PDN ゲートウェイの設定

この章では、PDN ゲートウェイ（P-GW）の設定について説明します。

重要 この章にあるすべてのコマンドの情報は、『*Command Line Interface Reference*』で確認できます。

各ワイヤレスネットワークはそれぞれ異なるため、システムは、さまざまなワイヤレスネットワーク環境で動作できるように、さまざまなパラメータを使用して設計されます。この章では、システムを動作させるための最小限のパラメータセットのみを示します。P-GW 製品に固有のオプションの設定コマンドは、『*Command Line Interface Reference*』に記載されています。

この章では、次の手順について説明します。

スタンドアロン eGTP P-GW としてのシステムの設定

この項では、テスト環境で eGTP P-GW として実行するようにシステムを設定するための一連の手順の概要と、関連する構成ファイルの例を示します。構成ファイルの完全な例については、付録「サンプル構成ファイル」を参照してください。ここでは次の内容について説明します。

必要な情報

以降のセクションでは、P-GW を設定し、ネットワーク上で動作させるために必要な最小限の情報について説明します。プロセスをより効率的なものにするため、システムを設定する前にこの情報を用意しておくことを推奨します。

ここでは説明していないその他の設定パラメータがあります。これらのパラメータは、主にネットワークでの P-GW の動作の微調整に対応します。これらのパラメータの詳細については、『*Command Line Interface Reference*』[英語] の該当するセクションを参照してください。

必要なローカルコンテキスト設定情報

次の表に、P-GW でローカルコンテキストを設定するために必要な情報を示します。

表 *1:* ローカルコンテキストの設定に必要な情報

必要な情報	説明
管理インターフェイスの設定	
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	管理インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
セキュリティ管理者名	システムに対して完全な権限を持つセキュリティ管理者の名前。
セキュリティ管理者のパスワード	オープンパスワードまたは暗号化パスワードを使用できます。
リモートアクセスタイプ	システムへのアクセスに使用するリモートアクセスプロトコルのタイプ（SSH など）。

必要な P-GW コンテキスト設定情報

次の表に、P-GW で P-GW コンテキストを設定するために必要な情報を示します。

表 *2 : P-GW* コンテキストの設定に必要な情報

必要な情報	説明
P-GW コンテキスト名	システムが P-GW コンテキストを認識するために使用する 1 ～ 79 文字（英字または数字）の識別文字列。
アカウンティングポリシー名	システムがアカウンティングポリシーを認識するために使用する 1 ～ 文字（英字または数字）の識別文字列。アカウンティングポリシーは Rf（オフライン課金）インターフェイスのパラメータを設定するため使用されます。
S5/S8 インターフェイスの設定（S-GW 間）	
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルーを設定するときに使用されます。
GTP-U サービスの設定	
GTP-U サービス名	システムが GTP-U サービスを認識するために使用する 1 ～ 63 文字（字または数字）の識別文字列。
IP address	S5/S8 インターフェイスの IPv4 アドレス。
P-GW サービス設定	
P-GW サービス名	システムが P-GW サービスを認識するために使用する 1 ～ 63 文字（字または数字）の識別文字列。 複数の P-GW サービスを使用する場合は、複数の名前が必要です。

必要な情報	説明
PLMN ID	MCC 番号：PLMN の識別子のモバイル国コード（MCC）部分（100 ～ 999 の整数値）。 MNC 番号：PLMN の識別子のモバイルネットワークコード（MNC）部分（00 ー 999 の 2 桁または 3 桁の整数値）。
eGTP サービスの設定	
eGTP サービス名	システムが eGTP サービスを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。

必要な PDN コンテキスト設定情報

次の表に、P-GW で PDN コンテキストを設定するために必要な情報を示します。

表 *3: PDN* コンテキストの設定に必要な情報

必要な情報	説明
PDN コンテキスト名	システムが PDN コンテキストを認識するために使用する 1 ～ 79 文字（英字および/または数字）の識別文字列。
IP アドレスプールの設定	
IPv4アドレスプールの名前と範囲	システムが IPv4 プールを認識するために使用する 1 ～ 31 文字（英字と数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義される IPv4アドレスの範囲。
IPv6アドレスプールの名前と範囲	システムが IPv6 プールを認識するために使用する 1 ～ 31 文字（英字や数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義される IPv6アドレスの範囲。
アクセス制御リストの設定	
IPv4 アクセスリスト名	システムが IPv4 アクセスリストを認識するために使用する 1 ～ 47 文字（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。
IPv6 アクセスリスト名	システムが IPv6 アクセスリストを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。

必要な情報	説明
拒否/許可タイプ	タイプは次のとおりです。 • any • ホスト IP アドレスによる • IP パケットによる • 送信元 ICMP パケットによる • 送信元 IP アドレスマスキングによる • TCP/UDP パケットによる
アドレス再指定またはリダイレクトタイプ	タイプは次のとおりです。 • サーバーのアドレス再指定 • コンテキストのリダイレクト • CSS 配信シーケンスのリダイレクト • redirect css service コマンドで使用可能なキーワードとオプション ついては、『Command Line Interface Reference』の • redirect nexthop
SGi インターフェイスの設定（IPv4 PDN へ/IPv4 PDN から）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
SGi インターフェイスの設定（IPv6 PDN へ/IPv6 PDN から）	

必要な情報	説明
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。

必要な AAA コンテキスト設定情報

次の表に、P-GW で AAA コンテキストを設定するために必要な情報を示します。

表 *4: AAA* コンテキストの設定に必要な情報

必要な情報	説明
Gx インターフェイスの設定（PCRF 対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。

必要な情報	説明
Gx Diameter エンドポイントの設定	
エンドポイント名	Gx Diameter エンドポイントの設定がシステムによって認識される 1～63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Gx 送信元ホストがシステムによって認識される、1～255 文字（英字数字）の識別文字列。
元のホストアドレス	Gx インターフェイスの IP アドレス。
ピア名	上述の Gx エンドポイント名。
ピアレルム名	上述の Gx 発信元レルム名。
ピアのアドレスとポート番号	PCRF の IP アドレスとポート番号。
ルートエントリピア	上述の Gx エンドポイント名。
Gy インターフェイスの設定（オンライン課金サーバー対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1～79 文字（字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネトが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカドが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルーを設定するときに使用されます。
Gy Diameter エンドポイントの設定	

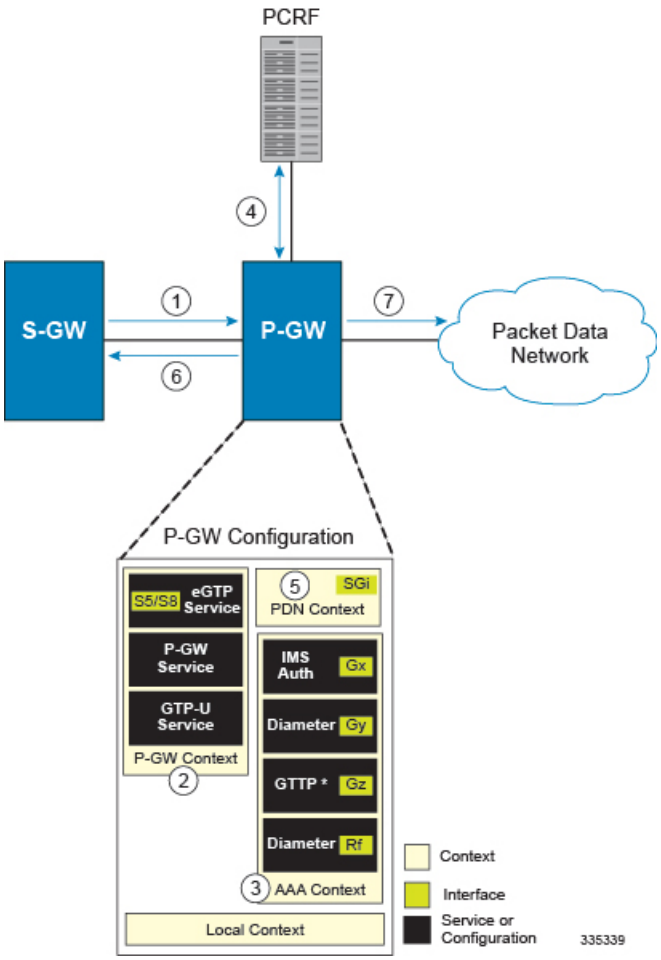
必要な情報	説明
エンドポイント名	Gy Diameter エンドポイントの設定がシステムによって認識される 1 ー 63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Gy 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字や数字）の識別文字列。
元のホストアドレス	Gy インターフェイスの IP アドレス。
ピア名	上述の Gy エンドポイント名。
ピアレルム名	上述の Gy 発信元レルム名。
ピアのアドレスとポート番号	OCS の IP アドレスとポート番号。
ルートエントリピア	上述の Gy エンドポイント名。
Gz インターフェイスの設定（オフライン課金サーバーに対する）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
Rf インターフェイスの設定（オフライン課金サーバーに対する）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。

必要な情報	説明
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネトが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカドが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルーを設定するときに使用されます。
Rf Diameter エンドポイントの設定	
エンドポイント名	Rf Diameter エンドポイントの設定がシステムによって認識される 1 ～63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Rf 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字数字）の識別文字列。
元のホストアドレス	Rf インターフェイスの IP アドレス。
ピア名	上述の Rf エンドポイント名。
ピアレルム名	上述の Rf 発信元レルム名。
ピアのアドレスとポート番号	OFCS の IP アドレスとポート番号。
ルートエントリピア	上述の Rf エンドポイント名。

この設定が動作する仕組み

次の図と補足テキストは、GTP LTE ネットワークから発信されるサブスクライバコールを処理するために、単一の送信元と接続先のコンテキストを持つこの設定がシステムによってどのように使用されるかを示しています。

図 *1 : GTP P-GW* 構成要素



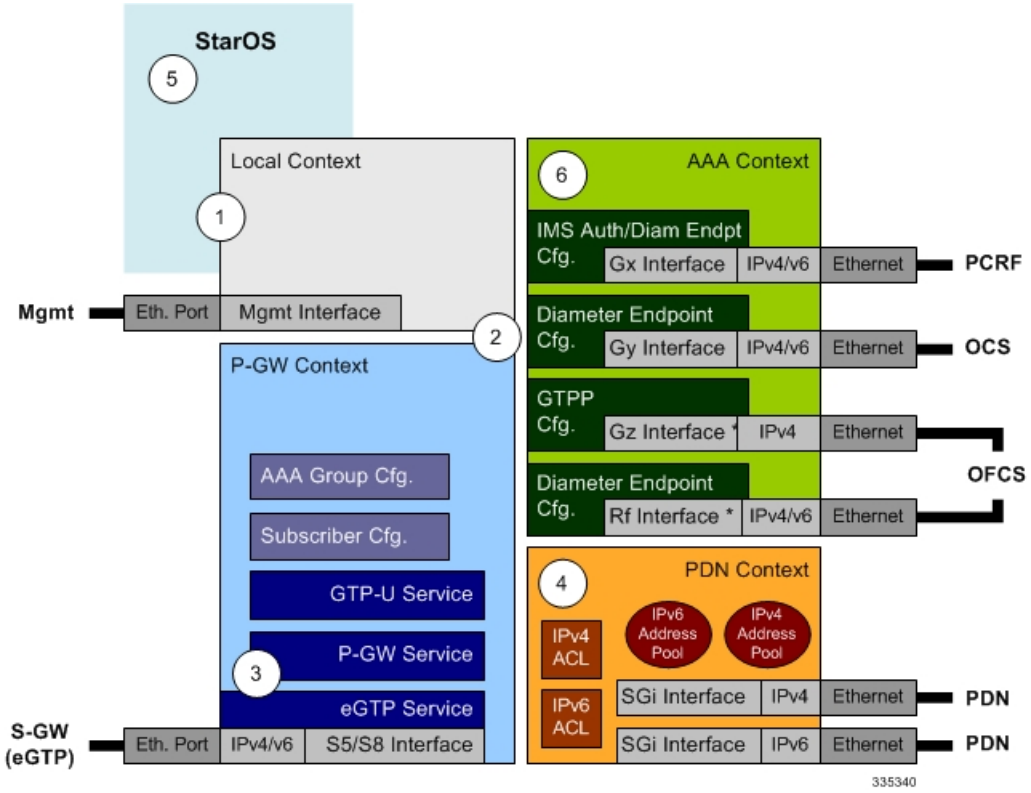
1. S-GW は、アクセスポイント名（APN）を含むセッション作成要求メッセージを P-GW に送信することにより、S5/S8 接続を確立します。
2. P-GW サービスは、セッションに AAA 機能を提供するために使用するコンテキストを決定します。このプロセスについては、『*System Administration Guide*』の「*Understanding the System Operation and Configuration*」の章にある「*How the System Selects Contexts*」の項で説明しています。
3. P-GW は、設定済みの Gx Diameter エンドポイントを使用して IP-CAN セッションを確立します。
4. P-GW は、IP-CAN セッションの確立を示すために CCRF に CC 要求（CCR）メッセージを送信し、PCRF は CC 応答（CCA）で確認応答します。
5. P-GW は APN 設定を使用して PDN コンテキストを選択します。選択した PDN コンテキストで設定された IP プールから IP アドレスが割り当てられます。
6. P-GW は、割り当てられたアドレスと追加情報を含むセッション作成応答メッセージで S-GW に応答します。

7. S5/S8 データプレーントンネルが確立され、P-GW は PDN との間でパケットを送受信できます。

eGTP P-GW 設定

スタンドアロン eGTP P-GW として動作するようにシステムを設定するには、次の手順を実行します。

図 *2 : eGTP P-GW* の設定可能項目



手順

ステップ 1 『*System Administration Guide*』[英語] に記載されている設定例を適用して、PSC のアクティブ化などのシステム設定パラメータを設定します。

ステップ 2 「初期設定 （12 ページ）」に記載されている設定例を適用して、コンテキストやサービスの作成などの初期設定パラメータを設定します。

ステップ 3 システムを eGTP P-GW として動作するように設定し、「P-GW サービス設定 （16 ページ）」に記載されている設定例を適用して、eGTP インターフェイスや IP ルートなどの基本的な P-GW パラメータを設定します。

ステップ 4 「P-GW PDN コンテキストの設定 （17 ページ）」の設定例を適用して、PDN コンテキストを設定します。

ステップ 5 「アクティブ課金サービス設定 （18 ページ）」の設定例を適用して、Gx インターフェイスのサポートのためのアクティブ課金サービスを有効にし、設定します。

ステップ 6 「ポリシーの設定 （20 ページ）」の設定例を適用して、AAA コンテキストを作成し、ポリシーのパラメータを設定します。

ステップ 7 「設定の確認と保存 （22 ページ）」の手順に従って、設定を確認して保存します。

初期設定

手順

ステップ 1 「ローカルコンテキストの変更 （12 ページ）」の設定例を適用して、ローカルシステム管理パラメータを設定します。

ステップ 2 「eGTP P-GW コンテキストの作成と設定 （13 ページ）」の設定例を適用して、eGTP サービスを配置したコンテキストを作成します。

ステップ 3 「P-GW コンテキストでの APN の作成と設定 （14 ページ）」の設定例を適用して、P-GW コンテキストで APN を作成および設定します。

ステップ 4 「P-GW コンテキストでの AAA グループの作成と設定 （15 ページ）」の設定例を適用して、P-GW コンテキストで AAA サーバーグループを作成および設定します。

ステップ 5 「eGTP サービスの作成と設定 （15 ページ）」の設定例を適用して、新しく作成されたコンテキスト内に eGTP サービスを作成します。

ステップ 6 「GTP-U サービスの作成と設定 （16 ページ）」の設定例を適用して、P-GW コンテキスト内に GTP-U サービスを作成および設定します。

ステップ 7 「P-GW PDN コンテキストの作成 （16 ページ）」の設定例を適用して、PDN へのインターフェイスが配置されるコンテキストを作成します。

ローカルコンテキストの変更

デフォルトサブスクライバを設定し、ローカルコンテキストでリモートアクセス機能を設定するには、次の例を使用します。

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
        exit
      server ftpd
        exit
      server telnetd
        exit
      subscriber default
        exit
      administrator <name> encrypted password <password> ftp
```

```
      ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
      exit
  port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
    end
```

eGTP P-GW コンテキストの作成と設定

次の例を使用して、P-GW コンテキストを作成し、S5 または S8 IPv4 インターフェイス（S-GW との間のデータトラフィック用）を作成し、S5 または S8 インターフェイスを設定済みのイーサネットポートにバインドします。

```
configure
  gtpp single-source
  context <pgw_context_name> -noconfirm
    interface <s5s8_interface_name>
      ip address <ipv4_address>
      exit
    gtpp group default
      gtpp charging-agent address <gz_ipv4_address>
      gtpp echo-interval <seconds>
      gtpp attribute diagnostics
      gtpp attribute local-record-sequence-number
      gtpp attribute node-id-suffix <string>
      gtpp dictionary <name>
      gtpp server <ipv4_address> priority <num>
      gtpp server <ipv4_address> priority <num> node-alive enable
      exit
    policy accounting <rf_policy_name> -noconfirm
      accounting-level {level_type}
      accounting-event-trigger interim-timeout action stop-start
      operator-string <string>
      cc profile <index> interval <seconds>
      exit
    exit
  subscriber default
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5s8_interface_name> <pgw_context_name>
    end
```

注：

- **gtpp single-source** が有効になり、各 AAA マネージャが独自の UDP ポートで要求を生成するのではなく、システムが単一の UDP ポートを使用して（AAA プロキシ機能によって）アカウンティングサーバーへの要求を生成できるようになりました。
- S5 または S8（P-GW から S-GW）インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。

- Rf（オフライン課金）インターフェイスのアカウンティングポリシーを設定します。アカウンティングレベルのタイプは、Flow、PDN、PDN-QCI、QCI、および Subscriber です。このコマンドの詳細については、『*Command Line Interface Reference*』の「*Accounting Profile Configuration Mode Commands*」の章を参照してください。
- Gz アカウンティングの GTPP グループを設定します。

P-GW コンテキストでの APN の作成と設定

次の設定を使用して、APN を作成します。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      associate accounting-policy <rf_policy_name>
      ims-auth-service <gx_ims_service_name>
      aaa group <rf-radius_group_name>
      dns primary <ipv4_address>
      dns secondary <ipv4_address>
      ip access-group <name> in
      ip access-group <name> out
      mediation-device context-name <pgw_context_name>
      ip context-name <pdn_context_name>
      ipv6 access-group <name> in
      ipv6 access-group <name> out
      active-charging rulebase <name>
      end
```

注：

- IMS 承認サービスは、AAA コンテキストで作成および設定されます。
- 複数の APN を、異なるドメイン名をサポートするように設定できます。
- 事前設定済みのアカウンティングポリシーをこの APN に関連付けるには、**associate accounting-policy** コマンドを使用します。アカウンティングポリシーは、P-GW コンテキストで設定されます。その例が「eGTP P-GW コンテキストの作成と設定 （13 ページ）」で示されています。

Gz インターフェイスパラメータを含む APN を作成するには、次の設定を使用します。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      bearer-control-mode mixed
      selection-mode sent-by-ms
      accounting-mode gtpp
      gtpp group default accounting-context <aaa_context_name>
      ims-auth-service <gx_ims_service_name>
      ip access-group <name> in
      ip access-group <name> out
```

```
      ip context-name <pdn_context_name>
      active-charging rulebase <gz_rulebase_name>
      end
```

注：

- IMS 承認サービスは、AAA コンテキストで作成および設定されます。
- 複数の APN を、異なるドメイン名をサポートするように設定できます。
- accounting-mode GTPP および GTPP group コマンドは、この APN を Gz アカウンティング用に設定します。

P-GW コンテキストでの AAA グループの作成と設定

RADIUS および Rf アカウンティングをサポートする AAA グループを作成および設定するには、次の例を使用します。

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter accounting endpoint <rf_cfg_name>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
    aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter accounting endpoint <rf_cfg_name>
      diameter accounting server <rf_cfg_name> priority <num>
      end
```

eGTP サービスの作成と設定

eGTP サービスを作成するには、次の設定例を使用します。

```
configure
  context <pgw_context_name>
    egtp-service <egtp_service_name> -noconfirm
      interface-type interface-pgw-ingress
      validation mode default
      associate gtpu-service <gtpu_service_name>
      gtpc bind address <s5s8_interface_address>
      end
```

注：

- 同じ ASR 5500 で P-GW サービスをコロケーションするには、**gtpc bind address** コマンドで、P-GW サービスがバインドされているのと同じ IP アドレスを使用する必要があります。

GTP-U サービスの作成と設定

次の設定例を使用して、GTP-U サービスを作成します。

```
configure
   context <pgw_context_name>
      gtpu-service <gtpu_service_name> -noconfirm
         bind ipv4-address <s5s8_interface_address>
         end
```

注：

- **bind** コマンドは、**ipv6-address** コマンドを使用して IPv6 アドレスとしても指定できます。

P-GW PDN コンテキストの作成

P-GW PDN コンテキストおよびイーサネット インターフェイスを作成し、インターフェイスを設定済みのイーサネットポートにバインドするには、次の例を使用します。

```
configure
   context <pdn_context_name> -noconfirm
      interface <sgi_ipv4_interface_name>
         ip address <ipv4_address>
      interface <sgi_ipv6_interface_name>
         ipv6 address <address>
         end
```

P-GW サービス設定

手順

ステップ 1 「P-GW サービスの設定 （16 ページ）」の設定例を適用して、P-GW サービスを設定します。

ステップ 2 「固定 IP ルートの設定 （17 ページ）」の設定例を適用して、eGTP サービングゲートウェイへの IP ルートを指定します。

P-GW サービスの設定

次の例を使用して、P-GW サービスを設定します。

```
configure
   context <pgw_context_name>
      pgw-service <pgw_service_name> -noconfirm
           plmn id mcc <id> mnc <id>
           associate egtp-service <egtp_service_name>
```

```
associate qci-qos-mapping <name>
end
```

注：

- QCI-QoS マッピング設定は AAA コンテキストで作成されます。詳細については、QCI-QoS マッピングの設定 （21 ページ）を参照してください。
- 同じ ASR 5500 で P-GW サービスをコロケーションするには、P-GW サービス内で **associate pgw-service** *name* コマンドを設定する必要があります。

固定 IP ルートの設定

次の例を使用して、eGTP サービングゲートウェイとのコントロールプレーンおよびユーザープレーンのデータ通信の IP ルートを設定します。

```
configure
  context <pgw_context_name>
    ip route <sgw_ip_addr/mask> <sgw_next_hop_addr> <pgw_intrfc_name>
    end
```

P-GW PDN コンテキストの設定

次の例を使用して、IP プールと APN を設定し、PDN コンテキストのインターフェイスにポートをバインドします。

```
configure
  context <pdn_context_name> -noconfirm
    interface <sgi_ipv4_interface_name>
      ip address <ipv4_address>
      exit
    interface <sgi_ipv6_interface_name>
      ip address <ipv6_address>
      exit
    ip pool <name> range <start_address end_address> public <priority>
    ipv6 pool <name> range <start_address end_address> public <priority>
    subscriber default
      exit
    ip access-list <name>
      redirect css service <name> any
      permit any
      exit
    ipv6 access-list <name>
      redirect css service <name> any
      permit any
      exit
      aaa group default
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <sgi_ipv4_interface_name> <pdn_context_name>
    exit
```

```
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <sgi_ipv6_interface_name> <pdn_context_name>
    end
```

アクティブ課金サービス設定

アクティブ課金を有効化および設定するには、次の例を使用します。

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule>
        .
        .
      <rule>
      exit
    ruledef default
      ip any-match = TRUE
      exit
    ruledef icmp-pkts
      icmp any-match = TRUE
      exit
    ruledef qci3
       icmp any-match = TRUE
      exit
    ruledef static
      icmp any-match = TRUE
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    charging-action icmp
      billing-action egcdr
      exit
    charging-action qci3
      content-id <id>
      billing-action rf
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft packet-filter qci3
      exit
    charging-action static
      service-identifier <id>
      billing-action rf
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft packet-filter qci3
```

```
      exit
    packet-filter <packet_filter_name>
      ip remote-address = { <ipv4/ipv6_address> | <ipv4/ipv6_address/mask> }
      ip remote-port { = <port_number> | range <start_port_number> to
<end_port_number> }
      exit
    rulebase default
             exit
    rulebase <name>
      <rule_base>
        .
        .
      <rule_base>
      exit
    rulebase <gx_rulebase_name>
      dynamic-rule order first-if-tied
      egcdr tariff minute <minute> hour <hour>(optional)
      billing-records egcdr
      action priority 5 dynamic-only ruledef qci3 charging-action qci3
      action priority 100 ruledef static charging-action static
      action priority 500 ruledef default charging-action icmp
      action priority 570 ruledef icmp-pkts charging-action icmp
      egcdr threshold interval <interval>
      egcdr threshold volume total <bytes>
      end
```

注：

- ルールベースとは、ルール定義および関連する課金アクションの集合です。
- 上記のように、複数のルール定義、課金アクション、およびルールベースを設定して、さまざまな課金シナリオをサポートできます。
- 課金アクションは、ルール定義が一致したときに実行するアクションを定義します。
- ルーティングルールや課金ルールの定義を作成および設定できます。作成できるルーティングルール定義の最大数は 256 です。課金ルール定義の最大数は 2048 です。
- Gz アカウンティングの場合、charge-action *qc13*、*icmp*、および *static* の例にある billing-action egcdr コマンドが必要です。
- Gz ルールベースの例では、オフライン課金用の Gz インターフェイスがサポートされます。Gz アカウンティングには、**billing-records egcdr** コマンドが必要です。その他のコマンドはすべてオプションです。

重要 専用ベアラーでアップリンクパケットを受信している場合は、専用ベアラーにインストールされているルールだけが照合されます。静的ルールは一致せず、一致しないパケットはドロップされます。

ポリシーの設定

手順

ステップ 1 「AAA コンテキストの作成と設定 （20 ページ）」の設定例を適用して、ポリシーとアカウンティングのインターフェイスを設定します。

ステップ 2 「QCI-QoS マッピングの設定 （21 ページ）」に記載されている設定例を適用して、QCI から QoS へのマッピングを作成し、設定します。

AAA コンテキストの作成と設定

次の例を使用して、Diameter サポートとポリシー制御を含む AAA コンテキストを作成および設定し、このコンテキストと PCRF、OCS、および OFCS 間のトラフィックをサポートしているインターフェイスにイーサネットポートをバインドします。

```
configure
  context <aaa_context_name> -noconfirm
    interface <gx_interface_name>
      ipv6 address <address>
      exit
    interface <gy_interface_name>
      ipv6 address <address>
      exit
    interface <gz_interface_name>
      ip address <ipv4_address>
      exit
    interface <rf_interface_name>
      ip address <ipv4_address>
      exit
    subscriber default
      exit
    ims-auth-service <gx_ims_service_name>
      p-cscf discovery table <#> algorithm round-robin
      p-cscf table <#> row-precedence <#> ipv6-address <pcrf_ipv6_adr>
      policy-control
        diameter origin endpoint <gx_cfg_name>
        diameter dictionary <name>
        diameter host-select table <#> algorithm round-robin
       diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

        exit
      exit
    diameter endpoint <gx_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv6_address>
      peer <gx_cfg_name> realm <name> address <pcrf_ipv4_or_ipv6_addr>
      route-entry peer <gx_cfg_name>
```

```
      exit
    diameter endpoint <gy_cfg_name>
      origin realm <realm_name>
      origin host <name> address <gy_ipv6_address>
      connection retry-timeout <seconds>
      peer <gy_cfg_name> realm <name> address <ocs_ipv4_or_ipv6_addr>
      route-entry peer <gy_cfg_name>
      exit
    diameter endpoint <rf_cfg_name>
      use-proxy
      origin realm <realm_name>
      origin host <name> address <rf_ipv4_address>
      peer <rf_cfg_name> realm <name> address <ofcs_ipv4_or_ipv6_addr>
      route-entry peer <rf_cfg_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gx_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gy_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gz_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <rf_interface_name> <aaa_context_name>
    end
```

注：

- **ims-auth-service** の下の **p-cscf table** コマンドでも、PCRF に IPv4 アドレスを指定できます。
- Gx インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。
- Gy インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。
- Rf インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。

QCI-QoS マッピングの設定

QCI 値を作成し、適用可能な QoS パラメータにマッピングするには、次の例を使用します。

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
```

```
qci 3 user-datagram dscp-marking <hex>
qci 9 user-datagram dscp-marking <hex>
end
```

注：

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

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

  3GPP リリース 8 以降では、通信事業者固有/非標準の QCI がサポートされ、キャリアは QCI 128- 254 を定義できます。

- 上記の設定は、1 つのキーワードの例のみを示しています。**qci** コマンドおよびサポートされるその他のキーワードの詳細については、『*Command Line Interface Reference*』の「*QCI - QOS Mapping Configuration Mode Commands*」[英語] の章を参照してください。

設定の確認と保存

Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

DHCP サービス設定

システムは、動的ホスト制御プロトコル（DHCP）を使用して PDP コンテキストに IP アドレスを割り当てるように設定できます。DHCP を使用した IP アドレスの割り当ては、APN での設定に従い、次の方法で行います。

DHCP プロキシ：システムはクライアント（MS）のプロキシとして機能し、クライアント（MS）に代わって DHCP 検出要求を開始します。DHCP 検出要求への応答で DHCP サーバーから割り当てられた IP アドレスを受信すると、受け取った IP アドレスを MS に割り当てます。割り当てられたこのアドレスは、システムの IP アドレスプールに設定されているアドレスと一致している必要があります。この手順全体は MS からは認識できません。

メモリ内のアドレス数が減少すると、システムは DHCP サーバーに追加のアドレスを要求します。メモリに保存されているアドレスの数が設定された制限を超えると、それらは DHCP サーバーに返却されます。

通信先 DHCP サーバーと IP アドレスの処理方法を指定するパラメータを最初に設定する必要があります。これらのパラメータは、DHCP サービスの一部として設定されます。

重要 ここでは、DHCP ベースの IP 割り当てのために DHCP サービスを設定する際に必要な最小限の命令セットについて説明します。追加の DHCP サーバーパラメータとこれらのコマンドの動作を設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*DHCP Service Configuration Mode Commands*」の章を参照してください。

以下の手順は、『システム管理ガイド』で説明されているシステムレベルの設定と、この章の「*eGTP P-GW* 設定」セクションで説明されている P-GW サービスがすでに設定済みであることを前提としています。

DHCP サービスを設定するには、次の手順を実行します。

手順

ステップ 1 システムコンテキストで DHCP サービスを作成し、「DHCP サービスの作成 （23 ページ）」の設定例を適用してバインドします。

ステップ 2 「DHCP サーバーパラメータ設定 （24 ページ）」の設定例を適用して、DHCP サーバーと、DHCP サーバーからの応答で受け入れられる最小および最大の許容リース時間を設定します。

ステップ 3 DHCPv6 サービス設定の確認 （29 ページ） の手順に従って、DHCP サービスの設定を確認します。

ステップ 4 「設定の確認と保存」セクションの説明に従って、設定を保存します。

DHCP サービスの作成

DHCP ベースのアドレス割り当てをサポートするように DHCP サービスを作成するには、次の例を使用します。

```
configure
   context <dest_ctxt_name>
      dhcp-service <dhcp_svc_name>
         bind address <ip_address> [nexthop-forwarding-address
<nexthop_ip_address> [mpls-label input <in_mpls_label_value> output
<out_mpls_label_value1> [out_mpls_label_value2]]]
         end
```

注：

- 適切に動作させるには、DHCP 機能を接続先コンテキスト内で設定する必要があります。
- オプションのキーワード **nexthop-forwarding-address** *<nexthop_ip_address>* **[mpls-label input** *<in_mpls_label_value>* **output** *<out_mpls_label_value1>* **[** *out_mpls_label_value2* **]]** により、MPLS トラフィックでの DHCP が適用されます。

DHCP サーバーパラメータ設定

DHCP ベースのアドレス割り当てをサポートするように DHCP サーバーパラメータを設定するには、次の例を使用します。

```
configure
   context <dest_ctxt_name>
      dhcp-service <dhcp_svc_name>
         dhcp server <ip_address> [priority <priority>
         dhcp server selection-algorithm {first-server | round-robin}
         lease-duration min <minimum_dur> max <max_dur>
         dhcp deadtime <max_time>
         dhcp detect-dead-server consecutive-failures <max_number>
         max-retransmissions <max_number>
         retransmission-timeout <dur_sec>
         end
```

注：

- 複数の DHCP サービスを設定できます。**dhcp server** コマンドを複数回入力することで、各サービスに複数の DHCP サーバーを構成できます。最大 225 の DHCP サービスを構成でき、それぞれの DHCP サービスには最大 8 つの DHCP サーバーを構成できます。
- **dhcp detect-dead-server** コマンドと **max-retransmissions** コマンドは、相互に連携して動作します。
- retransmission-timeout コマンドは **max-retransmissions** コマンドと連携して動作します。

DHCP サービス設定の確認

手順

ステップ 1 EXEC モードで次のコマンドを入力して、DHCP サーバーが正しく設定されていることを確認します。

```
show dhcp service all
```

このコマンドは、次に示すような出力を生成します。この例では、DHCP 名は *dhcp1* です。

```
Service name:                       dhcp1
Context:                                    isp
Bind:                                       Done
Local IP Address:                           150.150.150.150
Next Hop Address:                           192.179.91.3
              MPLS-label:
               Input:                       5000
         Output:                            1566    1899
Service Status:                             Started
Retransmission Timeout:                     3000 (milli-secs)
Max Retransmissions:                        2
Lease Time:                                 600 (secs)
Minimum Lease Duration:                     600 (secs)
Maximum Lease Duration:                     86400 (secs)
DHCP Dead Time:                             120 (secs)
DHCP Dead consecutive Failure:              5
```

```
DHCP T1 Threshold Timer:                  50
DHCP T2 Threshold Timer:                  88
DHCP Client Identifier:                   Not Used
DHCP Algorithm:                           Round Robin
DHCP Servers configured:
 Address: 150.150.150.150                 Priority: 1
DHCP server rapid-commit:                 disabled
DHCP client rapid-commit:                 disabled
DHCP chaddr validation:                   enabled
```

ステップ 2 EXEC モードで次のコマンドを入力して、DHCP サービスのステータスを確認します。

show dhcp service status

DHCPv6 サービス設定

IPv6 の Dynamic Host Configuration Protocol（DHCP）が表示されるようにシステムを設定し、IPv6 ネットワークアドレスなどの設定パラメータを IPv6 ノードに渡すことができます。DHCPv6 の設定は APN 内で行います。

以下の手順は、『*System Administration Guide*』で説明されているシステムレベルの設定と P-GW PDN コンテキストの設定 （45 ページ）で説明されている APN がすでに設定済みであることを前提としています。

DHCPv6 サービスを設定するには、次の手順を実行します。

手順

ステップ 1 システムコンテキストで DHCPv6 サービスを作成し、DHCPv6 サービスの作成 （25 ページ）の設定例を適用してバインドします。

ステップ 2 DHCPv6 サーバーパラメータ設定 （26 ページ）の設定例を適用して、DHCPv6 サーバーや、更新時間、再バインド時間、優先ライフタイム、有効なライフタイムに関する設定可能なその他の値を設定します。

ステップ 3 DHCPv6 クライアントパラメータ設定 （27 ページ）の設定例を適用して、DHCPv6 クライアントや、最大再送信回数、サーバーのデッド回数、サーバーの復帰時間に関するその他の設定可能な値を設定します。

ステップ 4 DHCPv6 プロファイル設定 （27 ページ）の設定例を適用して、DHCPv6 プロファイルを設定します。

ステップ 5 DHCPv6 設定の関連付け （29 ページ）の設定例を適用して、DHCPv6 プロファイルの設定を APN に関連付けます。

ステップ 6 DHCPv6 サービス設定の確認 （29 ページ）の手順に従って、DHCPv6 サービスの設定を確認します。

ステップ 7 「設定の確認と保存」の章の説明に従って、設定を保存します。

DHCPv6 サービスの作成

DHCP ベースのアドレス割り当てをサポートするように DHCPv6 サービスを作成するには、次の例を使用します。

```
configure
  context <dest_ctxt_name>
    dhcpv6-service <dhcpv6_svc_name>
      bind address <ipv6_address> port <port>
      end
```

注：

- 適切に動作させるには、DHCPv6 機能を接続先コンテキスト内で設定する必要があります。
- ポートはリッスンポートを指定し、そのポートにバインドされたDHCPv6サーバーを起動するために使用されます。これはオプションであり、指定されていない場合、デフォルトのポートは 547 です。

（注） DHCPv6インターフェイスにはリンクローカルアドレスとユニキャストアドレスのみを使用します

DHCPv6 サーバーパラメータ設定

DHCPv6ベースのアドレス割り当てをサポートするようにDHCPv6サーバーパラメータを設定するには、次の例を使用します。

```
configure
  context <dest_ctxt_name>
    dhcpv6-service <dhcpv6_svc_name>
      dhcpv6-server
      renew-time <renewal_time>
      rebind-time <rebind_time>
      preferred-lifetime <pref_lifetime>
      valid-lifetime <valid_lifetime>
      end
```

注：

- **dhcp server** コマンドを複数回入力することで、複数の DHCP を設定できます。システムごとに（タイプに関係なく）最大 256 のサービスを設定できます。
- **renew-time** は、DHCP サービスによって割り当てられるプレフィックスの更新時間を設定します。デフォルトは 900 秒です。
- **rebind-time** は、DHCP サービスによって割り当てられるプレフィックスの再バインド時間を設定します。デフォルトは 900 秒です。
- **preferred-lifetime** は、DHCP サービスによって割り当てられるプレフィックスの優先ライフタイムを設定します。デフォルトは 900 秒です。
- **valid-lifetime** は、DHCP サービスによって割り当てられるプレフィックスの有効なライフタイムを設定します。デフォルトは 900 秒です。

DHCPv6 クライアントパラメータ設定

DHCPv6 ベースのアドレス割り当てをサポートするように DHCPv6 クライアントパラメータを設定するには、次の例を使用します。

```
configure
   context <dest_ctxt_name>
      dhcpv6-service <dhcpv6_svc_name>
         dhcpv6-client
            server-ipv6-address <ipv6_addr> port <port> priority <priority>
            max-retransmissions <max_number>
            server-dead-time <dead_time>
            server-resurrect-time <revive_time>
            end
```

注：

- DHCPv6 クライアントの設定には、IPv6 アドレス、ポート、および優先順位が必要です。ポートは DHCPv6 サーバーとの通信に使用されます。指定しない場合、デフォルトのポート 547 が使用されます。優先順位パラメータでは、試行するサーバーの優先順位を定義します。
- **max-retransmissions**：DHCPV6 クライアントが DHCPV6 サーバーに対して行う再送信の最大回数を設定します。デフォルトは 20 です。
- **server-dead-time**：PDN DHCPV6 サーバーは、クライアントから指定回数だけ試行しても応答しない場合、デッドと見なされます。デフォルトは 5 です。
- **server-resurrect-time**：PDN DHCPV6 サーバーは、指定された秒数のデッド状態後にアライブ状態と見なされます。デフォルトは 20 です。

DHCPv6 プロファイル設定

DHCPv6 プロファイルを設定するには、次の例を使用します。

```
configure
   context <dest_ctxt_name>
      dhcp-server-profile <server_profile>
         enable rapid-commit-dhcpv6
         process dhcp-option-from { AAA | LOCAL | PDN-DHCP } priority
<priority>
         dhcpv6-server-preference <pref_value>
         enable dhcpv6-server-unicast
         enable dhcpv6-server-reconf
         exit
      dhcp-client-profile <client_profile>
         dhcpv6-client-unicast
         client-identifier { IMSI | MSISDN }
         enable rapid-commit-dhcpv6
         enable dhcp-message-spray
         request dhcp-option dns-address
         request dhcp-option netbios-server-address
```

```
request dhcp-option sip-server-address
end
```

注：

- **dhcp-server-profile** コマンドは、サーバープロファイルを作成し、DHCP サーバープロファイル コンフィギュレーション モードを開始します。
- **enable rapid-commit-dhcpv6** コマンドは、DHCPv6 サーバーで高速コミットを有効にします。デフォルト設定は無効です。ネットワーク内に複数の DHCPv6 サーバーがある場合、rapid-commit-option を使用してこれを実行すると、UE のリソースすべてが確実に予約されます。
- **process dhcp-option-from** コマンドは、特定のクライアント要求に対して設定オプションを処理する順序を設定します。特定のクライアント設定の場合、値は AAA、PDN-DHCP-SERVER、LOCAL から取得できます。デフォルトでは、AAA が PDN-DHCP よりも優先され、PDN-DHCP は LOCAL の設定よりも優先されます。
- **dhcpv6-server-preference**：RFC-3315 に従って、DHCPv6-CLIENT は DHCPv6-SERVERS からのクエリへの応答を検討する前に、指定された時間だけ待機する必要があります。サーバーがプリファレンス値 255 で応答した場合、DHCPv6-CLIENT はそれ以上待つ必要はありません。デフォルト値は 0 で、1 ～ 255 の任意の整数を設定できます。
- **enable dhcpv6-server-unicast** コマンドは、DHCPv6 のサーバー ユニキャスト オプションを有効にします。デフォルトでは、無効になっています。
- **enable dhcpv6-server-reconf** コマンドは、サーバーからの再設定メッセージのサポートを設定します。デフォルトでは、無効になっています。
- **dhcpv6-client-unicast** コマンドを指定すると、クライアントはサーバーに向けてユニキャストアドレスでメッセージを送信できるようになります。
- **dhcp-client-profile** コマンドは、クライアントプロファイルを作成し、DHCP クライアント プロファイル コンフィギュレーション モードを開始します。
- **client identifier** コマンドは、外部 DHCP サーバーに送信されるクライアント識別子を設定します。デフォルトでは、IMSI が送信されます。もう 1 つの使用可能なオプションとして電話番号があります。
- **enable rapid-commit-dhcpv6** コマンドは、クライアントの高速コミットを設定します。デフォルトでは、DHCPv4 と DHCPv6 の両方で高速コミットオプションが有効になっています。
- **enable dhcp-message-spray** コマンドを指定すると、DHCP クライアントは、PDN 内で設定されているすべての DHCP サーバーに DHCP メッセージを配信できるようになります。デフォルトでは無効になっています。高速コミットで DHCP メッセージを送信できるサーバーは 1 つだけです。
- **request dhcp-option** コマンドは、DHCP クライアントが要求できる DHCP オプションを設定します。次のオプションを使用できます。
  - dns-address

- netbios-server-address
- sip-server-address

DHCPv6 設定の関連付け

DHCPv6 プロファイルを APN に関連付けるには、次の例を使用します。

```
configure
   context dest_ctxt_name
      apn apn_name
         dhcpv6 service-name dhcpv6_svc_name server-profile server_profile
client-profile client_profile
        dhcpv6 ip-address-pool-name dhcpv6_ip_pool allow-static-allocation

        dhcpv6 context-name <dest_ctxt>
        end
```

注：

- **dhcpv6 service-name** *dhcpv6_svc_name* **server-profile** *server_profile* **client-profile** *client_profile*：システムがDHCPv6サーバー コンフィギュレーションモードに移行できるようにします。このモードで DHCPv6 サーバーのパラメータを設定します。
- **dhcpv6 service-name** *dhcpv6_svc_name* **client-profile** *client_profile*：システムが DHCPv6 クライアント コンフィギュレーションモードに移行できるようにします。このモードでDHCPv6 クライアントのパラメータを設定します。
- **dhcpv6 ip-address-pool-name** *dhcpv6_ip_pool* **allow-static-allocation**：DHCPv6 プロファイルを APN と関連付けます。

（注） **allow-static-allocation** パラメータは、IPv6 プールを設定する場合にのみ使用します。

DHCPv6 サービス設定の確認

手順

ステップ 1 Exec モードで次のコマンドを入力して、DHCPv6 サーバーが正しく設定されていることを確認します。

```
show dhcpv6-service all
```

このコマンドは、次に示すような出力を生成します。この例では、DHCPv6 サービス名は *dhcp6-service* です。

```
Service name:               dhcpv6-service
Context:                            A
Bind Address:                       2092::192:90:92:40
```

```
Bind :                                Done
Service Status:                       Started
Server Dead Time:                     120 (secs)
Server Dead consecutive Failure:5
Server Select Algorithm:              First Server
Server Renew Time:                    400 (secs)
Server Rebind Time:                   500 (secs)
Server Preferred Life Time:           600 (secs)
Server Valid Life Time:               700 (secs)
Max Retransmissions:                  3 (secs)
Server Dead Tries:                    4 (secs)
Server Resurrect Time:                10 (secs)
ipv6_nd_flag:                         O_FLAG
DHCPv6 Servers configured:
         Address:                     2092::192:90:92:40 Priority: 1    enabled
```

ステップ 2 Exec モードで次のコマンドを入力して、DHCPv6 サービスのステータスを確認します。

show dhcpv6 status service *dhcpv6_service_name*

LTE-SAE ネットワークでのスタンドアロン PMIP P-GW としてのシステムの設定

ここでは、LTE-SAE テスト環境で P-MIP P-GW として動作するようにシステムを設定するための一連の手順の概要と、関連する構成ファイルの例を示します。構成ファイルの完全な例については、付録「サンプル構成ファイル」を参照してください。ここでは次の内容について説明します。

必要な情報

以降のセクションでは、P-GW を設定し、ネットワーク上で動作させるために必要な最小限の情報について説明します。プロセスをより効率的なものにするため、システムを設定する前にこの情報を用意しておくことを推奨します。

ここでは説明していないその他の設定パラメータがあります。これらのパラメータは、主にネットワークでの P-GW の動作の微調整に対応します。これらのパラメータの詳細については、『*Command Line Interface Reference*』[英語] の該当するセクションを参照してください。

必要なローカルコンテキスト設定情報

次の表に、P-GW でローカルコンテキストを設定するために必要な情報を示します。

表 *5:* ローカルコンテキストの設定に必要な情報

必要な情報	説明
管理インターフェイスの設定	
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	管理インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
セキュリティ管理者名	システムに対して完全な権限を持つセキュリティ管理者の名前。
セキュリティ管理者のパスワード	オープンパスワードまたは暗号化パスワードを使用できます。
リモートアクセスタイプ	システムへのアクセスに使用するリモートアクセスプロトコルのタイプ（SSH など）。

必要な P-GW コンテキスト設定情報

次の表に、P-GW で P-GW コンテキストを設定するために必要な情報を示します。

表 *6: P-GW* コンテキストの設定に必要な情報

必要な情報	説明
P-GW コンテキスト名	システムが P-GW コンテキストを認識するために使用する 1 ～ 79 文字（英字または数字）の識別文字列。
アカウンティングポリシー名	システムがアカウンティングポリシーを認識するために使用する 1 ～ 79 文字（英字または数字）の識別文字列。アカウンティングポリシーは、Rf（オフライン課金）インターフェイスのパラメータを設定するために使用されます。
S5/S8 インターフェイスの設定（S-GW 間）	

必要な情報	説明
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
P-GW サービス設定	
P-GW サービス名	システムが P-GW サービスを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。 複数の P-GW サービスを使用する場合は、複数の名前が必要です。
LMA サービスの設定	
LMA サービス名	システムが LMA サービスを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。

必要な PDN コンテキスト設定情報

次の表に、P-GW で PDN コンテキストを設定するために必要な情報を示します。

表 *7: PDN* コンテキストの設定に必要な情報

必要な情報	説明
P-GW コンテキスト名	システムが P-GW コンテキストを認識するために使用する 1 ～ 79 文字（英字と数字）の識別文字列。
IP アドレスプールの設定	

必要な情報	説明
IPv4アドレスプールの名前と範囲	システムが IPv4 プールを認識するために使用する 1 ～ 31 文字（英字数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義されるIPv4アドレスの範囲
IPv6アドレスプールの名前と範囲	システムが IPv6 プールを認識するために使用する 1 ～ 31 文字（英字数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義されるIPv6アドレスの範囲
アクセス制御リストの設定	
IPv4 アクセスリスト名	システムが IPv4 アクセスリストを認識するために使用する 1 ～ 47 文（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。
IPv6 アクセスリスト名	システムが IPv6 アクセスリストを認識するために使用する 1 ～ 79 文（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。
拒否/許可タイプ	タイプは次のとおりです。 • any • ホスト IP アドレスによる • IP パケットによる • 送信元 ICMP パケットによる • 送信元 IP アドレスマスキングによる • TCP/UDP パケットによる
アドレス再指定またはリダイレクトタイプ	タイプは次のとおりです。 • アドレス再指定サーバー • コンテキストのリダイレクト • CSS 配信シーケンスのリダイレクト • redirect css service コマンドで使用可能なキーワードとオプションついては、『Command Line Interface Reference』の • redirect nexthop

必要な情報	説明
SGi インターフェイスの設定（IPv4 PDN へ/IPv4 PDN から）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
SGi インターフェイスの設定（IPv6 PDN へ/IPv6 PDN から）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。

必要な AAA コンテキスト設定情報

次の表に、P-GW で AAA コンテキストを設定するために必要な情報を示します。

表 *8 : AAA* コンテキストの設定に必要な情報

必要な情報	説明
Gx インターフェイスの設定（PCRF 対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（ 字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 ア レス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネ トが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカ ドが取り付けられているシャーシスロット番号とその後に続くカード の物理コネクタの番号によって識別されます。たとえば、ポート 17/ は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルー を設定するときに使用されます。
Gx Diameter エンドポイントの設定	
エンドポイント名	Gx Diameter エンドポイントの設定がシステムによって認識される 1 ～ 63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはす ての Diameter メッセージに存在し、通常は会社名またはサービス名で す。
発信元ホスト名	Gx 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字 数字）の識別文字列。
元のホストアドレス	Gx インターフェイスの IP アドレス。
ピア名	上述の Gx エンドポイント名。
ピアレルム名	上述の Gx 発信元レルム名。
ピアのアドレスとポート番号	PCRF の IP アドレスとポート番号。
ルートエントリピア	上述の Gx エンドポイント名。
S6b インターフェイスの設定（3GPP AAA 対応）	

必要な情報	説明
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
S6b Diameter エンドポイントの設定	
エンドポイント名	S6b Diameter エンドポイント設定がシステムによって認識される 1 ー 63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameter アイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	S6b 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字や数字）の識別文字列。
元のホストアドレス	S6b インターフェイスの IP アドレス。
ピア名	上述の S6b エンドポイント名。
ピアレルム名	上述の S6b 発信元レルム名。
ピアのアドレスとポート番号	AAA サーバーの IP アドレスとポート番号。
ルートエントリピア	上述の S6b エンドポイント名。
Gy インターフェイスの設定（オンライン課金サーバー対応）	

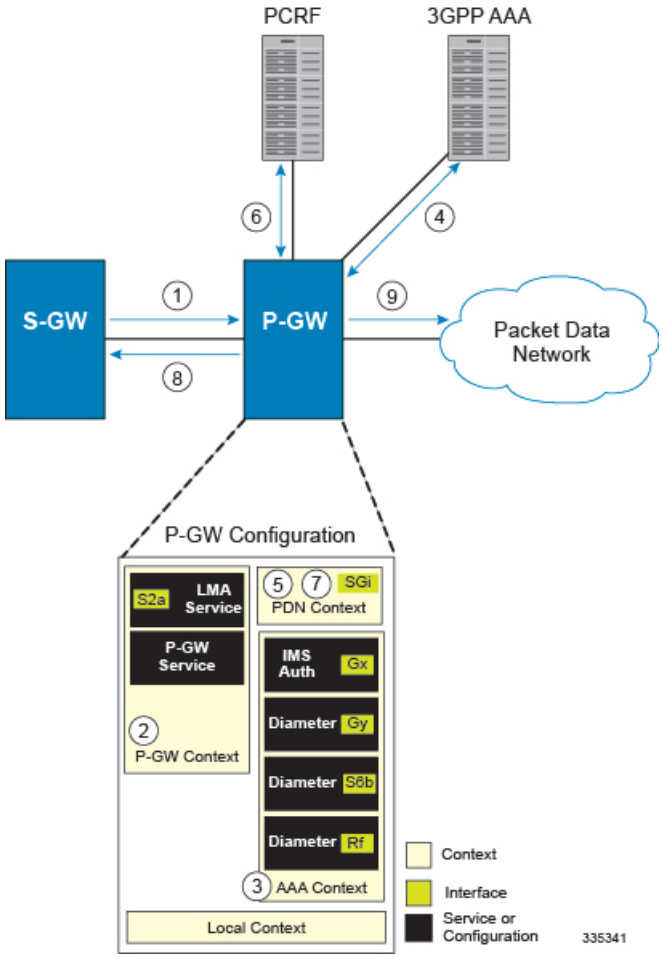
必要な情報	説明
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネトが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカドが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルーを設定するときに使用されます。
Gy Diameter エンドポイントの設定	
エンドポイント名	Gy Diameter エンドポイントの設定がシステムによって認識される 1～63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Gy 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字数字）の識別文字列。
元のホストアドレス	Gy インターフェイスの IP アドレス。
ピア名	上述の Gy エンドポイント名。
ピアレルム名	上述の Gy 発信元レルム名。
ピアのアドレスとポート番号	AAA サーバーの IP アドレスとポート番号。
ルートエントリピア	上述の Gy エンドポイント名。
Rf インターフェイスの設定（オフライン課金サーバーに対する）	

必要な情報	説明
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
Rf Diameter エンドポイントの設定	
エンドポイント名	Rf Diameter エンドポイントの設定がシステムによって認識される 1 ー 63 文字（英字や数字）の識別文字列。
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameter アイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Rf 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字や数字）の識別文字列。
元のホストアドレス	Rf インターフェイスの IP アドレス。
ピア名	上述の Rf エンドポイント名。
ピアレルム名	上述の Rf 発信元レルム名。
ピアのアドレスとポート番号	PCRF の IP アドレスとポート番号。
ルートエントリピア	上述の Rf エンドポイント名。

この設定が動作する仕組み

次の図と補足テキストは、PMIP LTE ネットワークから発信されるサブスクライバコールを処理するために、単一の送信元と接続先のコンテキストを持つこの設定がシステムによってどのように使用されるかを示しています。

図 *3 : LTE* ネットワークの *PMIP P-GW* の要素



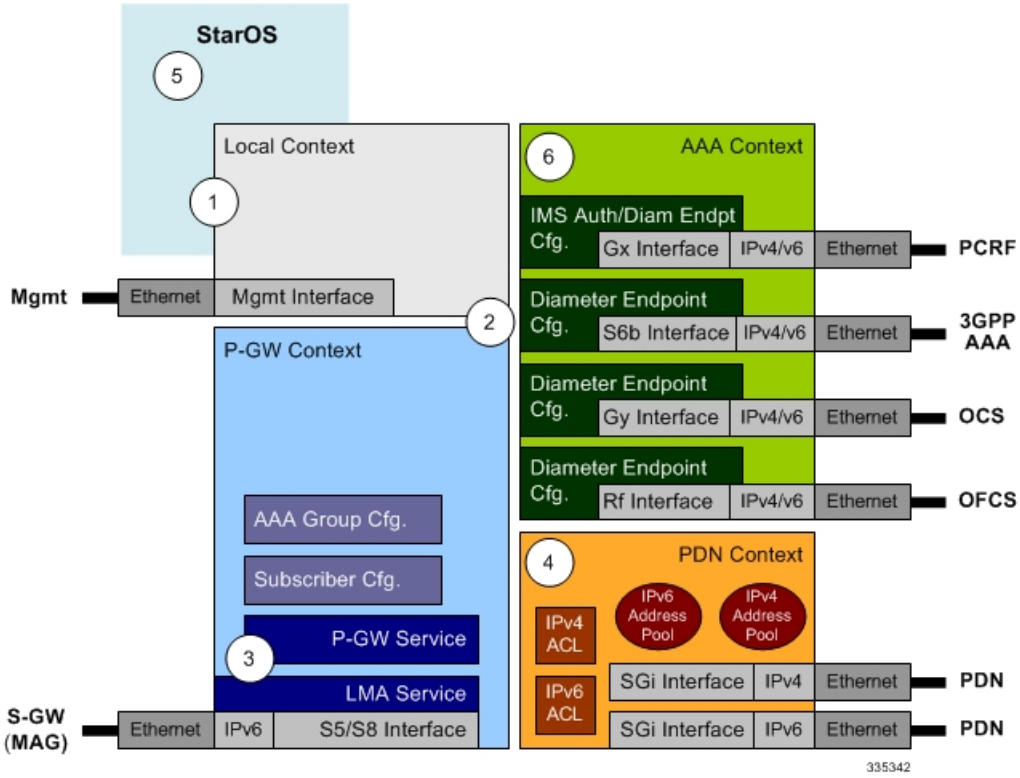
1. S-GW は、アクセスポイント名（APN）を含むセッション作成要求メッセージを P-GW に送信することにより、S5/S8 接続を確立します。
2. P-GW サービスは、セッションに AAA 機能を提供するために使用するコンテキストを決定します。このプロセスについては、『*System Administration Guide*』の「*Understanding the System Operation and Configuration*」の章にある「*How the System Selects Contexts*」の項で説明しています。
3. P-GW は、設定済みの Gx Diameter エンドポイントを使用して IP-CAN セッションを確立します。
4. P-GW は、IP-CAN セッションの確立を示すために CCRF に CC 要求（CCR）メッセージを送信し、PCRF は CC 応答（CCA）で確認応答します。

5. P-GW は APN 設定を使用して PDN コンテキストを選択します。選択した PDN コンテキストで設定された IP プールから IP アドレスが割り当てられます。
6. P-GW は、割り当てられたアドレスと追加情報を含むセッション作成応答メッセージで S-GW に応答します。
7. S5/S8 データプレーントンネルが確立され、P-GW は PDN との間でパケットを送受信できます。

P-MIP P-GW（LTE）設定

LTE-SAE ネットワーク環境でスタンドアロン P-MIP P-GW として動作するようにシステムを設定する場合は、次の図とその後の手順を確認してください。

図 *4 : PMIP P-GW*（*LTE*）が設定可能



手順

ステップ 1 『*System Administration Guide*』[英語] に記載されている設定例を適用して、PSC のアクティブ化などのシステム設定パラメータを設定します。

ステップ 2 「初期設定 （41 ページ）」に記載されている設定例を適用して、コンテキストやサービスの作成などの初期設定パラメータを設定します。

ステップ 3 システムを PMIP P-GW として動作するように設定し、「P-GW サービス設定 （44 ページ）」に記載されている設定例を適用して、PMIP インターフェイスや IP ルートなどの P-GW の基本的なパラメータを設定します。

ステップ 4 「P-GW PDN コンテキストの設定 （45 ページ）」の設定例を適用して、PDN コンテキストを設定します。

ステップ 5 「アクティブ課金サービス設定 （46 ページ）」の設定例を適用して、Gx インターフェイスのサポートのためのアクティブ課金サービスを有効にし、設定します。

ステップ 6 「AAA とポリシーの設定 （68 ページ）」の設定例を適用して、AAA コンテキストを作成し、AAA およびポリシーのパラメータを設定します。

ステップ 7 設定の確認と保存 （50 ページ） の手順に従って、設定を確認して保存します。

初期設定

手順

ステップ 1 「ローカルコンテキストの変更 （41 ページ）」の設定例を適用して、ローカルシステム管理パラメータを設定します。

ステップ 2 「P-MIP P-GW コンテキストの作成と設定 （42 ページ）」の設定例を適用して、P-GW サービスを配置したコンテキストを作成します。

ステップ 3 「P-GW コンテキストでの APN の作成と設定 （42 ページ）」の設定例を適用して、P-GW コンテキストで APN を作成および設定します。

ステップ 4 「P-GW コンテキストでの AAA グループの作成と設定 （43 ページ）」の設定例を適用して、P-GW コンテキストで AAA サーバーグループを作成および設定します。

ステップ 5 「LMA サービスの作成と設定 （44 ページ）」の設定例を適用して、新しく作成されたコンテキスト内のローカルモビリティアンカー（LMA）サービスを作成および設定します。

ステップ 6 「P-GW PDN コンテキストの作成 （44 ページ）」の設定例を適用して、PDN へのインターフェイスが配置されるコンテキストを作成します。

ローカルコンテキストの変更

デフォルトサブスクライバを設定し、ローカルコンテキストでリモートアクセス機能を設定するには、次の例を使用します。

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
        exit
      server ftpd
        exit
      server telnetd
        exit
```

```
      subscriber default
        exit
      administrator <name> encrypted password <password> ftp
      ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
      exit
  port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
    end
```

P-MIP P-GW コンテキストの作成と設定

次の例を使用して、P-GW コンテキストを作成し、S5 または S8 IPv6 インターフェイス（S-GW との間のデータトラフィック用）を作成し、S5 または S8 インターフェイスを設定済みのイーサネットポートにバインドします。

```
configure
  context <pgw_context_name> -noconfirm
    interface <s5s8_interface_name> tunnel
      ipv6 address <ipv6_address>
      tunnel-mode ipv6ip
      source interface <name>
      destination address <ipv6 address>
      exit
    exit

  policy accounting <rf_policy_name> -noconfirm
    accounting-level {level_type}
    accounting-event-trigger interim-timeout action stop-start
    operator-string <string>
    exit
  subscriber default
    exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5s8_interface_name> <pgw_context_name>
    end
```

注：

- S5 または S8（P-GW から S-GW）インターフェイスは、IPv6 アドレスである必要があります。
- Rf（オフライン課金）インターフェイスのアカウンティングポリシーを設定します。アカウンティングレベルのタイプは、Flow、PDN、PDN-QCI、QCI、および Subscriber です。このコマンドの詳細については、『*Command Line Interface Reference*』の「*Accounting Profile Configuration Mode Commands*」の章を参照してください。

P-GW コンテキストでの APN の作成と設定

次の設定を使用して、APN を作成します。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      ims-auth-service <gx_ims_service_name>
      aaa group <rf-radius_group_name>
      dns primary <ipv4_address>
      dns secondary <ipv4_address>
      ip access-group <name> in
      ip access-group <name> out
      mediation-device context-name <pgw_context_name>
      ip context-name <pdn_context_name>
      ipv6 access-group <name> in
      ipv6 access-group <name> out
      active-charging rulebase <name>
      end
```

注：

- IMS 承認サービスは、AAA コンテキストで作成および設定されます。
- 複数の APN を、異なるドメイン名をサポートするように設定できます。

P-GW コンテキストでの AAA グループの作成と設定

RADIUS および Rf アカウンティングをサポートする AAA グループを作成および設定するには、次の例を使用します。

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
    aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      end
```

LMA サービスの作成と設定

LMA サービスを作成するには、次の設定例を使用します。

```
configure
  context <pgw_context_name>
    lma-service <lma_service_name> -noconfirm
      no aaa accounting
      revocation enable
      bind address <s5s8_ipv6_address>
      end
```

注：

- **no aaa acounting** コマンドは、重複アカウンティングパケットを防止するために使用されます。
- 失効を有効にすると、MIP の失効が MAG とネゴシエートされて MIP バインディングが終了した場合に、MIP 登録の失効が可能になり、LMA は MAG に失効メッセージを送信できます。

P-GW PDN コンテキストの作成

P-GW PDN コンテキストおよびイーサネット インターフェイスを作成し、インターフェイスを設定済みのイーサネットポートにバインドするには、次の例を使用します。

```
configure
  context <pdn_context_name> -noconfirm
    interface <sgi_ipv4_interface_name>
      ip address <ipv4_address>
    interface <sgi_ipv6_interface_name>
      ipv6 address <address>
      end
```

P-GW サービス設定

手順

ステップ 1 「P-GW サービスの設定 （44 ページ）」の設定例を適用して、P-GW サービスを設定します。

ステップ 2 「固定 IP ルートの設定 （45 ページ）」の設定例を適用して、P-MIP サービングゲートウェイへの IP ルートを指定します。

P-GW サービスの設定

次の例を使用して、P-GW サービスを設定します。

```
configure
  context <pgw_context_name>
    pgw-service <pgw_service_name> -noconfirm
```

```
plmn id mcc <id> mnc <id>
associate lma-service <lma_service_name>
associate qci-qos-mapping <name>
authorize external
fqdn host <domain_name> realm <realm_name>
end
```

注：

- QCI-QoSマッピング設定はAAAコンテキストで作成されます。詳細については、「*QCI-QoS* マッピングの設定」の項を参照してください。
- 外部承認は、S6bインターフェイスを介して3GPP AAAサーバーによって実行されます。内部承認（APN）がデフォルトです。
- **fqdn host** コマンドは、S6bインターフェイスを介したP-GWと3GPP AAAサーバー間のメッセージで使用される、P-GWサービスの完全修飾ドメイン名を設定します。

固定 IP ルートの設定

P-GWとS-GW間のデータトラフィックのスタティックIPルートを設定するには、次の例に示すコマンドを使用します。

```
configure
  context <pgw_context_name>
    ipv6 route <ipv6_addr/prefix> next-hop <sgw_addr> interface
<pgw_sgw_intrfc_name>
    end
```

注：

- スタティック IP ルーティングは、ダイナミック ルーティング プロトコルを使用する設定には必要ありません。

P-GW PDN コンテキストの設定

次の例を使用して、IP プールと APN を設定し、PDN コンテキストのインターフェイスにポートをバインドします。

```
configure
  context <pdn_context_name> -noconfirm
    interface <pdn_sgi_ipv4_interface_name>
      ip address <ipv4_address>
      exit
    interface <pdn_sgi_ipv6_interface_name>
      ip address <ipv6_address>
      exit
    ip pool <name> range <start_address end_address> public <priority>
    ipv6 pool <name> range <start_address end_address> public <priority>
    subscriber default
    ip access-list <name>
      redirect css service <name> any
      permit any
```

```
    exit
  ipv6 access-list <name>
    redirect css service <name> any
    permit any
    exit
  aaa group default
    exit
  exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <pdn_ipv4_interface_name> <pdn_context_name>
  exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <pdn_ipv6_interface_name> <pdn_context_name>
  end
```

アクティブ課金サービス設定

アクティブ課金を有効化および設定するには、次の例を使用します。

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule>
        .
        .
      <rule>
      exit
    ruledef default
      ip any-match = TRUE
      exit
    ruledef icmp-pkts
      icmp any-match = TRUE
      exit
    ruledef qci3
       icmp any-match = TRUE
      exit
    ruledef static
      icmp any-match = TRUE
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    charging-action icmp
      billing-action egcdr
      exit
    charging-action qci3
```

```
        content-id <id>
        billing-action rf
        qos-class-identifier <id>
        allocation-retention-priority <priority>
        tft packet-filter qci3
        exit
      charging-action static
        service-identifier <id>
        billing-action rf
        qos-class-identifier <id>
        allocation-retention-priority <priority>
        tft packet-filter qci3
        exit
      packet-filter <packet_filter_name>
        ip remote-address = { <ipv4/ipv6_address> | <ipv4/ipv6_address/mask> }
        ip remote-port { = < port_number> | range <start_port_number> to
<end_port_number> }
        exit
      rulebase default
               exit
      rulebase <name>
        <rule_base>
           .
           .
        <rule_base>
        end
```

注：

- ルールベースとは、ルール定義および関連する課金アクションの集合です。
- 上記のように、複数のルール定義、課金アクション、およびルールベースを設定して、さまざまな課金シナリオをサポートできます。
- ルーティングルールや課金ルールの定義を作成および設定できます。作成できるルーティングルール定義の最大数は 256 です。課金ルール定義の最大数は 2048 です。
- 課金アクションは、ルール定義が一致したときに実行するアクションを定義します。

重要 専用ベアラーでアップリンクパケットを受信している場合は、専用ベアラーにインストールされているルールだけが照合されます。静的ルールは一致せず、一致しないパケットはドロップされます。

AAA とポリシーの設定

手順

ステップ 1 「AAA コンテキストの作成と設定 （48 ページ）」の設定例を適用して、AAA とポリシーのインターフェイスを設定します。

ステップ 2 「QCI-QoS マッピングの設定 （50 ページ）」の設定例を適用して、QCI から QoS へのマッピングを作成し、設定します。

AAA コンテキストの作成と設定

次の例を使用して、Diameter のサポートとポリシー制御を含む AAA コンテキストを作成および設定し、このコンテキストと PCRF 間のトラフィックをサポートしているインターフェイスにポートをバインドします。

```
configure
  context <aaa_context_name> -noconfirm
    interface <s6b_interface_name>
      ip address <ipv4_address>
      exit
    interface <gx_interface_name>
      ipv6 address <address>
      exit
    interface <gy_interface_name>
      ipv6 address <address>
      exit
    interface <rf_interface_name>
      ip address <ipv4_address>
      exit
    subscriber default
      exit
    ims-auth-service <gx_ims_service_name>
      p-cscf discovery table <#> algorithm round-robin
      p-cscf table <#> row-precedence <#> ipv6-address <pcrf_adr>
      policy-control
        diameter origin endpoint <gx_cfg_name>
        diameter dictionary <name>
        diameter host-select table <#> algorithm round-robin
       diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

        exit
      exit
    diameter endpoint <s6b_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv4_address>
      peer <s6b_cfg_name> realm <name> address <aaa_ipv4_addr>
      route-entry peer <s6b_cfg_name>
```

```
      exit
    diameter endpoint <gx_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv6_address>
      peer <gx_cfg_name> realm <name> address <pcrf_addr>
      route-entry peer <gx_cfg_name>
      exit
    diameter endpoint <gy_cfg_name>
      use-proxy
      origin realm <realm_name>
      origin host <name> address <gy_ipv6_address>
      connection retry-timeout <seconds>
      peer <gy_cfg_name> realm <name> address <ocs_ipv6_addr>
      route-entry peer <gy_cfg_name>
      exit
    diameter endpoint <rf_cfg_name>
      origin realm <realm_name>
      origin host <name> address <rf_ipv4_address>
      peer <rf_cfg_name> realm <name> address <ofcs_ipv4_addr>
      route-entry peer <rf_cfg_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s6b_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gx_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gy_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <rf_interface_name> <aaa_context_name>
    end
```

注：

- **ims-auth-service** の下の **p-cscf table** コマンドでも、PCRF に IPv4 アドレスを指定できます。
- S6b インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。
- Gx インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。
- Gy インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。

- Rf インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。

QCI-QoS マッピングの設定

QCI 値を作成し、適用可能な QoS パラメータにマッピングするには、次の例を使用します。

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
    qci 3 user-datagram dscp-marking <hex>
    qci 9 user-datagram dscp-marking <hex>
    end
```

注：

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

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

  3GPP リリース 8 以降では、通信事業者固有/非標準の QCI がサポートされ、キャリアは QCI 128- 254 を定義できます。

- 上記の設定は、1 つのキーワードの例のみを示しています。**qci** コマンドおよびサポートされるその他のキーワードの詳細については、『*Command Line Interface Reference*』の「*QCI - QOS Mapping Configuration Mode Commands*」[英語] の章を参照してください。

設定の確認と保存

Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

eHRPD ネットワークをサポートするスタンドアロン PMIP P-GW としてのシステムの設定

ここでは、テスト環境で eGTP P-GW として eHRPD のサポートを実行するようにシステムを設定するための一連の手順の概要と、関連する構成ファイルの例を示します。構成ファイルの完全な例については、付録「サンプル構成ファイル」を参照してください。ここでは次の内容について説明します。

- 必要な情報 （51 ページ）
- この設定が動作する仕組み （59 ページ）
- P-MIP P-GW（eHRPD）設定 （61 ページ）

必要な情報

以降のセクションでは、P-GW を設定し、ネットワーク上で動作させるために必要な最小限の情報について説明します。プロセスをより効率的なものにするため、システムを設定する前にこの情報を用意しておくことを推奨します。

ここでは説明していないその他の設定パラメータがあります。これらのパラメータは、主にネットワークでの P-GW の動作の微調整に対応します。これらのパラメータの詳細については、『*Command Line Interface Reference*』[英語] の該当するセクションを参照してください。

必要なローカルコンテキスト設定情報

次の表に、P-GW でローカルコンテキストを設定するために必要な情報を示します。

表 *9:* ローカルコンテキストの設定に必要な情報

必要な情報	説明
管理インターフェイス コンフィギュレーション	
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	管理インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
セキュリティ管理者名	システムに対して完全な権限を持つセキュリティ管理者の名前。
セキュリティ管理者のパスワード	オープンパスワードまたは暗号化パスワードを使用できます。
リモートアクセスタイプ	システムへのアクセスに使用するリモートアクセスプロトコルのタイプ（SSH など）。

必要な P-GW コンテキスト設定情報

次の表に、P-GW で P-GW コンテキストを設定するために必要な情報を示します。

表 *10 : P-GW* コンテキストの設定に必要な情報

必要な情報	説明
P-GW コンテキスト名	システムが P-GW コンテキストを認識するために使用する 1 ～ 79 文字（英字または数字）の識別文字列。
アカウンティングポリシー名	システムがアカウンティングポリシーを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。アカウンティングポリシーは、Rf（オフライン課金）インターフェイスのパラメータを設定するために使用されます。
S2a インターフェイスの設定（HSGW 間）	
インターフェイス名	システムがインターフェイスを認識するための 1 ～ 79 文字（英字または数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
P-GW サービス設定	
P-GW サービス名	システムが P-GW サービスを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。 複数の P-GW サービスを使用する場合は、複数の名前が必要です。
PLMN ID	MCC 番号：PLMN の識別子のモバイル国コード（MCC）部分（100 ～ 999 の整数値）。 MNC 番号：PLMN の識別子のモバイルネットワークコード（MNC）部分（00 ー 999 の 2 桁または 3 桁の整数値）。
LMA サービスの設定	
LMA サービス名	システムが LMA サービスを認識するために使用する 1 ～ 63 文字（英字または数字）の識別文字列。

必要な PDN コンテキスト設定情報

次の表に、P-GW で PDN コンテキストを設定するために必要な情報を示します。

表 *11 : PDN* コンテキストの設定に必要な情報

必要な情報	説明
P-GW コンテキスト名	システムが P-GW コンテキストを認識するために使用する 1 ～ 79 文字（英字と数字）の識別文字列。
IP アドレスプールの設定	
IPv4アドレスプールの名前と範囲	システムが IPv4 プールを認識するために使用する 1 ～ 31 文字（英字数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義される IPv4 アドレスの範囲
IPv6アドレスプールの名前と範囲	システムが IPv6 プールを認識するために使用する 1 ～ 31 文字（英字数字）の識別文字列。 複数のプールを設定する場合は、複数の名前が必要です。 開始アドレスと終了アドレスによって定義される IPv6 アドレスの範囲
アクセス制御リストの設定	
IPv4 アクセスリスト名	システムが IPv4 アクセスリストを認識するために使用する 1 ～ 47 文字（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。
IPv6 アクセスリスト名	システムが IPv6 アクセスリストを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のリストを設定する場合は、複数の名前が必要です。
拒否/許可タイプ	タイプは次のとおりです。 • any • ホスト IP アドレスによる • IP パケットによる • 送信元 ICMP パケットによる • 送信元 IP アドレスマスキングによる • TCP/UDP パケットによる

必要な情報	説明
アドレス再指定またはリダイレクトタイプ	タイプは次のとおりです。 • サーバーのアドレス再指定 • コンテキストのリダイレクト • CSS 配信シーケンスのリダイレクト • redirect css service コマンドで使用可能なキーワードとオプションについては、『Command Line Interface Reference』の • redirect nexthop
SGi インターフェイスの設定（IPv4 PDN へ/IPv4 PDN から）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
SGi インターフェイスの設定（IPv6 PDN へ/IPv6 PDN から）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。

必要な情報	説明
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。

必要な AAA コンテキスト設定情報

次の表に、P-GW で AAA コンテキストを設定するために必要な情報を示します。

表 *12 : AAA* コンテキストの設定に必要な情報

必要な情報	説明
Gx インターフェイスの設定（PCRF 対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカードの物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
Gx Diameter エンドポイントの設定	
エンドポイント名	Gx Diameter エンドポイントの設定がシステムによって認識される 1 ～ 63 文字（英字や数字）の識別文字列。

必要な情報	説明
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Gx 送信元ホストがシステムによって認識される、1 ～ 255 文字（英字や数字）の識別文字列。
元のホストアドレス	Gx インターフェイスの IP アドレス。
ピア名	上述の Gx エンドポイント名。
ピアレルム名	上述の Gx 発信元レルム名。
ピアのアドレスとポート番号	PCRF の IP アドレスとポート番号。
ルートエントリピア	上述の Gx エンドポイント名。
S6b インターフェイスの設定（3GPP AAA 対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
S6b Diameter エンドポイントの設定	
エンドポイント名	S6b Diameter エンドポイント設定がシステムによって認識される 1 ー 63 文字（英字や数字）の識別文字列。

必要な情報	説明
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはす ての Diameter メッセージに存在し、通常は会社名またはサービス名で す。
発信元ホスト名	S6b 送信元ホストがシステムによって認識される、1 ～ 255 文字（英 や数字）の識別文字列。
元のホストアドレス	S6b インターフェイスの IP アドレス。
ピア名	上述の S6b エンドポイント名。
ピアレルム名	上述の S6b 発信元レルム名。
ピアのアドレスとポート番号	AAA サーバーの IP アドレスとポート番号。
ルートエントリピア	上述の S6b エンドポイント名。
Rf インターフェイスの設定（オフライン課金サーバーに対する）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（ 字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 ア レス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネ トが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカ ドが取り付けられているシャーシスロット番号とその後に続くカード の物理コネクタの番号によって識別されます。たとえば、ポート 17/ は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	管理インターフェイスから特定のネットワークへのスタティック IP ル トを設定するときに使用されます。
Rf Diameter エンドポイントの設定	
エンドポイント名	Rf Diameter エンドポイントの設定がシステムによって認識される 1 ～ 63 文字（英字や数字）の識別文字列。

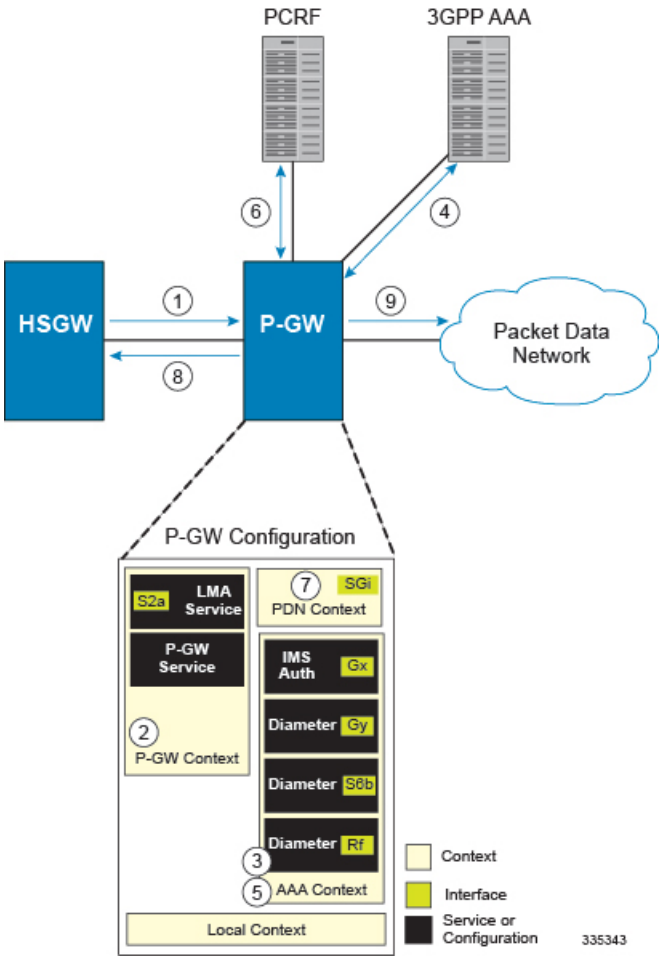
必要な情報	説明
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Rf送信元ホストがシステムによって認識される、1 ～ 255 文字（英字や数字）の識別文字列。
元のホストアドレス	Rf インターフェイスの IP アドレス。
ピア名	上述の Rf エンドポイント名。
ピアレルム名	上述の Rf 発信元レルム名。
ピアのアドレスとポート番号	OFCS の IP アドレスとポート番号。
ルートエントリピア	上述の Rf エンドポイント名。
Gy インターフェイスの設定（オンライン課金サーバー対応）	
インターフェイス名	システムがインターフェイスを認識するために使用する 1 ～ 79 文字（英字や数字）の識別文字列。 複数のインターフェイスを設定する場合は、複数の名前が必要です。
IP アドレスとサブネット	インターフェイスに割り当てられている IPv4 アドレスまたは IPv6 アドレス。 複数のインターフェイスを設定する場合は、複数のアドレスとサブネットが必要です。
物理ポート番号	インターフェイスがバインドされる物理ポート。ポートは、ラインカードが取り付けられているシャーシスロット番号とその後に続くカード上の物理コネクタの番号によって識別されます。たとえば、ポート 17/1 は、スロット 17 にあるカードのコネクタ番号 1 を示します。 単一の物理ポートで複数のインターフェイスに対応できます。
ゲートウェイ IP アドレス	インターフェイスから特定のネットワークへのスタティック IP ルートを設定するときに使用されます。
Gy Diameter エンドポイントの設定	
エンドポイント名	Gy Diameter エンドポイントの設定がシステムによって認識される 1 ー 63 文字（英字や数字）の識別文字列。

必要な情報	説明
発信元レルム名	1 ～ 127 文字の識別文字列。 このレルムは、Diameterアイデンティティです。発信者のレルムはすべての Diameter メッセージに存在し、通常は会社名またはサービス名です。
発信元ホスト名	Gy送信元ホストがシステムによって認識される、1 ～ 255 文字（英字数字）の識別文字列。
元のホストアドレス	Gy インターフェイスの IP アドレス。
ピア名	上述の Gy エンドポイント名。
ピアレルム名	上述の Gy 発信元レルム名。
ピアのアドレスとポート番号	OCS の IP アドレスとポート番号。
ルートエントリピア	上述の Gy エンドポイント名。

この設定が動作する仕組み

次の図と補足テキストは、GTP LTE ネットワークから発信されるサブスクライバコールを処理するために、単一の送信元と接続先のコンテキストを持つこの設定がシステムによってどのように使用されるかを示しています。

図 *5 : eHRPD* ネットワークをサポートする *PMIP P-GW* の要素



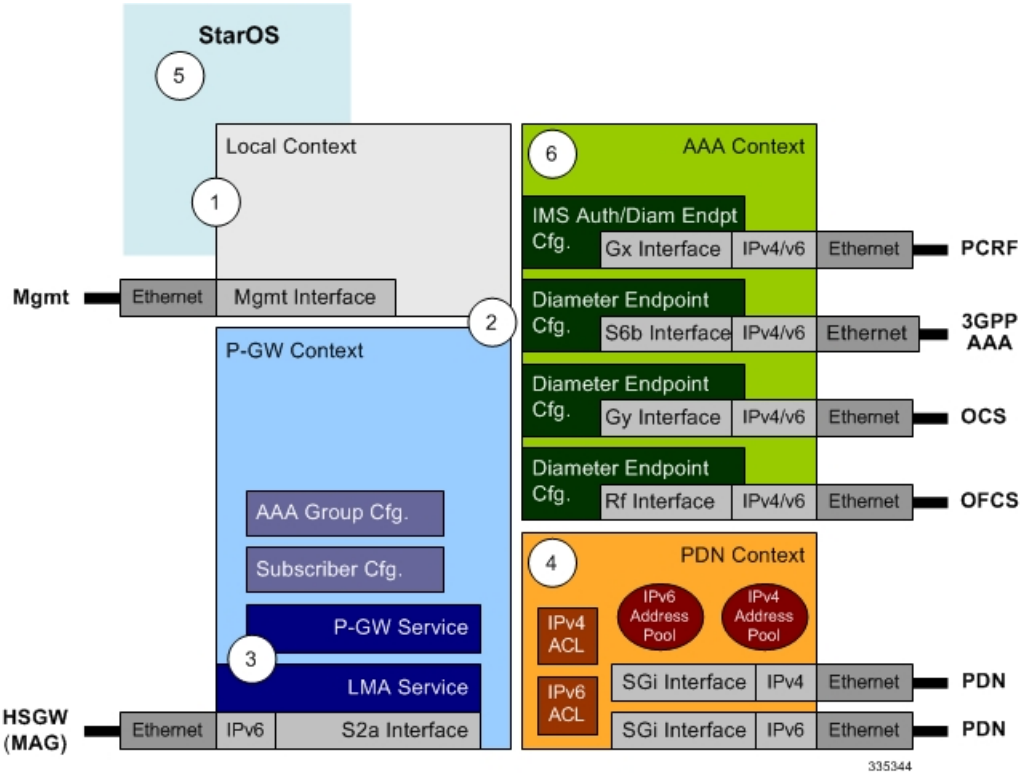
1. S-GW は、アクセスポイント名（APN）を含むセッション作成要求メッセージを P-GW に送信することにより、S5/S8 接続を確立します。
2. P-GW サービスは、セッションに AAA 機能を提供するために使用するコンテキストを決定します。このプロセスについては、『*System Administration Guide*』の「*Understanding the System Operation and Configuration*」の章にある「*How the System Selects Contexts*」の項で説明しています。
3. P-GW は、設定済みの Gx Diameter エンドポイントを使用して IP-CAN セッションを確立します。
4. P-GW は、IP-CAN セッションの確立を示すために CCRF に CC 要求（CCR）メッセージを送信し、PCRF は CC 応答（CCA）で確認応答します。
5. P-GW は APN 設定を使用して PDN コンテキストを選択します。選択した PDN コンテキストで設定された IP プールから IP アドレスが割り当てられます。
6. P-GW は、割り当てられたアドレスと追加情報を含むセッション作成応答メッセージで S-GW に応答します。

7. S5/S8 データプレーントンネルが確立され、P-GW は PDN との間でパケットを送受信できます。

P-MIP P-GW（eHRPD）設定

eHRPD ネットワーク環境でスタンドアロン P-MIP P-GW として動作するようにシステムを設定する場合は、次の図とその後の手順を確認してください。

図 *6 : P-MIP P-GW（eHRPD）設定*



手順

ステップ 1 『*System Administration Guide*』[英語] に記載されている設定例を適用して、PSC のアクティブ化などのシステム設定パラメータを設定します。

ステップ 2 「初期設定」に記載されている設定例を適用して、コンテキストやサービスの作成などの初期設定パラメータを設定します。

ステップ 3 システムを P-MIP P-GW として動作するように設定し、「P-GW サービス設定 （65 ページ）」に記載されている設定例を適用して、P-MIP インターフェイスや IP ルートなどの P-GW の基本的なパラメータを設定します。

ステップ 4 「P-GW PDN コンテキストの設定 （66 ページ）」の設定例を適用して、PDN コンテキストを設定します。

ステップ 5 「アクティブ課金サービス設定 （67 ページ）」の設定例を適用して、Gx インターフェイスのサポートのためのアクティブ課金サービスを有効にし、設定します。

ステップ 6 「AAA とポリシーの設定」の設定例を適用して、AAA コンテキストを作成し、AAA およびポリシーのパラメータを設定します。

ステップ 7 「設定の確認と保存 （71 ページ）」の手順に従って、設定を確認して保存します。

初期設定

手順

ステップ 1 「ローカルコンテキストの変更 （62 ページ）」の設定例を適用して、ローカルシステム管理パラメータを設定します。

ステップ 2 「P-MIP P-GW コンテキストの作成と設定 （63 ページ）」の設定例を適用して、P-GW サービスを配置したコンテキストを作成します。

ステップ 3 「P-GW コンテキストでの APN の作成と設定 （63 ページ）」の設定例を適用して、P-GW コンテキストで APN を作成および設定します。

ステップ 4 「P-GW コンテキストでの AAA グループの作成と設定 （64 ページ）」の設定例を適用して、P-GW コンテキストで AAA サーバーグループを作成および設定します。

ステップ 5 「LMA サービスの作成と設定 （65 ページ）」の設定例を適用して、新しく作成されたコンテキスト内に eGTP サービスを作成します。

ステップ 6 「P-GW PDN コンテキストの作成 （65 ページ）」の設定例を適用して、PDN へのインターフェイスが配置されるコンテキストを作成します。

ローカルコンテキストの変更

デフォルトサブスクライバを設定し、ローカルコンテキストでリモートアクセス機能を設定するには、次の例を使用します。

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
      exit
    server ftpd
      exit
    server telnetd
      exit
    subscriber default
      exit
    administrator <name> encrypted password <password> ftp
    ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
    exit
```

```
port ethernet <slot#/port#>
  no shutdown
  bind interface <lcl_cntxt_intrfc_name> local
  end
```

P-MIP P-GW コンテキストの作成と設定

次の例を使用して、P-GW コンテキストを作成し、S2a IPv6 インターフェイス（HSGW との間のデータトラフィック用）を作成し、S2a インターフェイスを設定済みのイーサネットポートにバインドします。

```
configure
  context <pgw_context_name> -noconfirm
    interface <s2a_interface_name> tunnel
      ipv6 address <address>
      tunnel-mode ipv6ip
        source interface <name>
        destination address <ipv4 or ipv6 address>
        exit
      exit
    policy accounting <rf_policy_name> -noconfirm
      accounting-level {level_type}
      accounting-event-trigger interim-timeout action stop-start
      operator-string <string>
      cc profile <index> interval <seconds>
      exit
    subscriber default
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s2a_interface_name> <pgw_context_name>
    end
```

注：

- S2a（P-GW から HSGW）インターフェイスは、IPv6 アドレスである必要があります。
- Rf（オフライン課金）インターフェイスのアカウンティングポリシーを設定します。アカウンティングレベルのタイプは、Flow、PDN、PDN-QCI、QCI、および Subscriber です。このコマンドの詳細については、『*Command Line Interface Reference*』の「*Accounting Profile Configuration Mode Commands*」の章を参照してください。

P-GW コンテキストでの APN の作成と設定

次の設定を使用して、APN を作成します。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      associate accounting-policy <rf_policy_name>
      ims-auth-service <gx_ims_service_name>
```

```
aaa group <rf-radius_group_name>
dns primary <ipv4_address>
dns secondary <ipv4_address>
ip access-group <name> in
ip access-group <name> out
mediation-device context-name <pgw_context_name>
ip context-name <pdn_context_name>
ipv6 access-group <name> in
ipv6 access-group <name> out
active-charging rulebase <name>
end
```

注：

- IMS 承認サービスは、AAA コンテキストで作成および設定されます。
- 複数の APN を、異なるドメイン名をサポートするように設定できます。
- 事前設定済みのアカウンティングポリシーをこの APN に関連付けるには、associate accounting-policy コマンドを使用します。アカウンティングポリシーは、P-GW コンテキストで設定されます。P-MIP P-GW コンテキストの作成と設定 （63 ページ） その例があります。

P-GW コンテキストでの AAA グループの作成と設定

RADIUS および Rf アカウンティングをサポートする AAA グループを作成および設定するには、次の例を使用します。

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
    aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
```

LMA サービスの作成と設定

LMA サービスを作成するには、次の設定例を使用します。

```
configure
   context <pgw_context_name>
      lma-service <lma_service_name> -noconfirm
         no aaa accounting
         revocation enable
         bind address <s2a_ipv6_address>
         end
```

注：

- **no aaa acounting** コマンドは、重複アカウンティングパケットを防止するために使用されます。
- 失効を有効にすると、MIP の失効が MAG とネゴシエートされて MIP バインディングが終了した場合に、MIP 登録の失効が可能になり、LMA は MAG に失効メッセージを送信できます。

P-GW PDN コンテキストの作成

P-GW PDN コンテキストおよびイーサネット インターフェイスを作成するには、次の例を使用します。

```
configure
   context <pdn_context_name> -noconfirm
      interface <sgi_ipv4_interface_name>
         ip address <ipv4_address>
         exit
      interface <sgi_ipv6_interface_name>
         ipv6 address <address>
         end
```

P-GW サービス設定

手順

ステップ 1 P-GW サービスの設定 （65 ページ）の設定例を適用して、P-GW サービスを設定します。

ステップ 2 固定 IP ルートの設定 （66 ページ）の設定例を適用して、HRPD サービングゲートウェイへの IP ルートを指定します。

P-GW サービスの設定

次の例を使用して、P-GW サービスを設定します。

```
configure
   context <pgw_context_name>
```

```
pgw-service <pgw_service_name> -noconfirm
  associate lma-service <lma_service_name>
  associate qci-qos-mapping <name>
  authorize external
  fqdn host <domain_name> realm <realm_name>
  plmn id mcc <id> mnc <id>
  end
```

注：

- QCI-QoS マッピング設定は AAA コンテキストで作成されます。詳細については、QCI-QoS マッピングの設定 （70 ページ）を参照してください。
- 外部承認は、S6b インターフェイスを介して 3GPP AAA サーバーによって実行されます。内部承認（APN）がデフォルトです。
- **fqdn host** コマンドは、S6b インターフェイスを介した P-GW と 3GPP AAA サーバー間のメッセージで使用される、P-GW サービスの完全修飾ドメイン名を設定します。

固定 IP ルートの設定

P-GW と HSGW 間のデータトラフィックのスタティック IP ルートを設定するには、次の例に示すコマンドを使用します。

```
configure
  context <pgw_context_name>
    ipv6 route <ipv6_addr/prefix> next-hop <hsgw_addr> interface
<pgw_hsgw_intrfc_name>
    end
```

注：

- スタティック IP ルーティングは、ダイナミック ルーティング プロトコルを使用する設定には必要ありません。

P-GW PDN コンテキストの設定

IP プールと IP アクセス制御リスト（ACL）を設定し、ポートを PDN コンテキストのインターフェイスにバインドするには、次の例に示すコマンドを使用します。

```
configure
  context <pdn_context_name> -noconfirm
    ip pool <name> range <start_address end_address> public <priority>
    ipv6 pool <name> range <start_address end_address> public <priority>
    subscriber default
      exit
    ip access-list <name>
      redirect css service <name> any
      permit any
      exit
    ipv6 access-list <name>
      redirect css service <name> any
      permit any
```

```
      exit
    aaa group default
      exit
        exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <pdn_sgi_ipv4_interface_name> <pdn_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <pdn_sgi_ipv6_interface_name> <pdn_context_name>
    end
```

アクティブ課金サービス設定

アクティブ課金を有効化および設定するには、次の例を使用します。

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule_definition>
        .
        .
      <rule_definition>
      exit
    ruledef <name>
      <rule_definition>
        .
        .
      <rule_definition>
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    packet-filter <packet_filter_name>
      ip remote-address = { < ipv4/ipv6_address> | <ipv4/ipv6_address/mask>
}
      ip remote-port { = < port_number> | range <start_port_number> to
<end_port_number> }
      exit
    rulebase default
```

```
exit
rulebase <name>
  <rule_base>
    .
    .
  <rule_base>
  end
```

注：

- ルールベースとは、ルール定義および関連する課金アクションの集合です。
- 最適化モードでのアクティブ課金により、ACS マネージャの一部ではなく、セッションマネージャの一部としてサービスを利用できるようになります。
- 上記のように、複数のルール定義、課金アクション、およびルールベースを設定して、さまざまな課金シナリオをサポートできます。
- ルーティングルールや課金ルールの定義を作成および設定できます。作成できるルーティングルール定義の最大数は 256 です。課金ルール定義の最大数は 2048 です。
- 課金アクションは、ルール定義が一致したときに実行するアクションを定義します。

重要 専用ベアラーでアップリンクパケットを受信している場合は、専用ベアラーにインストールされているルールだけが照合されます。静的ルールは一致せず、一致しないパケットはドロップされます。

AAA とポリシーの設定

手順

ステップ 1 「AAA コンテキストの作成と設定 （68 ページ）」の設定例を適用して、AAA とポリシーのインターフェイスを設定します。

ステップ 2 「QCI-QoS マッピングの設定 （70 ページ）」の設定例を適用して、QCI から QoS へのマッピングを作成し、設定します。

AAA コンテキストの作成と設定

次の例を使用して、Diameter サポートとポリシー制御を含む AAA コンテキストを作成および設定し、このコンテキスト、PCRF、3GPP AAA サーバー、オンライン課金サーバー、およびオフライン課金サーバー間のトラフィックをサポートするインターフェイスにポートをバインドします。

```
configure
  context <aaa_context_name> -noconfirm
```

```
interface <s6b_interface_name>
  ip address <ipv4_address>
  exit
interface <gx_interface_name>
  ipv6 address <address>
  exit
interface <rf_interface_name>
  ip address <ipv4_address>
  exit
interface <gy_interface_name>
  ipv6 address <address>
  exit
subscriber default
  exit
ims-auth-service <gx_ims_service_name>
  p-cscf discovery table <#> algorithm round-robin
  p-cscf table <#> row-precedence <#> ipv6-address <pcrf_adr>
  policy-control
    diameter origin endpoint <gx_cfg_name>
    diameter dictionary <name>
    diameter host-select table <#> algorithm round-robin
    diameter host-select row-precedence <#> table <#> host
<gx_cfg_name>
    exit
  exit
diameter endpoint <s6b_cfg_name>
  origin realm <realm_name>
  origin host <name> address <aaa_ctx_ipv4_address>
  peer <s6b_cfg_name> realm <name> address <aaa_ip_addr>
  route-entry peer <s6b_cfg_name>
  exit
diameter endpoint <gx_cfg_name>
  origin realm <realm_name>
  origin host <name> address <aaa_context_ip_address>
  peer <gx_cfg_name> realm <name> address <pcrf_ipv6_addr>
  route-entry peer <gx_cfg_name>
  exit
diameter endpoint <rf_cfg_name>
  origin realm <realm_name>
  origin host <name> address <aaa_ip_address>
  peer <rf_cfg_name> realm <name> address <ofcs_ip_addr>
  route-entry peer <rf_cfg_name>
  exit
diameter endpoint <gy_cfg_name>
  use-proxy
  origin realm <realm_name>
  origin host <name> address <aaa_ip_address>
  connection retry-timeout <seconds>
  peer <gy_cfg_name> realm <name> address <ocs_ip_addr>
  route-entry peer <gy_cfg_name>
  exit
```

```
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s6b_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gx_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gy_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <rf_interface_name> <aaa_context_name>
    end
```

注：

- **ims-auth-service** の下の **p-cscf table** コマンドでも、PCRF に IPv4 アドレスを指定できます。
- S6b インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。
- Gx インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。
- Gy インターフェイスの IP アドレスは、**ip address** コマンドを使用して IPv4 アドレスとして指定することもできます。
- Rf インターフェイスの IP アドレスは、**ipv6 address** コマンドを使用して IPv6 アドレスとして指定することもできます。

QCI-QoS マッピングの設定

QCI 値を作成し、適用可能な QoS パラメータにマッピングするには、次の例を使用します。

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
    qci 3 user-datagram dscp-marking <hex>
    qci 9 user-datagram dscp-marking <hex>
    end
```

注：

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

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

3GPP リリース 8 以降では、通信事業者固有/非標準の QCI がサポートされ、キャリアは QCI 128- 254 を定義できます。

- 上記の設定は、1 つのキーワードの例のみを示しています。**qci** コマンドおよびサポートされるその他のキーワードの詳細については、『*Command Line Interface Reference*』の「*QCI - QOS Mapping Configuration Mode Commands*」[英語] の章を参照してください。

設定の確認と保存

EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

P-GW でのオプション機能の設定

この項の設定例はオプションであり、稼働中のネットワークでの P-GW の最も一般的な使用に対応するために提供されています。これらの例の目的は、テスト用の基本設定を提供することです。

S5 インターフェイスでの ACL ベースのノード間 IP セキュリティの設定

この項の設定例では、S5 インターフェイス上で IKEv2/IPSec ACL ベースのノード間トンネルエンドポイントを作成します。

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

暗号アクセス制御リストの作成および設定

次に、暗号 ACL（アクセス制御リスト）を設定する例を示します。この ACL では、IPSec トンネルを介したサブスクライバ データ パケットのルーティングに使用される一致基準が定義されます。

```
configure
  context <pgw_context_name> -noconfirm
    ip access-list <acl_name>
      permit tcp host <source_host_address> host <dest_host_address>
      end
```

注：

- この例の **permit** コマンドは、指定の送信元ホストの IPv4 アドレスを持つサーバーから、指定の宛先ホストの IPv4 アドレスを持つサーバーに、IPv4 トラフィックをルーティングします。

IPSec トランスフォームセットの作成および設定

IPSec トランスフォームセットの設定例を次に示します。このトランスフォームセットは、インターフェイス上のデータを保護するために使用されるプロトコルを決定するセキュリティアソシエーションを定義するために使用されます。

```
configure
  context <pgw_context_name> -noconfirm
    ipsec transform-set <ipsec_transform-set_name>
      encryption aes-cbc-128
      group none
      hmac sha1-96
      mode tunnel
      end
```

注：

- 暗号化アルゴリズム **aes-cbc-128**（Advanced Encryption Standard 暗号ブロック連鎖）は、システムに設定されている IPSec トランスフォームセットのデフォルトアルゴリズムです。
- **group none** コマンドは、暗号強度を含めず、Perfect Forward Secrecy を無効にすることを指定します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。
- **hmac** コマンドは、Encapsulating Security Payload（ESP）整合性アルゴリズムを設定します。**sha1-96** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。
- **mode tunnel** コマンドは、IP ヘッダーを含む IPSec ヘッダーでパケット全体をカプセル化するように指定します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。

IKEv2 トランスフォームセットの作成および設定

次の例では、IKEv2 トランスフォームセットを設定します。

```
configure
  context <pgw_context_name> -noconfirm
    ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
      end
```

注：

- 暗号化アルゴリズム **aes-cbc-128**、すなわち Advanced Encryption Standard 暗号ブロック連鎖は、システムに設定されている IKEv2 トランスフォームセットのデフォルトアルゴリズムです。
- **group 2** コマンドは、中程度のセキュリティを示すグループ 2 として Diffie-Hellman アルゴリズムを指定します。Diffie-Hellman アルゴリズムは、暗号指数の強度を制御します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。
- **hmac** コマンドは、Encapsulating Security Payload（ESP）整合性アルゴリズムを設定します。**sha1-96** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。
- **lifetime** コマンドは、セキュリティキーが存在できる時間を秒単位で設定します。
- **prf** コマンドは、秘密キーがないとランダムなビットストリングと区別できないスビットストリングを生成する IKE 疑似乱数関数を設定します。**sha1** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。
- NATT を使用した IKEv2 ACL モードはサポートされません。
- VRF を使用した IKEv2 はサポートされていません。

クリプトマップの作成と設定

次の例では、IKEv2 クリプトマップを設定します。

```
configure
  context <pgw_context_name>
    crypto map <crypto_map_name> ikev2-ipv4
      match address <acl_name>
      peer <ipv4_address>
      authentication local pre-shared-key key <text>
      authentication remote pre-shared-key key <text>
      ikev2-ikesa transform-set list  <name1> . . . name6>
      payload <name> match ipv4
        lifetime <seconds>
        ipsec transform-set list <name1> . . . <name4>
        exit
      exit
    interface <s5_intf_name>
      ip address <ipv4_address>
      crypto-map <crypto_map_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
```

```
bind interface <s5_intf_name> <pgw_context_name>
end
```

注：

- この例で使用するクリプトマップのタイプは、IPv4 アドレッシングの場合は IKEv2/IPv4 です。IKEv2/IPv6 クリプトマップも IPv6 アドレッシングに使用できます。
- **ipsec transform-set list** コマンドは、最大 4 つの IPsec トランスフォームセットを指定します。

APN を緊急として設定

このセクションの設定例では、VoLTE ベース E911 サポート用の緊急 APN を設定します。

APN コンフィギュレーション モードで、緊急 APN の名前を指定し、緊急非アクティブタイムアウトを次のように設定します。APN に P-CSCF FQDN サーバー名を設定することもできます。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      emergency-apn
      timeout emergency-inactivity <seconds>
      p-cscf fqdn <fqdn>
      end
```

注：

- デフォルトでは、APN は非緊急と見なされます。
- **timeout emergency-inactivity** コマンドは、緊急セッションでの非アクティブな状態をチェックするためのタイムアウト期間（秒単位）を指定します。<*seconds*> は 1 ～ 3600 の整数にする必要があります。
- デフォルトでは、緊急非アクティブタイムアウトは無効（0）になっています。
- **p-cscf fqdn** コマンドは、APN の P-CSCF FQDN サーバー名を設定します。<*fqdn*> は、1 ～ 256 文字の長さの文字列である必要があります。
- P-CSCF FQDN は、CLI で設定された P-CSCF IPv4 および IPv6 アドレスよりも重要です。

共通ゲートウェイ アクセス サポートの設定

この項では、同じ IP アドレッシング動作とサブスクライバ承認のための 3GPP AAA へのアクセスを使用して、複数のアクセスネットワーク（CDMA、eHRPD、および LTE）に加え、国際ローミング用の GSM/UMTS をサポートするためのいくつかの高度な機能設定について説明します。静的 IP アドレッシングを使用するサブスクライバは、アクセステクノロジーに関係なく、同じ IP アドレスを取得できます。

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

重要 この機能はライセンス対応のサポートであり、この設定に関連する一部のコマンドを使用するには、機能固有のセッションライセンスをシステムにインストールする必要がある場合があります。

以下の手順は、『*System Administration Guide*』で説明されているシステムレベルの設定と P-GW サービスがすでに設定済みであることを前提としています。

S6b およびその他の高度な機能を設定するには、次の手順を実行します。

1. Diameter エンドポイントの設定 （75 ページ）の設定例を適用して、Diameter エンドポイントを設定します。
2. AAA グループの設定 （75 ページ）の設定例を適用して、AAA グループを作成または変更します。
3. S6b を介した承認の設定 （76 ページ）の設定例を適用して、HSS を使用した承認を許可するように P-GW サービスを変更します。
4. オプションです。DNS クライアント設定 （76 ページ）の設定例を適用して、DNS クライアントパラメータを作成し、関連付けます。
5. オプションです。重複コールの受け入れ設定 （77 ページ）の設定例を適用して、同じ IP アドレスで受信した場合に重複コールを受け入れるように P-GW サービスを変更します。
6. 共通ゲートウェイ アクセス サポートの設定の確認 （77 ページ）の手順に従って、S6b の設定を確認します。
7. 「設定の確認と保存」の章の説明に従って、設定を保存します。

Diameter エンドポイントの設定

次の例を使用して、Diameter エンドポイントを設定します。

```
configure
  context <pgw_ctxt_name> -noconfirm
    diameter endpoint <s6b_endpoint_name>
      origin host <host_name> address <ip_address>
     peer <peer_name> realm <realm_name> address <ip_address> port <port_num>

    end
```

注：

- *<pgw_ctxt_name>* は、システム上の P-GW サービスを含むコンテキストの名前です。

AAA グループの設定

この機能に関して AAA グループを作成/変更するには、次の例を使用します。

```
configure
  context <fa_ctxt_name>
    aaa group <aaa_grp_name>
      diameter authentication dictionary aaa-custom15
        diameter authentication endpoint <s6b_endpoint_name>
        diameter authentication server <server_name> priority <priority>

        end
```

注：

- <*s6b_endpoint_name*> は、既存の Diameter エンドポイントの名前です。

S6b を介した承認の設定

3GPP AAA/HSS を使用した P-GW サービスで S6b インターフェイスを有効にするには、次の例を使用します。

```
configure
  context <pgw_ctxt_name>
    pgw-service <pgw_svc_name>
      plmn id mcc <number> mnc <number>
      authorize-with-hss
      fqdn host <host_name> realm <realm_name>
      end
```

注：

- <*pgw_svc_name*> には、システムで作成済みの P-GW サービス名を指定します。

DNS クライアント設定

3GPP AAA/HSS を使用した P-GW サービスで S6b インターフェイスを有効にするには、次の例を使用します。

```
configure
  context <pgw_ctxt_name>
    ip domain-lookup
    ip name-servers <ip_address/mask>
    dns-client <dns_name>
      bind address <ip_address>
      resolver retransmission-interval <duration>
      resolver number-of-retries <retrie>
      cache ttl positive <ttl_value>
      exit
    pgw-service <pgw_svc_name>
      default dns-client context
      end
```

注：

- <*pgw_svc_name*> には、システムで作成済みの P-GW サービス名を指定します。

重複コールの受け入れ設定

同じ IP アドレスの要求を含む重複セッションコールを受け入れるように P-GW サービスを設定するには、次の例に示すコマンドを使用します。

```
configure
  context <pgw_ctxt_name>
    pgw-service <pgw_svc_name>
      newcall duplicate-subscriber-requested-address accept
      end
```

注：

- <*pgw_svc_name*> には、システムで作成済みの P-GW サービス名を指定します。

共通ゲートウェイ アクセス サポートの設定の確認

1. EXEC モードで次のコマンドを入力して、共通ゲートウェイ アクセス サポートが正しく設定されていることを確認します。

   show pgw-service all

   このコマンドの出力は、次に示すサンプルのようになります。この例では、*PGW1* という名前の P-GW サービスが、*vpn1* コンテキストで設定されています。

```
Service name:                   pgw1
Context:                        cn1
Associated PGW svc:             None
Associated GTPU svc:            None
Accounting Context Name:        cn1
dns-client Context Name:        cn1
Authorize:                      hss
Fqdn-name:                      xyz.abc@starent.networks.com
Bind:                           Not Done
Local IP Address:               0.0.0.0          Local IP Port:
  2123
Self PLMN:                      Not defined
Retransmission Timeout:         5 (secs)
```

S5 インターフェイスでの動的なノード間 IP セキュリティの設定

この項の設定例では、S5 インターフェイス上で IPSec/IKEv2 動的ノード間トンネルエンドポイントを作成します。

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

IPSec トランスフォームセットの作成および設定

IPSec トランスフォームセットの設定例を次に示します。このトランスフォームセットは、インターフェイス上のデータを保護するために使用されるプロトコルを決定するセキュリティアソシエーションを定義するために使用されます。

```
configure
  context <pgw_context_name> -noconfirm
    ipsec transform-set <ipsec_transform-set_name>
      encryption aes-cbc-128
      group none
      hmac sha1-96
      mode tunnel
      end
```

注：

- 暗号化アルゴリズム **aes-cbc-128**（Advanced Encryption Standard 暗号ブロック連鎖）は、システムに設定されている IPSec トランスフォームセットのデフォルトアルゴリズムです。
- **group none** コマンドは、暗号強度を含めず、Perfect Forward Secrecy を無効にすることを指定します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。
- **hmac** コマンドは、Encapsulating Security Payload（ESP）整合性アルゴリズムを設定します。**sha1-96** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。
- **mode tunnel** コマンドは、IP ヘッダーを含む IPSec ヘッダーでパケット全体をカプセル化するように指定します。これは、システムに設定される IPSec トランスフォームセットのデフォルト設定です。

IKEv2 トランスフォームセットの作成および設定

次の例では、IKEv2 トランスフォームセットを設定します。

```
configure
  context <pgw_context_name> -noconfirm
    ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
      end
```

注：

- 暗号化アルゴリズム **aes-cbc-128**、すなわち Advanced Encryption Standard 暗号ブロック連鎖は、システムに設定されている IKEv2 トランスフォームセットのデフォルトアルゴリズムです。

- **group 2** コマンドは、中程度のセキュリティを示すグループ 2 として Diffie-Hellman アルゴリズムを指定します。Diffie-Hellman アルゴリズムは、暗号指数の強度を制御します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。
- **hmac** コマンドは、Encapsulating Security Payload（ESP）整合性アルゴリズムを設定します。**sha1-96** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。
- **lifetime** コマンドは、セキュリティキーが存在できる時間を秒単位で設定します。
- **prf** コマンドは、秘密キーがないとランダムなビットストリングと区別できないビットストリングを生成する IKE 疑似乱数関数を設定します。**sha1** キーワードは、160 ビットの秘密鍵を使用して 160 ビットのオーセンティケータ値を生成します。これは、システムに設定される IKEv2 トランスフォームセットのデフォルト設定です。

暗号テンプレートの作成と設定

次の例では、IKEv2 暗号テンプレートを設定します。

```
configure
  context <pgw_context_name> -noconfirm
    crypto template <crypto_template_name> ikev2-dynamic
      ikev2-ikesa transform-set list <name1> . . . <name6>
      ikev2-ikesa rekey
      payload <name> match childsa match ipv4
        ipsec transform-set list <name1> . . . <name4>
        rekey
        end
```

注：

- **ikev2-ikesa transform-set list** コマンドは、最大 6 つの IKEv2 トランスフォームセットを指定します。
- **ipsec transform-set list** コマンドは、最大 4 つの IPsec トランスフォームセットを指定します。

S5 IP アドレスの暗号テンプレートへのバインド

次の例は、暗号テンプレートへの S5 インターフェイスのバインドを設定します。

```
configure
  context <pgw_ingress_context_name> -noconfirm
    gtpu-service <gtpu_ingress_service_name>
      bind ipv4-address <s5_interface_ip_address> crypto-template
<sgw_s5_crypto_template>
      exit
    egtp-service <egtp_ingress_service_name>
      interface-type interface-pgw-ingress
      associate gtpu-service <gtpu_ingress_service_name>
```

```
      gtpc bind ipv4-address <s5_interface_ip_address>
      exit
    pgw-service <pgw_service_name> -noconfirm
      plmn id mcc <id> mnc <id> primary
      associate egtp-service <egtp_ingress_service_name>
      end
```

注：

- GTP-U および eGTP サービス設定の **bind** コマンドは、**ipv6-address** コマンドを使用して IPv6 アドレスとして指定することもできます。

セッション作成要求処理時のガードタイマーの設定

P-GW には、60 秒にハードコードされている既存のタイマー「session setup-timeout」があり、セッション作成のガードタイマーとして使用されます。このタイマーは、すべての APN に使用され、セッション作成のためにセッション作成要求を受信すると開始されます。

内部または外部の処理の問題や、Gx/Gy などの外部インターフェイスでの遅延により、セッション作成要求の処理が、エンドツーエンドのコールセットアップで予想される時間よりも長く実行される場合があります。タイマーの期限が切れたときにセッションの処理が完了していない場合、セッション作成要求の処理が停止し、P-GW は、対応する他のセッション（Gx/Gy など）をすべて停止して、内部のクリーンアップを行います。P-GW は、セッション作成失敗応答で応答し、S-GW で使用可能なリソースがないことを示します。遅延がない正常の場合は、セッション作成応答の送信中にタイマーが停止します。

以前にハードコードされたデフォルトのセッション セットアップ タイムアウト値である 60 秒を、設定可能な値で上書きできるようにする新しいCLI コマンドが導入されました。これは、エンドツーエンドのコールセットアップ時間に関してP-GWでコールセットアップ時間を微調整するのに役立ちます。

セッション タイムアウトの設定

次の設定例は、P-GW セッションのセットアップタイムアウトを設定可能にしています。

```
configure
  context  context_name
    pgw-service  service_name
      setup-timeout  timer-value
      [  default | no ] setup-timeout
      end
```

注：

- **setup-timeout**：セッションのセットアップタイムアウト時間を秒単位で指定します。タイマーが期限切れになる前に P-GW がセッション作成要求メッセージを処理できる場合、P-GW はタイマーを停止し、「成功」セッション作成応答を送信します。

  timer_value は、1 ー 120 の整数である必要があります。

  デフォルト：60 秒

- **default**：デフォルト値は 60 秒です。値が設定されていない場合、P-GW サービスはタイマーをデフォルト値に設定します。
- **no**：タイマーをデフォルト値の 60 秒に設定します。

GTP エコータイマーの設定

ASR 5500 P-GW の GTP エコー タイマーは、2 つの異なるタイプのパス管理（デフォルトとダイナミック）をサポートするように設定できます。このタイマーは、GTP-C と GTP-U の両方またはそのいずれかで設定できます。

デフォルトの GTP エコータイマーの設定

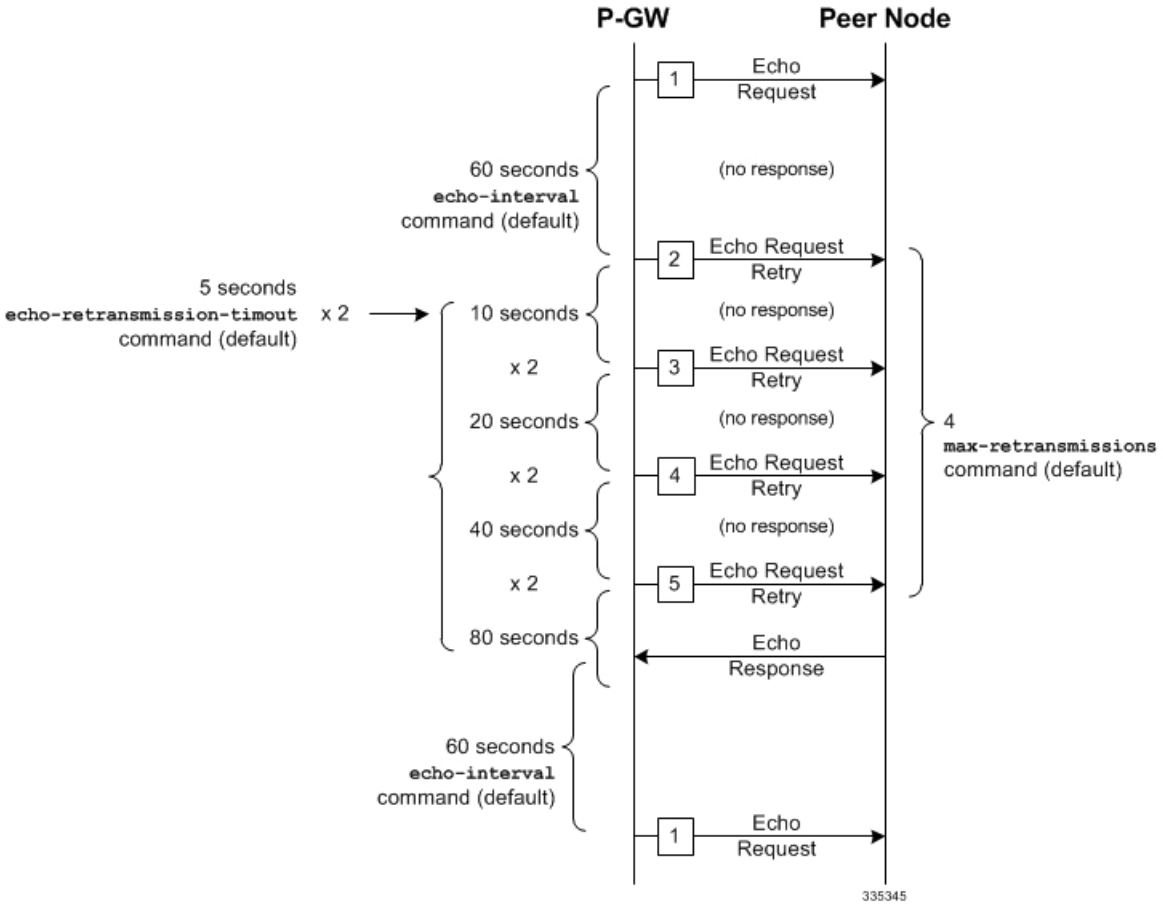
次の例では、デフォルトの eGTP-C および GTP-U インターフェイスのエコータイマーの設定について説明します。

eGTP-C

```
configure
     configure
          context <context_name>
               egtp-service <egtp_service_name>
                    gtpc echo-interval <seconds>
                    gtpc echo-retransmission-timeout <seconds>
                    gtpc max-retransmissions <num>
                    end
```

注：

- 次の図は、上記の例の 3 つの **gtpc** コマンドのデフォルト設定を使用した障害発生と回復シナリオを示しています。



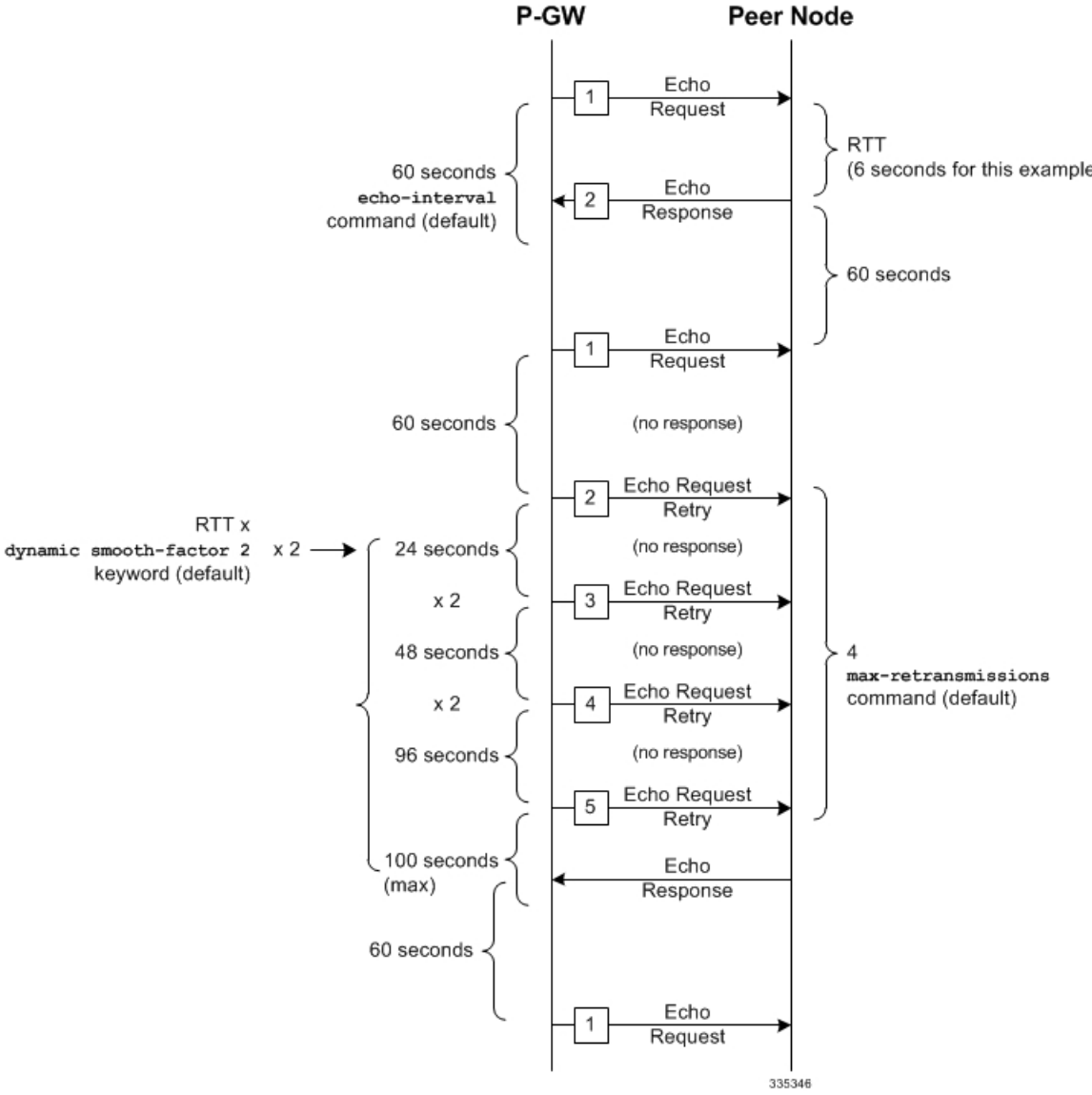
- 乗数（x2）はシステムのコードであり、設定できません。

GTP-U

```
configure
  configure
    context <context_name>
      gtpu-service <gtpu_service_name>
        echo-interval <seconds>
        echo-retransmission-timeout <seconds>
        max-retransmissions <num>
        end
```

注：

- 次の図は、上記の例にある 3 つの GTP-U コマンドのデフォルト設定を使用した障害発生と回復シナリオを示しています。



- 乗数（x2）はシステムのコードであり、設定できません。

動的 GTP エコータイマーの設定

次の例では、動的な eGTP-C および GTP-U インターフェイスのエコータイマーの設定について説明します。

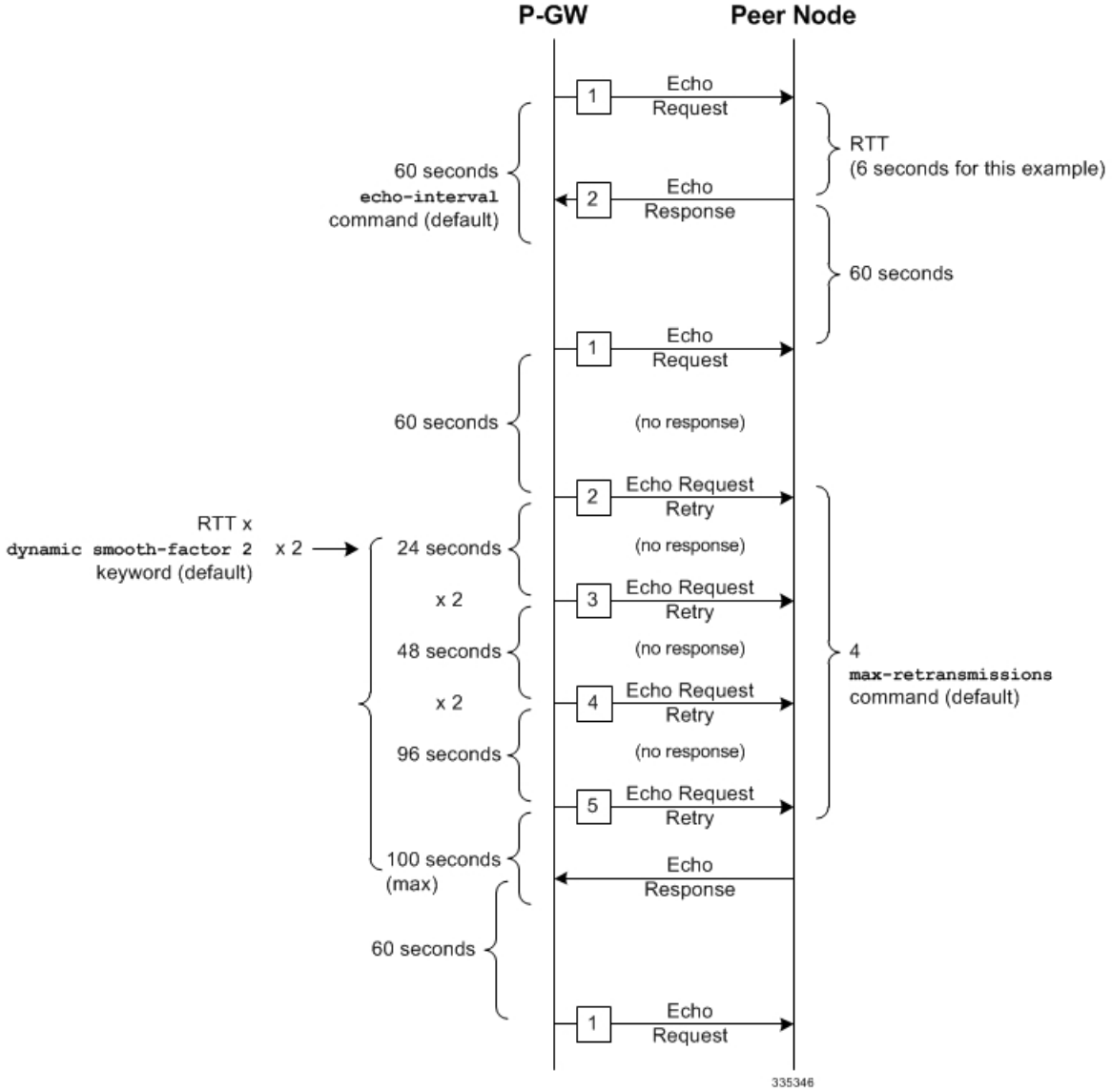
eGTP-C

```
configure
  configure
    context <context_name>
      egtp-service <egtp_service_name>
        gtpc echo-interval <seconds> dynamic smooth-factor <multiplier>
        gtpc echo-retransmission-timeout <seconds>
```

```
gtpc max-retransmissions <num>
end
```

注：

- 次の図は、上記の 3 つの **gtpc** コマンドのデフォルト設定と、6 秒のラウンドトリップタイマー（RTT）の例を使用した障害発生と回復のシナリオを示しています。



- 乗数（x2）と最大 100 秒はシステムコードであり、設定できません。

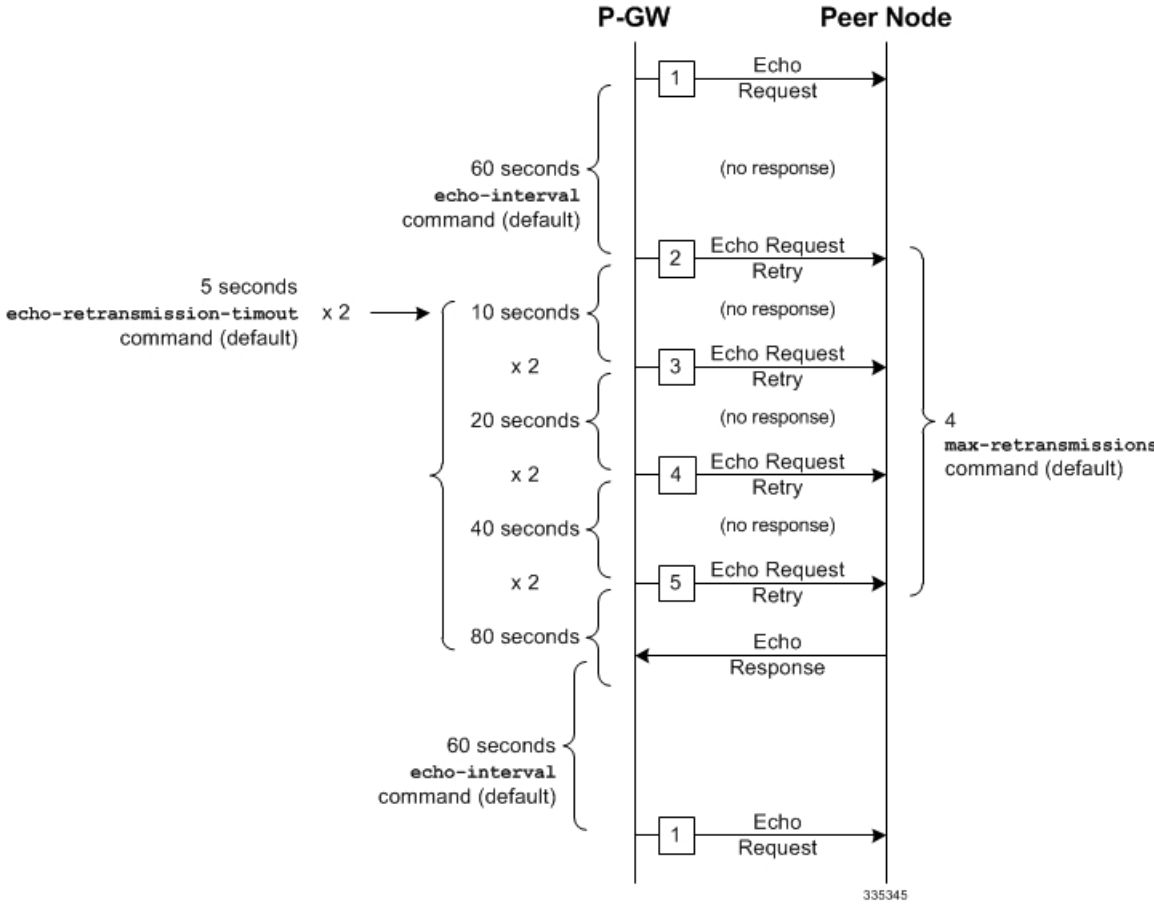
GTP-U

```
configure
  configure
    context <context_name>
      gtpu-service <gtpu_service_name>
        echo-interval <seconds> dynamic smooth-factor <multiplier>
```

```
echo-retransmission-timeout <seconds>
max-retransmissions <num>
end
```

注：

- 次の図は、上記の 3 つの **gtpc** コマンドのデフォルト設定と、6 秒のラウンドトリップタイマー（RTT）の例を使用した障害発生と回復のシナリオを示しています。



- 乗数（x2）と最大 100 秒はシステムコードであり、設定できません。

P-GW での GTPP オフラインアカウンティングの設定

デフォルトでは、P-GW サービスは GTPP アカウンティングをサポートします。GTPP オフライン課金機能を提供するには、次の例に示すパラメータを使用して P-GW を設定します。

```
configure
      gtpp single-source
      context <ingress_context_name>
            subscriber default
                  accounting mode gtpp
                  exit
            gtpp group default
                  gtpp charging-agent address <gz_ipv4_address>
                  gtpp echo-interval <seconds>
```

```
            gtpp attribute diagnostics
            gtpp attribute local-record-sequence-number
            gtpp attribute node-id-suffix <string>
            gtpp dictionary <name>
            gtpp server <ipv4_address> priority <num>
            gtpp server <ipv4_address> priority <num> node-alive enable
            exit
      policy accounting <gz_policy_name>
            accounting-level {type}
            operator-string <string>
            cc profile <index> buckets <num>
            cc profile <index> interval <seconds>
            cc profile <index> volume total <octets>
            exit
      exit
context <ingress_context_name>
      apn apn
            associate accounting-policy <gz_policy_name>
            exit
      interface <gz_interface_name>
            ip address <address>
            exit
      exit
port ethernet <slot_number/port_number>
      no shutdown
      bind interface <gz_interface_name> <ingress_context_name>
      end
```

注：

- **gtpp single-source** が有効になり、各 AAA マネージャが独自の UDP ポートで要求を生成するのではなく、システムが単一の UDP ポートを使用して（AAA プロキシ機能によって）アカウンティングサーバーへの要求を生成できるようになりました。
- **gtpp** は、**accounting mode** コマンドのデフォルトオプションです。
- コール制御プロファイルに設定されたアカウンティングモードは、この設定を上書きします。
- **accounting-level** のタイプは、Flow、PDN、PDN-QCI、QCI、および Subscriber です。このコマンドの詳細については、『*Command Line Interface Reference*』の「*Accounting Profile Configuration Mode Commands*」の章を参照してください。

GTP スロットリング機能の設定

GTP スロットリング機能を使用すると、通信事業者は P-GW/GGSN での着信/発信メッセージのレートを制御できます。

発信制御メッセージスロットリングの設定

次の設定は、発信制御メッセージスロットリングを有効にするのに役立ちます。

```
configure
  context context_name
  [no] gtpc overload-protection egress rlf-template rlf_template_name
```

```
throttling-overload-policy throttling_overload_policy_name
  end
```

着信制御メッセージスロットリングの設定

次の設定は、着信制御メッセージスロットリングを有効にするのに役立ちます。

```
configure
  context context_name
  [no] gtpc overload-protection ingress msg-rate msg_rate
[delay-tolerance msg_queue_delay ] [ queue-size queue_size ]
  end
```

ローカル QoS ポリシーの設定

この項の設定例では、ローカルQoSポリシーを作成します。ローカルQoSポリシーは、QoS、データ使用量、サブスクリプションプロファイル、サーバー使用率など、セッションのさまざまな側面をローカルに定義されたポリシーに従って制御するために使用されます。

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

ローカル QoS ポリシーの作成と設定

次の設定例では、P-GW でローカル QoS ポリシーを有効にします。

```
configure
  local-policy-service <name> -noconfirm
    ruledef <ruledef_name> -noconfirm
      condition priority <priority> <variable> match <string_value>
      condition priority <priority> <variable> match <int_value>
      condition priority <priority> <variable> nomatch <regex>
      exit
    actiondef <actiondef_name> -noconfirm
      action priority <priority> <action_name> <arguments>
      action priority <priority> <action_name> <arguments>
      exit
    actiondef <actiondef_name> -noconfirm
      action priority <priority> <action_name> <arguments>
      action priority <priority> <action_name> <arguments>
      exit
    eventbase <eventbase_name> -noconfirm
      rule priority <priority> event <list_of_events> ruledef <ruledef_name>
 actiondef <actiondef_name>
      end
```

注：

- 最大 16 のローカル QoS ポリシーサービスがサポートされます。
- パフォーマンス上の理由から、ローカル QoS ポリシーサービスでは ruledef の数を 256 以下にすることを推奨します。
- **condition** コマンドを複数回入力すると、ruledef の複数の条件を設定できます。一致する条件が見つかり、対応する条件が適用されるまで、優先順位に従って条件が検証されます。
- パフォーマンス上の理由から、ローカル QoS ポリシーサービスでは actiondef の数を 256 以下にすることを推奨します。
- **action** コマンドを複数回入力すると、actiondef の複数のアクションを設定できます。一致するアクションが見つかり、対応するアクションが適用されるまで、優先順位に従ってアクションが検証されます。
- 現在、1 つのイベントベースのみがサポートされており、「default」という名前にする必要があります。
- **rule** コマンドを複数回入力すると、イベントベースの複数のルールを設定できます。
- パフォーマンス上の理由から、イベントベースの数を 256 以下にすることを推奨します。
- ルールは優先順位に従って実行され、ルールが一致すると、actiondef で指定されたアクションが実行されます。イベント修飾子がルールに関連付けられている場合、ルールはその特定のイベントについてのみ照合されます。**continue** の修飾子がルールの最後にある場合、後続のルールも照合されます。それ以外の場合、ルールの評価は最初に一致した時点で終了します。

ローカル QoS ポリシーのバインド

オプション 1：次の設定例では、以前に設定済みのローカル QoS ポリシーをバインドしています。

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      ims-auth-service <local-policy-service name>
      end
```

注：

- 最大 30 項目の承認サービスをシステムにグローバルに設定できます。設定するサービスの合計最大数にはシステムでの制限もあります。
- 緊急コールの場合に役立ちます。PCRF は関与しません。

オプション 2：次の設定例は、以前に設定済みのローカル QoS ポリシーまたは障害処理テンプレートをバインドする場合にも使用できます。

```
configure
  context <pgw_context_name> -noconfirm
```

```
ims-auth-service <auth_svc_name>
  policy-control
    associate failure-handling-template <template_name>
    associate local-policy-service <service_name>
    end
```

注：

- IMS 承認サービスに関連付けることができる障害処理テンプレートは 1 つだけです。このコマンドを発行する前に、障害処理テンプレートを設定する必要があります。
- 障害処理テンプレートは、Diameter アプリケーションで、result-code の示す失敗、tx-expiry、または response-timeout が発生したときに実行するアクションを定義します。アプリケーションは、テンプレートで指定されたアクションを実行します。障害処理テンプレートの詳細については、『*Command Line Interface Reference*』の「*Diameter Failure Handling Template Configuration Mode Commands*」の章を参照してください。
- ローカルポリシーへのフォールバックをサポートするには、障害処理テンプレートで「local-fallback」を選択する必要があります。
- PCRF で障害が発生した場合にローカルポリシーへのフォールバックをサポートするには、ローカルポリシーサービスを IMS 承認サービスに関連付ける必要があります。障害時には、ims-auth サービスに関連付けられているローカルポリシーテンプレートがフォールバック用に選択されます。

ローカル QoS ポリシーの確認

次の設定例では、ローカル QoS サービスが適用されているかどうかを確認します。

```
logging filter active facility local-policy level debug
logging active
show local-policy statistics all
```

注：

- コンソールポートや実稼働ノードではロギング機能を使用しないように、十分注意してください。

X.509 証明書ベースのピア認証の設定

ここにある設定例により、X.509 証明書ベースのピア認証が有効になります。これは、P-GW での IP セキュリティ用の認証方法として使用できます。

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

次の設定例により、P-GW での X.509 証明書ベースのピア認証が有効になります。

グローバル コンフィギュレーション モードで、次のように X.509 証明書と CA 証明書の名前を指定します。

```
configure
  certificate name <cert_name> pem url <cert_pem_url> private-key pem url
 <private_key_url>
  ca-certificate name <ca_cert_name> pem url <ca_cert_url>
  end
```

注：

- **certificate name** コマンドと **ca-certificate list ca-cert-name** コマンドは、使用される X.509 証明書と CA 証明書を指定します。
- 証明書および CA 証明書の PEM 形式のデータを指定することも、この例に示すように、指定した URL を介してファイルから情報を読み取ることもできます。

コンテキスト コンフィギュレーション モードで IPSec の暗号テンプレートを作成する場合、次のように、X.509 証明書と CA 証明書を暗号テンプレートにバインドし、X.509 証明書ベースのピア認証をローカルノードとリモートノードに対して有効にします。

```
configure
  context <pgw_context_name> -noconfirm
    crypto template <crypto_template_name> ikev2-dynamic
      certificate name <cert_name>
      ca-certificate list ca-cert-name <ca_cert_name>
      authentication local certificate
      authentication remote certificate
      end
```

注：

- システムごとに最大 16 の証明書と 16 の CA 証明書がサポートされます。サービスごとに 1 つの証明書がサポートされ、最大 4 つの CA 証明書を 1 つの暗号テンプレートにバインドできます。
- **certificate name** コマンドと **ca-certificate list ca-cert-name** コマンドは、証明書と CA 証明書を暗号テンプレートにバインドします。
- **authentication local certificate** コマンドと **authentication remote certificate** コマンドは、X.509証明書ベースのピア認証をローカルノードとリモートノードに対して有効にします。

RLF バイパス機能の設定

レート制限のバイパス機能は、既存の GTP スロットリング機能を拡張したものです。RLF 機能により、通信事業者はスロットリングされている一部のメッセージのバイパスを制御できるようになりました。

既存の CLI コマンド **gtpc overload-protection egress rlf-template rlf-temp** に新しいコマンドオプション **throttling-override-policy** が追加されました。これにより、設定されたメッセージタイプ、または緊急コールまたはプライオリティコールのすべてのメッセージ、または設定された

APNのコールのすべてのメッセージに対して、スロットリングを選択的にバイパスできます。新しい CLI コマンドモード **throttling-override-policy** も導入され、スロットリングのオーバーライドポリシーの汎用シンタックスが使用できるようになりました。

スロットリング オーバーライド ポリシー モードの設定

GTP-C スロットリング オーバーライド ポリシーを作成し、GTP-C スロットリング オーバーライド ポリシー モードを開始する場合、次の設定が役立ちます。

```
configure
   throttling-override-policy throttling-override-policy_name
```

注：

上記のコマンドシーケンスを入力すると、次のプロンプトが表示されます。

```
[local]host_name(config-throttling-override-policy)#
```

RLF バイパス機能の設定

次の設定では、レート制限機能をバイパスできるメッセージタイプを設定します。

```
configure
   throttling-override-policy  throttling-override-policy_name
     [  default | no ] egress bypass-rlf pgw { msg-type { cbr | dbr |
ubr | emergency-call | earp-pl-list {1 | 2 | 3 | 4 | 5 … | 15 }+ |
apn-names  <apn-name1>  <apn-name2>  <apn-name3>   }
     end
```

注：

- 空の throttling-override-policy が作成された場合、すべての設定可能な項目のデフォルト値はゼロまたは無効になります。
- throttling-override-policy が関連付けられていない場合、P-GW の **show service configuration** はそれを「n/a」と表示します。
- 追加できる throttling-override-policy の最大数は 1024 です。この制限は、RLF テンプレートの最大数と同じです。

例

次のコマンドは、P-GW ノードでベアラー作成要求メッセージタイプを設定して、スロットリングをバイパスするようにしています。

```
egress bypass-rlf pgw msg-type cbr
```

VoLTE セッションの自動修正

機能情報

要約データ

[ステータス（Status）]	変更された機能
導入されたリリース	21.2
変更されたリリース	該当なし
対象製品	P-GW
該当プラットフォーム	ASR 5500
デフォルト設定	無効
関連する CDETS ID	CSCvc72275
このリリースでの関連する変更点	N/A
関連資料	*P-GW Administration Guide* *Command Line Interface Reference*

マニュアルの変更履歴

重要 リリース 21.2 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース	リリース日
このリリースの新機能。	21.2	2017 年 4 月 27 日

機能説明

スイッチオーバー後にIPマルチメディアサブシステム（IMS）セッションのダイナミックルールが失われると、VoLTE コールが影響を受けます。コールを回復するには、IMS セッションを手動でクリアして、正しいダイナミックルールでPDNを再確立する必要があります。VoLTE セッションの自動修正機能により、ダイナミックルールチェックが可能になります。これにより、P-GWがRAR（再承認要求）メッセージを受信したときに、手動による介入なしに、問題が自動的に特定され、修正されます。この機能は、チェックのトリガーとして「RAR」メッセージを使用するように設定された APN にのみ適用されます。

機能の仕組み

APN がポリシー制御および課金ルール機能（PCRF）から RAR メッセージを受信すると、再承認応答（RAA）メッセージがすぐに送信されます。この機能が有効になっている場合、P-GW で追加のチェックが実行され、デフォルトのベアラーに関連付けられたダイナミックルールがあるかどうかが確認されます。デフォルトのベアラーで Session Initiation Protocol（SIP）ルールが回復した場合は、他の専用ベアラーも回復されます。ダイナミックルールがデフォルトのベアラーに関連付けられていない場合、コールは終了されます。その後、原因コード「再アクティベーションが必要です」を含むベアラー削除要求がデフォルトのベアラーに送信されます。原因コードが確実に送信されるようにするには、「pdn-behavior ims」を使用して APN を設定する必要があります。続いて、Credit-Control-Request-Type（CCR-T）が PCRF および他の Diameter インターフェイス（s6b、Gy、および Rf）に送信されます。 したがって、異常が検出された場合の自動回復手順には、サブスクライバ接続の終了が含まれます。サブスクライバは後でネットワークに再接続する必要があります。スイッチオーバー後にダイナミックルールが失われたサブスクライバのモバイル発信またはモバイル着信コールは拒否されます。

VoLTE セッションの自動修正機能の設定

次の項では、この機能を有効または無効にするための設定コマンドについて説明します。

ダイナミックルールチェックの有効化または無効化

VoLTE セッションの自動修正のためのダイナミックルールチェックを有効にするために、新しい CLI コマンドの **pdn validate-post-switchover** が追加されました。この機能を有効にするには、ベース APN でこのコマンドを設定します。この機能は、自動リカバリが必要な VoLTE/IMS APN に対してのみ設定する必要があります。

この機能はデフォルトで無効に設定されています。

この機能を有効または無効にするには、以下のコマンドを入力します。

```
configure
  context <context_name>
    apn <apn_name>
      [no] pdn validate-post-switchover
      end
```

注：

- **no:** ベース APN で VoLTE セッションの設定済みの自動修正を無効にします。
- **pdn validate-post-switchover:** スイッチオーバー後の自動回復用のダイナミックルールを検証します。

モニタリングおよびトラブルシューティング

ここでは、VoLTE セッションの自動修正機能のサポートにおける show コマンドおよびその出力について説明します。

コマンドの表示

ここでは、この機能をモニターするために使用できるすべての show コマンドについて説明します。

show configuration apn

この機能が APN レベルで有効になっているかどうかを確認できるよう、上記の CLI コマンドが導入されました。「pdn validate-post-switchover」があれば、この機能は有効になっています。

show active-charging service statistics

このコマンドは、以下の出力を表示するように変更されました。

```
show active-charging service statistics
ACS Data Statistics:
  Packets Dropped due to System-Limit L4-Flows:                          0
  Packets Dropped - Invalid Len in IP Hdr(Dwlink):                       0
  Packets Dropped - Invalid Ver in IP Hdr(Dwlink):                       0
  Packets Not Processed due to Flow-limit:                               0
  Packets Not Processed due to CLP not found:                            0
  Packets Dropped CLP in Preservation Mode:                              0
  Total Pkts:                                                            0
  Total Collisions in data session hash:                                 0

ACS Reject Reason:
  RuleBase Mismatch  :                                                   0
  Bandwidth-Policy Mismatch  :                                           0
  CBB-Policy Mismatch  :                                                 0
  CF Policy Mismatch  :                                                  0
  No RuleBase configured in APN/Subs:                                    0
  No active rule in Rulebase/Subs:                                       0
  No Bandwidth-Policy configured in APN/Subs:                            0
  No Resources:                                                          0
  Max Sessions:                                                          0
  Reject Probability Exceeded:                                           0
  Rule Recovery Failed:                                                  0
  CDR Flow Control Initiated:                                            0

Protocol Reject stats:
  WTP Non-initial PDU:                                                   0
  WSP-CO Non-initial Connect PDU                                         0

Dynamic Rule Statistics:
  Total Subscribers:                0   Current Subscribers:             0
  Charging Msg Received:            0   Rule Defn Received:              0
  Installs Received:                0   Removes Received:                0
  Installs Succeeded:               0   Removes Succeeded:               0
  ADC Rules Received:               0   Total ADC Rules:                 0
  ADC Install Succeeded:            0   ADC Install Failed:              0
  ADC Custom Mute Received:         0   ADC Custom Unmute Received:      0
  ADC Start Sent:                   0   ADC Stop Sent:                   0
  L7 Rules Received:                0
  L7 Install Succeeded:             0   L7 Install Failed:               0
  Installs Failed:                  0   Removes Failed:                  0
  Install Failure Reason:
    No Resources:                   0   No Rulebase Match:               0
    No RuleName Match:              0   Rulebase Count Exceeded:         0
    Local Copy Failed:              0   Invalid Protocol:                0
    Invalid Source Mask:            0   Invalid Dest Mask:               0
    No Grp-of-Rdef Match:           0
```

```
    ADC Invalid Rule:               0   ADC Invalid Readdress:             0
    L7 Rule Invalid:                0
    L7 Protocol Invalid:            0   L7 Field Invalid:                  0
    L7 Operator Invalid:            0   L7 Value Invalid:                  0
    L7 Case-Sens Invalid:           0
  Remove Failure Reason:
    No RuleName Match:              0   No Grp-of-Rdef Match:              0
    Local Copy Failed:              0

Bandwidth Limiting Statistics:
    ITC Drops:
      Uplink Packets:                  0   Uplink Bytes:                  0
      Downlink Packets:                0   Downlink Bytes:                0
    Dynamic Rule Bandwidth Limiting Drops:
      Uplink Packets:                  0   Uplink Bytes:                  0
      Downlink Packets:                0   Downlink Bytes:                0
    Per-Bearer Bandwidth Limiting Drops:
      Uplink Packets:                  0   Uplink Bytes:                  0
      Downlink Packets:                0   Downlink Bytes:                0

Credit-Control Group Statistics:
  CC Dropped Uplink Packets:       0  CC Dropped Uplink Bytes:           0
  CC Dropped Downlink Packets:     0  CC Dropped Downlink Bytes:         0

Readdressing Failure Statistics (Packets):
  Non SYN Flow:                    0  Duplicate Key:                     0
  Dropped Pkts:                    0


First-request-only redirections:                                       0

Fallback Statistics:
  Bandwidth Policy Applied:                                            0
  Bandwidth Policy Failed:                                             0
```

バルク統計

このセクションでは、この機能をサポートするために追加、変更、または廃止されたすべてのバルク統計のリストを示します。

ECS スキーマ

このセクションでは、ダイナミックリカバリの失敗を示すために追加された新しいバルク統計を示します。

- dyn_rule_recovery_failure:

  ダイナミックルールリカバリの失敗により終了したセッションの合計数。
- dyn_rule_recovery_num_sess_not_terminated:

  ダイナミックルールがデフォルトベアラーにインストールされていなかったために、スイッチオーバー後に終了しなかったセッションの合計数。

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。