） 21.22 より前のリリースでは、モニタリングキー値の範囲は 0 ～ 134217727 でした。

21.22 以降のリリースでは、モニタリングキー値の範囲は 1 ～ 4000000000 となります。

6. PCEF は、しきい値に達した後、PCRF によって新しいしきい値が提供されるまで、データ使用状況を追跡し続けます。使用状況が報告された IP-CAN セッション変更の確認応答で、PCRF から新しい使用状況しきい値が提供されない場合、その IP CAN セッションを対象とした PCEF での使用状況モニタリングは続行されません。

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

サポートされる規格

Gx を介したボリュームレポート機能は、次の標準規格に基づいています。3GPP TS 29.212 V9.5.0 (2010-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 9)

VoGx のコントロールプレーンの処理

セッションセットアップ中の URR の作成

- Sx セッション確立要求は、GxSPI フレームワークに従って使用されます。
- コントロールプレーン機能は、Sx セッション確立要求で URR のリストと、対応する PDR での参照先を送信します。

接続解除要求における URR 処理

- URR 情報は、Sx セッション削除応答の一部として PGW-U によって送信されます。
- PGW-C は、これらの URR を対応するモニタリングキーバケットにマッピングし、使用状況レポートを含む CCR-T を送信します。

Sx セッションレポート要求

PGW-U は、ボリュームしきい値に対する使用状況レポートを送信します。PGW-C は対応するモニタリングキーバケットに URR をマッピングし、それに応じて Gx CCR-U を生成します。

使用状況モニタリング関連の AVP を使用した RAR の処理

Gx エイリアスルールに関連付けられたモニタリングキーを含む使用状況モニタリング情報が、ルールが関連付けられていない RAR で受信されると、使用状況モニタリング情報（ボリュームまたは時間）を含む Create URR IE が UP に送信されます。

VoGx のユーザープレーンの処理

ボリュームのしきい値違反

データパケットが特定の PDR と一致し、その PDR に関連付けられている URR の測定方法がボリュームに設定されている場合、アップリンクおよびダウンリンクの使用状況カウンタは、PDR 送信元インターフェイスのタイプに応じて増分されます。特定の URR のボリュームしきい値を超えると、Sx セッションレポート要求メッセージが生成され、使用状況レポートのトリガーがボリュームしきい値に設定されて送信されます。報告された URR のすべての使用状況カウンタは、メッセージが生成されてコントロールプレーンに送信されるとクリアされます。ただし、既存のしきい値制限は、以降のトランザクションに適用されます。

制限事項

VoGx 機能には、次の制限事項があります。

- 次のイベントトリガー中の PCRF への使用状況のレポートは、CUPS ではサポートされません。
  - トリガー
    - PGW_TRACE_CONTROL (24)
    - QOS_CHANGE_EXCEEDING_AUTHORIZATION (11)
    - APN_AMBR_MODIFICATION_FAILURE (29)
    - CHARGING_CORRELATION_EXCHANGE (28)
    - OUT_OF_CREDIT (15)
    - REALLOCATION_OF_CREDIT (16)

- UE_IP_ADDRESS_ALLOCATE (18)
- UE_IP_ADDRESS_RELEASE (19)
- APPLICATION_START (39)
- APPLICATION_STOP (40)
- REVALIDATION_TIMEOUT (17)

- トリガーベースの使用状況レポートは、CUPS の 3G ではサポートされません。

VoGx モニタリングキー範囲の設定

リリース 21.22 以降では、静的ルールおよび事前定義ルールの一部として、PCEF でローカルに設定されたすべてのモニタリングキーの **monitoring-key urr-id-prefix** エントリを定義する必要があります。

モニタリングキーの範囲を有効にするには、次の設定を使用します。

```
configure
  active-charging service service_name
    mon-key-urr-list list_name
      monitoring-key value urr-id-prefix urr_id
      end
```

注：

- **mon-key-urr-list** *list_name*：モニタリングキーリスト名を指定します。*list_name* は、1 ～ 63 文字の文字列である必要があります。
- **monitoring-key** *value*：*value* は 1 ～ 4000000000 までの整数である必要があります。
- **urr-id-prefix** *urr_id*：*urr_id* は 1 ～ 8388607 までの整数である必要があります。
- リスト名には、モニタリングキーと URR ID の複数の組み合わせを設定できます。推奨されるエントリ数の上限は 2500 です。
- この CLI コマンドは、コントロールプレーンとユーザープレーンの両方で設定できます。コントロールプレーンでこの CLI コマンドを設定した後、PFD プッシュメカニズムを使用して設定をユーザープレーンにプッシュする必要があります。RCM の場合、CLI を設定する前にユーザープレーンで **require rcm-configmgr** を設定しておく必要があります。RCM 設定の CLI を使用して、コントロールプレーンとユーザープレーンの両方を設定する必要があります。
- 設定するモニタリングキーと URR-ID の組み合わせは、すべて一意である必要があります。**mon-key-urr-list** で設定された URR-ID が、**urr-list** で設定された URR-ID と一致していけません。このような設定を試みた場合、CLI はエラーをスローします。
- コントロールプレーンでランタイムにこの CLI が追加された場合、PFD プッシュメカニズムを使用して CLI をプッシュし、UP と CP の両方で設定を更新できるようにする必要が

あります。これらの設定は、次回のコール以降、または次の URR の作成時に適用されます。

VoGx のモニタリングと障害対応

ここでは、CUPS の VoGx のモニタリングと障害対応で使用できる CLI コマンドについて説明します。

show コマンドと出力

show active-charging subsystem all debug-only

この CLI コマンドの出力範囲が拡張され、CUPS の VoGx 機能をサポートする次のフィールドが追加されました。

- Total Mon-Key Urr Entries in list
- Total Mon-Key lookup success
- Total Mon-Key lookup failure

show user-plane-service monitoring-key-urr-id-list all

この CLI コマンドを使用すると、コントロールプレーンからユーザープレーンにプッシュされたすべてのモニタリングキーが表示されます。

第 98 章

VPN マネージャリカバリのサポート

機能の概要と変更履歴

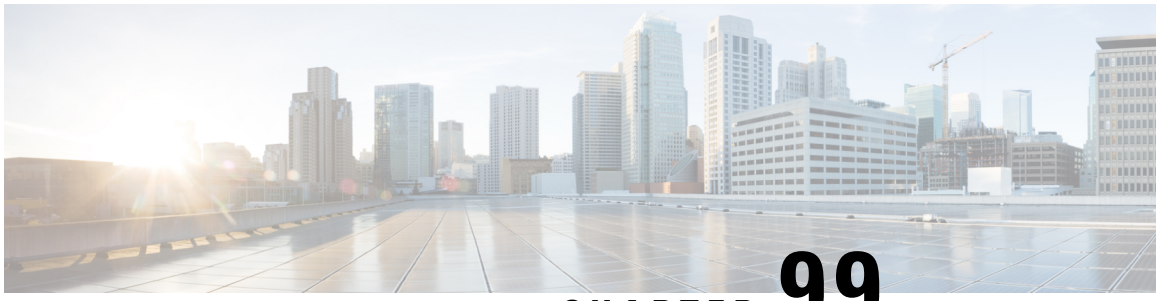
（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

VPN マネージャリカバリサポート機能では、VPN マネージャ（vpnmgr）のクラッシュ後にチャンクを回復できます。クラッシュ後にチャンクを回復するために、チャンクが保存され、ローカル VPN マネージャの特定の VPN マネージャに割り当てられます。

プールの VPN マネージャがクラッシュすると、ローカル VPN マネージャからチャンクを回復し、すべてのセッションマネージャから使用されているすべての IP を回復します。



CHAPTER 99

VPP のサポート

Vector Packet Processing（VPPMOB）は、オープンソース ソリューションである fd.io の VPP に基づくモビリティ中心のソリューションです。特に IP 転送、回送、およびプロトコルの分野で fd.io の開発を活用しています。

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
このリリースでは、CUPS のフローごとの Fast Path 情報に対する VPP ctrl のサポートを追加。	21.27.x
このリリースでは、DNS アドレス再指定先サーバーリストのサポートを追加。	21.25.4
初版	21.24 より前

課金サポート

使用状況レポートは、コールの削除またはボリュームや時間のしきい値違反が発生すると、課金サーバーに通知されます。

ストリームがユーザープレーンで作成されると、課金を含むフローは、ストリーム作成中に設定された課金固有の操作に関連付けられます。オフロードと非オフロードの両方に関するすべてのフローの課金カウンタは、高速パスで維持されます。

ボリュームしきい値のオーバーフロー時に、高速パスはバケットカウンタを含む通知を送信し（PUSH モード）、時間しきい値に達した場合、アプリケーションは高速パスから課金カウンタを読み取ります（PULL モード）。ユーザープレーンは、これらのカウンタをそれぞれの URR で集約し、Sx インターフェイスを介して使用状況レポートをトリガーします。

重要 このリリースでは、ボリュームと時間しきい値の両方で URR がサポートされています。複数の SDF と 1 つのベアラーレベル URR がサポートされています。

ルールベースによる遅延課金

サポートされる delay-charging のフレーバーは次のとおりです。

- Charge-to-application all-packets：フローのすべての制御パケット（ハンドシェイク、セッション中、およびティアダウン）が、アプリケーションパケットに一致する charging-action に基づいて課金されます。

- Charge-to-application initial-packets：フローのハンドシェイクパケットが、アプリケーションパケットに一致する charging-action に基づいて課金されます。
- Charge-to-application tear-down-packets：フローのティアダウンパケットが、アプリケーションパケットに一致する charging-action に基づいて課金されます。
- Charge-separate-from-application：すべての制御パケットのルール照合を行い、最も優先順位の高いルールに基づいて課金されます。

上記のすべてのシナリオで、遅延するのは課金のみですが、ルール照合はパケットの内容を対象に行われます。

重要

- [Charge-separate-from-application mid session packets] はサポートされません。オフロードされたフローは、引き続き最後に一致したルールに一致します。

遅延課金機能を有効にすると、TCP ハンドシェイクパケットは到着時にルールにヒットします。TCP ハンドシェイクパケットは、設定に基づく IP または TCP ルールにヒットします。**show active-charge** CLI コマンドを実行すると、TCP ハンドシェイクパケットがまだデフォルトルールにヒットしていることがわかります。最初の L7 パケットが到着するまでは、このルールによる課金は考慮されません。最初の L7 パケットが L7 ルールにヒットすると、クォータ要求の送信時に、L7 パケットと TCP ハンドシェイクパケットが同じ L7 RG に加えられます。

フローのアイドルタイムアウト

設定可能な idle-time out がサポートされ、最大値は 24 時間です。以前のリリースでは、一部の特定の値に対してのみ使用がサポートされていました。

HTTP のサポート

このリリースでは、HTTP トラフィックの分析と、このような HTTP ベースルールのポリシー照合がサポートされています。HTTP フローのオフロードは、WebSocket、CONNECT メソッド、または要求/応答内にコンテンツが存在する場合にのみサポートされます。

IP 再アドレス指定

このリリースでは、IPv4 および IPv6 の IP 再アドレス指定がサポートされています。

IP 再アドレス指定は、課金アクションに関連付けられた課金ルールまたは後処理ルールを使用して設定できます。

ストリームは、IP再アドレス指定動作セットとともにそれらのルールに一致するフローの高速パスで作成されます。一致するすべてのフロー（オフロードと非オフロードの両方）の高速パスに IPv4/IPv6 アドレスが設定されます。

DNS アドレス再指定先サーバーリスト

許可されていない DNS サーバーを使用すると必ず、要求が変更され、DNS IP アドレスを再指定し、許可されたサーバーを使用するように求められます。**Ruledef** によって、パケットが DNS クエリに属しているかどうか、および DNS クエリが一連の許可された DNS サーバーに属しているかどうかを判別します。DNS クエリが許可された DNS サーバーに属していない場合、フローアクションが **readdress-server-list** から DNS サーバーを取得することになります。

readdress-server-list はアクティブ課金サーバーで設定されます。フローが **ruledef** に一致する場合に **readdress-server-list** のサーバーを使用するようにフローアクションを設定できます。

readdress-server-list で **active-charging service** を次のように設定します。

```
configure
  active-charging service service_name
    readdress-server-list name_of_list
      server ipv4_address [ port ]
      server ipv6_address [ port ]
```

（注） **readdress-server-list** には最大 10 のサーバーを設定でき、[active-charging service] には最大 10 の **readdress-server-lists** を設定できます。同じ **readdress-server-list** 内に、IPv4 アドレスと IPv6 アドレスの両方を設定できます。

次の 2 つの方法のいずれかを使用して、リストから **readdress-server-list** を選択します。

- ラウンドロビン：新しいフローごとにラウンドロビン方式でサーバーが選択されます。選択時に、リスト内の非アクティブサーバーは考慮されません。
- 階層型：このアプローチでは、サーバーは **readdress-server-list** で定義されている順序に応じて、プライマリ、セカンダリ、ターシャリというようにタグ付けされます。すべてのフローのアドレス再指定先は、プライマリサーバーが使用可能である限り、プライマリサーバーです。プライマリサーバーがダウンした場合は、フローのアドレス再指定先はセカンダリサーバーとなり、その後も同じロジックが繰り返されます。プライマリサーバーが再びアクティブになると、フローのアドレス再指定先はプライマリサーバーに戻ります。

次の CLI コマンドは、サーバー選択のアプローチを定義します。

```
charging-action action_name
  flow action readdress-server-list name_of_list [ hierarchy | round-robin
 ]
```

前述のコードに記載されているCLIコマンドでオプションが指定されていない場合、**round-robin** オプションがデフォルトのオプションと見なされます。

[active-charging service] で次の CLI コマンドを設定します。

```
configure
  active-charging service service_name
    readdress-server-list name_of_list
      server ipv4_address [ port ]
      server ipv6_address [ port ]
      consecutive-failures integer_value
      response-timeout integer_value
      reactivation-time integer_value

      charging-action action_name
        flow action readdress server-list name_of_list
    exit
```

（注） 前述のコードに記載されている CLI コマンドを設定するにあたり、次の値を検討してください。

- **consecutive-failures**：整数値で、1 ～ 10 の範囲で指定する必要があります。デフォルト値は *5* です。
- **response-timeout**：整数値で、1 ～ 10000 ミリ秒の範囲で指定する必要があります。デフォルト値は *1000* です。
- **reactivation-time**：整数値で、1 ～ 1800 秒の範囲で指定する必要があります。デフォルト値は *300* です。

アドレス再指定先サーバーの状態

アドレス再指定先サーバーの状態は、次のとおりです。

- アクティブ状態：一度設定すると、すべてのサーバーが [Active] としてマークされます。
- 非アクティブ状態：アドレス再指定先サーバーからの応答が受信されない場合、サーバーは [Inactive] としてマークされます。
- アクティブ保留状態：サーバーが [Active-Pending] 状態になると、アドレス再指定要求を受け付け可能となります。この状態のサーバー宛てに要求のアドレスが再指定され、応答が返ると、このサーバーの状態は [Active] に変更されます。それ以外の場合は、[Inactive] 状態に戻ります。

LTE ハンドオーバー

次のタイプのハンドオーバーがサポートされています。

- X2 ベースのハンドオーバーの S-GW 再配置（OI は 1 に設定）。
- S1 ベースのハンドオーバーの S-GW 再配置（OI は 0 に設定）。
- eNodeB F-TEIDu の更新。

S-GW 再配置の場合、次の組み合わせがサポートされています。

- P-GW アンカーコール。
- Collapsed コールへの P-GW アンカーコール。
- P-GW アンカーコールへの Collapsed コール。

ネクストホップ

このリリースでは、IPv4 および IPv6 のネクストホップアドレスがサポートされています。

ネクストホップアドレスは、課金アクションに関連付けられた課金ルールまたは後処理ルールを使用して設定できます。

ストリームは、これらのルールに一致するフローの高速パスでネクストホップ動作セットとともに作成されます。一致するすべてのフロー（オフロードと非オフロードの両方）の高速パスにネクストホップアドレスが設定されます。

PDN の更新

PDN 更新手順は、このリリースの VPP でサポートされています。

Gx 手順を介してルールの追加、変更、削除が受信されるたびに、すべてのフローが SM-U にオンロードされます。これらのオンロードされたフロー上のすべてのパケットは、SM-U に送信されます。フローのトランスポート レベル マーキングおよび課金パラメータが変更された場合も、フローはオンロードされます。これらのフローは、ルール一致条件が変更されるか、トランザクション ルール マッチング（TRM）が再び関与するパケットで再びオフロードされます。

ポリシング

ポリサー設定では、セッションマネージャからの入力を使用します。これらの入力は、PCRF から AMBR として、またはフローレベルの QoS 情報から受信されます。セッションレベルの

AMBR ポリシングでは、PCRF から受信した値を常に受け付けます。ただし、フローレベルのポリシングが優先される場合（それが使用可能な場合）、AMBR ポリシングが順番に適用されます。つまり、ポリサーエンジンは階層型ポリシングを適用します。最初にフローレベル/ルールの帯域幅制限が適用され、次にセッションレベルの帯域幅制限が適用されます。

（注） RAR または CCA-U を介したセッション実行時の AMBR の変更が適用されます。

セッションマネージャから受信した入力値は、ポリサー設定およびポリサートークンバケットにプッシュされます。アップリンクまたはダウンリンクの各方向に対し、ポリサー設定とポリサートークンバケット用の新しいレコードが作成されます。

ポリサー設定はポリサーエンジンの参照先であり、ポリサートークンバケットは値の計算と復元に使用されます。

現在、ポリシングは、PCRF から受信した AMBR およびダイナミックルールのルールレベルの QoS 情報でサポートされています。静的ルールおよび事前定義ルールの場合、帯域幅制限は帯域幅ポリシー設定によって実施されます。コントロールプレーンの [Active Charging Service Configuration] モードの帯域幅ポリシー設定で設定された拡張ビットレートは、設定プッシュメカニズムの一部としてユーザープレーンに提供され、ユーザープレーンによるポリシングにも同じものが適用されます。以下に、帯域幅ポリシーの設定例を示します。

```
configure
   active-charging service ACS
      bandwidth-policy BWP

         flow limit-for-bandwidth id 1 group-id 1

         flow limit-for-bandwidth id 2 group-id 2
         group-id 1 direction uplink peak-data-rate 256000 peak-burst-size 32000
violate-action discard
         group-id 1 direction downlink peak-data-rate 256000 peak-burst-size 32000
violate-action discard
         group-id 2 direction uplink peak-data-rate 128000 peak-burst-size 16000
violate-action discard
         group-id 2 direction downlink peak-data-rate 56000 peak-burst-size 7000
violate-action discard
         exit
```

制限事項

このリリースでは、ポリシングに次の制限があります。

- **bandwidth-policy** の変更はサポートさません。
- ITC 帯域幅制限、トークンの補充（APN レベルおよび ACL レベルの両方）などの他の機能とのインタラクションはサポートされません。
- 現在、ポリサーベースの統計はサポートされていません。

（注） 現在、ポリサー統計はサポートされていないため、オペレータはネットワーク パフォーマンス モニタリング ツールを使用して帯域幅制限を確認できます。

Pure-S のサポート

Pure-S デフォルトベアラー VPP 統合が CUPS アーキテクチャでサポートされるようになりました。これまで、CUPS での Pure-S コールは IFTASK を使用することでサポートされていました。今後は、Pure-S コールデータパスも VPP を使用します。

Pure-S コールの VPP 統合の一環として、SAEGW-UP のコールは、1 方向あたり 1 つのベアラーストリーム（3 タプル：GTPU サービス IP アドレス、TEID、VRF ID）をインストールし、1 方向あたり 1 つの TEP 行も作成されます。

サポートされる機能：

Pure-S でサポートされる機能は、次のとおりです。

- MME とネットワーク開始型シナリオ（MBR/CBR/UBR/DBR）間のコリジョンに関するほとんどの手順。
- DBCmd および BRCmd コマンド。
- SAEGW-UP は、[IDLE] から [ACTIVE] に遷移中の IPv4 から IPv6 へ、または IPv6 から IPv4 への IP トランスポートの動作、および S1-u インターフェイスでのハンドオーバー手順をサポートします。接続時に S1-u で選択されたトランスポートもサポートされます。たとえば、IPv4 eNodeB から IPv6 eNodeB への eNode ハンドオーバーなどです。

サービススキーマを介した応答ベースの課金

HTTP リクエストは、HTTP レスポンスの一致した課金アクションに対して課金されます。

サービススキーマを介した応答ベースの TRM

アップリンクストリームのトランザクション ルール マッチング（TRM）は、HTTP レスポンスを受信した後にのみ実行されます。

ToS マーキング

機能説明

このリリースでは、IPv4 および IPv6 の ToS マーキングがサポートされています。

内部 IP ToS マーキングアドレスは、課金アクションに関連付けられた課金ルールまたは後処理ルールを使用して設定できます。外部 IP ToS マーキングは、コントロールプレーンで設定された QCI-DSCP マーキングテーブルを使用して実行されます。

ストリームは、これらのルールに一致するフローの高速パスで動作セットとともに作成されます。一致するすべてのフロー（オフロードと非オフロードの両方）には、高速パスで IPv4/IPv6 ToS マーキングが設定されます。

ボリュームベースのオフロード

HTTP プロトコルの場合、要求/応答のコンテンツ（存在する場合）は、フロー内の各トランザクションの fastpath にオフロードされます。コンテンツの最後のパケットがストリームをパッシブ状態に戻し、パケットがセッションマネージャに到達します。

サポートされる機能

このリリースでは、次のコールフレーバーがサポートされます。

- Pure-P IPv4/IPv6 コール
- Collapsed IPv4/IPv6 コール
- デフォルトベアラー
- Pure-S 機能
- 専用ベアラー
- ハンドオーバー

このリリースでは、次の機能がサポートされます。

- ペイロードパケット（課金アクション）および外部 GTP-U パケット（QCI/QoS マッピングテーブル）の ToS マーキング。
- ネクストホップ機能（IPv4/IPv6）。
- IP アドレス再設定機能（IPv4/IPv6）。
- アクションが [discard] の後処理ルール。
- アクションが [Next hop forwarding (IPv4/IPv6)] の後処理ルール。

- アクションが [ToS marking (UL and DL)] の後処理ルール。
- アクションが [Readdressing (IPv4/IPv6)] の後処理ルール。
- URR 機能（Gz のみ）：SDF 1 つ、ベアラーレベルの URR 1 つ。
- Gz 課金のみがサポートされます。
- VPP でのフラグメンテーションとリアセンブルがサポートされます。
- HTTP トラフィックポリシー照合がサポートされます。HTTP オフロードがサポートされるのは、CONNECT および WebSocket 要求のみです。
- このリリースは、サブスクライバあたり、すべてのアプリケーションを合わせて最大 5000 フローをサポートすることが検証されています。この制限はソフトウェアの性能によるものではありませんが、運用上推奨される制限です。この制限を超えるとアプリケーション障害が発生する可能性があるため、[Rulebase Configuration] モードで次の CLI を設定することを推奨します：**flow limit-across-applications** *5000*

制限事項

次の機能は、このリリースではサポートされていません。

- Gy と Rf は個々にサポートされますが、同じサブスクライバに対して両方を同時に有効にすることはできません。
- Fast Path CLI が以前に有効化されている場合は、無効にできます。ただし、ユーザープレーンをリロードする必要があります。
- **VPP クラッシュログのサポート**：クラッシュレコードとミニコアファイルの生成がサポートされます。VPP の完全なコアファイルの生成はサポートされていません。

ユーザープレーンサービスでの高速パスの有効化

ユーザープレーンサービスで Fast Path（VPP）を有効にするには、次の CLI コマンドを使用します。

```
configure
  context context_name
    user-plane-service service_name
      associate fast-path service
      end
```

注：

- **fast-path**：Fast Path 関連のパラメータを指定します。
- **service**：Fast Path 関連の設定を指定します。

SI プラットフォームでの VPP の有効化

VPP を起動するには、次の手順を実行します。

1. ホストマシンにログオンし、staros_param.cfg ファイルを含む ISO イメージを作成します。
2. FORWARDER_TYPE=vpp という行を含むファイルを作成します。
3. 次のように、staros_param.cfg ファイルを含む ISO ファイルを作成します。

   ```
   genisoimage -l -o ssi_vpp.iso -r vppiso/
   ```

   genisoimage がインストールされていない場合は、次のコマンドを実行します。

   ```
   sudo apt-get install genisoimage
   ```

4. VM が実行されている場合は停止します。

   ```
   virsh destroy <vm_name>
   ```

5. VPP がフォワーダとして識別されていない VM にディスクがすでに接続されている場合は、そのディスクを切り離します。

   VM で **dumpxml** コマンドを実行して、ディスクが接続されているか確認します。

   ディスクを切り離すには、次のコマンドを実行します。

   ```
   virsh detach-disk <vm_name> hdc –config
   ```

6. staros_param.cfg ファイルを含む ISO ファイルを添付します。

   ```
   virsh attach-disk <vm_name> <Path_of_ISO_FILE> hdc –type cdrom –config
   ```

VPP 高速パスのモニタリングと障害対応

フローがオフロードされているか判断するには、次の CLI コマンドの出力で高速パスの統計情報を確認します。

- **show subscribers user-plane-only full all**
- **show user-plane-service all**
- **show user-plane-service statistics analyzer name ip**
- **show user-plane-service statistics analyzer name ipv6**
- **show user-plane-service statistics analyzer name tcp**
- **show user-plane-service statistics analyzer name udp**
- **show user-plane-service statistics analyzer name http**

フローごとの高速パス情報を確認するには、次の CLI コマンドの出力で Fast Path Info フィールドを確認します。

- **show subscribers user-plane-only callid** *call_id* **flows full**

VPP 設定パラメータのオーバーライドのサポート

VPP 設定パラメータの設定については、『*VPC-SI Administration Guide*』[英語] を参照してください。これらのパラメータはオーバーライドできます。オーバーライド値の特定については、シスコのアカウント担当者にお問い合わせください。

第 100 章

CUPS の VRF のサポート

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

CUPS での VRF サポート機能により、IP プールと Virtual Routing and Forwarding（VRF）との関連付けが可能になります。これらの IP プールは、他のプールと同様にチャンクに分割されます。このプールから分割されたチャンクは、これらのプールを使用するように設定されているユーザープレーン（UP）に割り当てられます。既存の展開と同様に、CUPS における VRF に関連付けられたプールのタイプは、[STATIC] または [PRIVATE] のみとなります。

プライベート VRF プールのチャンクは、通常のプライベートプールと同様に UP が登録される際に割り当てられます。静的 VRF プールのチャンクは、通常の静的プールと同様に、そのチャンクでコールが発生した場合にのみ割り当てられます。

（注） UP あたりの VRF の上限は 205 です。

同じ UP 内の重複プール

重複プールは共通の IP 範囲を使用します。重複プールのタイプは、[STATIC] または [PRIVATE] のいずれかです。パブリックプールを重複プールとして設定することはできません。各重複プールは、異なる VRF（回送ドメイン）およびプールグループに属します。また、1 つの APN が使用できるプールグループは 1 つのみであるため、重複プールは異なる APN に属します。

この機能がなければ、重複プールを CP で設定することはできますが、2 つの重複プールのチャンクを同じ UP に送信することはできません。つまり、UP は 2 つの異なる重複プールのチャンクを処理できないということです。したがって、同じ IP 範囲を共有するには、UP と同じ数だけ重複プールが必要になります。

この機能があることで、UP は 2 つの異なる重複プールのチャンクを処理できます。つまり、単一の UP が、同じ IP 範囲を共有する重複プールをいくつでも処理できます。

（注） CUPS では、VRF ベースの重複プールのみがサポートされます。NH ベース、VLAN ベースなど、重複プールの他のフレーバーは、CUPS ではサポートされません。

同じ UP 内の重複プールの機能は次のとおりです。

- 特定のプールのチャンクが UP にインストールされると、対応する vrf-name がチャンクとともに送信されます。
- UP がチャンクの VRF を認識するため、UP は対応する VRF にチャンクをインストールし、チャンクデータベースは VRF の下に入力されます。
- コールの割り当て、解放、リカバリなど VPNMgr へのあらゆる通信には、UP の対応する SessMgr に vrf-id が含まれます。これにより、VPNMgr は、指定された vrf-id でその IP の正しいチャンクを選択して処理できます。

VRF での IP プールの VPNMgr クラッシュ障害の改善

Demux カードを移行する場合、または VPNMgr がダウンした場合、VPNMgr がデータベースを再構築するまで、新しいコールは拒否されます。多数の VRF がある企業向けソリューションの場合、新しいコールの影響は予想よりも大きくなる可能性があります。

CLI 制御機能である遅延 VRF プログラミングは、VPNMgr のリカバリ（再起動およびスイッチオーバー）シナリオ中に IP プール VRF のプログラミングを遅延させることで、新しいコールの影響を軽減するために導入されました。

遅延 VRF プログラミングの設定

次の CLI コマンドを使用して、CP および UP で IP プールが設定されている VRF を使用した VPNMgr の高速リカバリを有効にします。

```
configure
  context context_name
    ip vrf vrf_name
```

```
ip delay-vrf-programming-during-recovery
end
```

注：

- デフォルトでは、 キーワードや機能は無効になっています。
- CLI キーワードは、CP VRF 設定と UP VRF 設定の両方に適用できます。
- 非 IP プール VRF でこの機能を有効にすることは推奨されません。
- IP プール VRF では、TCP 接続やカーネルの相互作用を必要とする他の制御プロトコル（SRP など）が有効になっていないことを前提としています。
- 遅延間隔の間：
  - VRF を回復するためにカーネルの操作が必要な機能は動作しません。サブスクライバデータの障害は想定されていません。
  - ルート/BGP/BFD/インターフェイス/VRF に関連する設定の変更は失敗するため、設定を再適用する必要があります。

CLI 構文の変更

この機能の一部として、**show ip vrf** *vrf_name_string* CLI コマンドの構文が、非 CUPS を含むすべてのプラットフォームで変更されました。

次に、新しい構文を示します。**show ip vrf name** *vrf_name_string*

また、**show ip vrf** *vrf_name_string* の後に指定する既存のすべてのオプションキーワードが **show ip vrf name** *vrf_name_string* に変更されましたが、CLI コマンドの出力に変更はありません。

VRF の設定

CUPS の VRF サポートを実装するには、次の手順を実行します。

コントロールプレーンで実行する手順：

1. IP プールを VRF に関連付けます。
2. このプールを使用する APN を作成します。
3. UP を UP グループに関連付けて、UP が特定の APN のみを使用するようにします。

   重複プールがある場合は、プールごとに個別の APN を作成してください。また、各 APN をそれぞれ異なる UP が使用するようにします。

以下に、CP の設定例を示します。

```
context EPC2
  apn mpls1.com
    pdp-type ipv4 ipv6
    bearer-control-mode mixed
    selection-mode subscribed sent-by-ms chosen-by-sgsn
```

```
      ims-auth-service iasGx
      ip access-group css in
      ip access-group css out
      ip context-name isp
      ip address pool name PRIVATE
      ipv6 address prefix-pool PRIVATEV6
      ipv6 access-group css6 in
      ipv6 access-group css6 out
      cc-profile any prepaid-prohibited
      active-charging rulebase cisco
      user-plane-group mpls1
    exit
    apn mpls2.com
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode subscribed sent-by-ms chosen-by-sgsn
      ims-auth-service iasGx
      ip access-group css in
      ip access-group css out
      ip context-name isp
      ip address pool name PRIVATE_1
      ipv6 address prefix-pool PRIVATEV6_1
      ipv6 access-group css6 in
      ipv6 access-group css6 out
      cc-profile any prepaid-prohibited
      active-charging rulebase cisco
      user-plane-group mpls2
    exit

config
  context isp
    ip vrf mpls-vrf-1
    ip vrf mpls-vrf-2
    #exit

    #exit
    cups enable
   ip pool PRIVATE 209.165.200.225 255.255.255.224 private 0 chunk-size 64 vrf mpls-vrf-1

    ip pool PRIVATE_1 209.165.200.225 255.255.255.224 private 0 chunk-size 64 vrf
mpls-vrf-2
    ip pool STATIC 209.165.200.226 255.255.255.224 static vrf mpls-vrf-1
    ipv6 pool PRIVATEV6 prefix 8001::aaaa/54 private 0 chunk-size 64 vrf mpls-vrf-1
    ipv6 pool PRIVATEV6_1 prefix 8001::aaaa/54 private 0 chunk-size 64 vrf mpls-vrf-2
    ipv6 pool v6pool2 prefix 2a02:2121:2c4::/46 static 0 vrf mpls-vrf-1
exit

  user-plane-group mpls1
    peer-node-id ipv4-address 209.165.200.226
  #exit
  user-plane-group mpls2
    peer-node-id ipv4-address 209.165.200.228
  #exit
```

ユーザープレーンで実行する手順：

CP からチャンクがプッシュされる前に、UP で VRF を設定しておくことを推奨します。設定されていない場合、IP プールトランザクション全体（VRF に属さないチャンクを含む）が失敗し、しばらくしてから CP による再試行が発生します。

以下に、UP の設定例を示します。

ユーザープレーン 1：

```
Config
  context EPC2
    sx-service sx
      instance-type userplane
      bind ipv4-address 209.165.200.226 ipv6-address bbbb:aaaa::4
    exit
    user-plane-service up
      associate gtpu-service pgw-gtpu pgw-ingress
      associate gtpu-service sgw-ingress-gtpu sgw-ingress
      associate gtpu-service sgw-engress-gtpu sgw-egress
      associate gtpu-service saegw-sxu cp-tunnel
      associate sx-service sx
      associate fast-path service
      associate control-plane-group g1
    exit

  context isp
    ip vrf mpls-vrf-1
    #exit
    ip vrf mpls-vrf-2
    #exit
    apn mpls1.com
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode sent-by-ms
      ip context-name isp
    exit
exit
control-plane-group g1
    peer-node-id ipv4-address 209.165.200.227
  #exit
  user-plane-group default
```

ユーザープレーン 2：

```
Config
  context EPC2
    sx-service sx
      instance-type userplane
      bind ipv4-address 209.165.200.228 ipv6-address bbbb:aaaa::5
    exit
    user-plane-service up
      associate gtpu-service pgw-gtpu pgw-ingress
      associate gtpu-service sgw-ingress-gtpu sgw-ingress
      associate gtpu-service sgw-engress-gtpu sgw-egress
      associate gtpu-service saegw-sxu cp-tunnel
      associate sx-service sx
      associate fast-path service
      associate control-plane-group g1
    exit
exit

  context isp
    ip vrf mpls-vrf-1
    #exit
    ip vrf mpls-vrf-2
    #exit
    apn mpls2.com
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode sent-by-ms
      ip context-name isp
    exit
exit
```

```
control-plane-group g1
    peer-node-id ipv4-address 209.165.200.228
  #exit
  user-plane-group default
```

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングとトラブルシューティングのサポートに使用できるCLIコマンドに関する情報を提供します。

コマンドや出力の表示

この項では、この機能のサポートにおけるshowコマンドまたはその出力について説明します。

show ip chunks

この CLI コマンドの出力には、そのコンテキストのすべてのチャンクが表示されます。

同じ UP 内の重複プール機能により、CLI **show ip chunks vrf** *vrf_name* に VRF オプションが導入され、VRF の下のチャンクのみが表示されます。

- chunk-id
- chunk-size
- vrf-name
- start-addr
- end-addr
- used-addrs
- ピア アドレス（Peer Address）

show ipv6 chunks

この CLI コマンドの出力には、そのコンテキストのすべてのチャンクが表示されます。

同じ UP 内の重複プール機能により、CLI **show ipv6 chunks vrf** *vrf_name* に VRF オプションが導入され、VRF の下のチャンクのみが表示されます。

- chunk-id
- chunk-size
- vrf-name
- start-prefix
- end-prefix
- used-prefixes

- ピア アドレス（Peer Address）

第 101 章

X ヘッダーの挿入と暗号化

マニュアルの変更履歴

改訂の詳細	リリース
xheader-format コマンドの **delete-existing** キーワードオプションを使用した、x-header フィールドのスプーフィング検出を有効にする CLI のサポートを追加。	21.28.m0
最初の導入。	21.25

機能説明

X-Header の挿入および X-Header 暗号化機能は、総称してヘッダーエンリッチメントと呼ばれます。この機能により、モバイルアドバタイズメントの挿入（MSISDN、IMSI、IP アドレス、ユーザーによるカスタマイズが可能なものなど）をはじめ、エンドアプリケーションで使用する HTTP または WSP の GET および POST 要求パケット、および HTTP レスポンスパケットにヘッダーを追加できます。

機能の仕組み

X-Header の挿入

この項では、X-Header の挿入機能の概要について説明します。

拡張ヘッダー（X-Header）フィールドは、RFC や標準規格では定義されていませんが、特定の目的でプロトコルヘッダーに追加できるフィールドです。X-Header メカニズムでは、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。

X-Header の挿入機能を使用すると、HTTP または WSP の GET および POST 要求パケットと HTTP レスポンスパケットに X-Header を挿入できます。HTTP または WSP 要求および HTTP レスポンスパケットに X-Header を挿入するオペレータは、挿入ルールを設定できます。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。

X-Header の暗号化

ここでは、X-Header の暗号化機能の概要を説明します。

X-Header の暗号化により X-Header の挿入機能が強化され、X-Header に挿入でき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。

IP フローに対して（いずれかの X-Header フォーマットにより）すでに X-Header が挿入されていて、かつ現在の charging-action に [first-request-only] フラグが設定されている場合、そのフォーマットによる X-Header の挿入は行われません。charging-action に [first-request-only] フラグが設定されていない場合、該当する IP フローの他の適切なパケットに対しては、その X-Header フォーマットによる挿入が続行されます。

X-Header フォーマットの設定を変更しても、既存のコールの再暗号化はトリガーされません。ただし、新しいコールには変更された設定が適用されます。変更された設定は、次の再暗号化のときに、再暗号化のタイムアウトが指定されている既存のコールにも適用されます。データのフロー中にパラメータの暗号化が有効になった場合、暗号化された値が使用できなくなるため、そのパラメータの挿入は停止します。

（注） この機能では、フローのリカバリはサポートされません。

X-Header の挿入と暗号化の設定

この項では、X-Header の挿入および暗号化機能（総称して、ヘッダーの機能拡張）の設定方法について説明します。

X-Header の挿入

表 *54 :* 手順

ステップ	説明
1	X-Header を挿入する必要がある HTTP/WSP パケットを識別するための ruledef を作成および設定します。
2	ルールベースを作成および設定し、HTTP/WSP パケットに X-Header フィールドを挿入する課金アクションを設定します。
3	X-Header 形式を作成および設定します。
4	課金アクションのメッセージタイプに基づいて X-Header フィールドの挿入を設定します。

X-Header の暗号化

表 *55 :* 手順

ステップ	説明
1	X-Header の挿入、暗号化、および暗号化証明書は CLI で設定されます。
2	コールが接続されると、各再生成時間の後に、暗号化証明書を使用して文字列が暗号化されます。
3	課金アクションで X-Header 形式が設定されている ruledef にパケットがヒットすると、そのパケットへの X-Header の挿入は、指定された X-Header 形式を使用して行われます。
4	暗号化としてマークされているフィールドに対して X-Header を挿入する場合、以前に暗号化された値がそのフィールドに適宜入力されます。

X ヘッダーの挿入の設定

ここでは、X-Header の挿入機能の設定方法について説明します。

X-Header の挿入機能を設定するには、次の手順を実行します。

表 *56 :* 手順

ステップ 1	X-Header を挿入する必要がある HTTP パケットを識別するための ruledef を作成または設定します。
ステップ 2	rulebase を作成または設定し、charging-action を設定します。これにより、HTTP パケットに X-headerフィールドが挿入されます。
ステップ 3 :	「*X-Header* フォーマットの作成」の説明に従って、X-Header フォーマットを作成します。
ステップ 4	「*X-Header* フォーマットの設定」の説明に従って、X-Header フォーマットを設定します。

X-Header フォーマットの作成

X-Header フォーマットを作成するには、次の設定を使用します。

```
configure
  active-charging service ecs_service_name
    xheader-format xheader_format_name
    end
```

X-Header フォーマットの設定

X-Header フォーマットを設定するには、次の設定を使用します。

```
configure
  active-charging service ecs_service_name
    xheader-format xheader_format_name
      insert xheader_field_name string-constant xheader_field_value | variable
 { bearer { 3gpp { apn | charging-characteristics | charging-id | imei
 | imsi | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | customer-id
 | ggsn-address | mdn | msisdn-no-cc | radius-string |
radius-calling-station-id | session-id | sn-rulebase |
subscriber-ip-address | username } [ encrypt ] [ delete-existing ] |
http { host | url } }
       end
```

X ヘッダーの暗号化の設定

ここでは、X ヘッダーの暗号化機能を設定する方法について説明します。

表 *57 :* 手順

ステップ 1	「*X* ヘッダーの挿入の設定」の説明に従って、X ヘッダーの挿入を設定します。

ステップ 2	「*X* ヘッダーの暗号化の設定」の説明に従って、ルールベースを作成または設定し、使用する暗号化証明書と再暗号化パラメータを設定します。
ステップ 3	「暗号化証明書の設定」の説明に従って、使用する暗号化証明書を設定します。

X ヘッダーの暗号化の設定

X ヘッダーの暗号化を設定するには、次の設定例を参考にしてください。

```
configure
   active-charging service ecs_service_name
     rulebase rulebase_name
        xheader-encryption certificate-name certificate_name
        xheader-encryption re-encryption period re-encryption_period
        end
```

注：

- この設定により、指定したルールベースに基づいて、すべてのサブスクライバに対して X ヘッダーの暗号化が有効になります。
- 証明書が削除されても、ECS ではそのコピーが引き続き使用されます。証明書名がルールベースから削除されると、コピーは解放されます。
- X ヘッダーのフォーマット設定を変更しても、既存のコールの再暗号化はトリガーされません。ただし、新しいコールには変更された設定が適用されます。変更された設定は、次の再暗号化のときに、再暗号化のタイムアウトが指定されている既存のコールにも適用されます。データのフロー中にパラメータの暗号化が有効になった場合、暗号化された値が使用できなくなるため、そのパラメータの挿入は停止します。

暗号化証明書の設定

暗号化証明書を設定するには、次の設定を使用してください。

```
configure
   certificate name certificate_name pem { { data pem_certificate_data
private-key pem [ encrypted ] data pem_pvt_key } | { url url private-key
pem { [ encrypted ] data pem_pvt_key | url url } }
   end
```

X-Header の挿入と暗号化の設定の確認

Exec モードで次のコマンドを入力して設定を確認します。

xheader-format *xheader_format_name*

X-Header の挿入および暗号化機能のモニタリングとトラブルシューティング

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show active-charging charging-action statistics name

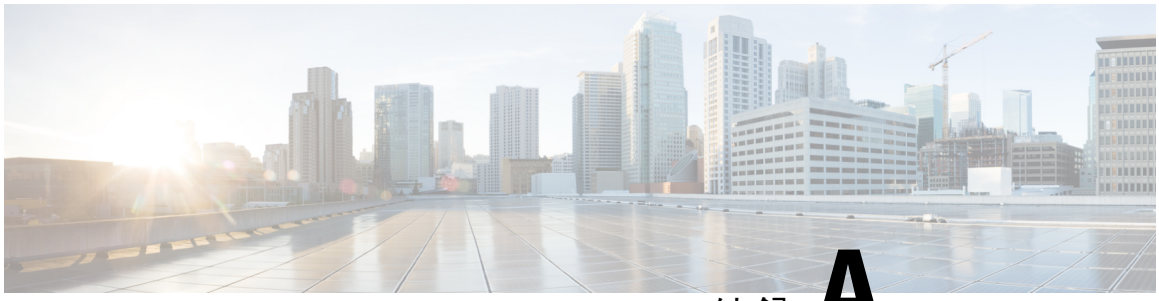
このコマンドの出力には、X-Header の統計情報が表示されます。

- XHeader 情報：
  - 挿入された XHeader のバイト数
  - 挿入された XHeader のパケット数
  - XHeader によって消費される IP フラグメント数
  - 削除された XHeader のバイト数
  - 削除された XHeader のパケット数

show active-charging rulebase statistics name

このコマンドの出力には、ヘッダーエンリッチメントの統計が表示されます。

- HTTP ヘッダーのバッファリング制限到達



付録 A

IP プールプランニングのガイドライン

CUPS アーキテクチャでの IP 配信

IP プールが UP で設定されている場合、UP に緊密に結合されます。未使用の IP プールの割合が大きいと、リソースの無駄になります。IP リソースが不足している UP では、未使用のリソースが利用できればメリットが得られます。同様に、1 つの UP が到達不能になった場合、その UP に割り当てられている IP 範囲は再利用できません。こうした制限を克服するために、IP チャンキングメカニズムが導入されました。

CUPS アーキテクチャでは、IP プールは CP で設定され、CP が IP プールの管理を担当します。CP で設定された IP プールは、設定されたサイズのチャンクに分割されます。UP 登録プロセス中に、CP はその特定の UP によってサービスが提供されている APN と、各 APN の関連する IP プール設定を確認します。CP はこれらの IP プールから UP にチャンクを割り当てます。CP は **chunk-threshold-timer** の秒数ごとに、各 UP のプールレベルのチャンク使用率をモニターし、チャンクしきい値に達すると、UP に新しいチャンクを割り当てます。同様に、UP 内の特定の IP チャンクが使用されておらず、そのプール用に十分な空きチャンクが CP に予約されていない場合、CP はそれぞれの UP からそれらの IP チャンクリソースを取り消します。

CUPS アーキテクチャでは、IP プールは UP 選択のリソース/基準とは見なされません。UP 間での不均等な負荷分散を回避するために、オペレータは UP グループ内のすべての APN と UP で十分な容量の IP チャンクが使用可能な状態であることを確認する必要があります。

UP グループの概念

UP が CP に関連付けられると、APN に関連付けられた IP プールからのチャンクが UP に配布されます。その後 UP は、APN に関連付けられている単一の UP グループに関連付けられるため、APN の一部として設定されている IP プールからのチャンクは、その APN に関連付けられた UP グループに属する UP に配布されます。したがって、プールサイズとチャンクサイズを計画する際は、UP グループのサイズを考慮する必要があります。

（注） UP は単一の UP グループにのみ属することができます。未定義の動作を引き起こす可能性があるため、2 つの UP グループに UP を追加しないでください。

デフォルトの UP グループ

APN に明示的に設定された UP グループがない場合、デフォルトの UP グループに属していると見なされます。デフォルトの UP グループはコンシューマトラフィックに主に使用され、APN が大規模すぎるため、多数のサブスクライバに対応し、大規模な IP プールで動作する 大きすぎる

特定の UP グループ

特定の APN のトラフィックを選択的に一部の UP に転送するには、特定の UP グループを使用します。たとえば、APN と IP プールが小規模な（256 程度の）企業サブスクライバのケースを考えてみます。この場合、プールをチャンクに分割するのではなく、APN 全体を 1 つの UP のみで構成される UP グループ専用にするのが得策です。では次に、大規模な APN と 20 以上の UP で構成されるきわめて大規模な展開を考えてみます。この場合も、サービスを提供するために 20 の UP すべてを必要とする大規模な APN はありません。IP プールのチャンク分割メカニズムをより効果的に活用するため、これらの UP と APN をいくつかの特定の UP グループに分割します。

たとえば、UP の数が 20 で、それぞれが 100,000 のサブスクライバにサービスを提供する必要があるとします。また、それぞれプールサイズが 16,000、チャンクサイズが 1,000 の APN が 25、プールサイズが 64,000、チャンクサイズが 1,000 の APN が 6 あるとします。この場合、IP プールをより効率的に使用するため、2 つの UP グループを作成できます。UP group-1 は 4 つの UP で 25 の小規模 APN に対応し、UP group-2 は 16 の UP と 6 つの大規模 APN で構成されます。

新しいプールの追加時期

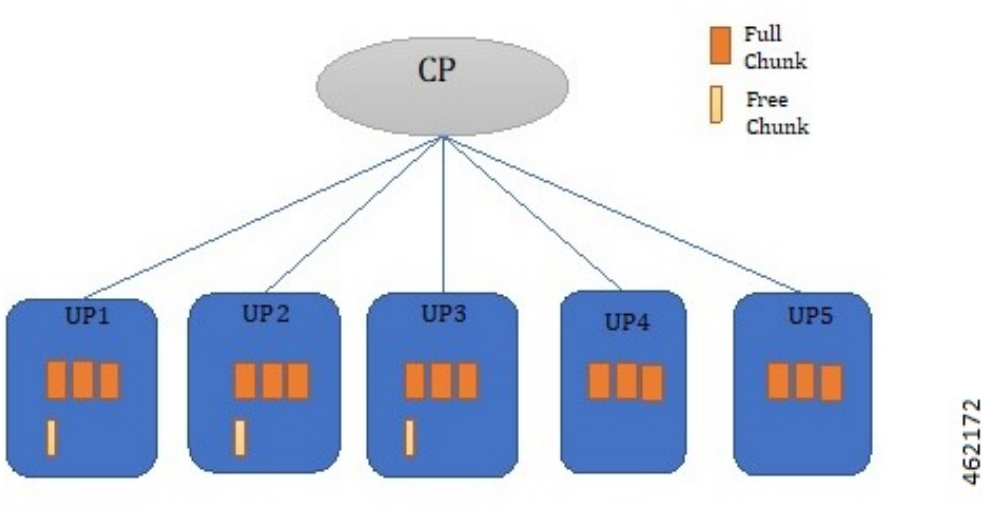
APN に残っている空きチャンクの量が UP グループ内の UP の数よりも少ない場合、および選択した UP にすべてのチャンクが完全に使用されている場合（つまり、空きチャンクが残って

IP プールプランニングのガイドライン

いない場合）、負荷分散が不均一になります。また、UP 選択アルゴリズムがオーバーライドされ、使用可能なチャンクがある UP から IP が指定されます。

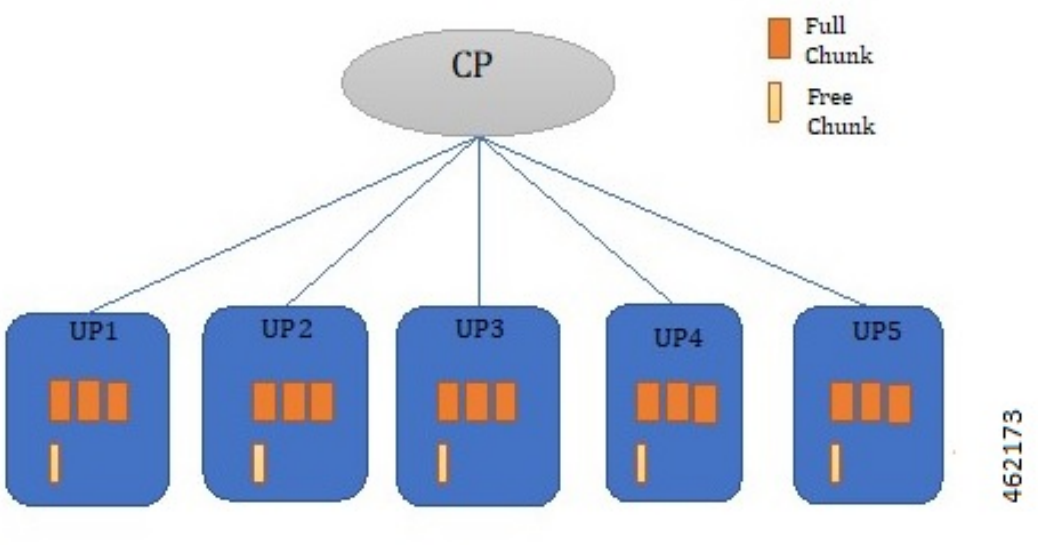
このシナリオは次の図に示されています。

図 *51* : 新しいプールの追加時期



当該 APN にプールを追加して不均一な負荷分散を回避し、チャンクの割り当てを可能な限り均等にするためにチャンキングを実行する必要があります。

図 *52* : 新しいプールが追加された後のシナリオ



（注） 将来の使用に備えて事前にディメンショニングを計画し、不均一な負荷分散を避けるためにチャンクを追加することを推奨します。

IP プールの微調整パラメータ

しきい値タイマー

CP は、すべての UP との間でチャンクを定期的にプッシュまたは削除します。周期性は、**chunk-threshold-timer** を使用して設定されます。プールから割り当てられたアドレスの 70% を超えるチャンクが UP で使用されている場合、新しいチャンクが UP にプッシュされます。同様に、UP で IP プールリソースが十分に活用されていない場合、CP は未使用のチャンクを UP からプルバックします。チャンクの削除は、「チャンクの取り消し」で説明されている他の要因にも左右されます。

チャンクの取り消し

CP の空きチャンクが **min-chunks-threshold-per-pool** 未満の場合、CP は定期的にそのプールの使用率が低い UP からチャンクを取り消します。UP が使用しているのがプールの割り当て済み IP アドレスの 40% 未満の場合、UP に 2 つを超える使用可能な空きチャンクがあれば、1 つのチャンクがプールから取り消されます。

プッシュされる初期チャンク

各 UP にプッシュされる最初のチャンクは、**cups max-user-plane** キーワードを使用して制御できます。このキーワードはコンテキストレベルで機能します。最初のチャンクは、次の要因に応じてプッシュされます。

- プール内の空きチャンクの合計数（**show ip pool** コマンドでこの値が表示されます）
- プール内の合計チャンク（**cups max-user-planes** CLI で設定された値）。デフォルトでは、max-user-planes の値は 10 に設定されます。
- 3 つのチャンク

例 1:

CUPS の **max-user-plane** CLI コマンドは、登録時に UP にプッシュされる初期チャンクの数を決定するために使用されます。プッシュされる初期チャンクの数は、次の要因によって異なります。

- チャンクが **max-user-plane** 値**未満**の場合、1 つのチャンクがプッシュされます。

- チャンクがそれより多い場合、最小値は（chunks/**max-user-plane**, 3）です。

  max-user-plane のデフォルト値は 10 です。

8 つのチャンクプールがあり、展開で 4 つの UP を使用するとします。すべてのチャンクをすべての UP に直接割り当てることができます。**max-user-plane** を 4 に設定すると、同じ処理を実行できます。同様に、8 つの UP を展開する場合は、値を 8 に設定すると、1 つのチャンクだけが UP にプッシュされます。

さらに、サブスクライバの急増に対応するためのバッファとして機能できる追加のチャンクを提供します。このサブスクライバの急増により、通常のしきい値のチャンク補充レートを超える可能性があります。32 個のチャンクと 2k サイズの 4 つの UP から構成される 1 つのプールがあり、着信サブスクライバレートが 1 分あたり 2k であるとします。追加のバッファチャンクを確保したい場合、つまり、短い期間に着信サブスクライバがチャンクの補充レートを上回り、負荷の不均衡が発生するのを回避するためにチャンクを保護するには、**max-user-plane** CLI を使用します。この CLI を使用しない場合は、1000 に設定すると、常に 1 つのチャンクがプッシュされます。

チャンクサイズ

チャンクサイズは、UP グループ内の UP の数に関して、CEPS とチャンクの均等性の両方を考慮して計画する必要があります。設定するチャンクが大きすぎると、UP 間で IP アドレスが不均一になる可能性があります。ただし、チャンクが小さすぎる場合、チャンクの補充レートが着信サブスクライバよりも低くなる可能性があります。チャンクの補充率が低いと、UP のオーバーライドや負荷の不均衡が発生します。

ダイナミック IP プールプランニングのガイドライン

チャンクのガイドライン

チャンクは、UP グループの規模を考慮して計画する必要があります。チャンクサイズが大きすぎるまたは小さすぎると、それに関連した影響が出るため、適切なバランスを維持することが重要です。

- チャンクサイズが小さいほど、UP 間のチャンク分散の不均衡が減少します。ただし、チャンクサイズが非常に小さいと、UP でのチャンクの枯渇が速くなり、CEPS レートに悪影響を及ぼします。
- チャンクサイズが非常に大きいと、UP 間でチャンクが不均等に分散される可能性があります。この問題により、IP アドレスが別の UP で引き続き使用可能であるにもかかわらず、特定の UP で UP のオーバーライドや負荷の不均衡が発生して、使用可能な IP がない状態に陥る可能性があります。

適切な IP プールリソースプランニングが推奨される設定例を以下に示します。

- **IPv6 プール**：Poolv6_example_1 pool_group_example1 x:x:x:x::/48 chunk_size = 8192

IP プールプランニングのガイドライン

- **IPv6 プール**：Poolv6_example_1 pool_group_example1 x:x:x:x::/48 chunk_size = 8192
- **APN に関連付けられた UP**：UP1、UP2、UP3、UP4、UP5
- **しきい値タイマー**：60 秒
- **UP あたりの着信サブスクライバレート**：6,000 サブスクライバ/分

（この UP グループがサービスを提供している APN に接続されている IP プールグループは 1 つだけであることを前提としています）

これで、両方の IP プールには 65536 個の IP アドレスがあります。

チャンクサイズが大きすぎる場合：アドレスが 8 つのチャンクに分割され、5 つの UP に分配されるとします。つまり、すべての UP が同等の数の IP リソースを取得できるわけではなく、一部の UP は他の UP よりも早く IP リソースを使い果たします。

IP リソースが枯渇すると、そのような UP で UP オーバーライドや負荷の不均衡が発生します。この例では、プールあたり約 40960 のアドレスまたは IP プールグループレベルで約 81920 のアドレスが使用された後に、このような状況が発生する可能性があります。

- Pool1：（**UP1** = 8192 + 8192, **UP2** = 8192 + 8192, **UP3** = 8192 + 8192, **UP4**=8192, **UP5**=8192）
- Pool2：（**UP1** = 8192 + 8192, **UP2** = 8192 + 8192, **UP3** = 8192 + 8192, **UP4**=8192, **UP5**=8192）

チャンクサイズが小さすぎる場合：前の項と同じプールが、チャンクサイズ 512、チャンク数 128 で設計されているとします。この場合は、次のようになります。

- Pool1：（**UP1** = 26 *512, **UP2** =26*512, **UP3** = 26*512, **UP4**=25*512, **UP5**=25*512）
- Pool2：（**UP1** = 26 *512, **UP2** =26*512, **UP3** = 26*512, **UP4**=25*512, **UP5**=25*512）

この場合、チャンクの不均衡による UP オーバーライドまたは負荷の不均衡は、128000（50 チャンク * 512 サイズ * 5 UP）のアドレスが使用された後に発生します。各 UP には各 UP から 1 分あたり 1k アドレスしかありません。しきい値タイマーは 60 秒ですが、着信サブスクライバレートは 6k であるため、各 UP では 5k のサブスクライバの負荷の不均衡が発生します。

正しい設計の場合：IP プールをチャンクサイズ（4096 個の IP アドレスなど）に分割すると、適切な設計になります。この設計では、5 つの UP に配布するための 16 のチャンクが CP に提供されます。

Pool1：（**UP1** = 4096 + 4096 + 4096 + 4096, **UP2** = 4096 + 4096 + 4096, **UP3** = 4096 + 4096 + 4096, **UP4**= 4096 + 4096 + 4096, **UP5**= 4096 + 4096 + 4096）

この場合、チャンクの不均衡による UP オーバーライドまたは負荷の不均衡は、122880（6 チャンク *4096 サイズ *5 UP）のアドレスが使用された後に発生します。各 UP には各 UP から 1 分あたり 8k アドレスしかありませんが、しきい値タイマーが 60 秒で着信サブスクライバレートが 6k であるため、UP はすべてのサブスクライバに対応できます。

この例から明らかなように、チャンクサイズが 4096 の場合は、チャンクサイズが 8096 の場合よりも UP 間で IP リソースが分散されます。IP リソースが枯渇すると、そのような UP で UP オーバーライドや負荷の不均衡が発生します。この例では、プールごとに約 61440 のアドレスが使用された後に発生し始めます。また、プールグループには同時に 2 つの IP プールがある

ため、チャンクの補充は pool1 からの 4k と pool2 からの 4k となり、必要なレートである 6k よりも大きくなります。

UP グループ化のガイドライン

コンシューマカスタマーとエンタープライズカスタマーは、それぞれの IP プールサイズやルーティング要件が異なるため、異なる UP グループに分ける必要があります。デフォルトの UP グループは、コンシューマカスタマーに使用されます。エンタープライズカスタマーには特定のユーザーグループを作成し、エンタープライズ APN と関連付けることを推奨します。チャンクメカニズムは、大きなプールの効率的な IP アドレス管理を提供しますが、プールサイズが小さい場合（たとえば、IP プールサイズが 4k 未満の場合）は避ける必要があります。小さい IP プールは特定の UP 専用にすることを推奨します。これを実現するには、特定の UP グループに単一の UP を設定し、APN に関連付けます。

5 つの UP があり、256 アドレスの 40 の小規模エンタープライズ APN と、それぞれ 64k アドレスの 8 つの大規模コンシューマ APN にサービスを提供する場合について考えます。この場合、2 つの UP グループを作成します。1 つの UP と 40 の小規模エンタープライズ APN で構成される UPGroup1 と、4 つの UP と 8 つの大規模コンシューマ APN で構成される UPGroup2 です。

UP 追加のガイドライン

オペレータは、UP グループに新しい UP を追加する前に、すべての APN に使用可能な空きチャンクが CP にあることを確認する必要があります。チャンクは、UP 登録時に割り当てることができます。その結果、ある APN にこの UP に使用可能な IP アドレスがない場合でも、この UP がコール分配用に選択されるため、不均等な負荷分散がなくなります。

その他のガイドライン

- プール使用率のしきい値アラームを使用して、IP プールリソースの補充に関する警告を受けます。適切なアクションを実行します。つまり、プールグループに新しいプールを追加します。
- ダイナミック v4v6 アドレス割り当ての場合の IPv4v6 セッションでは、UE に割り当てる必要がある IPv4 アドレスと IPv6 アドレスは両方とも同じ UP に属します。IP プールの計画では、v4v6 コールが予想される UP ごとにそれぞれ十分な v4 および v6 IP アドレスを使用可能にしておく必要があります。

  「poolv4」という名前の IPv4 プール（x.x.x.x/17 という表記のアドレス 32,000 個）と、「poolv6」という名前の IPv6 プール（x:x:x:x:/48 という表記のアドレス 64,000 個）を例に考えてみましょう。2 つの APN があるとします。APN1 は v4v6 コールを実行し、「poolv4」と「poolv6」の両方で動作します。

  ip pool poolv4 209.165.200.224/17 – APN1 で使用される 32,000 個のアドレス

  ipv6 pool poolv6 prefix 2003::/48 - APN2 で使用される 64,000 個のアドレス

APN2 が使用する IPv6 アドレスが 32,000 個を超えてしまった場合、APN の計画が不十分であるために、APN1 の v4v6 に対応できるだけの十分な IPv6 アドレスが残らない可能性があります。この場合、poolv6 の 64,000 個のアドレスを、APN1 で使用する 32,000 個のアドレス（poolv6_1）と APN2 で使用する 32,000 個のアドレス（poolv6_2）に分けます。より多くの IP アドレスが必要なのであれば、APN1 に正当に割り当てられたアドレスを枯渇させるのではなく、必要に応じて APN2 に IPv6 プールを追加する必要があります。

静的 IP プールのガイドライン

静的 IP プールは、次のシナリオで使用されます。

- UE が初期接続で IP アドレスを送信する場合。
- AAA/S6b が IP アドレスを返した場合。
- DHCP が IP アドレスを返した場合。

静的 IP プールの場合、アドレスはすでに UE によって決定されているため、UP を選択する利点はありません。選択した IP アドレスを含むチャンクを持つ UP だけが、そのコールを処理できます。静的 IP プールの場合、UE が未使用のチャンクから最初の IP を要求すると、チャンクが UP に与えられます。これらのチャンクは、UP グループ内の UP にラウンドロビン方式で割り当てられます。一度割り当てられた静的チャンクは、Sx が再起動する場合を除き、UP から取り戻されることはありません。静的プールに関するガイドラインは以下のとおりです。

- 静的 IP プールでは、MOP 手順の中で 1 回コールを行い、そのチャンクを特定の UP 専用にします。チャンクは最初のコールでのみプッシュされるため、これは最初のコールの遅延を回避するのに役立ちます。
- 静的 IP プールでは、静的 IP プールを持つすべての APN にサービスを提供する UP 数が限られているデフォルト以外の UP グループを使用します。
- 静的 IP プールでは、すべてのプールで均一なチャンクサイズを使用します。前述したように、UP の選択は静的 IP プールでは使用できないため、UP での負荷の不均衡を回避するために、プールのサイズを統一する必要があります。
- 静的 IPv4v6 PDN を正常に動作させるには、IPv4 アドレスと IPv6 アドレスの両方が同じ UP 上にある必要があります。確実に動作させる唯一の方法は、UP グループに含める UP を 1 つにすることです。
- 1 つの PDN を静的、もう 1 つの PDN を動的で同じ APN 上のマルチ PDN を正常に動作させるには、両方のアドレスが同じ UP 上にある必要があります。動的プールの場合、アドレスは UP 選択アルゴリズムによって選択されます。静的アドレスの場合、UP は選択された IP によって決定されるため、負荷の不均衡を回避する唯一の方法は、UP グループに含める UP を 1 つにすることです。

非常に大きなチャンクサイズを取得する意味

プールシステムの制限

現在、CP DI-Large モデルは、次の表に示すパラメータのスケーリング数をサポートしています。各制限は、使用されるチャンクサイズの値に関係なく一定であり、特定のパラメータの最大許容制限を表します。最大値に達したパラメータの制限により、後続のパラメータの上限値が制限されます。

（注） 中小規模のモデルでは、制限は比較的低くなっています。

パラメータ	制限
コンテキストごとの IPv4 プール	2000
コンテキストごとの IPv6 プール	256
シャーシごとの IP プール	5,000（v4 と v6 の両方を含む）
ダイナミックプールアドレス	コンテキストあたり 1,600 万 シャーシあたり 3,200 万
スタティックプールアドレス	コンテキストあたり 3,200 万 シャーシあたり 9,600万
VRF の数	コンテキストあたり 300 シャーシあたり 2,048
最大 IP プールサイズ	512k
最大 IPv6 プールサイズ	1,000,000

UP グループのチャンクサイズの意味：

プールはチャンクの割り当ての基本単位であり、すべての UP には関連するプールからチャンクが割り当てられます。チャンクサイズ値が 65,536 のチャンクを取得できる UP の数は最大で、100 万/65,536 = 16 なので、チャンクサイズ値が 65,536 の場合、各 UP グループでサポートされる UP は 16 のみです。

APN のチャンクサイズの意味：

APN 設定で使用される単一の UP グループの場合、制限は UP グループ制限値と同じです。

IP プールプランニングのガイドライン

APN 設定で使用される複数の UP グループについては、「グループ固有の IP プールを持つ複数の UP グループ」の章を参照してください。サポートされる 16 の UP の最大 UP グループ数は、コンテキストごとに 1,600 万アドレス、または 100 万アドレスプールなので、16 の UP APN で合計 16 の UP グループを設定できます。

v6 プール内のすべてのプール設定が枯渇すると、同じ VPN コンテキストで動作する残りの APN では同じ IPv6 プールが使用されます。その他の場合、制限は想定より低くなるため、16 の UP で 16 UP グループというのは、IPv4 アドレスがないという前提に基づいています。システムでは約 3,200 万のダイナミックアドレスがサポートされますが、許可される SGI コンテキストは 2 つだけです。

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