L2TP アクセスコンセントレータ

この章では、Cisco ASR 5500 シャーシのレイヤ 2 トンネリングプロトコル（L2TP）アクセスコンセントレータ（LAC）機能サポートについて、またその設定方法について説明します。

製品アドミニストレーションガイドには、システム上での基本サービスの設定例と手順が示されています。この章に記載する手順を実行する前に、それぞれの製品のアドミニストレーションガイドの説明に従って、お使いのサービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定することを推奨します。

重要 L2TP アクセスコンセントレータは、シスコのライセンス供与された機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『システム管理ガイド』の「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

セッションライセンスと機能使用キーによって有効にすると、システムで L2TP がサポートされ、LAC と 1 つまたは複数の L2TP ネットワークサーバー（LNS）ノードの間のデータパケットがカプセル化されます。システムでは、このオプションのパケットカプセル化（トンネリング）は、コンテキスト内で L2TP アクセスコンセントレータ（LAC）サービスを設定することによって実行されます。

重要 LAC から LNS への L2TP セッションの確立中に、ユーザーの PPP 接続が確立されます。サーバーは、CHAP 認証プロトコルを使用して接続を認証します。サーバーが受信した CHAP チャレンジに対する CHAP 応答を計算しているとき、サーバーは CHAP パスワードを考慮しません。

重要 LAC サービスは、UDP ポート 13660 から 13668 を、LNS にパケットを送信するための送信元ポートとして使用します。

この章は、次の内容で構成されています。

対象製品と関連するセクション

LAC 機能は、さまざまな製品でサポートされています。この機能がサポートされている製品と、その製品に関連する章の参照先を次の表にを示します。

対象製品	参照先

PDSN/FA/HA	• *PDSN* 簡易 *IP* でサポートされる *LAC* サービス設定
	• モバイル *IP* でサポートされる *LAC* サービス設定
	• *L2TP* サポート用のサブスクライバプロファイルの設定
	  • 使用される *RADIUS* とサブスクライバのプロファイル属性
	  • *L2TP* サポート用のローカル サブスクライバ プロファイルの設定
	  • *RADIUS* 属性を使用しない特定コンテキスト内のすべてのサブスク
	  のトンネリング
	• *LAC* サービスの設定
	• *L2TP* サポートのための *PDSN* サービスの変更

GGSN/SGSN/FA/P-GW	• *GGSN* でサポートされる *LAC* サービス設定
	• モバイル *IP* でサポートされる *LAC* サービス設定
	• *L2TP* サポート用のサブスクライバプロファイルの設定
	  • 使用される *RADIUS* とサブスクライバのプロファイル属性
	  • *L2TP* サポート用のローカル サブスクライバ プロファイルの設定
	• *L2TP* を介したマルチキャストサービスの有効化
	• *LAC* サービスの設定
	• *L2TP* をサポートするための *APN* テンプレートの変更

対象製品	参照先
ASN GW	• モバイル *IP* でサポートされる *LAC* サービス設定 • *L2TP* サポート用のサブスクライバプロファイルの設定 • 使用される *RADIUS* とサブスクライバのプロファイル属性 • *L2TP* サポート用のローカル サブスクライバ プロファイルの設定 • *RADIUS* 属性を使用しない特定コンテキスト内のすべてのサブス のトンネリング • *LAC* サービスの設定

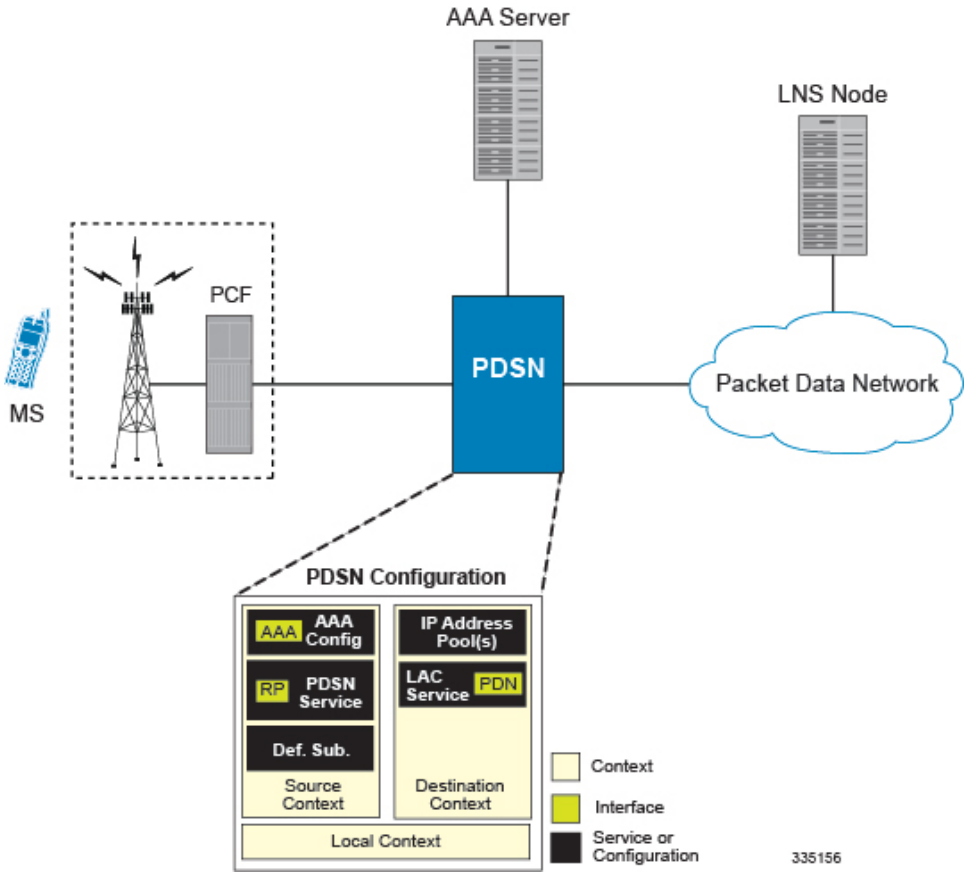
PDSN 簡易 IP でサポートされる LAC サービス設定

LACサービスを着信PPPセッションに適用するには、次のいずれかのメソッドを使用します。

- **属性ベースのトンネリング**：このメソッドは、認証中に識別された特定のユーザーのみのPPPパケットをカプセル化するために使用されます。このメソッドでは、通信可能なLACサービスパラメータと許可されるLNSノードが、特定のサブスクライバのユーザープロファイルによって制御されます。ユーザープロファイルは、システム上でローカルで設定できますし、RADIUSサーバー上でリモートで設定することもできます。
- **PDSN サービスベースの強制トンネリング**：このトンネリングメソッドは、RPインターフェイスからPDSNサービスに着信するすべての着信PPPトラフィックをカプセル化し、認証のためにそれをLNSピアにトンネリングするために使用されます。すべての認証がピアLNSによって実行されるため、このメソッドではサブスクライバの設定が考慮されないことに注意してください。

各LACサービスは、同じシステムコンテキスト内で設定された単一のシステムインターフェイスにバインドされます。次の図に示すように、このコンテキストを接続先コンテキストにすることを推奨します。

図 *1 : SIP* 用の *LAC* サービスの設定



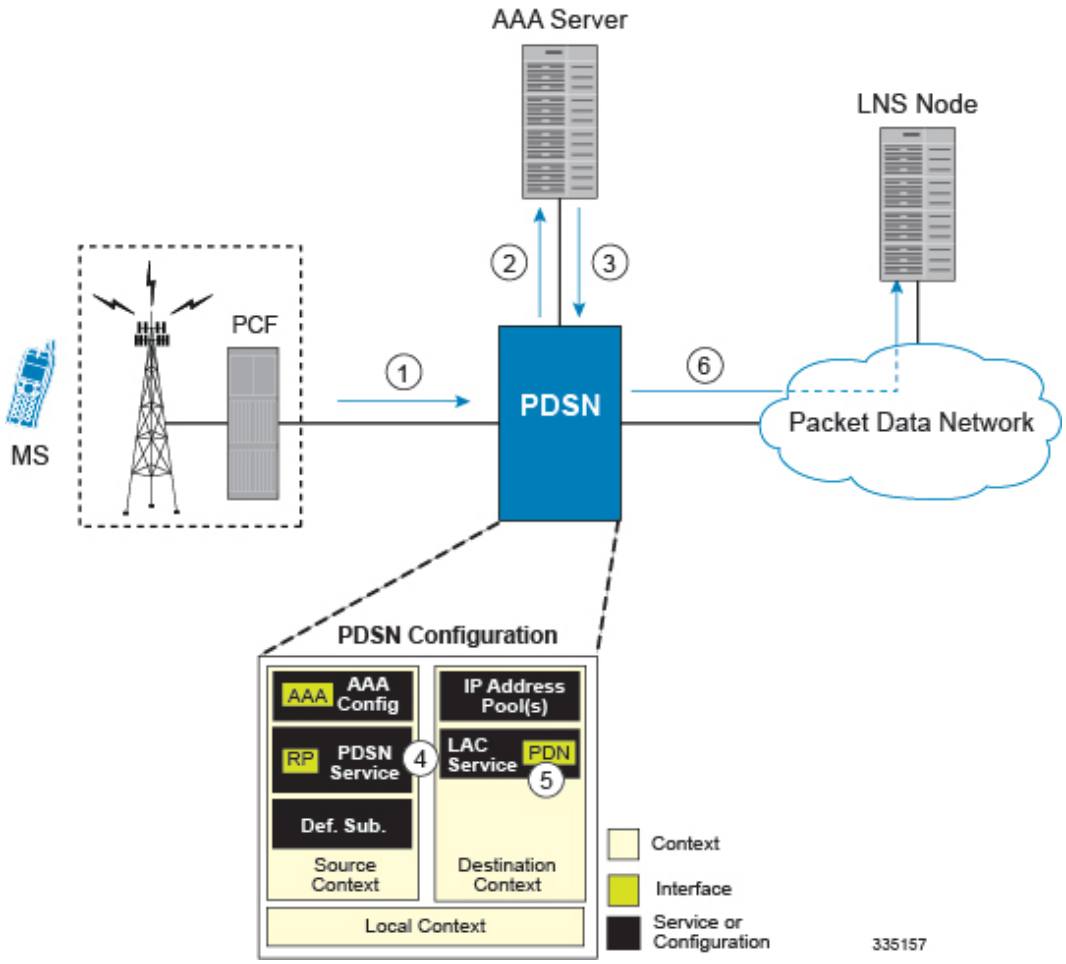
属性ベーストンネリング

このセクションでは、属性ベーストンネリングの動作とその設定について説明します。

属性ベース L2TP 設定の仕組み

次の図とその後のテキストは、システムを使用して属性ベーストンネリングがどのように実行されるかを示しています。

図 *2 : SIP* の属性ベース *L2TP* セッション処理



1. PCF からのサブスクライバセッションは、R-P インターフェイスを介して PDSN サービスによって受信されます。
2. PDSN サービスは、サブスクライバの認証を試みます。サブスクライバは、ローカルで設定することも、RADIUS サーバー上にリモートで設定することもできます。上図は、RADIUS AAA サーバーを使用したサブスクライバ認証を示しています。
3. RADIUS サーバーが Access-Accept メッセージを返します。このメッセージには、セッションデータが L2TP を使用してトンネリングされることを示す属性と、使用する LAC サービスの名前と場所が含まれています。接続先の LNS ピアを示す属性も提供されます。
4. PDSN サービスは、この情報を受信すると、宛先コンテキスト内に設定された LAC サービスにパケットを転送します。
5. LAC サービスは、パケットを受信すると、情報をカプセル化し、LNS に配信するために適切な PDN インターフェイスに転送します。
6. カプセル化されたパケットは、パケットデータネットワークを介してピア LNS に送信され、ここでカプセル化が解除されます。

PDSN 簡易 IP に対する属性ベースの L2TP サポートの設定

この項では、属性ベースの L2TP サポートを設定し、PDSN 簡易 IP アプリケーションで使用するために必要な手順のリストを示します。一覧表示されている各手順では、必要な手順を実行するための具体的な指示を含む別のセクションが参照されています。

重要 これらの手順は、システムがサブスクライバ データ セッションを PDSN としてサポートするように事前に設定されていることを前提としています。

手順

ステップ 1 この章の「*L2TP* サポート用のサブスクライバプロファイルの設定」の項に記載されている情報および手順に従って、サブスクライバプロファイルを設定します。

ステップ 2 この章の「*LAC* サービスの設定」セクションに記載されている情報と手順に従って、1 つ以上の LAC サービスを設定します。

ステップ 3 この章の「*L2TP* サポートのための *PDSN* サービスの変更」の項に記載されている手順に従って、トンネル コンテキスト ロケーションを使用して PDSN サービスを設定します。

ステップ 4 Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

PDSN サービスベース強制トンネリング

このセクションでは、サービスベース強制トンネリングの動作とその設定について説明します。

PDSN サービスベース強制トンネリングの動作の仕組み

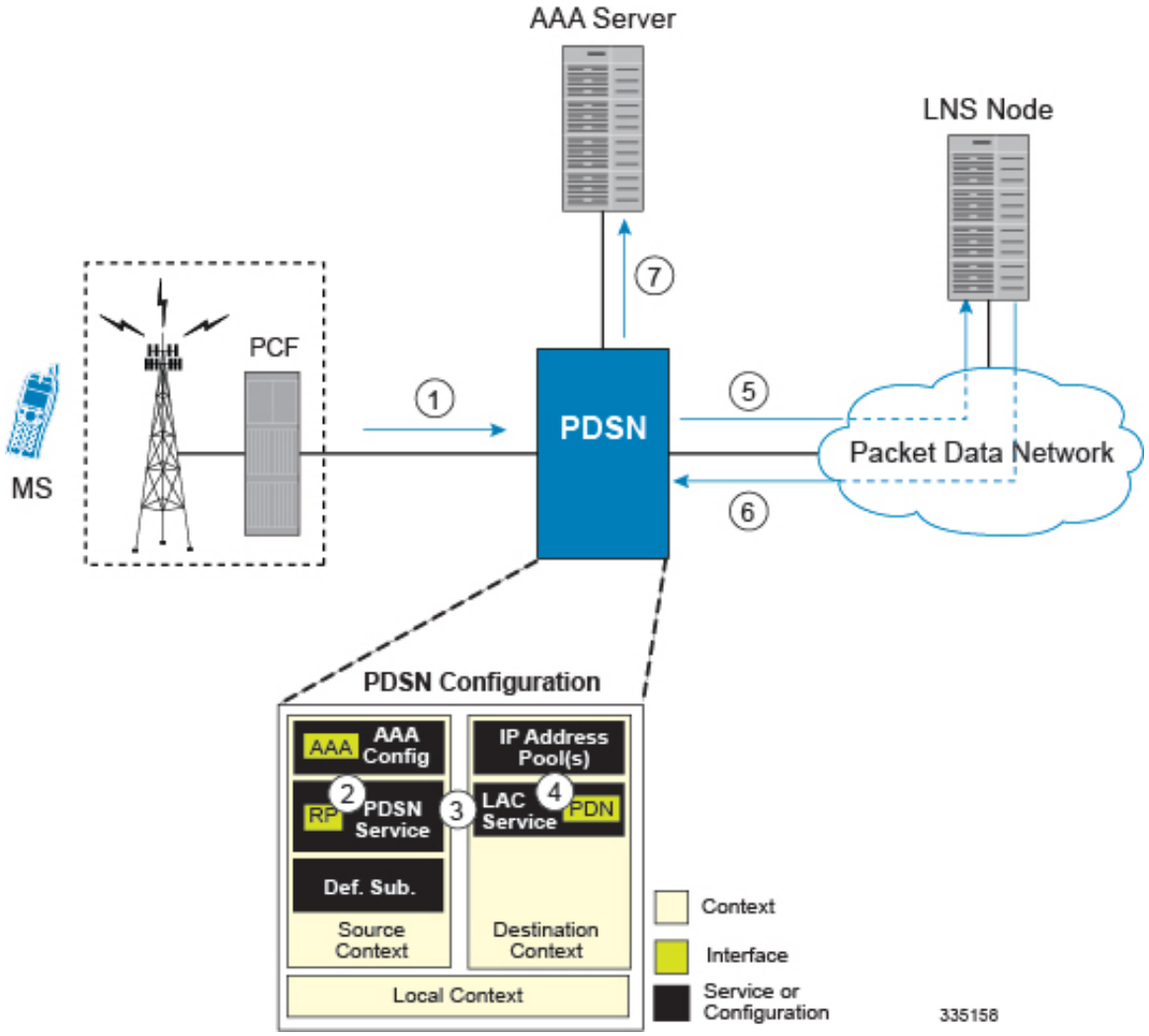
PDSN サービスベースの強制トンネリングにより、ワイヤレス通信事業者は、すべての PPP トラフィックを L2TP トンネルを介してリモート LNS ピアに送信し、認証を行うことができます。これは、システムで PPP 認証が実行されないことを意味します。

アカウンティング開始レコードと中間アカウンティングレコードは、引き続きシステムの AAA サービス設定で設定されたローカル RADIUS サーバーに送信されます。L2TP セッションのセットアップが完了すると、システムはコールカウンタを開始し、RADIUS サーバーに信号を送ってアカウンティングを開始します。アカウンティングレコードのサブスクライバ名は、セッションごとに作成される NAI 構造の名前に基づきます。

PDSN サービスベースの強制トンネリングでは、1 つ以上の PDSN サービスを変更し、1 つ以上の LAC サービスを設定する必要があります。

次の図およびそれに続くテキストは、システムを使用してPDSNサービスベースの強制トンネリングがどのように実行されるかを示しています。

図 *3 : PDSN* サービスベース強制トンネリングのセッション処理



1. PCF からのサブスクライバセッションは、R-P インターフェイスを介して PDSN サービスによって受信されます。
2. PDSN サービスは、その **tunnel-type** パラメータが L2TP に設定されていること、およびその **tunnel-context** パラメータが接続先コンテキストに設定されていることを検出します。
3. PDSN は、セッションのすべてのパケットを、接続先コンテキストで設定された LAC サービスに転送します。複数の LAC サービスが設定されている場合、セッショントラフィックはラウンドロビンアルゴリズムを使用して各サービスにルーティングされます。
4. LAC サービスは、設定の一部としてリストされている LNS ピアの 1 つへの L2TP トンネルを開始します。

5. セッションパケットは、認証のためにパケットデータネットワークを介して LNS に渡されます。
6. LNS はセッションを認証し、PDSN に Access-Accept を返します。
7. PDSN サービスでは、構造化された NAI を使用して、セッションのアカウンティングを開始します。

   セッション データ トラフィックは、ステップ 4 で確立した L2TP トンネルを介して渡されます。

PDSN 簡易 IP に対する L2TP 強制トンネリングのサポート

このセクションでは、L2TP 強制トンネリングのサポートを設定し、PDSN 簡易 IP アプリケーションで使用するために必要な手順のリストを示します。一覧表示されている各手順では、必要な手順を実行するための具体的な指示を含む別のセクションが参照されています。

重要 これらの手順は、システムがサブスクライバ データ セッションを PDSN としてサポートするように事前に設定されていることを前提としています。

手順

ステップ 1 この章の「*LAC* サービスの設定」セクションに記載されている情報と手順に従って、1 つ以上の LAC サービスを設定します。

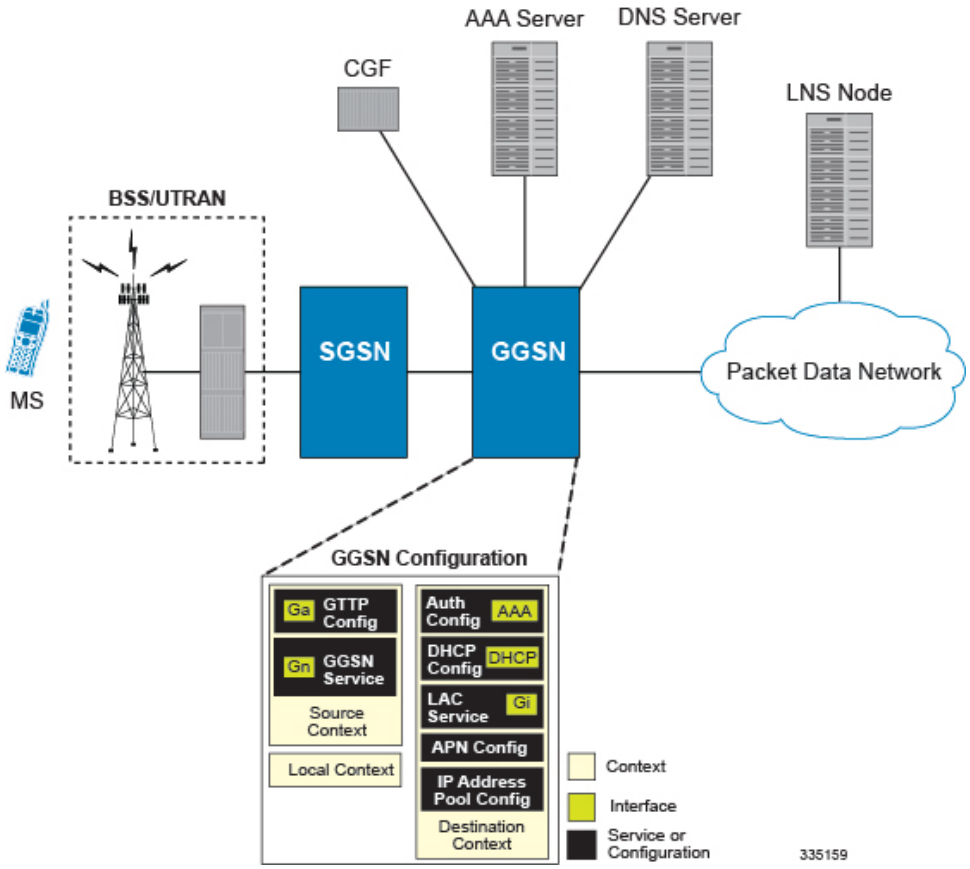
ステップ 2 この章の「*L2TP* サポートのための *PDSN* サービスの変更」セクションに記載されている手順に従って、PDSN サービスを設定します。

ステップ 3 Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイスやネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

GGSN および P-GW でサポートされる LAC サービス設定

前述したとおり、L2TP はシステムでの LAC サービス設定を通じてサポートされます。次の図に示すように、各 LAC サービスは、同じシステム接続先コンテキスト内で設定された単一のシステムインターフェイスにバインドされます。

図 *4 : GGSN LAC* サービスの設定



LAC サービスは、GGSN のアクセスポイント名（APN）のテンプレートまたはサブスクライバのプロファイルにある属性の設定に基づいて、着信サブスクライバの PDP コンテキストに適用されます。サブスクライバプロファイルは、システム上でローカルで設定することも、RADIUS サーバー上でリモートで設定することもできます。

LAC サービスは、LNS を使用したドメインベースの L2TP トンネリングもサポートします。この方法を利用して、LAC と LNS の間に複数のトンネルが作成されます。このとき、Access-Accept でトンネル選択と作成用のキーとして AAA サーバーから受信した「Tunnel-Client-Auth-ID」や「Tunnel-Server-Auth-ID」属性の値に基づいて作成されます。LAC が新しい L2TP セッションを確立する必要がある場合、まずキーの「Tunnel-Client-Auth-ID」や「Tunnel-Server-Auth-ID」の属性値に基づいて、ピア LNS との既存の L2TP トンネルがあるかどうかを確認します。キーにそのようなトンネルが存在しない場合は、LNS との新しいトンネルが作成されます。

LAC サービスが LNS との新しい L2TP セッション用に新しいトンネルを確立する必要があり、トンネル作成の上限に達したためにトンネル作成要求に失敗した場合、LAC は Access-Accept メッセージで AAA サーバーから受信した他の LNS アドレスを試します。使用可能なすべてのピア LNS が使い果たされている場合、LAC サービスはコールを拒否します。

L2TP トンネルパラメータは APN テンプレート内で設定され、APN にアクセスするすべてのサブスクライバに適用されます。ただし、以下で説明するように、L2TP の動作はサブスクライバの PDP コンテキストタイプによって異なります。

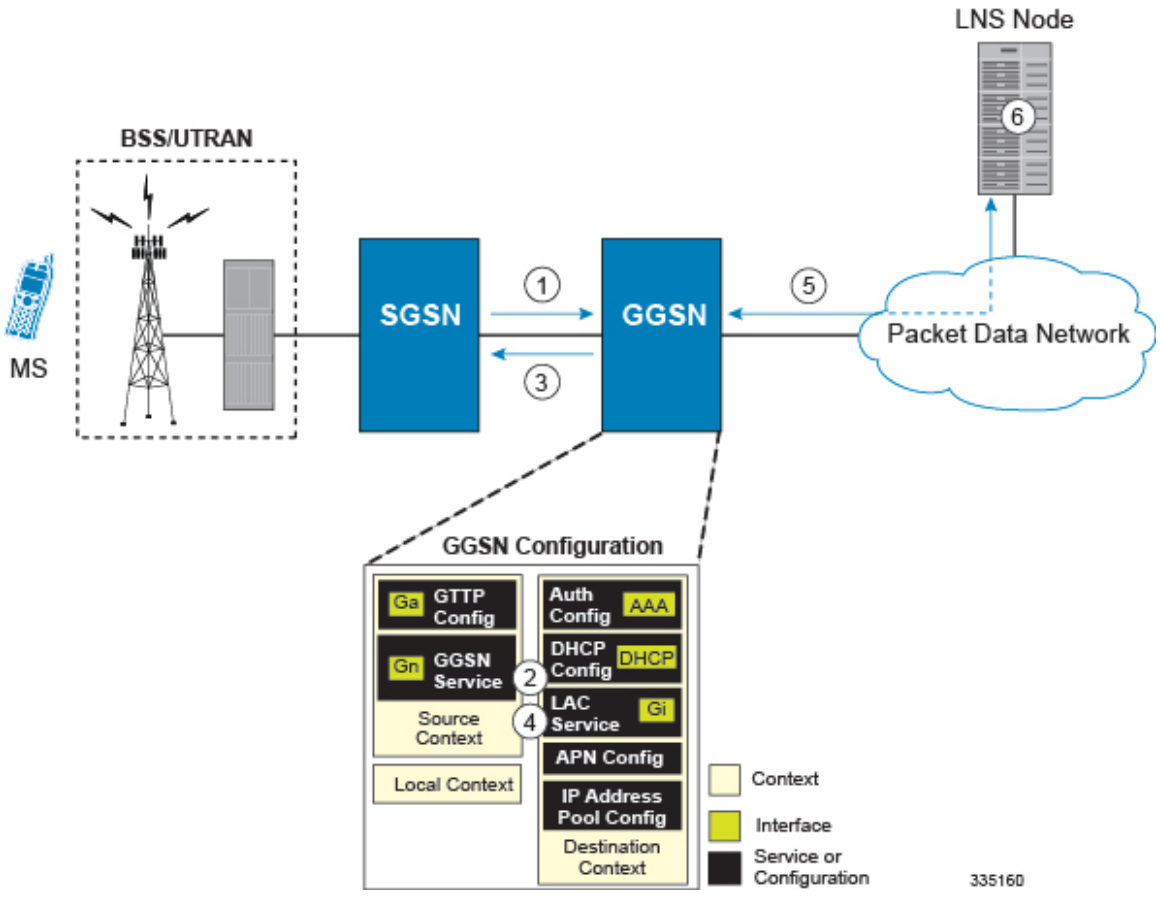
- **Transparent IP**：APNテンプレートのL2TPパラメータ設定がセッションに適用されます。
- **Non-transparent IP**：認証が必要であるため、サブスクライバプロファイルの L2TP パラメータ属性（設定されている場合）が APN テンプレートの設定よりも優先されます。
- **PPP**：APN テンプレートの L2TP パラメータ設定が適用され、サブスクライバのすべての PPP パケットが指定された LNS に転送されます。

詳細については、以降の項を参照してください。

L2TP サポートによる透過 IP PDP コンテキスト処理

次の図とその後のテキストで、L2TP トンネリングが有効な場合の透過 IP PDP コンテキストの処理方法について説明します。

図 *5: L2TP* トンネリングによる透過 *IP PDP* コンテキストのコール処理



1. サブスクライバセッションの PDP コンテキスト作成要求メッセージが、Gn インターフェイスを介して SGSN から GGSN サービスに送信されます。このメッセージには、PDP タイプ、APN、課金特性などの情報が含まれます。

2. GGSN が、メッセージで指定されたものと同じ APN が設定で使用されているかどうかを判定します。同じであれば、APNの設定に基づいてセッションの処理方法を決定します。

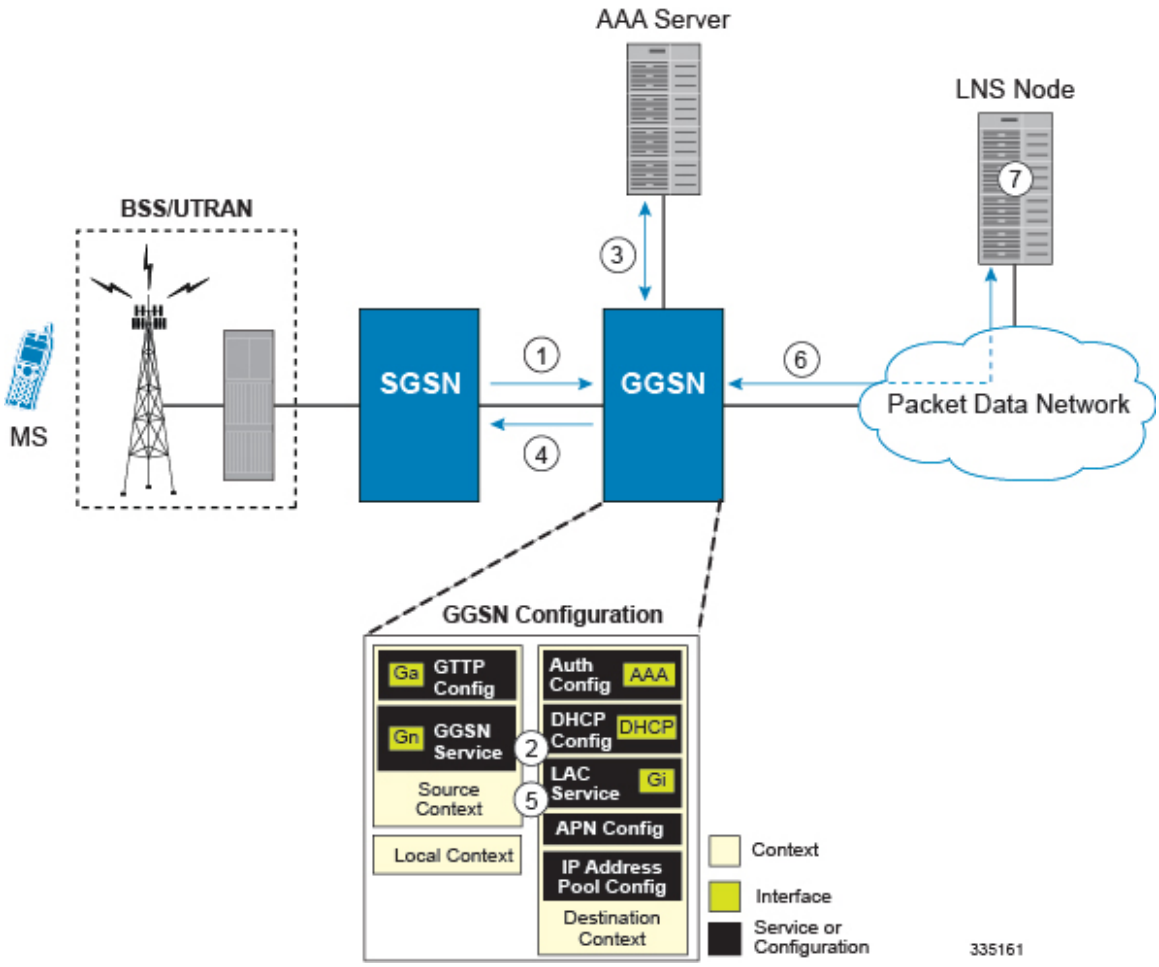
   APN 設定には、LNS の IP アドレス、LAC サービスが設定されているシステム接続先コンテキスト、着信セッションを認証するためにLNSが使用するアウトバウンドユーザー名とパスワードなどが示されています。アウトバウンド情報が設定されていない場合は、サブスクライバの International Mobile Subscriber Identity（IMSI）がピア LNS のユーザー名として使用されます。

1. GGSN が、Gn インターフェイスを介して SGSN に肯定的な PDP コンテキスト作成応答を返します。
2. GGSN が、MS から受信したデータを LAC サービスに渡します。
3. LAC サービスが、IP パケットをカプセル化し、適切な Gi インターフェイスに転送して LNS に配信します。
4. LNSはパケットのカプセル化を解除し、必要に応じて処理します。この処理には、IPアドレスの割り当てが含まれます。

L2TP サポートによる非透過 IP PDP コンテキスト処理

L2TP トンネリングが有効な場合の非透過 IP PDP コンテキストの処理方法について、次の図とともに解説します。

図 *6 : L2TP* トンネリングによる非透過 *IP PDP* コンテキストのコール処理



1. サブスクライバセッションの PDP コンテキスト作成要求メッセージが、Gn インターフェイスを介して SGSN から GGSN サービスに送信されます。このメッセージには、PDP タイプ、APN、課金特性などの情報が含まれます。
2. GGSN が、メッセージで指定されたものと同じ APN が設定で使用されているかどうかを判定します。同じであれば、APN の設定に基づいてセッションの処理方法を決定します。

   APN 設定には、LNS の IP アドレス、LAC サービスが設定されているシステム接続先コンテキスト、着信セッションを認証するために LNS が使用するアウトバウンドユーザー名とパスワードなどが示されています。アウトバウンド情報が設定されていない場合は、サブスクライバのユーザー名がピア LNS に送信されます。

3. GGSN サービスが、サブスクライバを認証します。サブスクライバは、ローカルで設定することも、RADIUS サーバー上にリモートで設定することもできます。上図は、RADIUS AAA サーバーを使用したサブスクライバ認証を示しています。

   認証の一部として、RADIUS サーバーが Access-Accept メッセージを返します。

このメッセージには、セッションデータが L2TP を使用してトンネリングされることを示す属性と、使用する LAC サービスの名前および場所が含まれる可能性があります。接続先の LNS ピアを示す属性も提供されます。

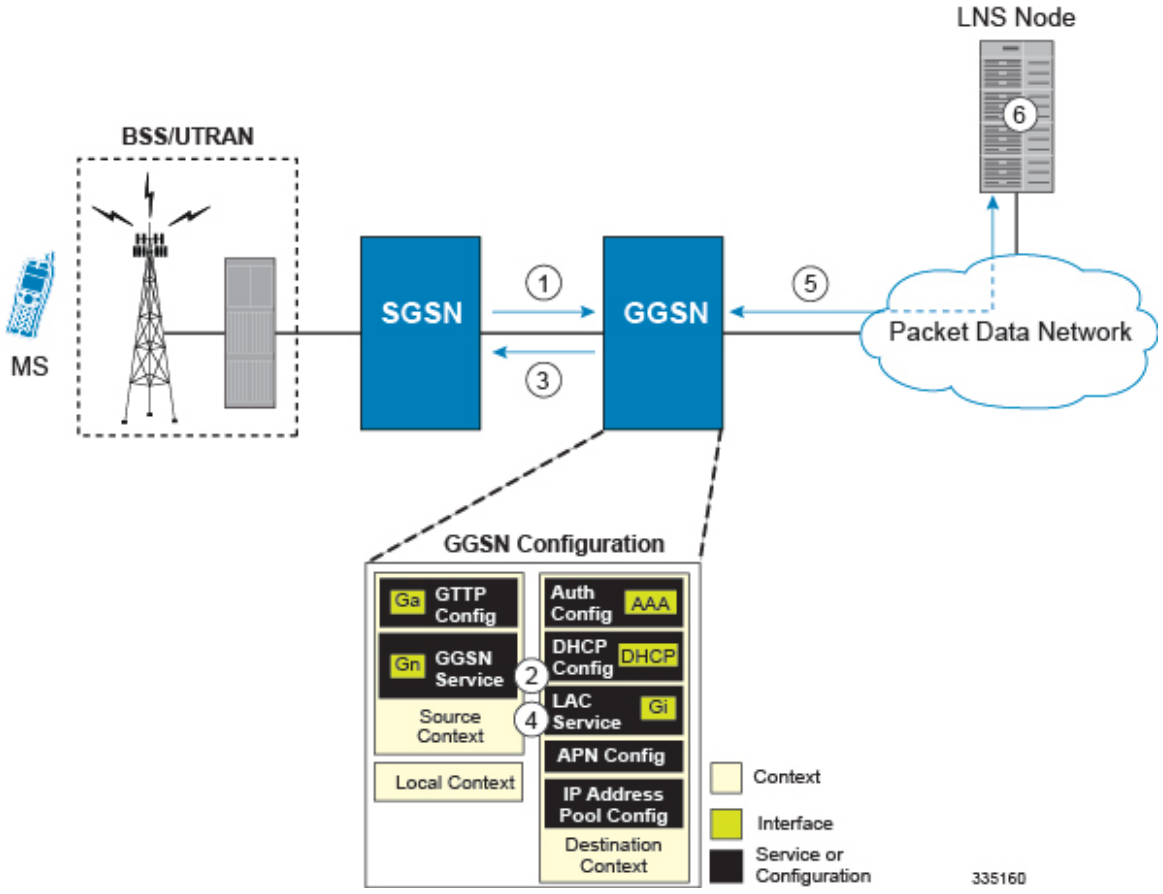
これらの属性が指定されている場合、それらは、APNテンプレートで指定されている属性よりも優先されます。

4. GGSN が、Gn インターフェイスを介して SGSN に肯定的な PDP コンテキスト作成応答を返します。
5. GGSN が、MS から受信したデータを LAC サービスに渡します。
6. LAC サービスが、IP パケットをカプセル化し、適切な Gi インターフェイスに転送して LNS に配信します。
7. LNS が、パケットのカプセル化を解除し、必要に応じて処理します。この処理には、認証と IP アドレスの割り当てが含まれます。

L2TP サポートによる PPP PDP コンテキスト処理

L2TP トンネリングが有効な場合の非透過 IP PDP コンテキストの処理方法について、次の図とともに解説します。

図 *7: L2TP* トンネリングによる *PPP PDP* コンテキストのコール処理



1. サブスクライバセッションの PDP コンテキスト作成要求メッセージが、Gn インターフェイスを介して SGSN から GGSN サービスに送信されます。このメッセージには、PDP タイプ、APN、課金特性などの情報が含まれます。
2. GGSN が、メッセージで指定されたものと同じ APN が設定で使用されているかどうかを判定します。同じであれば、APN の設定に基づいてセッションの処理方法を決定します。

   APN 設定には、LNS の IP アドレス、LAC サービスが設定されているシステム接続先コンテキストが示されています。

   L2TP サポートは、サブスクライバのプロファイルでも設定できます。APN が L2TP トンネリング用に設定されていない場合、システムはサブスクライバの認証を試みます。その後、サブスクライバのプロファイルのトンネリングパラメータを使用して、ピアの LNS が決定されます。
3. GGSN が、Gn インターフェイスを介して SGSN に肯定的な PDP コンテキスト作成応答を返します。
4. GGSN は、MS から受信した PPP パケットを LAC サービスに渡します。
5. LAC サービスは、PPP パケットをカプセル化し、適切な Gi インターフェイスに転送して LNS に配信します。
6. LNS はパケットのカプセル化を解除し、必要に応じて処理します。この処理には、PPP の終了、認証（サブスクライバから提供されたユーザー名/パスワードを使用）、IP アドレスの割り当てが含まれます。

L2TP をサポートするための GGSN または P-GW の設定

ここでは、L2TP をサポートするように GGSN または P-GW を設定するために必要な手順を示します。一覧表示されている各手順では、必要な手順を実行するための具体的な指示を含む別のセクションが参照されています。

重要 該当する指示は、システムがサブスクライバ データ セッションを GGSN または P-GW としてサポートするように事前に設定されていることを前提としています。

手順

ステップ 1 この章の「*L2TP* をサポートするための *APN* テンプレートの 変更」に示されている情報と手順に従って、L2TP トンネリングをサポートするよう に APN テンプレートを設定します。

重要
L2TP トンネリングは、APN テンプレートを使用したサポートの設定とは対照的に、またはそれに加えて、個々のサブスクライバプロファイル内で設定できます。サブスクライバプロファイルの設定については、この章の「*L2TP* サポート用のサブスクライバプロファイルの設定」を参照してください。

ステップ 2 この章の「*LAC* サービスの設定」セクションに記載されている情報と手順に従って、1 つ以上の LAC サービスを設定します。

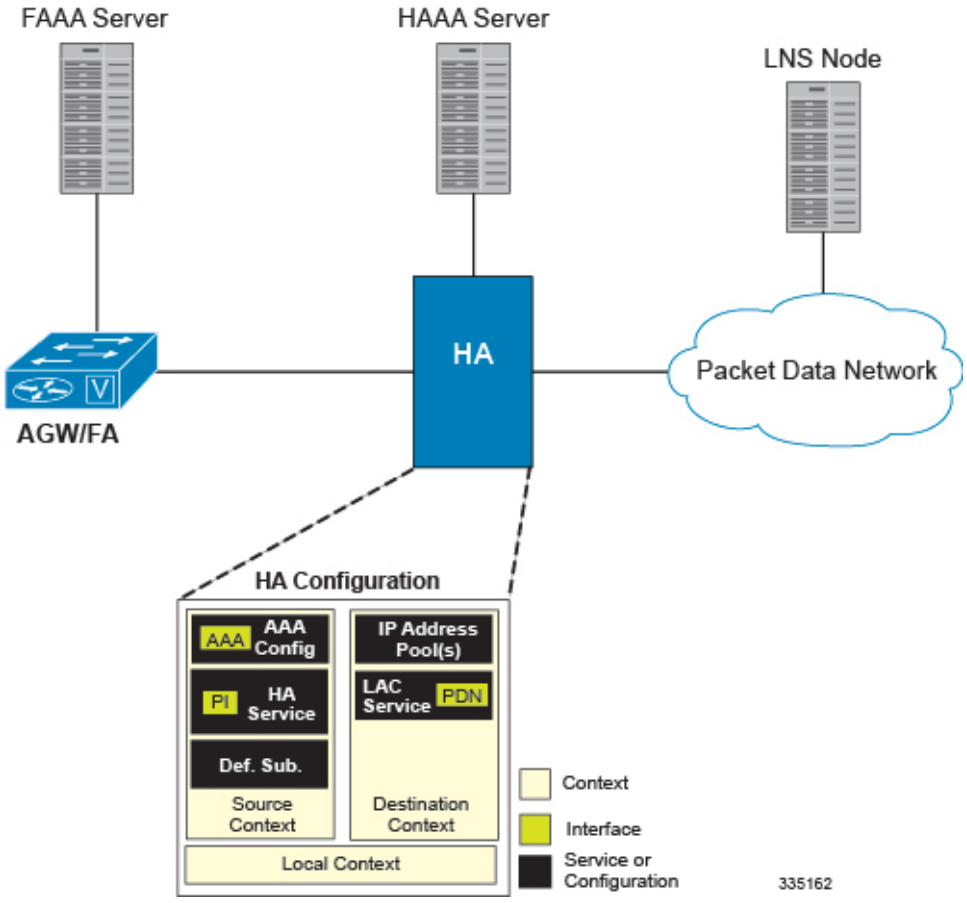
ステップ 3 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

モバイル IP でサポートされる LAC サービス設定

LAC サービスは、属性ベースのトンネリングを使用して、着信 MIP セッションに適用できます。属性ベースのトンネリングは、認証中に識別された特定のユーザーの PPP パケットをカプセル化するために使用されます。このメソッドでは、通信可能な LAC サービスパラメータと許可される LNS ノードが、特定のサブスクライバのユーザープロファイルによって制御されます。ユーザープロファイルは、システム上でローカルで設定できますし、RADIUS サーバー上でリモートで設定することもできます。

各 LAC サービスは、同じシステムコンテキスト内の単一のシステムインターフェイスにバインドされます。次の図に示すように、このコンテキストを接続先コンテキストにすることを推奨します。

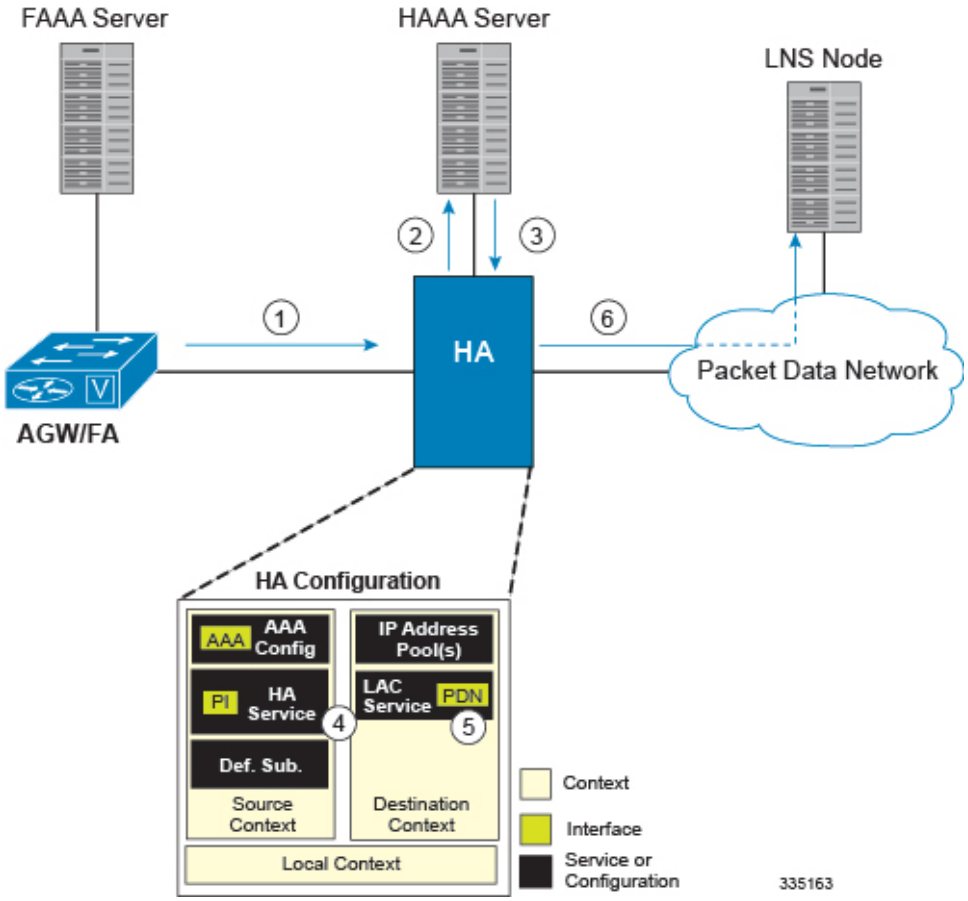
図 *8 : MIP* 用の *LAC* サービスの設定



MIP の属性ベース L2TP 設定の仕組み

次の図とその後のテキストは、システムを使用して MIP の属性ベーストンネリングがどのように実行されるかを示しています。

図 *9 : MIP* の属性ベース *L2TP* セッション処理



1. FA からのサブスクライバセッションは、Pi インターフェイスを介して HA サービスによって受信されます。
2. HA サービスは、サブスクライバの認証を試みます。サブスクライバは、ローカルで設定することも、RADIUS サーバー上にリモートで設定することもできます。上図は、RADIUS AAA サーバーを使用したサブスクライバ認証を示しています。
3. RADIUS サーバーが Access-Accept メッセージを返します。このメッセージには、セッションデータが L2TP を使用してトンネリングされることを示す属性と、使用する LAC サービスの名前と場所が含まれています。接続先の LNS ピアを示す属性も提供されます。
4. HA サービスは、この情報を受信すると、宛先コンテキスト内に設定された LAC サービスにパケットを転送します。
5. LAC サービスは、パケットを受信すると、情報をカプセル化し、LNS に配信するために適切な PDN インターフェイスに転送します。
6. カプセル化されたパケットは、パケットデータネットワークを介してピア LNS に送信され、ここでカプセル化が解除されます。

HA モバイル IP に対する属性ベースの L2TP サポートの設定

ここでは、属性ベースの L2TP サポートを設定し、HA モバイル IP アプリケーションで使用するために必要な手順のリストを示します。一覧表示されている各手順では、必要な手順を実行するための具体的な指示を含む別のセクションが参照されています。

重要 該当する指示は、システムがサブスクライバ データ セッションを HA としてサポートするように事前に設定されていることを前提としています。

手順

ステップ 1 この章の「*L2TP* サポート用のサブスクライバプロファイルの設定」の項に記載されている情報および手順に従って、サブスクライバプロファイルを設定します。

ステップ 2 この章の「*LAC* サービスの設定」セクションに記載されている情報と手順に従って、1 つ以上の LAC サービスを設定します。

ステップ 3 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

L2TP サポート用のサブスクライバプロファイルの設定

この項では次のプロシージャの機能と操作手順について説明します。

重要 サブスクライバの設定手順は RADIUS サーバーアプリケーション間で異なるため、この項では、サブスクライバプロファイルに追加できる個々の属性についてのみ説明します。サブスクライバの設定手順については、RADIUS サーバーに付属のマニュアルを参照してください。

使用される RADIUS とサブスクライバのプロファイル属性

属性ベースの L2TP トンネリングは、システムにローカルに保存されているか、またはリモートで RADIUS サーバーに保存されているサブスクライバプロファイルに設定された属性を使用

してサポートされます。次の表に、LACサービスのサポートで使用される属性を示します。これらの属性は、標準ディクショナリと VSA ディクショナリに含まれています。

表 *1 : L2TP* サポートのためのサブスクライバ属性

RADIUS 属性	ローカルサブスクライバ属性	説明	変数
Tunnel-Type	tunnel l2tp	サブスクライバセッションに使用されるトンネルのタイプを指定します。	L2TP
Tunnel-Server-Endpoint	tunnel l2tp peer-address	トンネルの接続先であるピア LNS の IP アドレスを指定します。	引用符で囲まれたドッ式の IPv4 アドレス
Tunnel-Password	tunnel l2tp secret	LAC と LNS との間での共有秘密を指定します。	引用符で囲まれた 1 ～英字および数字の文字
Tunnel-Private-Group-ID	tunnel l2tp tunnel-context	使用する LAC サービスが配置されているシステムに設定されている、接続先コンテキストの名前を指定します。 **重要** LAC サービスと出力インターフェイスがコアサービスまたはHAサービスと同じコンテキストで設定されている場合、この属性は必要ありません。	引用符で囲まれた 1 ～英字および数字の文字
Tunnel-Preference	tunnel l2tp preference	複数の LNS ノードが設定されている場合に、各ピア LNS の優先順位を設定します。 **重要** この属性は、**loadbalance-tunnel-peers** パラメータまたは **SN-Tunnel-Load-Balancing** 属性が優先されるように設定されている場合にのみ使用されます。	1 ～ 65535 の整数

RADIUS 属性	ローカルサブスクライバ属性	説明	変数
SN-Tunnel-Load-Balancing	loadbalance-tunnel-peer	複数の LNS ピアがサブスクライバプロファイルに設定されている場合に、RADIUS サーバーでの LNS ノードの選択方法を定義する選択アルゴリズムを指定するために使用されるベンダー固有の属性（VSA）。	• **Random**：LNS の順序ダムに選択します。L選択において **Tunnel-Preference** 属用されません。 • **Balanced**：設定された の LNS ノード間で負等配置するよう LNS に選択します。LNS において **Tunnel-Pref** 属性は使用されませ • **Prioritized**：**Tunnel-Preference** 属り当てられた優先順位いて LNS が選択され
Client-Endpoint	local-address	サブスクライバの L2TP セッションを利用しやすくするために使用する、システムに設定されている特定の LAC サービスの IP アドレスを指定します。 この属性は、複数の LAC サービスが設定されている場合に使用されます。	ドット 10 進表記の IPv4 ア ス。（xxx.xxx.xxx.xxx）

RADIUS タギングのサポート

システムは、トンネル属性の RADIUS 属性タギングをサポートしています。ユーザープロファイルで複数の LNS ノードが定義されている場合、これらの「タグ」により、複数の属性が異なるグループに編成されます。タギングは、特定のサーバーに使用されるすべての属性をシステムがグループ化するために役立ちます。特定の RADIUS サーバーで属性タギングがサポートされていない場合、システムは、暗黙的に、アクセス承認パケットに列挙された順で属性を編成します。

L2TP サポート用のローカル サブスクライバ プロファイルの設定

ここでは、L2TP をサポートするように、ローカル サブスクライバ プロファイルをシステムで設定する手順について説明します。

重要 RADIUS ベースのサブスクライバプロファイルの設定については、このドキュメントでは説明していません。詳細については、ご使用の RADIUS サーバーに関するドキュメントを参照してください。

重要 ここでは、システムで L2TP サポート用のローカル サブスクライバ プロファイルを設定するための最小の命令セットについて説明します。追加のパラメータやオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*LAC Service Configuration Mode Commands*」の章 [英語] を参照してください。

L2TP サポートをサブスクライバに提供するようにシステムを設定するには、次の手順を実行します。

手順

ステップ 1 「ローカルサブスクライバの設定」の設定例を適用して、L2TP トンネルパラメータおよびロード バランシング パラメータとアクションを使用して「ローカル」サブスクライバを設定します。

ステップ 2 「*L2TP* の設定 の確認」の手順に従って、L2TP の設定を確認します。

ステップ 3 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

ローカルサブスクライバの設定

L2TP トンネルパラメータを使用してローカルサブスクライバを設定するには、次の例に示すコマンドを使用します。必要に応じて、複数の LNS サーバー間でロードバランシングを設定できます。

```
configure
   context <ctxt_name> [-noconfirm]
      subscriber name <subs_name>
         tunnel l2tp peer-address <lns_ip_address> [ preference <integer> | [
encrypted ] secret <secret_string> | tunnel-context <context_name> |
local-address <local_ip_address> }
         load-balancing { random | balanced | prioritized }
         end
```

注：

- *<ctxt_name>* は、サブスクライバプロファイルを設定するシステムコンテキストです。

- <*lns_ip_address*> は LNS サーバーノードの IP アドレスで、<*local_ip_address*> は LAC サービスにバインドされているシステムの IP アドレスです。

L2TP 設定の確認

これらの手順は、L2TP の設定を確認するために使用されます。

手順

特定のコンテキストの Exec モードで次のコマンドを入力して、L2TP が適切に設定されていることを確認します。

show subscriber configuration username *user_name*

このコマンドの出力には、サブスクライバパラメータの設定が簡潔に一覧表示されます。

RADIUS 属性を使用しない特定コンテキスト内のすべてのサブスクライバのトンネリング

システムでサポートされている他のサービスと同様に、RADIUS Access-Accept メッセージの一部として返されないサブスクライバプロファイル属性の値は、default というサブスクライバの、ローカルに設定されたプロファイルを使用して取得できます。default のサブスクライバプロファイルは、AAA コンテキスト（つまり、AAA 機能が設定されているコンテキスト）で設定する必要があります。

時間節約機能として、RADIUS ベースのサブスクライバ向けに追加の設定を行わずに、default というサブスクライバに対して L2TP サポートを設定できます。これは、特定のサブスクライバに個別の送信元/AAA コンテキストがある場合に特に役立ちます。

default というサブスクライバのプロファイルを設定するには、上記のローカルサブスクライバの設定手順に従い、default という名前を入力します。

機能説明

モバイル顧客宅内機器（CPE）にマルチキャストサービスが設定されている場合、APN は L2TP トンネルを使用して設定され、P-GW は L2TP アクセスコンセントレータ（LAC）として機能します。マルチキャストセッションを設定するには、ビデオクライアント/モバイル CPE が、SGi L2TP トンネルを介してビデオヘッドエンドサーバーとの間で PIM（プロトコル独立マルチキャスト）メッセージ（TTL=1）を送受信する必要があります。

P-GW は、デフォルトの L2TP LAC に従い、L2TP トンネル内のカプセル化された IP トラフィックを検査および処理します。このプロセスは、CPE と TTL=1 トラフィックを送信する LNS の間の特定のアプリケーションの機能を阻止します。21.21.1 より前のリリースでは、IP パケッ

トが送信されると、存続可能時間（TTL）値（255 など）がホップごとに 1 ずつ減少していました。P-GW は、TTL 値が 0 または 1 のパケットをドロップし、TTL 値を減少させ（TTL > 1 の場合）、データパケットの新しいチェックサムを計算しました。このリリースでは、CLI を使用して、L2TP 機能を介したマルチキャストセッションを有効にします。

- P-GW は TTL 値を無視してパケットを転送します。
- L2TP パケットと通常のパケットは sessmgr_ipv4.c の L2TP トンネルタイプで区別され、有効になっている CLI コンフィギュレーション モードが検証されます。

LAC サービスの設定

重要 すべてのコマンド、キーワード、および関数を使用できるわけではありません。機能はプラットフォームおよびライセンスによって異なります。

この項では、ピア LNS ノードと通信できるようにシステムで LAC サービスを設定するための情報と手順について説明します。

重要 システムで LAC サービス機能を設定するための最小の命令セットについて説明します。追加のパラメータとオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*LAC Service Configuration Mode Commands*」の章を参照してください。

システムで LAC サービスを設定するには、次の手順を実行します。

手順

ステップ 1 「*LAC* サービスの 設定」の項の設定例を適用して、システムに LAC サービスを設定し、IP アドレスにバインドします。

ステップ 2 オプションです。Tunnel-Service-Endpoint 属性がサブスクライバプロファイルで設定されていない場合、または PDSN 強制トンネリングがサポートされている場合は、「*LNS* ピアの設定」の項の設定例を適用して、LNS ピア情報を設定します。

ステップ 3 「LAC サービスの設定の確認」の項の手順に従って、LAC の設定を確認します。

ステップ 4 Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

LAC サービスの設定

LAC サービスを作成し、そのサービスを IP アドレスにバインドするには、次の例を使用します。

```
configure
   context <dst_ctxt_name> [-noconfirm]
      lac-service <service_name>
         bind address <ip_address>
         end
```

注：

- *<dst_ctxt_name>* は、LAC サービスを設定する接続先コンテキストです。

L2TP を介したマルチキャストサービスの設定

L2TP を介したマルチキャストセッション機能を有効または無効にするには、次の CLI コマンドを使用します。デフォルトでは、この機能は無効になっています。

```
configure
   context context_name
      lac-service service_name
         ttl-ignore
         end
```

注：

- **ttl-ignore**：TTL 値を無視してパケットを転送します。

LNS ピアの設定

LNS ピアや複数の LNS ピア間でのロードバランシングを設定するには、次の例を使用します。

```
configure
   context <dst_ctxt_name> [ -noconfirm ]
      lac-service <service_name>
         tunnel selection-key tunnel-server-auth-id
        peer-lns <ip_address> [encrypted] secret <secret> [crypto-map <map_name>
 {[encrypted] isakmp-secret <secret> }] [description <text>] [ preference
<integer>]
         load-balancing { random | balanced | prioritized }
         end
```

注：

- *<dst_ctxt_name>* は、LAC サービスを設定する接続先コンテキストです。

LAC サービス設定の確認

次の手順は、LAC サービスの設定を確認するために使用します。

手順

特定のコンテキストの Exec モードで次のコマンドを入力して、LAC サービスが適切に設定されていることを確認します。

show lac-service name *service_name*

以下の出力では、LAC サービスのパラメータの設定が簡潔に一覧で示されます。

```
Service name: vpn1
Context:                        isp1
Bind:                           Done
Local IP Address:               192.168.2.1
First Retransmission Timeout:   1 (secs)
Max Retransmission Timeout:     8 (secs)
Max Retransmissions:            5
Max Sessions:                   500000      Max Tunnels: 32000
Max Sessions Per Tunnel:        512
Data Sequence Numbers:          Enabled     Tunnel Authentication:  Enabled
Keep-alive interval:            60          Control receive window: 16
Max Tunnel Challenge Length:    16
Proxy LCP Authentication:       Enabled
Load Balancing:                 Random
Service Status:                 Started
Newcall Policy:                 None
```

L2TP サポートのための PDSN サービスの変更

PDSN サービスの変更は強制トンネリングでは必須であり、属性ベースのトンネリングでは任意です。

属性ベースのトンネリングでは、設定エラーが発生する可能性があります。例えば、認証が成功すると、システムは、サブスクライバセッションが L2TP を必要としていると判断するものの、提供された属性からでは、適切な LAC サービスが設定されているコンテキストの名前を特定できません。予防措置として、PDSN サービス設定オプションにパラメータが 1 つ追加されました。このパラメータは、使用するコンテキストの名前を示します。このパラメータを設定することを強く推奨します。

この項では、強制または属性ベースのいずれかのトンネリング用にPDSNサービス設定を変更する手順について説明します。

重要 この項では、システムで L2TP をサポートするように PDSN サービスを変更するための最小の命令セットについて説明します。追加のパラメータやオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*LAC Service Configuration Mode Commands*」の章 [英語] を参照してください。

システムで LAC サービスを設定するには、次の手順を実行します。

手順

ステップ 1 「*PDSN* サービスの変更」セクション の設定例を適用して、LAC コンテキストを関連付け、トンネルタイプを定義して、L2TP をサポートするように PDSN サービスを変更します。

ステップ 2 「*L2TP* サポートのための *PDSN* サービスの確認」の項の手順に従って、PDSN サービスを変更するための設定を確認します。

ステップ 3 Exec モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、および/またはネットワークの場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

PDSN サービスの変更

次の例を使用して、LAC コンテキストを関連付けてトンネルタイプを定義することで、L2TP をサポートするように PDSN サービスを変更します。

```
configure
  context <source_ctxt_name> [ -noconfirm ]
    pdsn-service <pdsn_service_name>
      ppp tunnel-context <lac_context_name>
      ppp tunnel-type { l2tp | none }
      end
```

注：

- <*source_ctxt_name*> は、L2TP サポートのために変更する PDSN サービスを含むソースコンテキストの名前です。
- <*pdsn_service_name*> は、L2TP サポートのために変更する事前設定済みの PDSN サービスの名前です。
- <*lac_context_name*> は通常、LAC サービスが設定されている接続先コンテキストです。

L2TP サポートのための PDSN サービスの確認

PDSN サービスの設定を確認するには、これらの手順を使用します。

手順

特定のコンテキストの Exec モードで次のコマンドを入力して、PDSN が適切に設定されていることを確認します。

```
show pdsn-service name pdsn_service_name
```

このコマンドの出力には、PDSN サービスのパラメータの設定が簡潔に一覧表示されます。

L2TP をサポートするための APN テンプレートの変更

ここでは、システムで設定されている APN テンプレートで L2TP サポートを追加する手順について説明します。

重要 システムで LAC サービス機能を設定するための最小の命令セットについて説明します。追加のパラメータやオプションを設定するコマンドの詳細については、『*Command Line Interface Reference*』の「*LAC Service Configuration Mode Commands*」の章 [英語] を参照してください。

システムで LAC サービスを設定するには、次の手順を実行します。

手順

ステップ 1 「*APN* テンプレートでの *LNS* ピアアドレスの割り当て」の項の設定例を参考にして、LNS サーバーアドレスやその他のパラメータを使用して L2TP をサポートするように APN テンプレートを変更します。

ステップ 2 オプションです。L2TP を使用してトランスペアレント IP PDP コンテキストをトンネリングする場合は、「アウトバウンド認証の設定」の項の設定例を適用して、APN のアウトバウンドユーザー名とパスワードを設定します。

ステップ 3 「*APN* の設定 の確認」の項の手順に従って、APN の設定を確認します。

ステップ 4 EXEC モードコマンド **save configuration** を使用して、フラッシュメモリ、外部メモリデバイス、もしくはネットワーク上の場所に設定を保存します。構成ファイルを検証して保存する方法の詳細については、『*System Administration Guide*』および『*Command Line Interface Reference*』を参照してください。

APN テンプレートでの LNS ピアアドレスの割り当て

APN テンプレートに LNS サーバーアドレスを割り当てるには、次の例を使用します。

```
configure
   context <dst_ctxt_name> [-noconfirm]
      apn <apn_name>
         tunnel l2tp [ peer-address <lns_address> [ [ encrypted ] secret
<l2tp_secret> ] [ preference <integer> ] [ tunnel-context <l2tp_context_name> ]
[ local-address <local_ip_address> ] [ crypto-map <map_name> { [ encrypted ]
isakmp-secret <crypto_secret> } ]
         end
```

注：

- <*dst_ctxt_name*> は、APN が設定されているシステム接続先コンテキストの名前です。
- <*apn_name*> は、L2TP サポートのために変更する、事前設定された APN テンプレートの名前です。
- <*lns_address*> は LNS サーバーノードの IP アドレスで、<*local_ip_address*> は LAC サービスにバインドされているシステムの IP アドレスです。

アウトバウンド認証の設定

LNS ピアや複数の LNS ピア間でのロードバランシングを設定するには、次の例を使用します。

```
configure
   context <dst_ctxt_name> [ -noconfirm ]
      apn <apn_name>
         outbound { [ encrypted ] password <pwd> | username <name> }
         end
```

注：

- <*dst_ctxt_name*> は、APN テンプレートが設定されている接続先コンテキストです。
- <*apn_name*> は、L2TP サポートのために変更する、事前設定された APN テンプレートの名前です。

APN 設定の確認

次の手順は、APN の設定を確認するために使用されます。

手順

特定のコンテキストの Exec モードで次のコマンドを入力して、APN が適切に設定されていることを確認します。

```
show apn name apn_name
```

出力では、APN のパラメータの設定が簡潔に一覧表示されます。

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。