



# Cisco パケット データ サービス ノード リリース 5.1 (Cisco IOS リリース 12.4(22)XR2 対応)

Cisco Packet Data Serving Node Release 5.1 for Cisco IOS Release 12.4(22)XR2

---

OL-20782-01-J

**【注意】** シスコ製品をご使用になる前に、安全上の注意 ([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)) をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

## 機能履歴

この表で、Cisco Packet Serving Node (PDSN; Cisco パケット サービス ノード) リリースの機能サポートを説明しています。

リリース	変更内容
12.4(22)XR1	<p>Cisco PDSN のリリース 5.1。次の新機能が追加されました。</p> <ul style="list-style-type: none"> <li>「簡易 IP クライアントの IP アカウンティングのサポート」</li> <li>「PCF 単位の SNMP の新規 MIB オブジェクト」</li> <li>「一般的な NAI のサポート」</li> <li>「最新の IS-835 に合わせたプロキシ MIP の変更」</li> <li>「簡易 IPv6 サポート」</li> <li>「Access-Request アトリビュート」</li> <li>「新しい PCF カウンタ単位の PPP」</li> <li>「VPDN 条件付きデバッグ」</li> <li>「Revocation メッセージの GRE CVSE および MN NAI 拡張」</li> </ul>
12.4(22)XR	<p>Cisco PDSN のリリース 5.0。次の新機能が追加されました。</p> <ul style="list-style-type: none"> <li>「ブレード単位の単一 IP」</li> <li>「Osler のサポート」</li> <li>「改善されたスループットとトランザクション処理」</li> <li>「単一 IP ブレードのクラスタ コントローラのサポート」</li> <li>「IMSI および PCF のリダイレクション」</li> <li>「China Telecom 用モバイル IP および AAA アトリビュート」</li> <li>「MIB のサポート」</li> <li>「AAA サーバ非応答に対するトラップ生成」</li> <li>「スーパーバイザのサポート」</li> <li>「Data Over Signaling」</li> <li>「Differentiated Services Code Point マーキングのサポート」</li> <li>「Nortel Aux A10 のサポート」</li> <li>「IMSI プレフィックスのマスキング解除」</li> <li>「永続的な TFT のサポート」</li> <li>「FA-HA IP-in-IP トンネルの場合の一意的な IP-ID の保存」</li> <li>「GRE CVSE Support in FA-HA Tunnel」</li> <li>「リモートアドレス アカウンティング」</li> <li>「デフォルトのサービス オプション実装」</li> <li>「Configurable Per-Flow アカウンティング オプション」</li> <li>「IP フロー識別子の PCF 下位互換性サポート」</li> <li>「max-class 値に対する DSCP のコメントのサポート」</li> <li>「フラグメンテーション サイズのコマンド サポート」</li> <li>「China Telecom 向けの新しい統計カウンタ」</li> </ul>

12.4(15)XR2	<p>Cisco PDSN のリリース 4.1。次の新機能が追加されました。</p> <ul style="list-style-type: none"> <li>• アトリビュートのサポート <ul style="list-style-type: none"> <li>- 「Served MDN」</li> <li>- 「Framed Pool」</li> <li>- 「3GPP2 DNS サーバ IP」</li> </ul> </li> <li>• 「サブインターフェイスがある仮想ルート フォワーディング」</li> <li>• 「条件付きデバッグの機能拡張」</li> </ul>
12.4(15)XR	<p>Cisco PDSN のリリース 4.0。次の新機能が追加されました。</p> <ul style="list-style-type: none"> <li>• 「複数サービス接続」</li> <li>• 「データ プレーン」</li> <li>• 「加入者 QoS ポリシー」 (AAA サーバからのユーザ プロファイルごとのダウンロードと、ローカル プロファイルの設定)</li> <li>• 「QoS シグナリング」</li> <li>• 「トラフィック フロー テンプレート」</li> <li>• 「Per-flow アカウンティング」</li> <li>• 「コール アドミッション制御」</li> <li>• 「PDSN MIB の機能強化」</li> <li>• 「SAMI 上の PDSN」</li> </ul> <p>Closed-RP サポートはリリース 4.0 からなくなりました。</p> <p>PPPoGRE RP インターフェイス サポートはリリース 4.0 からなくなりました。</p>
12.4(15)XN	<p>Cisco PDSN のリリース 3.5。次の新機能が追加されました。</p> <ul style="list-style-type: none"> <li>• 「AAA サーバからダウンロードされたホーム エリア、最大認可集約帯域幅、およびユーザ間優先順位アトリビュート」 <ul style="list-style-type: none"> <li>- 「加入者 QoS ポリシー」</li> <li>- 「帯域幅のポリシング」</li> </ul> </li> </ul>
12.3(14)YX8	<p>Cisco PDSN のリリース 3.0。次のコマンドが更新されました。</p> <ul style="list-style-type: none"> <li>• cdma pdsn cluster member prohibit administratively</li> <li>• subscriber redundancy rate</li> </ul> <p>ODAP および PDN Selection ピアツーピアクラスタリングの章を削除しました。</p>
12.3(14)YX1	<p>Cisco PDSN のリリース 3.0。次の新機能が追加されました。</p> <ul style="list-style-type: none"> <li>• 「Mobile Equipment Identifier のサポート」</li> </ul>

12.3(14)YX	<p>Cisco PDSN のリリース 3.0。次の新機能が追加されました。</p> <ul style="list-style-type: none"> <li>「<a href="#">パケット データ サービスのアクセス</a>」 <ul style="list-style-type: none"> <li>「<a href="#">簡易 IPv6 アクセス</a>」</li> </ul> </li> <li>「<a href="#">セッション冗長性のインフラストラクチャ</a>」</li> <li>「<a href="#">RADIUS サーバのロード バランシング</a>」</li> <li>「<a href="#">PPPoGRE RP インターフェイス</a>」</li> <li>「<a href="#">ドメインに基づく加入者認可</a>」</li> <li>「<a href="#">PDSN MIB の機能強化</a>」</li> <li>「<a href="#">条件付きデバッグの機能拡張</a>」</li> </ul>
12.3(11)YF3	<p>Cisco PDSN のリリース 2.1。</p> <p>次のサポートが追加されました。</p> <ul style="list-style-type: none"> <li>「<a href="#">IMSI 処理のランダム化</a>」</li> </ul> <p>次の新しいコマンドが追加されました。</p> <ul style="list-style-type: none"> <li><code>ip mobile cdma imsi dynamic</code></li> </ul>
12.3(11)YF2	<p>Cisco PDSN のリリース 2.1。</p> <p>次のサポートが追加されました。</p> <ul style="list-style-type: none"> <li>「<a href="#">SDB 指示の場合のデータ パケットの識別</a>」</li> <li>「<a href="#">PPP コントロール パケットの SDB インジケータ マーキング</a>」</li> <li>「<a href="#">Acct-Stop および暫定レコードでの G17 アトリビュートのサポート</a>」</li> </ul> <p>次の新しいコマンドが追加または修正されました。</p> <ul style="list-style-type: none"> <li><code>cdma pdsn a11 dormant sdb-indication match-qos-group</code></li> <li><code>cdma pdsn compliance</code></li> <li><code>cdma pdsn attribute send g17</code></li> </ul>
12.3(11)YF1	<p>Cisco PDSN のリリース 2.1。</p> <p>Registration Revocation の制限事項がなくなりました。</p> <p>次の新しいコマンドが追加または修正されました。</p> <ul style="list-style-type: none"> <li><code>cdma pdsn compliance</code></li> <li><code>debug cdma pdsn prepaid</code></li> <li><code>debug cdma pdsn radius disconnect nai</code></li> <li><code>show cdma pdsn statistics prepaid</code></li> <li><code>clear cdma pdsn session</code></li> <li><code>clear cdma pdsn statistics adds radius statistics</code></li> <li><code>cdma pdsn mobile-advertisement-burst</code></li> <li><code>ip mobile foreign-service</code></li> </ul>
12.3(11)YF	<p>Cisco PDSN のリリース 2.1。Closed-RP インターフェイスを含む 4 つの新機能が追加されました。</p>
12.3(8)XW	<p>Cisco PDSN のリリース 2.0。常時接続を含む 5 つの新機能が追加されました。</p>

12.3(4)T	Cisco PDSN (Cisco IOS ソフトウェア) 機能が Cisco IOS リリース 12.3(4)T に統合されました。
12.2(8)ZB8	新しい CLI コマンドが 1 つ追加されました。
12.2(8)ZB7	CLI コマンドが 6 つ追加または修正されました。
12.2(8)ZB6	CLI コマンドが 2 つ追加または修正されました。
12.2(8)ZB5	CLI コマンドが新しく 4 つ追加されました。
12.2(8)ZB1	Cisco 7600 シリーズ ルータで Cisco PDSN 機能が導入されました。
12.2(8)ZB	Cisco Catalyst 6500 Switch で Cisco PDSN 機能が導入されました。
12.2(8)BY	Cisco 7200 シリーズ ルータで Cisco PDSN 機能が導入されました。

この文書では、Cisco 7600 シリーズ ルータに取り付けられた Cisco Service and Application Module for IP (SAMI) カードで使用する Cisco Packet Data Serving Node (PDSN; Cisco パケット サービス ノード) ソフトウェアについて説明しています。この文書には、製品の特長と機能、サポートするプラットフォーム、関連資料、設定作業についての情報が記載されています。

この文書は、次の内容で構成されています。

- [「機能の概要」 \(P.5\)](#)
- [「機能」 \(P.21\)](#)
- [「クラスタ コントローラ メンバ設定」 \(P.118\)](#)
- [「サポート対象プラットフォーム」 \(P.256\)](#)
- [「サポート対象の規格、MIB、および RFC」 \(P.256\)](#)
- [「設定作業」 \(P.258\)](#)
- [「システム要件」 \(P.258\)](#)
- [「PDSN のモニタリングとメンテナンス」 \(P.278\)](#)
- [「設定例」 \(P.280\)](#)
- [「PDSN アカウンティング」 \(P.326\)](#)
- [「AAA サーバの認証と認可のプロファイル」 \(P.332\)](#)
- [「アトリビュート」 \(P.334\)](#)
- [「用語集」 \(P.351\)](#)

## 機能の概要

PDSN で、インターネット、イントラネット、モバイル ステーション用 Wireless Application Protocol (WAP; ワイヤレス アプリケーション プロトコル) サーバに、Code Division Multiple Access 2000 (CDMA 2000; 符号分割多重接続 2000) Radio Access Network (RAN; 無線アクセス ネットワーク) を使用してアクセスできます。PDSN は、Cisco 7600 シリーズ ルータの SAMI カードで実行する Cisco IOS ソフトウェア機能で、PDSN は Simple IP (SIP; 簡易 IP) や Mobile IP (MIP; モバイル IP) ステーションのアクセス ゲートウェイとして動作します。PDSN では foreign agent (FA; 外部エージェント) がサポートされており、virtual private networking (VPN; 仮想プライベート ネットワーキング) のパケット転送を行います。また、Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウンティング) クライアントとしても動作します。

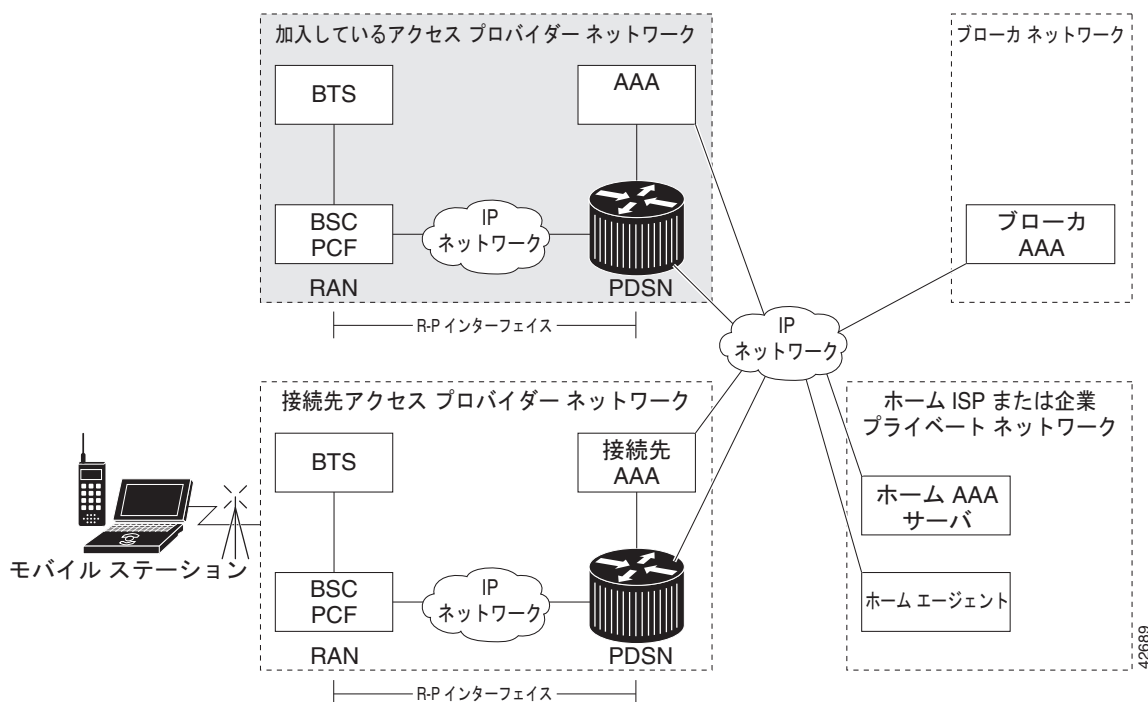
PDSN はすべての関連する 3rd Generation Partnership Project 2 (3GPP2; 第三世代パートナーシップ プロジェクト 2) 規格を、CDMA 2000 ネットワークの全体構造の定義や無線コンポーネントと PDSN 間のインターフェイスを含めてサポートしています。

# システムの概要

CDMA はモバイル ステーション通信の規格の 1 つです。一般的な CDMA 2000 ネットワークには、端末機器、モバイル ターミネーション、base transceiver stations (ベース トランシーバ ステーション; BTS)、base station controllers (ベース ステーション コントローラ; BSCs または Packet Control Functions (PCF; パケット制御機能))、PDSN、その他の CDMA およびデータ ネットワーク エンティティが含まれています。PDSN は、BSC または PCF とネットワーク ルータ間のインターフェイスです。

図 1 で、一般的な CDMA 2000 ネットワークのコンポーネントの関係を示しています。この図では、ローミング モバイル ステーション ユーザは、モバイル ステーション ユーザが加入しているアクセス プロバイダー ネットワークではなく、訪問したアクセス プロバイダー ネットワークからデータ サービスを受信します。

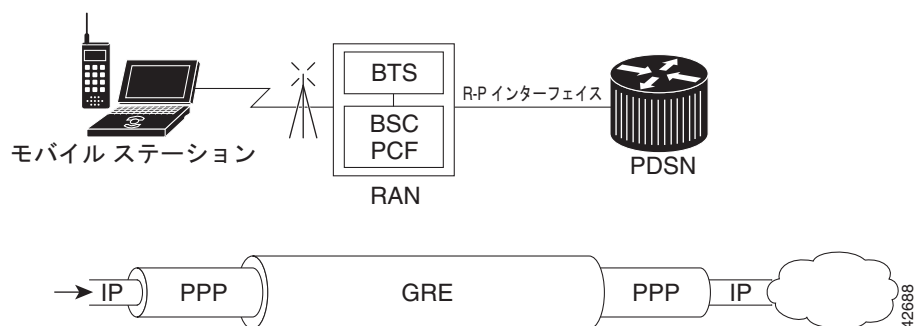
図 1 CDMA ネットワーク



図のように、モバイル ステーションは無線タワーおよび BTS に接続します。モバイル ステーションは、SIP または MIP のどちらかをサポートする必要があります。BTS は BSC に接続し、BSC には Packet Control Function (PCF; パケット制御機能) というコンポーネントが組み込まれています。PCF は A10/A11 インターフェイスを通じて、PDSN と通信します。A10 インターフェイスはユーザ データ用であり、A11 インターフェイスはコントロール メッセージ用です。このインターフェイスは RAN-PDSN (R-P) インターフェイスともいいます。

図 2 で、RAN および PDSN 間の通信を示しています。

図 2 RAN-to-PDSN 通信 : R-P インターフェイス



PDSN と外部データ ネットワーク間の IP ネットワーキングは、PDSN-イントラネットまたはインターネット (P<sub>i</sub>) インターフェイスを介して行われます。Cisco PDSN リリース 2.0 以上では、FE または GE インターフェイスのいずれかを P<sub>i</sub> インターフェイスとして使用できます。

AAA サーバや RADIUS サーバへの接続などの「バック オフィス」接続では、インターフェイスはメディアに依存しません。Cisco 7206 でサポートされているインターフェイスはどれも、これらのタイプのサービスへの接続に使用できます。ただし、Cisco は FE または GE インターフェイスのいずれかを使用することをお勧めします。

## PDSN の動作方法

モバイル ステーションがデータ サービス コールを行うと、PDSN にリンクする Point-to-Point Protocol (ポイントツーポイント プロトコル; PPP) が確立されます。PDSN は、AAA サーバと通信してモバイル ステーションを認証します。AAA サーバはユーザが有効な加入者かを検証し、利用できるサービスを決定し、請求を行うため使用をトラッキングします。

IP アドレスの割り当てに使用する方法や接続の種類は、サービスのタイプとネットワーク設定に依存します。SIP の操作と MIP の操作は、*service types* と呼ばれます。ユーザが利用できるサービスの種類は、モバイル プロバイダーが提供するサービスの種類によって決定されます。PDSN のコンテキストでは、モバイル ステーションは SIP と MIP の操作両方でエンド ユーザとなります。

モバイル ステーションが認証されると、IP アドレスを要求します。SIP ステーションは、Internet Protocol Control Protocol (IPCP; インターネット プロトコル制御プロトコル) を使用して要求をやり取りします。MIP ステーションは、MIP レジストレーションを使用して通信します。

次の章で、該当するトピックごとの IP アドレッシングと通信レベルについて説明します。

- [「PDSN 簡易 IP」](#)
- [「PDSN モバイル IP」](#)
- [「モバイル IP クライアントによる PMTU 検出」](#)

## PDSN 簡易 IP

SIP を使用して、サービス プロバイダーの Cisco PDSN は、PPP リンク設定中にダイナミックまたは固定 IP アドレスをモバイル ステーションに割り当てます。モバイル ステーションはこの IP アドレスを、アドレス割り当て PDSN に接続している無線ネットワークが使用されている限り、保持します。

したがって、モバイルステーションが同じ PDSN で使用されている RAN のエリア内にある限り、カバレッジエリア内に MS を移動あるいはローミングでき、同じ PPP リンクを維持できます。モバイルステーションが、特定の PDSN のカバレッジエリア外に移動した場合、モバイルステーションに新しい IP アドレスが割り当てられ、アプリケーションレベルの接続が終了します。

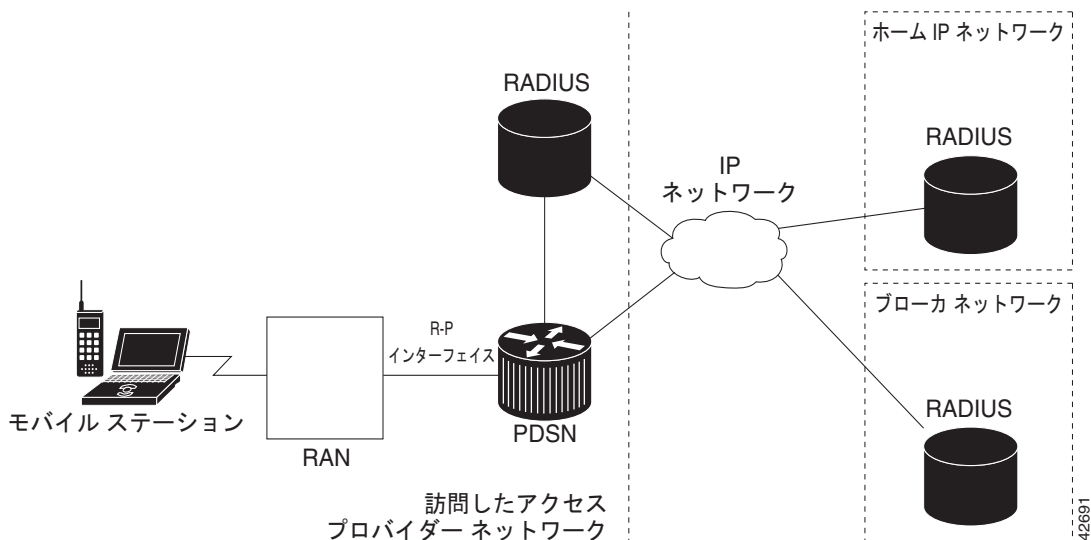


(注)

固定 IP アドレスはモバイルステーションから要求され、アドレスがアドレスのプールに存在し、使用可能な場合に割り当てられます。また、IP アドレスは、「Framed-IP-Address」アトリビュートを使用して、ユーザの AAA プロファイルでスタティックに指定できます。

図 3 では、簡易 IP シナリオでの PDSN の配置を示しています。

図 3 CDMA ネットワーク - 簡易 IP シナリオ



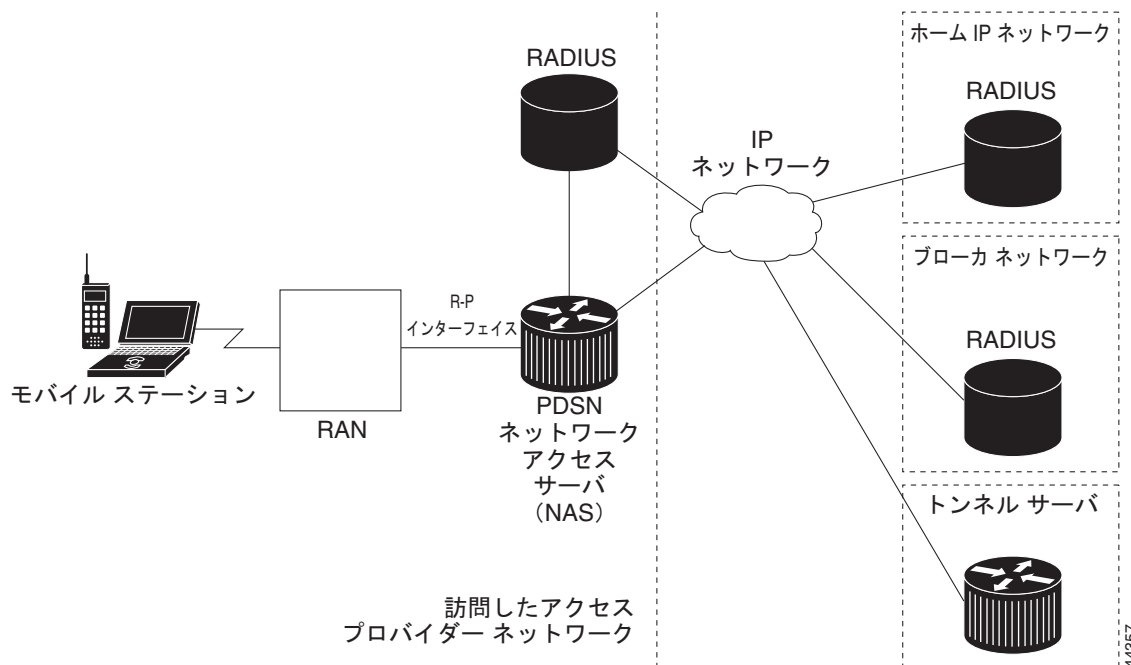
### VPDN を使用した PDSN 簡易 IP シナリオ

Virtual Private Data Network (VPDN; 仮想プライベート データ ネットワーク) で、プライベート ネットワーク ダイアルイン サービスを Network Access Server (NAS; ネットワーク アクセス サーバ) と呼ばれるリモート アクセス サーバに広げることができます。



図 4 は、SIP がある PDSN 環境での VPDN 接続を示しています。このシナリオでは、PDSN は NAS として動作します。

図 4 CDMA ネットワーク - VPDN を使用した簡易 IP シナリオ



VPDN 接続は、次の順番で確立されます。

1. PPP ピア (モバイルステーション) はローカル NAS (PDSN) に接続します。
2. NAS は、クライアントがダイヤルインを行う際に認証を開始します。NAS は、PPP リンクをクライアントのトンネルサーバに転送する必要があるかを決定します。トンネルサーバの位置は、Remote Authentication Dial-in User Service (RADIUS; リモート認証ダイヤルインユーザサービス) サーバによる認証の一部として提供されます。
3. トンネルサーバは、ユーザの認証そのものを実行し、PPP ネゴシエーションを開始します。トンネル設定とクライアントの両方の認証を実行します。

PPP クライアントは、User Datagram Protocol (UDP; ユーザデータグラムプロトコル) 上の Layer 2 Tunneling Protocol (L2TP; レイヤ 2 トンネリングプロトコル) トンネルを介して転送されます。

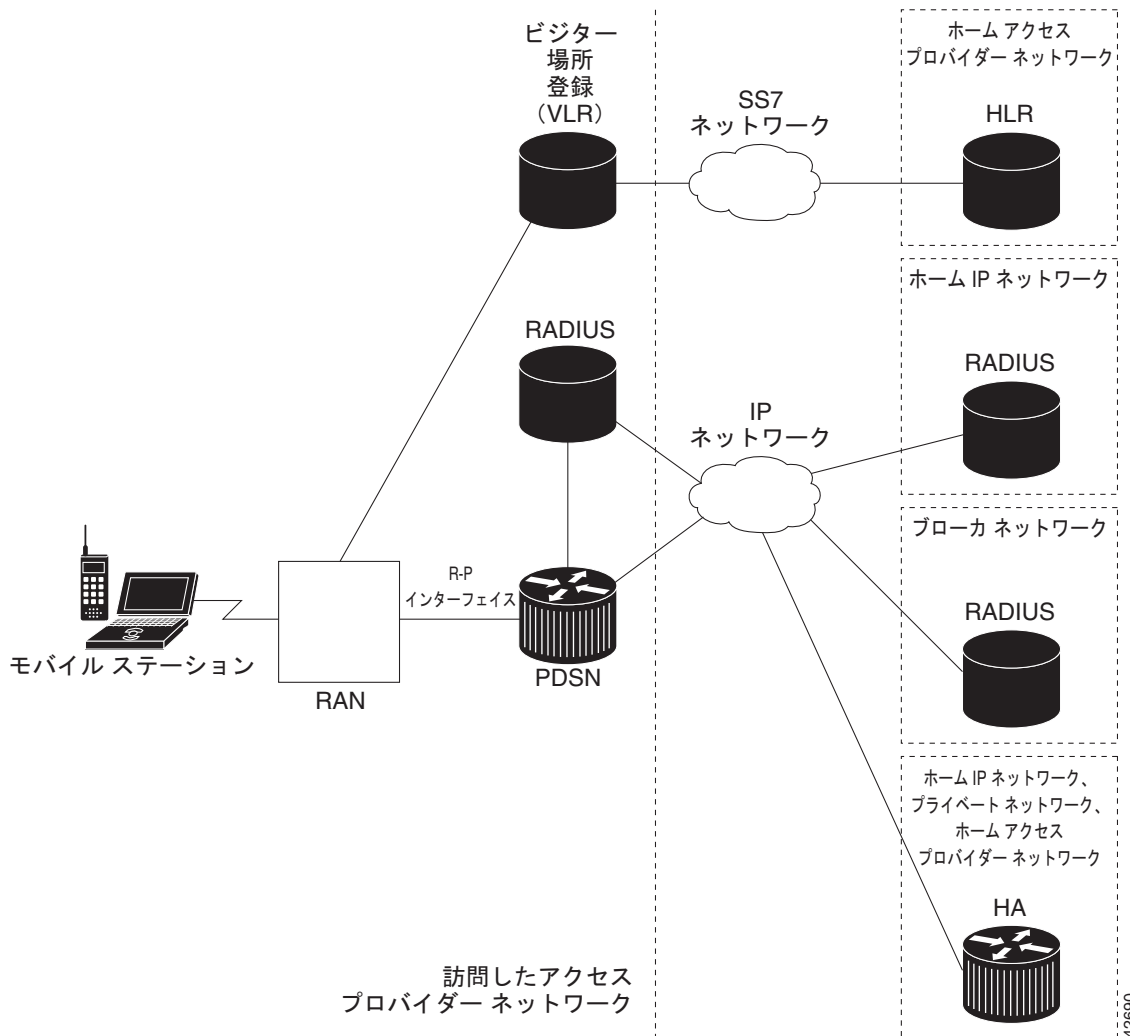
4. PPP 設定が完了し、クライアントとトンネルサーバ間のすべてのフレームが NAS を介して送信されます。PPP 内で実行しているプロトコルは NAS に対して透過的です。

## PDSN モバイル IP

MIP を使用する場合、モバイルステーションは所定の PDSN のカバー エリアを越えて移動でき、なおかつ同じ IP アドレスとアプリケーションレベルの接続を維持できます。

図 5 では、MIP シナリオでの PDSN の配置を示しています。

図 5 CDMA ネットワーク - モバイル IP 環境



通信プロセスの発生順は、次のとおりです。

1. モバイルステーションは、FA を通じて Home Agent (HA; ホーム エージェント) に登録します。今回の場合は PDSN です。
2. HA はレジストレーションを受け付け、モバイルステーションに IP アドレスを割り当て、FA へのトンネルを作成します。これで、モバイルステーションと FA (あるいは PDSN) 間で PPP リンクが行われ、FA と HA 間で IP-in-IP または Generic Routing Encapsulation (GRE; 総称ルーティングカプセル化) トンネルが確立します。

レジストレーション処理の一部として、HA はバインディングテーブルエントリを作成し、モバイルステーションのホームアドレスと対応する気付アドレスを関連付けます。



(注) ホームから離れている間、モバイルステーションは気付アドレスに関連付けられています。このアドレスは、現在のトポロジから見たモバイルステーションのインターネットへの接続ポイントを示し、このアドレスを使用してモバイルステーションにパケットがルーティングされます。IS-835-B ネットワークでは、外部エージェントのアドレスは常に気付アドレスとして使用されます。

3. HA はモバイルステーションにネットワークへの到達が可能であることを通知し、現在の位置のモバイルステーションにデータグラムをトンネリングします。
4. モバイルステーションは、送信元 IP アドレスとしてホームアドレスを指定してパケットを送信します。
5. モバイルステーション宛てのパケットは HA を通過します。HA が PDSN を介して、気付アドレスを使用したモバイルステーションへトンネリングします。
6. PPP リンクが新しい PDSN に引き渡されるときに、リンクの再ネゴシエーションが行われ、MIP レジストレーションが更新されます。
7. HA は新しい CoA を使用して、バインディングテーブルをアップデートします。



(注) MIP の詳細については、Cisco IOS リリース 12.2 のマニュアル『Cisco IOS IP Configuration Guide』および『Cisco IOS IP Command Reference』を参照してください。RFC 2002 で、詳細な仕様が規定されています。TIA/EIA/IS-835-B も、PDSN での MIP の実装方法を定義します。

## IMSI 処理のランダム化

PDSN は、EVDO への 1xRTT を IMSI の変更によるハンドオフとして認識できません。結果、アカウント停止メッセージの「cdma-reason-ind」は同じ内容を反映しません。

デフォルトでは、モバイルが固定ホームアドレスを行う場合、PDSN は最初のコールセッションを維持します。このリリースで、PDSN はダイナミックホームアドレスの場合の最初のコールセッションの削除（たとえば、IMSI がハンドオフ中に変更された場合の EVDO への 1xRTT のハンドオフ）をサポートします。

- コールが同じプロセッサに着信した場合、次のようになります。
  - 新しいセッションは PDSN ではアップにならず、古いセッションが維持されます。
  - 1xRTT および EVDO コール間のモバイルハンドオフ中は、上記のような PDSN の動作により、ハンドオフは成功しません。
- コールが異なるプロセッサに着信した場合、次のようになります。
  - アップしたコールと古いコールの両方が、レジストレーションライフタイムが期限切れになった時点で削除されます。新しいコールに対しては、ダウンストリームトラフィックは処理されません。

古いセッションを削除できる新しい CLI コマンドが、このリリースで導入されました。**ip mobile cdma imsi dynamic** コマンドを使用すると、PDSN は古いセッションをリリースし、新しいセッションをアップします。

この CLI コマンドには、「PLATFORM-3-SAMI\_IPC\_IXP\_FAIL: Msgcode 26: Bad Param Error received from IXP」というエラーメッセージが、高い負荷がかかるシナリオで表示されるという制約があります。

## モバイル IP クライアントによる PMTU 検出

サイズが約 1480 のパケットで PMTU 検出 (DF ビットを設定すると行われます) がモバイル IP クライアント (エンド ノード) で行われた場合、FTP によるアップロードとエンド ノードからの ping が失敗することがあります。PMTUD アルゴリズムが失敗するため、IP 送信元では MTU のより小さなパスはわかりません。しかし、大きすぎるパケットの再送信を、再送信がタイムアウトになるまで失敗しながら続けます。

Windows 2000 または Windows XP プラットフォームで PMTUD を無効にするには、「<http://www.cisco.com/warp/public/105/38.shtml#2000XP>」を参照してください。

## PDSN プロキシ モバイル IP

現在、市販の MIP クライアント ソフトウェアはありません。反対に、PPP は ISP (インターネット サービス プロバイダー) との接続に広く使用されており、IP デバイスには必ず存在します。MIP の代用として、シスコの Proxy Mobile IP (PMIP; プロキシ モバイル IP) 機能を使用できます。PDSN のこの機能は PPP と統合されており、MIP FA が認証 PPP ユーザにモバイル能力を提供できるようにします。



(注) PMIP では、MS は 1 PPP セッションあたり 1 つの IP フローだけを保持できます。

通信プロセスの発生順は、次のとおりです。

1. Cisco PDSN (FA として動作) がモバイル ステーション認証情報を収集して、AAA サーバに送信します。
2. モバイル ステーションが Cisco PDSN PMIP サービスの使用認証を受けると、AAA サーバがレジストレーション データおよび HA アドレスを返します。
3. FA はこの情報およびその他の情報を使用して、モバイル ステーションのために Registration Request (RRQ; レジストレーション要求) を生成し、HA に送信します。
4. レジストレーションに成功すると、HA が FA に、IP アドレスが指定された registration reply (RRP; レジストレーション応答) を送信します。
5. FA が IPCP を使用して、モバイル ステーションに (RRP で受け取った) IP アドレスを割り当てます。
6. HA と FA または PDSN 間にトンネルが設定されます。トンネルはモバイル ステーションに対して双方向でトラフィックを伝送します。

## SAMI 上の PDSN

SAMI ブレードは、Cisco PDSN リリース 5.1 のフィーチャ セットをサポートしており、Cisco 7600 シャーシは最大 6 つのアプリケーション モジュールをサポートしています。各アプリケーション モジュールには 6 つの PPC があり、それぞれ 2 ギガバイトの RAM を備えています。また、Cisco IOS ソフトウェア アプリケーション イメージのインスタンスを 1 つ使用します。各 PPC は PDSN として機能します。

さらに、このクラスタ コントローラ機能のインスタンスが、必要に応じて設定されます。1 つのアクティブおよびスタンバイ コントローラは、単一の IP PDSN メンバを 3 つサポートできます。各 PDSN イメージは、1,75,000 のユーザ セッションをサポートしています。

## 移行シナリオ

表 1 で、現在使用できる PDSN リリースと SAMI プラットフォームへの移行パスを表示します。

表 1 Cisco PDSN の移行パス

	Cisco PDSN リリース 3.0 以前	Cisco PDSN リリース 3.5	Cisco PDSN リリース 4.0	Cisco PDSN リリース 5.0 および 5.1
プラットフォーム	7200 NPE400/NPE-G1 および MWAM プラットフォーム (5 プロセッサのみ)	MWAM (5 プロセッサのみ)	SAMI	SAMI
シャーシ/電源モジュール、ファントレイ	7200VXR	6500/7600 シャーシ	7600 シャーシ	7600 シャーシ
-	-	SUP2/SUP720	SUP720/RSP720/SUP 32	SUP720
-	-	SUP32/SUP IOS SX ベース	SUP IOS - SRC ベースのイメージ (例 : <i>c7600s72033-advipservicesk9-mz.122-33.SRC.bin</i> )	SUP IOS - 最新の SRC ベースのイメージ
-	-	SUP 冗長性	SUP 冗長性	SUP 冗長性

表 2 に基づき、可能な移行シナリオは多くあります。この章では、現在のユーザの配置にもっとも近いシナリオについて説明します。実際の移行パスは、カスタマーごとにエンドツーエンドの配置に基づいて決定する必要があります。さらに、移行をきちんと計画する必要があります。移行は、自身の配置のメンテナンス ウィンドウで実行することを推奨します。

ユーザは、IP アドレス スキームの設計変更、ルーティング プロトコルの設定、PDSN と HA 間のネットワーク接続の設定、PDSN と AAA サーバ間のアプリケーション接続の設定、新しい SAMI PDSN あるいは HA でのルーティングの設定など、ネットワークを再設計する機会が得られます。



(注)

これらの移行計画ではすべて、ハードウェアとソフトウェアの両方で相当な設計変更があります。これらには、慎重な動作計画とネットワークの再設計が求められます。「移行手順」の章では、ネットワークの再設定とサービスの中断を最小限にできる移行手順について説明します。

表 2 で、最も一般的な移行シナリオを表示します。

表 2 Cisco PDSN リリース 5.1 の移行シナリオ

シナリオ	移行元	移行先	説明	ダウンタイム
1	<ul style="list-style-type: none"> <li>非 SR</li> <li>非クラスタ処理</li> <li>7600 シャーシ</li> <li>各プロセッサは、個々の Cisco PDSN として動作</li> </ul>	<ul style="list-style-type: none"> <li>非 SR</li> <li>非クラスタ処理</li> <li>7600 シャーシ</li> <li>ブレードごとに 1 つの Cisco PDSN (単一の IP アーキテクチャ)</li> </ul>	<ul style="list-style-type: none"> <li>すべてのプロセッサの既存の設定を消去します。</li> <li>Cisco PDSN リリース 5.0 または 5.1 にアップグレードした後、アクティブ ブレード PCOP (プロセッサ 3) だけが設定されていることを確認してください。</li> <li>Cisco IP PDSN リリース 5.0 および 5.1 (ブレード レベル) のアドレス プール要件は、PDSN リリース 4.0 (プロセッサ レベル) の設定の 5 倍です。</li> </ul>	あり
2	<ul style="list-style-type: none"> <li>非 SR</li> <li>非クラスタ処理</li> <li>7600 シャーシ</li> <li>各プロセッサの 1 つのブレードは個々の Cisco PDSN として動作</li> </ul>	<ul style="list-style-type: none"> <li>SR 対応</li> <li>非クラスタ処理</li> <li>7600 シャーシ</li> <li>ブレード レベルでの単一の Cisco PDSN 付き SAMI ブレード × 2 (同一シャーシ)</li> <li>自動同期対応</li> </ul>	<ul style="list-style-type: none"> <li>アクティブ ブレードとスタンバイ ブレードのすべてのプロセッサの既存の設定を消去します。</li> <li>Cisco PDSN リリース 5.0 または 5.1 にアップグレードした後、アクティブ ブレード PCOP (プロセッサ 3) だけが設定されていることを確認してください。</li> <li>スタンバイ SAMI ブレードは、アクティブを設定している間はシャットダウンされます。</li> <li>Cisco IP PDSN リリース 5.0 および 5.1 (ブレード レベル) のアドレス プール要件は、PDSN リリース 4.0 (プロセッサ レベル) の設定の 5 倍です。</li> </ul>	あり

表 2 Cisco PDSN リリース 5.1 の移行シナリオ (続き)

3	<ul style="list-style-type: none"> <li>SR 対応</li> <li>非クラスタ処理</li> <li>7600 シャーシ</li> <li>SAMI ブレード × 2 (同一シャーシ)</li> </ul>	<ul style="list-style-type: none"> <li>SR 対応</li> <li>非クラスタ処理</li> <li>7600 シャーシ</li> <li>SAMI ブレード × 2 (同一シャーシ)</li> <li>自動同期対応</li> </ul>	<ul style="list-style-type: none"> <li>アクティブ ブレードとスタンバイ ブレードのすべてのプロセッサの既存の設定を消去します。</li> <li>Cisco PDSN リリース 5.0 または 5.1 にアップグレードした後、アクティブ ブレード PCOP (プロセッサ 3) だけが設定されていることを確認してください。</li> <li>スタンバイ SAMI ブレードは、アクティブを設定している間はシャットダウンされます。</li> <li>Cisco IP PDSN リリース 5.0 および 5.1 (ブレード レベル) のアドレス プール要件は、PDSN リリース 4.0 (プロセッサ レベル) の設定の 5 倍です。</li> </ul>	あり
4	<ul style="list-style-type: none"> <li>非 SR</li> <li>クラスタ処理対応</li> <li>7600 シャーシ</li> <li>Cisco PDSN メンバが実行されている 1 つ以上のプロセッサ</li> </ul>	<ul style="list-style-type: none"> <li>非 SR</li> <li>クラスタ処理対応</li> <li>7600 シャーシ</li> <li>ブレードごとに 1 つの Cisco PDSN メンバ</li> </ul>	<ul style="list-style-type: none"> <li>アクティブ ブレードとスタンバイ ブレードのすべてのプロセッサの既存の設定を消去します。</li> <li>Cisco PDSN リリース 5.0 または 5.1 にアップグレードした後、アクティブ ブレード PCOP (プロセッサ 3) だけが設定されていることを確認してください。</li> <li>Cisco IP PDSN リリース 5.0 および 5.1 (ブレード レベル) のアドレス プール要件は、PDSN リリース 4.0 (プロセッサ レベル) の設定の 5 倍です。</li> </ul>	あり

表 2 Cisco PDSN リリース 5.1 の移行シナリオ (続き)

5	<ul style="list-style-type: none"> <li>SR 対応 (コントローラ冗長性)</li> <li>クラスタ処理対応</li> <li>7600 シャーシ</li> <li>プロセッサの 1 つでコントローラが実行</li> <li>冗長 SAMI ブレード (同一シャーシ)</li> </ul>	<ul style="list-style-type: none"> <li>SR 対応</li> <li>クラスタ処理対応</li> <li>7600 シャーシ</li> <li>コントローラとコロケーションメンバの両方を実行可能</li> <li>冗長 SAMI ブレード (同一シャーシ)</li> <li>自動同期対応</li> </ul>	<ul style="list-style-type: none"> <li>アクティブ ブレードとスタンバイ ブレードのすべてのプロセッサの既存の設定を消去します。</li> <li>Cisco PDSN リリース 5.0 または 5.1 にアップグレードした後、アクティブ ブレード PCOP (プロセッサ 3) だけが設定されていることを確認してください。</li> <li>スタンバイ SAMI ブレードは、アクティブを設定している間はシャットダウンされます。</li> <li>コロケーション メンバが設定された場合、セッションの冗長性が有効であることを確認してください。</li> <li>Cisco IP PDSN リリース 5.0 および 5.1 (ブレードレベル) のアドレス プール要件は、PDSN リリース 4.0 (プロセッサ レベル) の設定の 5 倍です。</li> </ul>	あり
6	<ul style="list-style-type: none"> <li>SR 対応</li> <li>クラスタ処理対応</li> <li>7600 シャーシ</li> <li>冗長 SAMI ブレード (二重シャーシ)</li> </ul>	<ul style="list-style-type: none"> <li>SR 対応</li> <li>クラスタ処理対応</li> <li>7600 シャーシ</li> <li>冗長 SAMI ブレード (シャーシ間)</li> <li>自動同期非対応 (デフォルト)</li> </ul>	<ul style="list-style-type: none"> <li>アクティブ ブレードとスタンバイ ブレードのすべてのプロセッサの既存の設定を消去します。</li> <li>Cisco PDSN リリース 5.0 または 5.1 にアップグレードした後、アクティブ ブレード PCOP (プロセッサ 3) だけが設定されていることを確認してください。</li> <li>設定すると、Cisco PDSN はコントローラおよびコロケーションメンバとして動作します。</li> <li>Cisco IP PDSN リリース 5.0 および 5.1 (ブレードレベル) のアドレス プール要件は、PDSN リリース 4.0 (プロセッサ レベル) の設定の 5 倍です。</li> </ul>	あり

## 移行手順

Cisco PDSN リリース 5.1 への移行とは、単に Multi-processor WAN Application Module (MWAM; マルチプロセッサ WAN アプリケーション モジュール) カードを SAMI モジュールに置き換えるだけではありません。移行は、既存のモバイル加入者のサービス接続に与える影響が最小限ですむように、十分に計画し実行する必要があります。Cisco PDSN リリース 5.1 イメージの移行とは、ブレードごとの単一の PDSN レベルのアーキテクチャを変更するということです。単一 IP 機能は、SAMI サービスブ



レードの機能を、6つの独立した IOS プロセッサの 4.0 モデルから再割り当てします。各 IOS プロセッサは、Control Plane (PCOP; 制御プレーン) プロセッサとして設計された1つの IOS プロセッサと、Traffic Plane (TCOP; トラフィックプレーン) プロセッサとして設定された他の5つのプロセッサがあるモデルへ、コントロールとトラフィック平滑化機能の両方を実行します。



(注)

- これらの移行計画はすべて、メンテナンス ウィンドウで実行する必要があります。
- 自動同期機能は、イントラシャーシ設定だけで、設定の同期をサポートしています。シャーシ間設定では、自動同期を無効にする必要があります。

表 3 で、表 2 で確立済みのシナリオに基づいた移行タスクを表示します。

表 3 Cisco PDSN 4.0 から 5.0 または 5.1 への移行手順

シナリオ	移行手順
1	<ul style="list-style-type: none"> <li>• Cisco PDSN リリース 4.0 の SAMI カードで、すべてのプロセッサの設定を消去し、Cisco PDSN をリロードします。</li> <li>• I/O memory (IOMEM; I/O メモリ) のサイズを、すべてのプロセッサで 256 MB に設定し、この設定を NVRAM に保存します。</li> </ul> <p> (注) IOMEM サイズを 64 MB に設定した場合、<b>memory lite</b> コマンドを設定していることを確認してください。ただし、推奨されるメモリ サイズは 256 MB です。</p> <ul style="list-style-type: none"> <li>• Cisco PDSN リリース 5.0 または 5.1 にアップグレードし、プロセッサ 3 の Cisco PDSN 設定を再設定します。</li> <li>• 新しく追加した Cisco PDSN リリース 5.0 ベースの PDSN IP を使用できるよう、MS と PCF をプロビジョニングします。</li> <li>• 新しく追加した、MIP 呼び出しを提供する HA がある PDSN をプロビジョニングします。</li> </ul> <p>プロビジョニング タスクを最小限に抑えるため、Cisco PDSN リリース 5.0 および 5.1 では、Cisco PDSN リリース 4.0 プロセッサの 1 つで使用されている IP アドレスとルーティング方式が再利用されています。</p>

表 3 Cisco PDSN 4.0 から 5.0 または 5.1 への移行手順 (続き)


2, 3	<ul style="list-style-type: none"> <li>• 新しい SAMI カードを、冗長設定で使用する 7600/720 にインストールします。</li> <li>• 既存の Cisco PDSN リリース 4.0 で、すべてのプロセッサの既存の設定を消去し、Cisco PDSN をリロードします。</li> <li>• IOMEM のサイズを、すべてのプロセッサで 256 MB に設定し、この設定を NVRAM に保存します。</li> </ul> <p> (注) IOMEM サイズを 64 MB に設定した場合、<b>memory lite</b> コマンドを設定していることを確認してください。ただし、推奨されるメモリ サイズは 256 MB です。</p> <ul style="list-style-type: none"> <li>• 両方の SAMI ブレードを Cisco PDSN リリース 5.0 または 5.1 にアップグレードします。</li> <li>• ブレードをスタンバイとして設定するため、シャットダウンします (unit2)。</li> <li>• アクティブなブレード (unit1) で、自動同期を有効にします。プロセッサ 3 のアクティブなブレードで、PDSN を設定します。冗長設定で、unit2 はスタンバイのままにします。冗長性の設定時、プロセッサ間通信 (IPC) の設定前に Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) メイン インターフェイスを設定する必要があります。</li> <li>• アクティブ ブレードの設定を保存します。</li> <li>• unit2 を Cisco PDSN リリース 5.0 または 5.1 イメージで起動します。設定がアクティブ ブレードと自動同期されます。</li> <li>• アクティブ ブレードとスタンバイ ブレード両方の <b>show redundancy state</b> および <b>show redundancy inter device</b> コマンドの出力で、冗長性が有効かを確認します。どちらかのブレードで、冗長性を有効にするためにリロードが必要だと出力された場合は、そのブレードをリロードします。</li> <li>• 新しく追加した Cisco PDSN リリース 5.0 または 5.1 ベースの PDSN IP を使用できるよう、MS と PCF をプロビジョニングします。</li> <li>• PDSN の CDMA-1x IP アドレスを、プロビジョニング時にコントローラまたはメンバ IP として使用します。</li> <li>• 新しく追加した、MIP 呼び出しを提供する HA がある PDSN をプロビジョニングします。</li> </ul> <p>プロビジョニング タスクを最小限に抑えるため、Cisco PDSN リリース 5.0 および 5.1 では、Cisco PDSN リリース 4.0 プロセッサの 1 つで使用されている IP アドレスとルーティング方式が再利用されています。</p>
------	--

表 3 Cisco PDSN 4.0 から 5.0 または 5.1 への移行手順 (続き)


4	<ul style="list-style-type: none"> <li>• Cisco PDSN リリース 4.0 の SAMI カードで、すべてのプロセッサの既存の設定を消去し、Cisco PDSN をリロードします。ブレードに、クラスタの一部である Cisco PDSN メンバが含まれている場合、リロード前に PDSN メンバを削除することをお勧めします。</li> <li>• IOMEM のサイズを、すべてのプロセッサで 256 MB に設定し、この設定を NVRAM に保存します。</li> </ul> <p> (注) IOMEM サイズを 64 MB に設定した場合、<b>memory lite</b> コマンドを設定していることを確認してください。ただし、推奨されるメモリ サイズは 256 MB です。</p> <ul style="list-style-type: none"> <li>• Cisco PDSN リリース 5.0 または 5.1 にアップグレードし、プロセッサ 3 の PDSN を再設定します。</li> <li>• Cisco PDSN を、コントローラとコロケーション メンバの両方として設定できます。Cisco PDSN リリース 5.0 および 5.1 は、Cisco PDSN リリース 3.0 または 4.0 コントローラまたはメンバと連携します。</li> <li>• 新しく追加した Cisco PDSN リリース 5.0 または 5.1 ベースの PDSN IP を使用できるよう、MS と PCF をプロビジョニングします。</li> <li>• PDSN の CDMA-1x IP アドレスを、プロビジョニング時にコントローラまたはメンバ IP として使用します。</li> <li>• 新しく追加した、MIP 呼び出しを提供する HA を持つ PDSN をプロビジョニングします。</li> </ul> <p>プロビジョニング タスクを最小限に抑えるため、Cisco PDSN リリース 5.0 および 5.1 では、Cisco PDSN リリース 4.0 プロセッサの 1 つで使用されている IP アドレスとルーティング方式が再利用されています。</p>
---	---

表 3 Cisco PDSN 4.0 から 5.0 または 5.1 への移行手順 (続き)


5	<ul style="list-style-type: none"> <li>• 新しい SAMI カードを、冗長設定で使用する 7600/720 にインストールします。</li> <li>• 既存の Cisco PDSN リリース 4.0 で、すべてのプロセッサの既存の設定を消去し、Cisco PDSN をリロードします。</li> <li>• IOMEM のサイズを、すべてのプロセッサで 256 MB に設定し、この設定を NVRAM に保存します。</li> </ul> <hr/> <p> (注) IOMEM サイズを 64 MB に設定した場合、<b>memory lite</b> コマンドを設定していることを確認してください。ただし、推奨されるメモリ サイズは 256 MB です。</p> <hr/> <ul style="list-style-type: none"> <li>• 両方の SAMI ブレードを Cisco PDSN リリース 5.0 または 5.1 にアップグレードします。</li> <li>• ブレードをスタンバイとして設定するため、シャットダウンします (unit2)。</li> <li>• アクティブなブレード (unit1) で、自動同期を有効にします。プロセッサ 3 のアクティブなブレードで、PDSN を設定します。冗長設定で、unit2 はスタンバイのままにします。冗長性の設定時、プロセッサ間通信 (IPC) の設定前に Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) メイン インターフェイスを設定する必要があります。</li> <li>• アクティブ ブレードの設定を保存します。</li> <li>• unit2 を Cisco PDSN リリース 5.0 または 5.1 イメージで起動します。設定がアクティブ ブレードと自動同期されます。</li> <li>• アクティブ ブレードとスタンバイ ブレード両方の <b>show redundancy state</b> および <b>show redundancy inter device</b> コマンドの出力で、冗長性が有効かを確認します。どちらかのブレードで、冗長性を有効にするためにリロードが必要だと出力された場合は、そのブレードをリロードします。</li> <li>• 新しく追加した Cisco PDSN リリース 5.0 または 5.1 ベースの PDSN IP を使用できるよう、MS と PCF をプロビジョニングします。</li> <li>• PDSN の CDMA-1x IP アドレスを、プロビジョニング時にコントローラまたはメンバ IP として使用します。</li> <li>• 新しく追加した、MIP 呼び出しを提供する HA がある PDSN をプロビジョニングします。</li> <li>• Cisco PDSN を、コントローラおよびコロケーション メンバとして動作するよう設定できます。 <ul style="list-style-type: none"> <li>– コロケーション メンバの場合、スタンバイがコロケーション メンバによって処理されるセッションと同期するよう、セッションの冗長性が有効であることを確認してください。</li> <li>– スタンバイ コントローラで情報を同期するアクティブ コントローラでは、すべてのリモート メンバがコントローラの HSRP メイン インターフェイスに接続していることを確認してください。</li> <li>– メンバ IP が設定されている場合、CDMA -1x インターフェイス IP アドレスと同じであることを確認してください。</li> </ul> </li> </ul>
---	---

表 3 Cisco PDSN 4.0 から 5.0 または 5.1 への移行手順 (続き)

6	<ul style="list-style-type: none"> <li>既存の Cisco PDSN リリース 4.0 で、すべてのプロセッサの既存の設定を消去し、Cisco PDSN をリロードします。</li> <li>IOMEM のサイズを、すべてのプロセッサで 256 MB に設定し、この設定を NVRAM に保存します。</li> </ul> <p> (注) IOMEM サイズを 64 MB に設定した場合、<b>memory lite</b> コマンドを設定していることを確認してください。ただし、推奨されるメモリ サイズは 256 MB です。</p> <ul style="list-style-type: none"> <li>両方の SAMI ブレードを Cisco PDSN リリース 5.0 または 5.1 にアップグレードします。</li> <li>Cisco PDSN を再設定し、シャーシ間 HSRP 冗長性を Cisco PDSN リリース 4.0 で有効にします。</li> <li>新しく追加した Cisco PDSN リリース 5.0 または 5.1 ベースの PDSN IP を使用できるよう、MS と PCF をプロビジョニングします。</li> <li>PDSN の CDMA-1x IP アドレスを、プロビジョニング時にコントローラまたはメンバ IP として使用します。</li> <li>新しく追加した、MIP 呼び出しを提供する HA を持つ Cisco PDSN をプロビジョニングします。</li> </ul>
---	--

1. MS = Mobile Station (モバイルステーション)。
2. PCF = Packet Control Function (パケット制御機能)。

## 機能

ここでは、現在のリリース (Cisco PDSN リリース 5.1) および以前のリリースで導入された機能について説明します。

- [「このリリースの新機能」](#)
- [「以前のリリースの機能」](#)

### このリリースの新機能

ここでは、Cisco PDSN リリース 5.1 の新機能について表示します。

- [「簡易 IP クライアントの IP アカウンティングのサポート」](#)
- [「PCF 単位の SNMP の新規 MIB オブジェクト」](#)
- [「一般的な NAI のサポート」](#)
- [「最新の IS-835 に合わせたプロキシ MIP の変更」](#)
- [「簡易 IPv6 サポート」](#)
- [「Access-Request アトリビュート」](#)
- [「新しい PCF カウンタ単位の PPP」](#)
- [「VPDN 条件付きデバッグ」](#)
- [「Revocation メッセージの GRE CVSE および MN NAI 拡張」](#)

## 以前のリリースの機能

ここでは、Cisco PDSN リリース 5.1 以前で導入された機能について表示します。

- 「一般的な NAI のサポート」
- 「ブレード単位の単一 IP」
- 「Osler のサポート」
- 「改善されたスループットとトランザクション処理」
- 「単一 IP ブレードのクラスタ コントローラのサポート」
- 「IMSI および PCF のリダイレクション」
- 「China Telecom 用モバイル IP および AAA アトリビュート」
- 「AAA サーバ非応答に対するトラップ生成」
- 「スーパーバイザのサポート」
- 「Data Over Signaling」
- 「Differentiated Services Code Point マーキングのサポート」
- 「Nortel Aux A10 のサポート」
- 「IMSI プレフィックスのマスキング解除」
- 「永続的な TFT のサポート」
- 「FA-HA IP-in-IP トンネルの場合の一意な IP-ID の保存」
- 「GRE CVSE Support in FA-HA Tunnel」
- 「リモートアドレス アカウンティング」
- 「デフォルトのサービス オプション実装」
- 「Configurable Per-Flow アカウンティング オプション」
- 「IP フロー識別子の PCF 下位互換性サポート」
- 「max-class 値に対する DSCP のコメントのサポート」
- 「フラグメンテーション サイズのコマンド サポート」
- 「China Telecom 向けの新しい統計カウンタ」
- アトリビュートのサポート
  - 「Served MDN」
  - 「Framed Pool」
  - 「3GPP2 DNS サーバ IP」
- 「サブインターフェイスがある仮想ルート フォワーディング」
- 「条件付きデバッグの機能拡張」 (Cisco PDSN リリース 4.1 用)
- 「複数サービス接続」
- 「データ プレーン」
- 「加入者 QoS ポリシー」 (AAA サーバからのユーザ プロファイルごとのダウンロードと、ローカル プロファイルの設定)
- 「QoS シグナリング」

- 「トラフィック フロー テンプレート」
- 「Per-flow アカウンティング」
- 「コール アドミッション制御」
- 「PDSN MIB の機能強化」 (Cisco PDSN リリース 4.0 用)
- 「SAMI 上の PDSN」
- 「ユーザ間の優先度」
- 「ローマー ID」
- 「帯域幅のポリシング」
- 「パケット データ サービスのアクセス」
  - 「簡易 IPv6 アクセス」
- 「セッション冗長性のインフラストラクチャ」
- 「RADIUS サーバのロード バランシング」
- 「ドメインに基づく加入者認可」
- 「PDSN MIB の機能強化」
  - 「Cisco PDSN リリース 3.0 の PPP カウンタ」
  - 「Cisco PDSN リリース 3.0 の RP カウンタ」
- 「条件付きデバッグの機能拡張」
  - 「Cisco PDSN リリース 3.0 のトレース機能」
- 「IMSI 処理のランダム化」
- 「プロトコルのレイヤ処理と RP 接続」
- 「PPPoGRE RP インターフェイス」
- 「A11 Session Update」
- 「SDB インジケータ マーキング」
- 「モバイル IP のリソース失効」
- 「パケット オブ ディスコネクト」
- 「IS-835 前払いのサポート」
- 「前払い請求」
- 「1 秒あたりのモバイル IP コール処理の改善」
- 「always-on 機能」
- 「PDSN MIB の機能強化」
- 「条件付きデバッグの機能拡張」
- 「シスコ独自の前払い請求」
- 「3DES 暗号化」
- 「モバイル IP の IPSec」
- 「IPSec Acceleration Module、Static IPSec を使用したハードウェアの IPSec アクセラレーション」
- 「1xEV-DO のサポート」
- 「組み込み外部エージェント」
- 「AAA サーバのサポート」

- 「VPDN のパケット トランスポート」
- 「プロキシ モバイル IP」
- 「複数のモバイル IP フロー」
- 「PDSN クラスタ コントローラとメンバー アーキテクチャ」



(注) PDSN ソフトウェアは、異なるイメージで使用できる複数の機能オプションを提供しています。その中には、イメージ固有の機能があり、すべてのイメージでは使用できません。表 4 の「PDSN 機能マトリクス」で、PDSN で使用できるイメージを表示しています。



(注) Cisco PDSN リリース 3.5 は、Cisco 7600 または Cisco 6500 シリーズ ルータ の Cisco MWAM カードでだけサポートされています。「PDSN 機能マトリクス」で表示されている機能は、以前のリリースからサポートされている機能です。

Cisco PDSN リリース 4.0 は Closed-RP クラスタ処理をサポートしていないことに注意してください。さらに、Closed-RP のサポートは、このリリースからなくなりました。

表 4 PDSN 機能マトリクス

機能名	c7svcsami-c 6ik9s-mz
セッションの冗長性	X
簡易 IPv6	X(P)
ユーザあたりのリソース失効	X
トレース機能	X
RADIUS サーバのロード バランシング	X
レルムに基づく RADIUS サーバの選択	X
PPPoGRE RP インターフェイス	X(P)
A11 Session Update	X
SDB インジケータ マーキング	X
パケット オブ ディスコネクト	X
リソース失効	X
常時接続機能	X
NPE-G1 プラットフォームのサポート	-
PDSN MIB の拡張	X
条件付きデバッグ	X
10000 セッション	-
25000 セッション	X
RevA のサポート	X
前払い請求 (IS-835-C)	X(P)
PDSN コントローラ / メンバ クラスタ処理	X
1xEV-DO のサポート	X



表 4 PDSN 機能マトリクス (続き)

機能名	c7svcsami-c 6ik9s-mz
請求での ESN	X
3DES 暗号化	X*
PPP 最適化	X

P は、この機能は Premium ライセンスでだけ使用可能であることを示します。

\* 適切なハードウェア サポートが必要です。



(注) PDSN の選択でより高い性能値が必要な場合、c6is-mz イメージを使用してください。これらのイメージは、PDSN 選択での PDSN コントローラメンバクラスタ機能を含んでいます。

## PDSN 性能メトリック

Cisco PDSN リリース 4.x 以降のリリースは、リリース 3.0 やリリース 3.5 と比べ、1XRTT コール設定レートの大幅な向上といった、性能の改善を実現しています。

Cisco 7600 シリーズ ルータでの性能メトリックは、次のようになります。

- 175,000 ユーザ セッション
- スタンドアロン PDSN での、SIP および MIP セッションの最大コール設定レート
- サイズが 64、350、512、1472 バイトの非断片化パケットの R-P インターフェイスでのスループット
- 25 バイトの断片化がある、サイズが 64、350、512、1472 バイト断片化パケットでの R-P インターフェイスでのスループット
- SIP および MIP セッションのスタンドアロン PDSN でのコール設定レート
- カード レベル スループットが 3 Gbps まで増加



(注) 引用値はイメージごとであり、各 SAMI は 6 つの PDSN イメージをサポート可能です。  
 コール設定レートの詳細については、性能データ シートを参照してください。

## パケット データ サービスのアクセス

PDSN は 2 種類のサービス アクセスをサポートしています。モバイルセッションのサービス アクセスの種類は、次のようにモバイル ステーションの性能によって決定されます。

- 簡易 IP ベースのサービス アクセス
- モバイル IP ベースのサービス アクセス

## 簡易 IP ベースのサービス アクセス

PDSN により、モバイル ユーザは SIP ベースのサービス アクセスを使用して、簡単にインターネットや企業イントラネットにアクセスできます。ただし、SIP モードでのアクセスは、PDSN のカバー エリアへのユーザ モビリティを制限します。PDSN 間のハンドオフにより、モバイル ステーションと新しい PDSN 間の PPP の再ネゴシエーションが発生します。以前の PDSN で割り当てられた古い IP アドレスは、通常新しい PDSN からのモバイル ユーザには割り当てられません。結果、ユーザ アプリケーションはリセットされ、再起動します。

SIP ベースのサービス アクセスの主な機能には、次があります。

- スタティック IP アドレスのサポート
- パブリック IP アドレス
- プライベート IP アドレス (VPDN サービス用など)
- ダイナミック IP アドレスのサポート
- PPP PAP/CHAP 認証のサポート
- MSID ベースのサービス アクセスのサポート
- TIA/EIA/IS-835-B 単位のパケット データ アカウンティングのサポート
- パケット フィルタリングのサポート
- 入力アドレス フィルタリング
- 入力アクセス リスト
- 出力アクセス リスト

ユーザ Network Access Identifier (NAI; ネットワーク アクセス識別子) は PPP CHAP/PAP 認証フェーズで使用できます。NAI のドメイン名情報で、ユーザ認証を行うドメインを決定します。パケット ルーティング モデルの種類に基づき、SIP ベースのサービス アクセスは次のように分類できます。

- 簡易 IP 経路選択済みアクセス
- 簡易 IP VPDN アクセス
- プロキシ モバイル IP サービス

## 簡易 IP 経路選択済みアクセス

PPP LCP ネゴシエーション中にユーザ名とパスワードを受信した後、PDSN は、認証情報をローカル AAA サーバに access-request メッセージ経由で送信します。これは、同様に、ユーザのホーム ドメインの AAA サーバに、必要に応じて、ブローカ AAA サーバ経由でプロキシすることができます。正常な認証では、ユーザはそのサービス プロファイルに基づいて認証されます。ユーザ クラス /CDMA\_IPTECH 情報は、他の認証パラメータとともに、ホーム AAA サーバからのアクセス許諾メッセージを使用して PDSN に返されます。IP アドレスの正常なネゴシエーションでは、SIP ベースのサービスをモバイル ユーザが使用できるようになります。

SIP 経路選択済みアクセスの方法は、VPDN または PMIP サービスが設定されていないユーザに適用されます。PDSN で終了する PPP を使用し、アップリンク ユーザ トラフィックは、PDSN から IP ネットワークに向かってルーティングされます。モバイル ユーザに割り当てられたアドレスは、PDSN ルーティング可能ドメイン内からになります。プライベート アドレスも、NAT が設定されている場合に使用できます。ユーザ モビリティは PDSN のカバレッジエリア内に制限されます。PCF 間ハンドオフによるサービスの中断はありません。しかし、PDSN 間ハンドオフは、新しい PDSN で PPP ネゴシエーションになり、違う IP アドレスが新しい PDSN に割り当てられ、ユーザ アプリケーションがリセットされ再起動されます。

## 簡易 IP VPDN アクセス

PPP LCP ネゴシエーション中にユーザ名とパスワードを受信した後、PDSN は、認証情報をローカル AAA サーバに `access-request` メッセージ経由で送信します。これは、同様に、ユーザのホーム ドメインの AAA サーバに、必要に応じて、ブローカ AAA サーバ経由でプロキシすることができます。正常な認証では、ユーザは自身のサービス プロファイルに基づいて認証されます。ユーザに VPDN ベースのアクセス サービスが設定されている場合、ユーザ クラス情報は、トンネリング オプションやトンネリング パラメータを含む他の認証パラメータと共に、ホーム AAA サーバから `access-accept` メッセージを介して PDSN に返されます。次の種類の VPDN サービスが、PDSN でサポートされています。

### L2TP - Layer 2 Tunneling Protocol (レイヤ 2 トンネリング プロトコル)

L2TP タイプ layer2 トンネリングでは、PDSN はトンネリング パラメータで指定されたトンネリング エンドポイントを使用して L2TP トンネルを確立します。L2TP トンネルは、PDSN の Link Control Protocol (LAC; リンク コントロール プロトコル) と、ユーザのホーム ドメインの NAS の L2TP Network Server (LNS; L2TP ネットワーク サーバ) との間で確立されます。PPP 接続は、モバイル ステーションとホーム ネットワークの LNS との間で行われます。PPP 接続が LNS で終了しても、PDSN は PPP セッションが非アクティブになるのを監視します。PPP 接続のステータスも、基本となる A10 接続のステータスと関連しています。基本となる A10 接続が削除されると、PPP 接続は削除されます。IP セキュリティ暗号化方式は、セキュリティを拡張するため、L2TP トンネル全体で有効にすることができます。

モバイルと LNS 間の IP アドレスの正常なネゴシエーションでは、IP ベースのサービスをモバイルで使用できます。

LNS を、PDSN からのチャレンジとチャレンジ レスポンス情報に基づいてモバイル ユーザを認証するよう設定できます。また、LNS はレイヤ 2 トンネルの確立後、再度ユーザのチャレンジを行うよう設定することもできます。L2TP では、次の認証オプションがサポートされています。

- プロキシ認証を使用した L2TP

LAC (PDSN) は、モバイル ユーザのチャレンジを行い、認証関連情報を、トンネル設定パラメータの一部として LNS に転送します。LNS は、LAC (PDSN) からの認証関連情報に基づき、ローカルまたはホーム AAA サーバ経由のどちらかでユーザを認証するよう設定できます。正常な認証では、モバイルと LNS は IPCP フェーズに進み、ユーザ セッションに IP アドレスをネゴシエートします。

- 二重認証を使用した L2TP

LAC (PDSN) は、モバイルのチャレンジを行い、認証関連情報をトンネル設定パラメータの一部として LNS に転送します。LNS は、LAC (PDSN) からの認証関連情報に基づき、ローカルまたはホーム AAA サーバ経由のどちらかでユーザを認証するよう設定できます。正常な認証では、LNS はモバイルを再度試行します。正常な認証後、LNS とモバイルは IPCP フェーズに進み、ユーザ セッションの IP アドレスをネゴシエートします。

## プロキシ モバイル IP アクセス

PPP LCP ネゴシエーション中にユーザ名とパスワードを受信した後、PDSN は、認証情報をローカル AAA サーバに `access-request` メッセージ経由で送信します。これは、同様に、ユーザのホーム ドメインの AAA サーバに、必要に応じてブローカ AAA サーバを使用してプロキシすることができます。正常な認証では、ユーザはそのサービス プロファイルに基づいて認証されます。ユーザ クラス情報は、他の認証パラメータとともに、ホーム AAA サーバからアクセス応答を介して PDSN に返されます。

ユーザが PMIP ベースのアクセスを設定している場合、ホーム AAA サーバからの認証パラメータには、HA アドレスと、モバイル ステーション用の MN-HA 認証拡張の計算に使用されるセキュリティ パラメータ (SPI) が含まれます。HA はホーム AAA サーバで設定された HA のリストから割り当てられます。ユーザ NAI に基づくラウンド ロビン またはハッシュ アルゴリズムが、AAA サーバ で HA

を割り当てるために使用できます。AAA サーバから返されるその他の認証アトリビュートには、RFC 3012 で定義された MN-AAA 認証拡張が含まれます。この情報に基づき、PDSN は、MIP レジストレーション要求メッセージを割り当てられた HA に送信することで、モバイル ユーザに代わって PMIP 手順を実行します。AAA サーバを使用したモバイルの正常な認証と HA でのレジストレーションでは、HA はこのモバイル ユーザにホーム アドレスを割り当てます。このアドレスは、IPCP IP アドレス ネゴシエーション フェーズでモバイルに返されます。

IP アドレスの正常なネゴシエーションでは、PMIP ベースのサービスをモバイル ユーザが使用できるようになります。モバイルにとっては、これらのサービスと HA を経由してトンネリングされた SIP サービスとの違いはありません。ただしこの機能は、コールのカバレッジエリアを PDSN サービスのカバレッジエリアを超えて拡張します。ハンドオフ イベントの結果、他の PDSN がコールに割り当てられた場合、ターゲットの PDSN は HA を使用した MIP レジストレーションを実行します。したがって、同じホームアドレスがモバイルに必ず割り当てられます。

## モバイル IP ベースのサービス アクセス

PDSN により、モバイル ステーションは MIP クライアント機能を使用してインターネットにアクセスしたり、MIP ベースのサービス アクセスを使用して企業イントラネットにアクセスできます。サービス アクセスのこのモードで、ユーザ モビリティは現在の PDSN サービスのカバレッジエリアを超えて拡張されます。ハンドオフの結果、他の PDSN がコールに割り当てられた場合、ターゲットの PDSN は HA を使用した MIP レジストレーションを実行します。したがって、同じホームアドレスがモバイルに必ず割り当てられます。

MIP サービス アクセスの特徴的な機能には、次があります。

- スタティック IP アドレスのサポート
- パブリック IP アドレス
- プライベート IP アドレス
- ダイナミック IP アドレスのサポート
- パブリック IP アドレス
- プライベート IP アドレス
- 単一 PPP 接続全体の複数の MIP ユーザ フロー
- スタティック アドレスまたはダイナミック アドレスを使用する、異なる NAI に対応するマルチフロー
- 異なるスタティック アドレスを使用する、同一 NAI に対するマルチフロー
- RFC 3012 の外部エージェント (FA) チャレンジ手順
- MIP エージェント アドバタイズ チャレンジの機能拡張
- MN-FA チャレンジの機能拡張
- MN-AAA 認証拡張機能
- RFC 2002 で規定された MIP 拡張機能
- MN-HA 認証拡張機能
- MN-FA 認証拡張機能
- FA-HA 認証拡張機能
- RFC 3220 で規定された MIP 拡張機能
- SPI を使用しなければならない認証。
- Mobile NAI Extension (モバイル NAI 拡張機能)、RFC 2794

- リバース トンネリング (RFC 2344)
- FA と HA 間の複数のトンネリング モード
- IP-in-IP カプセル化 (RFC 2003)
- 総称ルート カプセル化 (RFC 2784)
- PPP PAP/CHAP 認証のサポート
- MSID ベースのサービス アクセスのサポート
- ゾンビ PPP 接続を管理するためのバインディング アップデート メッセージ
- フロー ベースの TIA/EIA/IS-835-B 単位のパケット データ アカウンティング
- パケット フィルタリングのサポート
- 入力アドレス フィルタリング
- 入力アクセス リスト
- 出力アクセス リスト

MIP 可能なモバイル クライアントは、PPP LCP フェーズで PAP/CHAP ベースの認証をスキップできます。PPP が確立されると、PDSN は RFC 3012 で規定された MIP エージェント アドバタイズメント チャレンジ拡張を含む MIP エージェント アドバタイズメント メッセージのバーストを送信します。バーストの番号とタイミングは設定可能です。モバイル ユーザは、エージェント アドバタイズメント メッセージでのチャレンジに対し、モバイル ユーザの NAI および MN-FA チャレンジ拡張を含む MIP レジストレーション要求メッセージで応答します。モバイル ユーザが最初のバーストに応答しない場合、アドバタイズメントを要請することができます。

PDSN の外部エージェント機能で、アクセス要求メッセージをローカル AAA サーバに転送することでモバイル ユーザを認証するよう設定できます。ローカル AAA サーバは必要に応じて、ブローカ AAA サーバを経由してホーム AAA サーバにメッセージをプロキシします。正常な認証では、ホーム AAA サーバは HA をコールに割り当て、アクセス応答メッセージでそのアドレスを返すことができます。アクセス応答メッセージの他の認証パラメータには、FA と HA 間で使用される SPI や IPSec 共有キーがあります。PDSN または FA と、HA は安全性の高い IPSec トンネルを必要に応じて確立し、PDSN/FA はレジストレーション要求メッセージを HA に転送します。レジストレーション要求メッセージには、NAI や MN-FA チャレンジ拡張も含まれます。また、MN-AAA 認証拡張も含まれます。

HA を、ホーム AAA サーバで再度モバイルを認証するよう設定できます。正常な認証とレジストレーションでは、HA はレジストレーション応答メッセージでモバイル ステーションに転送された PDSN や FA に応答します。レジストレーション応答メッセージには、ユーザ セッションのホーム アドレスも含まれています (スタティックまたは動的に割り当てられたアドレス)。

潜在的ホーム アドレスが、次から PDSN に対して使用できます。

- モバイル ノードから受信した MIP レジストレーション要求
- HAAA から受信した FA-CHAP 応答
- HA から受信した MIP レジストレーション応答

モバイルを、RFC 3012 で規定された 外部エージェント (FA) チャレンジベースの認証に加えて PPP PAP/CHAP 認証を実行するよう設定することもできます。この場合、PDSN は 1 つ以上の MIP に加え、1 つの SIP フローをサポートします。

MIP サービスでは、HA は一般に ISP ネットワークまたは企業ドメイン内に配置されます。しかし、ISP や企業エンティティの多くは、サービス プロバイダーが第三世代パケット データ サービスの展開を開始しない限り、HA をプロビジョニングする準備ができていません。アクセス サービス プロバイダーは、この状況を、独自のドメイン内で HA をプロビジョニングし、パケットを ISP または企業ドメインに VPDN サービスを介して転送することで、緩和することができます。

## バインディング アップデート手順

モバイル ノードの初回のパケット データ サービス登録時には、PPP セッションおよび関連づけられている MIP フローがその PDSN で確立されます。PDSN 間のハンドオフが発生すると、ターゲット PDSN で別の PPP セッションが確立され、そのモバイル ノードは新しい PDSN/FS を介して HA に登録します。しかし、ビジター リストのバインディングと以前の PDSN での PPP セッションは、PPP 非アクティブ タイマーが時間切れになるまでリリースされません。

PDSN にアイドル状態または未使用の PPP セッションがあると、貴重なリソースが消費されます。PDSN と HA は、IS83C で規定されている MIP リソース失効 と、このようなアイドル PPP セッションをできる限り早くリリースするための Cisco Proprietary Binding Update および Binding Acknowledge メッセージをサポートしています。MIP リソース失効 は、16 章で詳しく説明しています。

Cisco Proprietary バインディング アップデート機能を使用している場合で、PDSN 間ハンドオフと MIP レジストレーションの際は、HA は新しい PDSN/FA の Care-of-Address (COA; 気付アドレス) を使用したモバイルのモビリティ バインディング情報をアップデートします。同時バインディングがイネーブルになっていない場合、HA は Binding Update メッセージの形で、前の PDSN/FA に通知を送信します。前の PDSN/FA は Binding Acknowledge で確認応答し、必要に応じて、その MIP セッションのビジター リスト エントリを削除します。前の PDSN/FA は、そのモバイル ステーションにアクティブ フローがなくなると、PPP セッションの解放を開始します。

バインディング アップデート メッセージの送信は、HA で設定できます。



(注)

同じ NAI に複数のフローが確立されると、各フローに異なる IP アドレスが割り当てられます。つまり、同時バインディングは、同じ IP アドレスへの複数フローを維持するために使用される場合は必要ありません。

## 簡易 IPv6 アクセス

PDSN SIP サービスが拡張され、簡易 IPv4 と簡易 IPv6 アクセスの両方が使用できるようになりました。これらのプロトコルは、一度に 1 つずつ、あるいは両方同時に使用できます。ipcp と ipv6cp は、各プロトコルで同等です。

IPv6 アクセスでは、AAA サーバアクセスと同じ PPP LCP 認証と認証手順を使用します。RP 接続が確立されると、MS は PDSN への新しい PPP セッションに使用する PPP Link Control Protocol (LCP; リンク コントロール プロトコル) Configuration-Request を送信します。PPP 認証 (CHAP/PAP/none) は、LCP フェーズでネゴシエートされるパラメータの 1 つです。LCP パラメータが MS と PDSN 間でネゴシエートされた後、LCP Configure-Acknowledge メッセージが交換されます。LCP がアップすると、PPP 認証が開始されます。

認証フェーズでは設定と LCP ネゴシエーションによって CHAP、PAP、または none が使用されます。認証後、NCP と、ipcp か pv6cp のいずれかまたは両方が開始されます。MS からの IPv4 と IPv6 の同時アクセスで、コモン LCP 認証と許可が、AAA サーバの関連 ID パラメータと同様に共有されます。

ipv6cp プロトコルは、MS と PDSN で使用する有効な非ゼロの 64 ビット IPv6 インターフェイス識別子をネゴシエートします。PDSN は、PPP 接続に関連するインターフェイス識別子を 1 つだけ保持します。したがって、この識別子は一意となります。ipv6cp が正常にネゴシエートされると、PDSN と MS の両方で、IPv6 インターフェイスで使用する一意のリンクローカルアドレスが生成されます。このリンクローカルアドレスは、リンクローカルプレフィックスの FE80:/64 を ipv6cp フェーズでネゴシエートされた 64 ビットインターフェイス識別子 (FE80::205:9AFF:FEFA:D806 など) へ保留済みにするので生成されます。これにより、128 ビットリンクローカルアドレスが付与されます。

PDSN はただちに、PPP リンクで MS へ初期未承諾 Router Advertisement (RA) メッセージを送信します。PDSN のリンクローカルアドレスはソースアドレスとして使用され、宛先アドレスは FF02::1 となり、「ローカルリンクのすべてのノード」の IPv6 アドレスとなります。PDSN は、MS に送信し

た RA メッセージにグローバルに一意な /64 プレフィックスを含めます。このプレフィックスはローカル プレフィックス プールまたは AAA サーバから取得することができます。MS は、RA で受信したプレフィックスを下位の 64 ビット インターフェイス識別子の先頭に追加して、グローバル IPv6 ユニキャスト アドレスを構築します。/64 プレフィックスが各 MS に対しグローバルに一意になるように PDSN を設定するよう注意する必要があります。

正常な ipv6cp ネゴシエーション フェーズとリンクローカル アドレスの設定後、指定された時間内に RA メッセージが PDSN から受信された場合、MS は Router Solicitation (RS) メッセージを送信します。MS で 128 ビットのグローバルユニキャスト アドレスを構築する際に、RA が必要です。

IPv4 と異なり、IPv6 MS は次を含む複数の IPv6 アドレスを保持しています。

- リンクローカル アドレス
- グローバルユニキャスト アドレス
- IPv6 Neighbor Discovery と IPv6 ICMP メッセージで使用される各種マルチキャスト アドレス

IPv6 アドレスは、ソースアドレスと宛先アドレスの両方で 128 ビットです。/64 を指定するということは、プレフィックスに 64 ビットが使用される (上位 64 ビット) ことを意味します。これは、IPv4 ネットマスクと同様です。/128 アドレスは、アドレス全体が使用されるということです。IPv6 アドレッシングの詳細や追加情報については、RFC 3513 を参照してください。



(注)

Cisco IOS リリース 12.3(14)YX の *Cisco Packet Data Serving Node (PDSN; パケット データ サービス ノード) 機能*では、簡易 IPv6 サポートが機能リリースに追加されました。

## 簡易 IPv6 の設定

次のコマンドが PDSN で簡易 IPv6 を設定するために使用されます。これらのコマンドは、*Cisco IOS IPv6 Command Reference* ガイドに示されています。

- **cdma pdsn ipv6** コマンドで PDSN IPv6 機能が有効になります。
- **cdma pdsn ipv6 ra-count number** コマンドで IPv6 Route Advertisements (RA; ルート アドバタイズメント) を設定します。
- **cdma pdsn ipv6 ra-count number ra-interval number** コマンドで、ipv6cp セッションがアップした時点で MN に送信された RA の数と間隔を制御します。
- **cdma pdsn accounting send ipv6-flows** コマンドで、IPv4 と IPv6 の同時セッションに使用されるフローと UDR レコードの数を制御します。
- **show cdma pdsn flow mn-ipv6-address** コマンドで、MN IPv6 アドレスによる CDMA PDSN ユーザ情報を表示します。
- **show cdma pdsn flow service simple-ipv6** コマンドで、簡易 IPv6 セッションのフローベース情報を表示します。
- **debug cdma pdsn ipv6** コマンドで、IPv6 エラーまたはイベント メッセージを表示します。

次の設定コマンドが IPv6 では必要です。

### グローバル設定コマンド

- **ipv6 unicast-routing** - IPv6 はデフォルトで無効です。
- **ipv6 cef** - cef 切り替えを有効にします。
- **ipv6 local pool PDSN-Ipv6-Pool 2001:420:10::/48 64** - Routing Advertisement (RA; ルーティング アドバタイズメント) として MS に送信される IPv6 プレフィックス アドレスのプールを有効にします。

**Virtual-template インターフェイス コマンド**

- **ipv6 enable** - インターフェイスでの IPv6 を有効にします。
- **no ipv6 nd suppress-ra** - Neighbor Discovery Routing Advertisement メッセージ（非イーサネット インターフェイスで抑制）の抑制を無効にします。
- **ipv6 nd ra-interval 1000** - 1000 秒ごとに ND Routing Advertisement を送信します。
- **ipv6 nd ra-lifetime 5000** - ND Routing Advertisement のライフタイムを 5000 秒に設定します。
- **peer default ipv6 pool PDSN-Ipv6-Pool** - このプールを RA プレフィックスに設定します。

**その他のコマンド**

- **show ipv6** - IPv6 を表示します。

これらの設定コマンドについての詳細情報については、次の URL の『Cisco IOS IPv6 Command Reference』を参照してください。

[http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6\\_book.html](http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html)

## セッション冗長性のインフラストラクチャ

Cisco PDSN リリース 5.0 では、次の 2 つの異なる時間に、セッションの詳細を使用して冗長な PDSN がアップデートされます。

- スタンバイ PDSN がアップした時点でのバルク同期化
- アクティブ PDSN とスタンバイ PDSN 両方がアップし、
  - セッションがアップまたはダウン
  - 再レジストレーションの受信でのセッションのリフレッシュ（更新された補助（aux）接続の詳細、IP フロー、それらのマッピングを含む）
  - フローのアップまたはダウン（単一 IP、MIP、PMIP を含む）
  - セッションはアクティブから休止、またはその反対へ
  - PPP 再ネゴシエーションの発生
  - TFT の受信または更新

この機能で導入された新しいパラメータが、両方のシナリオでスタンバイするよう同期されます。

## 機能概要

PDSN セッション冗長性は、フェールオーバーでユーザ フローを節約することを目的としています。課金記録の継続性、内部カウンタ、MIB 変数のサポートは二次的なものです。PDSN でフェールオーバーが成功するためには、次の条件が存在していることが必要です。

- ユーザがサービスの中断に気付かないこと。
- ユーザに超過課金や不正な課金が起らないこと。
- フェールオーバー後、ユーザがデータ サービスを再初期化できること。

PDSN Session Redundancy 機能で、モバイル ユーザ エクスペリエンスで PDSN の障害の影響を最小化するユーザ セッション フェールオーバーが行えます。PDSN では、アクティブな PDSN ごとに存在するスタンバイで 1:1 冗長モデルが使用されます。アクティブな PDSN は、必要ベースで同期するためのステータス情報をスタンバイ PDSN に送信します。PDSN 障害が発生すると、スタンバイ PDSN は、ステータス情報を既存のすべてのセッションへのサービスに提供する必要があります。その後、アク



ティブ PDSN とサービス ユーザ セッションとして引き継ぎ、セッションの冗長性を提供します。以前アクティブだった PDSN がオンラインに復帰すると、現在アクティブな PDSN に対してスタンバイの役割を担うと見なされ、既存のすべてのセッションのステータス情報を新しくアクティブになった PDSN から受信します。

通常の動作条件の下では、アクティブ PDSN とスタンバイ PDSN のペアは、同一の設定を持つ 2 つの別個の PDSN イメージです。これらは、1 つ以上の HSRP インターフェイスを共有します。これは、すべての外部エンティティで通信するために使用されます。アクティブな PDSN は、次に説明するイベントに基づいてセッションデータをスタンバイ PDSN に同期します。

## セッション イベント

新しいユーザ セッションを確立する必要がある場合、PCF は最初に、PCF に通知された HSRP アドレスを使用してアクティブな PDSN に A10 接続を設定します。MN は、A10 トンネルを使用したアクティブな PDSN との PPP 接続を設定します。コールが安定的な状態 (PPP セッションが正常) になると、アクティブな PDSN はスタンバイ PDSN に関連するステータス情報を同期します。その後、スタンバイは A10 接続や PPP セッションに関連するアクティブ PDSN の動作を複製し、アクティブからのその後のアップデートを待機します。次に示した他のイベントのいずれかが発生した場合、アクティブな PDSN はステータス情報をスタンバイに送信します。

フェールオーバーの場合の課金データの損失を最小限にするため、定期的な課金アップデートは、頻度が設定でき、アクティブ PDSN で実行されます。セッションの定期アップデートごとに、スタンバイ PDSN へ同期が送信され、課金データがアップデートされます。アクティブ PDSN で変更があったカウンタとアトリビュートだけが、スタンバイ PDSN に定期的に同期されます。最新の課金同期ポイント以降の情報は失われます。また、最新の情報が確実に正しく請求システムに送信されるよう、スタンバイ ユニットの AAA サーバに課金記録を送信することはありません。記録は、常にアクティブなユニットから送信されます。

同期が発生するセッション イベントには、次があります。

- コール設定
- コール ティアダウン
- フロー設定
- フロー ティアダウン
- 休止 - アクティブ間移行
- ハンドオフ
- A11 再レジストレーション
- 定期的な課金同期
- PPP 再ネゴシエーション

## アクティブ PDSN 障害

スタンバイ PDSN がアクティブ PDSN の障害を (HSRP を使用して) 検出した場合、アクティブ PDSN として引き継ぎます。すべての外部エンティティは、PCF、AAA サーバ、HA を含め、HSRP アドレスだけを使用して PDSN のペアと通信するよう設定されているため、スタンバイ PDSN がこれらのアドレスを引き継ぐと、障害を検出することができなくなります。また、すべての安定的なコールは、そのステータスをスタンバイと同期させます。したがって、スタンバイはアクティブを引き継ぐと、ユーザトラフィックの転送を開始できるようになります。スタンバイでは、すべてのタイム (A11 ライフタイム、PPP タイム、MIP ライフタイムなど) が、アクティブを引き継いだ時点で開始されます。課金データも、定期的な課金同期タイムが PDSN で設定されていた範囲で同期されます。

## スタンバイ PDSN の起動

既にアクティブがある場合に PDSN がアップすると、スタンバイの役割を引き継ぎます。アクティブ PDSN はスタンバイ PDSN が使用可能だと認識した場合、既存のすべてのユーザセッションのステータスデータをスタンバイに転送する、バルク同期と呼ばれる処理が行われます。この処理が完了すると、スタンバイ PDSN は障害の際にアクティブを引き継ぐ準備が整います。

## アクティブ-アクティブ シナリオの処理

リンク障害や中間ノードの障害があった場合、送信された HSRP パケットはピアに到達せず、スタンバイ ノードはアクティブがリロードされ、アクティブなステータスに遷移したとみなされます。これにより、アクティブ-アクティブ PDSN ノードの状態になります。PDSN の 1 つが、他がネットワークから独立している間にトラフィックを受信した場合、トラフィックを受信したノードが、リンクが復旧してもアクティブのままではなりません。

これを行うには、アプリケーション トラッキング オブジェクトを導入し、HSRP ピアが失われた後に PDSN がトラフィックを処理するかどうかに基づいて HSRP プライオリティを変更します。ピア PDSN が失われると、PDSN は HSRP のプライオリティを下げます。その後、PDSN がトラフィック (コントロールまたはデータ パケットのいずれか) を処理する時に、このプライオリティを、設定した値に戻します。これにより、PDSN 間のリンクが復旧された後にアクティブ ノードを選択できます。したがって、アクティブ-アクティブな状況でトラフィックを受信したノードは、リンクが復旧した後もアクティブのままとなります。

## その他の考慮事項

Redundancy Framework (RF; 冗長性フレームワーク) MIB は、2 つの PDSN のアクティブ ステータスとスタンバイ ステータスを監視するために使用できます。その他の MIB 変数と内部カウンタは、アクティブとスタンバイの間で同期されません。これらは、バックアップ イメージの IOS-Load または Reload の値から始まります。バックアップ イメージは、新しいボックスとして扱われます。

PDSN 冗長ペアは、クラスタ コントローラでは単一メンバとして扱われ、PDSN クラスタ処理メカニズムに透過されます。クラスタ コントローラは、アクティブ PDSN から冗長スタンバイへのフェールオーバーを認識しません。

同様に、PDSN 冗長ペアは PCF、HA、AAA サーバなどのすべての外部エンティティで単一の PDSN として表示されます。

FA-HA 接続の IPSec セキュリティ アソシエーションは、フェールオーバーでも維持されます。



(注) 現在、VPDN、Closed-RP、IPv6 および前払いサービスは、セッション冗長性の実装ではサポートされません。



(注) アクティブ ユニットとスタンバイ ユニット間の同期設定は、Cisco PDSN リリース 5.0 でサポートされています。新しい CLI コマンドのセットを使用して autosync-all 機能を有効にし、アクティブ ユニットの設定をスタンバイの設定と同期する必要があります。

## プロセス同期イベントでは

次の項目で、プロセス中のさまざまな同期イベントのセッションの冗長性において、PDSN の想定される動作を説明しています。

## コール設定

「sessions-in-progress」のステータスは、フェールオーバーでは維持されません。PCF からの R-P 接続リトライなどのメカニズムで、セッションが必要に応じて確立されます。

フェールオーバーは、PCF がユーザ フローの R-P セッションを確立した時点で発生する可能性があります。ユーザ フローは完全に確立されるわけではありません。この場合、フェールオーバーは R-P セッションがスタンバイでは存在しなくなります。PCF は、次の R-P セッション ライフタイムが更新されると、この R-P セッションをタイムアウトします。ユーザがこの時に新しいセッションを確立しようとすると、新しいセッションが作成されます。

## コール ティアダウン

セッションの終了には、次を含む 4 つのシナリオがあります。

- モバイル端末でセッション ティアダウンが開始
- PPP Idle Timeout が PDSN で時間切れ
- PDSN が Registration Update を開始
- PCF がライフタイムが 0 のレジストレーション要求を開始

これらの場合はいずれも、セッション ティアダウンが多段階プロセスです。たとえば、Registration Update メッセージが PDSN から送信され、ACK を受信しなかった場合にフェールオーバーが発生することがあります。この場合、スタンバイ PDSN は既にセッションを削除するよう指示されています。アクティブ PDSN は、PCF からのアップデート ACK を待機しません。

Registration Update を PCF に送信した後、スタンバイがセッションの削除を指示される前やセッションの削除要求が失われた後にフェールオーバーが発生した場合、スタンバイでセッションが確立したままになります。

その他にも、PPP コンテキストが、モバイルで行われた終了により削除され、その後フェールオーバーが R-P セッションが終了する前に発生した場合があります。

同様に、PDSN の PPP アイドル タイマの時間切れにより、PPP コンテキストが削除されてから、R-P セッションが終了する前にフェールオーバーが発生することがあります。

これらのケースでは、MIP Registration Lifetime または PPP Idle Timeout のいずれかが時間切れになり、セッションが終了します。

## フロー設定

確立されているプロセスのフローは保持されません。これは、フローの確立の失敗として表れ、フローを再確立する必要があります。

## フロー ティアダウン

ここでは、セッションに複数のフローがある場合に適用されます。現在、このケースは MIP コールでのみサポートしています。単一 IP コールでは、1 つのフローだけが許可されます。

MIP フローはスイッチオーバー後に保持されますが、レジストレーション ライフタイムの時間切れにより、フローが削除されることがあります。同じユーザが、ライフタイムの時間切れ前に再度レジストレーションを行うと、既存のビジターであるため、再レジストレーションだとみなされます。しかし、この再レジストレーションが成功するかどうかは、次の条件によって異なります。

- ユーザが、スイッチオーバーの前に前回のアクティブ ノードからのレジストレーション解除の Registration Reply (RRP; レジストレーション応答) を受け取り、その RRP 内の Foreign Agent Challenge (FAC; 外部エージェント チャレンジ) が現在アクティブなノードと同期していない場合 (この場合、フローがこのノードから削除されます)、この再レジストレーションは無効なチャレンジエラーとして拒否されます。ユーザは新しいアクティブ ノードへの要請を開始し、新しいチャレンジを受信し、Registration Request (RRQ; レジストレーション要求) を再送信する必要があります。

あります。この時、RRQ は有効な再レジストレーションとして扱われ、ライフタイムが更新されます。また、ユーザがこれを新しいレジストレーションだと認識していても、前回と同じ IP アドレスになります (FA と HA の場合、再レジストレーションです)。

- ユーザが、スイッチオーバーの前に前回のアクティブ ノードからのレジストレーション解除の RRP を受け取っていない場合、レジストレーション解除は現在アクティブなノードに再送信されます。このレジストレーション解除は、最新の FAC がスイッチオーバー前にスタンバイに同期しているかどうかにより、FAC が無効なため拒否される可能性があります。ユーザは新しい FAC の受け取り要請を送信して再度レジストレーション解除を送信するか、単にやめるかのどちらかを選択できます。ユーザが新しい FAC を受け取れない場合、ユーザが新しいアクティブ ノードへ要請を開始し、新しいチャレンジを受信し、Registration Request (RRQ; レジストレーション要求) を再送信する必要があります。

### 休止-アクティブ間移行

この移行は、アクティブとスタンバイの間で同期され、次のシナリオで発生します。

- PCF が RRQ に応答して RRP を受信し、移行ステータスがスイッチオーバーの前にスタンバイに同期すると、現在アクティブなノードに正しいセッションステータスが付与され、移行が正常に行われます。
- PCF が RRQ に応答して RRP を受信し、移行ステータスがスイッチオーバーの前にスタンバイに同期されなかった場合、現在アクティブなノードに誤ったセッションステータスが付与されます (このセッションが、アクティブでなければならないのに休止のマークが付けられます)。しかし、パケットはスイッチされ、カウントされます。PDSN 関連の **show** コマンドでは、セッションに関する正しい情報がすべて表示されない場合があります。後続の、アクティブから休止への移行では、PDSN でセッションは休止のままのため、問題は起こりません。
- スイッチオーバーの前に、PCF が RRQ に応答して RRP を受信せず、現在アクティブなノードで再度試行する場合、現在の日付で処理されます。
- スイッチオーバーの前に PCF が RRQ に応答して RRP を受信せず、現在アクティブなノードでの再試行が最大数を越えた場合、パケットはスイッチされカウントされます。

## ハンドオフ

### PCF 間ハンドオフ (休止またはアクティブ) - 同一 PDSN

ハンドオフで最も重大な問題は、ハンドオフがアクティブか休止かにかかわらず、保持されたセッションのターゲット PCF と現在アクティブな PDSN 間のデータ パスを再確立することです。さらに、実際に完了したハンドオフと、フェールオーバーが発生する可能性がある同期されたステータス間にウィンドウが存在します。

これには次のシナリオがあります。

- ターゲット PCF がアクティブ PDSN から RRP を受信し、ハンドオフのステータスがスイッチオーバーの前にスタンバイに同期された場合、ターゲット PCF と現在アクティブな PDSN 間のデータパスは、ハンドオフされたセッションで確立され、ユーザはサービスの中断に気づきません。古い PCF が、以前アクティブだったノードからの Registration Update を受信できるかどうかは、スイッチオーバーのポイントそのものによって異なります。Registration Update を受信し、RRQ (ライフタイム = 0) を送信した場合、コールは古い PCF で扱われる必要があります。古い PCF が Registration Update を受信せず、セッションが再度戻された場合、PCF でのこのケースの扱われ方ははっきりとは決まりません (これは、PCF にユーザの既存のコールがあり、新しいコール要求を同じユーザから受信した場合と同様です)。PCF が新しい要求を無視すると、正しいデータパスは存在せず、ユーザはトラフィックを転送できません。

- ターゲット PCF がアクティブ PDSN から RRP を受信しても、スイッチオーバー前にハンドオフステータスがスタンバイに同期されなかった場合、ターゲット PCF と現在アクティブな PDSN 間のデータパスは確立されません（セッションは古い PCF にポイントされたままです）。結果、エンドユーザはサービスの中断に気づきます。ユーザは、コールの終了（TERMREQ）の PPP パケットが現在アクティブな PDSN に到達できず、ターゲット PCF からの RRQ（ライフタイム=0）が現在アクティブな PDSN に到達しても、セッションがこれを有効なリモートトンネルエンドポイントだと認識されないため、正常にレジスタ解除できません。結果、レジストレーション解除は無視されます。セッションは、実際は PPP アイドル タイムまたはレジストレーション ライフタイムで削除されます。ユーザが再度登録すると、ハンドオフとして扱われます。セッションの現在のリモートトンネルエンドポイント（古い PCF）がターゲット PCF と異なるためです。この時、データパスが確立され、ユーザはサービスを受けられます。
- ターゲット PCF がスイッチオーバー前にアクティブ PDSN から RRP を受信せず、PCF が再度現在アクティブな PDSN に移行した場合、ハンドオフは現在の日付で同様に処理されます。

### PCF 間ハンドオフ（休止またはアクティブ） - 異なる PDSN

この種類のハンドオフは、PANID と CANID を含む A11 レジストレーション要求を受領することで指示されます。また、Mobility Event Indicator と Accounting Data（R-P Session Setup Air-link Record）も含まれます。ハイアベイラビリティの観点から、これは新しくアクティブになった PDSN での新しいセッションの確立や、古い PDSN での「通常の」セッション終了のようになります。

### A11 再レジストレーション

A11 Reregistration RRQ は、アクティブなユニットが受信します。レジストレーション ライフタイムはスタンバイでは開始されませんが、タイム値の追跡は保持しているため、アクティブになるとライフタイムを再度開始することができます。再レジストレーション RRQ のライフタイムが、以前の RRQ と異なる場合、新しいライフタイムがスタンバイに同期されます。たとえば、以前の RRQ のライフタイムが 300 秒で、現在新しい RRQ の値が 500 秒に変わっている場合、新しい値がスタンバイに同期されます。再レジストレーション RRQ に含まれている他の重要なパラメータもスタンバイに同期されません。

上記の例では、新しいライフタイムをスタンバイに同期する前にフェールオーバーが発生すると、スタンバイのライフタイムは 300 秒から開始します。

### PPP 再ネゴシエーション

PPP ネゴシエーションで、PDSN は RP セッションのすべてのフローを削除し、各フローで課金停止を送信します。PPP が再度アップすると、PDSN はこのセッションの新しいフローを作成します。したがって、PPP 再ネゴシエーションがアクティブになると、アクティブユニットがスタンバイの RP セッションからすべてのフローを削除する PPP 再ネゴシエーション通知をスタンバイに送信します。再度、PPP がアップして新しいフローがアクティブで作成されると、アクティブユニットは各フローのデータをスタンバイに送信します。PPP 再ネゴシエーションでフェールオーバーが発生すると、再ネゴシエーションは失敗し、セッションが新しくアクティブになったユニットでティアダウンされる場合があります。

## その他の考慮事項

### タイマ

セッションが確立すると、通常次のタイマが実行されます。

- R-P Session Lifetime
- PPP Idle Timeout
- MIP レジストレーション ライフタイム
- PPP Absolute Session Timeout

設定によっては、次のタイマが実行される場合があります。

- 定期的な課金（「セッション イベント」の項で説明した同期タイマと混同しないでください）。

これらのタイマは、フェールオーバーが発生すると再起動され、破棄された時間は、スタンバイに同期されません。この影響で、既に破棄された時間と等しい値までタイマが元の値を超えて拡張されます。これにより、ユーザがフェールオーバーのセッション障害に気づくことはありません。

## 制約事項

PDSN Session Redundancy 機能には次の制限事項があります。

- SR 設定でのリソース失効の制限。

Session Redundancy が許可されていない PMIP フローで失効タイムスタンプを「msec」（**ip mobile foreign-service revocation timeout 5 retransmit 4 timestamp msec**）に設定。

「msec」オプションは、timestamp フィールドに動作時間を入力し、スタンバイ ルータの動作時間は、スタンバイ PDSN がアクティブを引き継いだ場合（そして、PMIP フローが終了した場合）に、スイッチオーバー後にそれより小さい値になると考えられます。したがって、HA での失効は、失効メッセージの識別値が HA で考えられる値よりも小さくなるため、無視されます。

- **ip radius source interface** コマンドは仮想アドレス（HSRP）をサポートしていません。したがって、SR 設定で AAA サーバに到達するソース インターフェイスとして使用される Loopback インターフェイスで設定された IP アドレス（NAS IP アドレス）もサポートしていません。
- IP ローカル プール リサイクル遅延は、遅延値を 30 以上で設定する必要があります（**ip local pool pdsn-pool first\_ip last\_ip recycle delay 30**）。
- また、IP の枯渇によりセッションがドロップしないよう、バッファが必要とする値よりも余分な IP を最小限（秒単位のコール \* リサイクル遅延）用意するのが妥当です。

## 内部

次の章で、スタンバイ ユニットへの同期情報について説明します。

### ハイレベル データリンク コントロールの非同期

使用している Asynchronous High-Level Data Link Control（AHDLC; 非同期ハイレベル データリンク コントロール）チャンネル単位でコントロール文字マッピングが保持されます。通常デフォルトが使用されるため、これらは異なる部分だけ同期されます。AHDLC チャンネル番号は同期されません。使用できるチャンネルはスタンバイで個別に選択されます。

### GRE - RP インターフェイス

GRE Key が同期されます。シーケンス フラグがユーザ ベース単位で設定できるため、フラグは同期されます。

### RP シグナリング

A11 メッセージングの内容は、ここで説明したように処理されます。

- フラグ - 固定で、同期は不要です。
- ライフタイム - 同期されます。
- Home Address - 同期は不要です。
- HA - 同期は不要です。R-P インターフェイスの HSRP アドレスです。クラスタ処理が設定されている場合に、PDSN IP アドレスの提出に使用されます。提出された PDSN の HSRP アドレスになります。セッションが確立する前に使用されるだけです。

- Care-of-Address - 同期されます。R-P セッションの PCF IP アドレスです。
- A10 Source IP address - 同期されます。PCF の A10 IP アドレスです。
- 識別名 - 同期されません。再送保護のタイムスタンプが含まれます。
- Mobile-Home Authentication Extension - 同期されません。メッセージ単位で計算されます。
- Registration Update Authentication Extension - 同期されません。メッセージ単位で計算されます。
- Session-Specific Extension - 同期されます。Key、MN\_ID、SR-ID が同期されます。
- C-VOSE - 複数のアプリケーション タイプ、Accounting、MEI、DAI が含まれます。課金情報は同期されます。詳細については、課金の章で説明しています。
- N-VOSE の内容 - ANID は、セッションの確立の一部として、またハンドオフの結果変更された時点での両方で同期されます。ファスト ハンドオフはサポートされていません。そのため、PDSN 識別子はセッションの冗長性の説明とは無関係です。
- Radio Network Packet Data Inactivity Timer (RNPDIT; 無線ネットワーク パケット データ非アクティブ タイマ) - 同期されます。
- A11 への発信元 UDP ポートは同期されます。

## PPP

すべての LCP オプションは同期されます。IPCP では、IP アドレスと IPHC パラメータのみが同期されます。IPCP ネゴシエーションでネゴシエートされた DNS サーバ IP アドレスは、スタンバイ ユニットに同期されません。認証や許可で、AAA サーバからダウンロードされたユーザ単位のアトリビュートは、すべてスタンバイ ユニットに同期されます。

## 圧縮 - ヘッダーとペイロード

ヘッダーとペイロードのコンテキストは、どちらかみの圧縮の同期はありません。スタンバイ PDSN のフェールオーバーにより、圧縮コンテキストが再確立されます。

ヘッダーの圧縮 - スイッチオーバー後のセッションの最初のパケットはドロップし、ピアがタイムアウトの確認後、パケットを再送信します。

ペイロードの圧縮 - スタンバイでのスイッチオーバー後、圧縮履歴は存在しません。CCP リセットは、デコードが失敗すると自動的に生成されます。特別な処理は不要です。

## IP アドレスの割り当て

IP アドレスが、PDSN で設定されたプールから動的に割り当てられる場合、スタンバイは同じアドレスをセッションに関連付けます。IP アドレスは、PPP ステータスの一部として同期されます。IP アドレスが AAA サーバから受信されるか、ローカル プールからでないスタティック IP アドレスが使用されると、このアドレスは、スタンバイでセッションに関連付けられます。同様に、アドレス プールが同期されます。

## AAA - 認証と認可

表 5 に、関連する認証と認可パラメータについて示しています。これは、スタンバイで AAA ステータスを正確に再作成できるようにするために必要です。

表 5 認証と認可でサポートされている標準 AVP

Cisco IOS 名でサポートされる認証および認可 AVP	同期化	説明	許可	
			アクセス要求	アクセス受諾
User-Name	あり	認証および認可のユーザ名。	あり	不可
User-Password	不可	認証用のパスワード。	あり	不可
CHAP-Password	不可	CHAP パスワード。	あり	不可
NAS-IP-Address	不可	RADIUS サーバとの通信に使用する PDSN インターフェイスの IP アドレス。ループバック アドレスを、この目的で使用することができます。	あり	不可
Service-Type	不可	ユーザが利用するサービスのタイプ 次の値がサポートされます。 <ul style="list-style-type: none"> <li>MSID ベースのユーザ アクセスには「Outbound」</li> <li>他の種類のユーザ アクセスには「Framed」</li> </ul>	あり	あり
Framed-Protocol	不可	フレーミング プロトコル ユーザが使用。次の値がサポートされます。 <ul style="list-style-type: none"> <li>PPP</li> </ul>	あり	あり
Framed-IP-Address	あり	ユーザに割り当てられた IP アドレス。	あり	あり
Session-Time-Out	あり	セッションが終了するまでにユーザに与えられるサービスの最大秒数。 アトリビュート値は、ユーザごとの「絶対タイムアウト」になります。	不可	あり
Idle-Time-out	あり	セッションが終了するまでの、ユーザの最大連続アイドル接続秒数。 アトリビュート値は、ユーザごとの「アイドルタイムアウト」になります。	不可	あり
Calling-Station-ID	あり	モバイル ユーザの MSID 識別番号。	あり	不可
CHAP-Challenge (オプション)	不可	CHAP Challenge。	あり	不可
Tunnel-Type	不可	VPN トンネリング プロトコルを使用。次の値がサポートされます。 <ul style="list-style-type: none"> <li>PPTP は 1 (非サポート)</li> <li>L2TP は 3</li> </ul>	不可	あり
Tunnel-Medium-Type	不要：サポートされません	トンネルに使用するトランスポート メディア タイプ。	不可	あり
Tunnel-Client- Endpoint	不要：サポートされません	トンネルのクライアント エンドのアドレス。 Tunnel-Client-Endpoint を指定すると、Tunnel-Server はサポートされません。L2TP を使用	不可	あり
Tunnel-Server- Endpoint	不要：サポートされません	トンネルのサーバ エンドのアドレス。	不可	あり
Tunnel-Password	不要：サポートされません	リモート サーバの認証に使用するパスワード。	不可	あり



表 5 認証と認可でサポートされている標準 AVP (続き)

Cisco IOS 名でサポートされる認証および認可 AVP	同期化	説明	許可	
			アクセス要求	アクセス受諾
Tunnel-Assignment-ID	不要：サポートされません	トンネルの発信側に、セッションが割り当てられたトンネルの識別名を伝えます。	不可	あり
addr-pool	不要：サポートされません	アドレス取得元のローカル プール名。service=ppp および protocol=ip と使用されます。 「addr-pool」はローカル プーリングと 併用されます。 ローカル プール名（ローカルで事前に設定する必要があります）が指定されます。 ローカル プールの設定には、ip-local pool コマンドを使用してください。例： <ul style="list-style-type: none"> <li>ip address-pool local</li> <li>ip local pool boo 10.0.0.1 10.0.0.10</li> <li>ip local pool moo 10.0.0.1 10.0.0.20</li> </ul>	不可	あり
Inacl#<n>	あり	現在の接続期間に使用されるインターフェイスにインストールされ適用される、入力アクセス リストの ASCII アクセス リスト識別名。 service=ppp および protocol=ip、service service=ppp および protocol=ipx で使用されます。 <b>(注)</b> ユーザ単位のアクセス リストは、現在 ISDN インターフェイスでは使用できません。	不可	あり
Inacl	あり	インターフェイス 入力アクセス リストの ASCII 識別名。 service=ppp および protocol=ip と使用されます。 SLIP または PPP/IP の IP 出力アクセス リストが含まれません (intacl=4 など)。 アクセスリスト自体は、ルータで事前に設定する必要があります。	不可	あり
outacl#<n>	あり	現在の接続期間に使用されるインターフェイスにインストールされ適用される、インターフェイス出力アクセス リストの ASCII アクセス リスト識別名。 service=ppp および protocol=ip、service service=ppp および protocol=ipx で使用されます。	不可	あり
Outacl	あり	インターフェイス 出力アクセス リストの ASCII 識別名。 service=ppp および protocol=ip、service service=ppp および protocol=ipx で使用されます。 SLIP または PPP/IP の IP 出力アクセス リストが含まれません (outacl=4 など)。 アクセスリスト自体は、ルータで事前に設定する必要があります。	不可	あり

表 5 認証と認可でサポートされている標準 AVP (続き)

Cisco IOS 名でサポートされる認証および認可 AVP	同期化	説明	許可	
			アクセス要求	アクセス受諾
interface-config	あり	Virtual Profiles を持つ、ユーザ独自の AAA サーバインターフェイス設定情報。 等号 (=) が付いている情報は、すべての Cisco IOS インターフェイス設定コマンドとして使用できます。	不可	あり
SPI	あり	MIP レジストレーション中にモバイルユーザの認証に使用する、HA で必要な認証情報を伝えます。 SPI (セキュリティ パラメータ インデックス)、キー、認証アルゴリズム、認証モード、再送保護タイムスタンプ範囲を提供します。 コンフィギュレーション コマンド <b>ip mobile secure host address</b> と同じ構文の情報です。基本的に、そのストリングの後ろに残りのコンフィギュレーション コマンドを一字一句指定します。	不可	あり
IP-Pool-Definition	あり	X a.b.c Z という形式を使用したアドレスのプールを定義します。X はプール インデックス番号、a.b.c はプールの開始 IP アドレス、Z はプールの IP アドレスの番号です。 たとえば、3 10.0.0.1 5 はダイナミック割り当て用に 10.0.0.1 から 10.0.0.5 まで割り当てます。	不可	あり
Assign-IP-Pool	あり	識別された IP プールから、IP アドレスを割り当てます。	不可	あり
Framed-Compression	あり	リンクで使用される圧縮プロトコルを示します。次の値がサポートされます。 • 0 : なし • 1 : VJ-TCP/IP ヘッダー圧縮	不可	あり
Link-Compression	あり	使用されるリンク圧縮プロトコル。 次の値がサポートされます。 • 0 : なし • 1 : Stac • 2 : Stac-LZS • 3 : MS-Stac	不可	あり

GPP2 パケット データ サービスのアトリビュート

表 6 で、3GPP2 パケット データ サービス アトリビュートを示しています。

表 6 3GPP2 パケット データ サービスのアトリビュート

名前	同期化	説明	許可	
			アクセス要求	アクセス受諾
mobileip-mn-lifetime	あり	プロキシ MIP RRQ で使用するライフタイムを定義します。	不可	あり

表 6 3GPP2 パケット データ サービスの属性 (続き)

名前	同期化	説明	許可	
mobileip-mn-ipaddr	あり	スタティック アドレス割り当て用の MN IP アドレス。この属性が存在する場合、このアドレスは Proxy MIP RRQ で使用されます。	不可	あり
mobileip-mn-flags	あり	プロキシ MIP RRQ で使用するフラグを定義します。	不可	あり
CDMA-Realm	あり	MSID に基づいたアクセスの、MSID@realm 形式でユーザ名を構築するために使用する「レルム」情報。この方法で構築されたユーザ名は、課金目的でのみ使用されます。 レルム情報のフォーマットは、次のようになります。 <ul style="list-style-type: none"> <li>ユーザの登録済みドメインのレルムを指定する ASCII 文字列</li> </ul>	不可	あり
CDMA-User- Class	あり	ユーザが加入しているサービスのタイプ。 次の値をサポートしています。 <ul style="list-style-type: none"> <li>SIP は 1</li> <li>MIP は 2</li> </ul>	不可	あり
3GPP2-Reverse-Tunnel- Spec	あり	反転トンネリングの要不要を示します。 次の値をサポートしています。 <ul style="list-style-type: none"> <li>反転トンネリングが不要の場合、0</li> <li>反転トンネリングが必要な場合、1</li> </ul>	不可	あり
3GPP2-Home-Agent- Attribute	あり	HA のアドレス	あり	あり
3GPP2-IP-Technology	あり	ユーザが加入しているサービスのタイプを示します。 次の値をサポートしています。 <ul style="list-style-type: none"> <li>SIP は 1</li> <li>MIP は 2</li> </ul>	不可	あり
3GPP2-Correlation-Id	あり	特定のユーザ フロー向けに生成されたすべてのアカウントング レコードを示します。	あり	あり
3GPP2-Always-On	あり	常時接続サービスを示します。 次の値をサポートしています。 <ul style="list-style-type: none"> <li>常時接続でないユーザには 0</li> <li>常時接続のユーザには 1</li> </ul>	不可	あり
3GPP2-Security Level	あり	ホーム ネットワークが接続先のネットワークに必要なセキュリティの種類を示しています。	不可	あり
3GPP2- IKE Pre-shared Secret Request	不可	PDSN に、HA との Phase 1 IKE ネゴシエーションの共有秘密鍵が必要なことを示しています。	あり	不可
3GPP2-Pre-shared シークレット	不可	IKE の共有秘密鍵。	不可	あり
3GPP2- KeyID	不可	PDSN と HA の間の IKE 交換で使用される KeyID パラメータが含まれます。	不可	あり

表 6 3GPP2 パケット データ サービスの属性 (続き)

名前	同期化	説明	許可	
3GPP2-Allowed DiffServ マーキング	不可	ユーザが AF (A)、EF (E) でパケットにマーク付けが可能かどうかを指定します。Max Class (つまり Max Selector Class) は、ユーザがパケットに Max Class と等しいかそれより小さい Class Selector Code Point でマーク付けが可能かどうかを指定します。	不可	あり
3GPP2-MN-AAA Removal Indication	あり	RADIUS アクセス受諾メッセージで受信されると、PDSN は MN-AAA を含みません。	不可	あり
3GPP2-Foreign-Agent Address	不可	RRQ に格納された PDSN CoA の IPv4 アドレス。	あり	不可
サービス オプション	あり	使用されているサービスの種類を示しています。	あり	不可
DNS Update Required	不要 サポートされません	DNS アップデートが必要かどうかを示しています。	不可	あり
RN PDIT	あり	Radio Network Packet Data Inactivity Timer。	不可	あり
Session Termination Capability	あり	サポートされているリソース失効の性質を示しています。	あり	あり

## AAA サーバ アカウンティング

### GPP2 アカウンティング レコード フィールド

表 7 で、GPP2 課金記録フィールドを示します。

表 7 GPP2 アカウンティング レコード フィールド

項目	パラメータ	説明	同期化
A モバイル識別情報			
A1	MSID	MS ID (例: IMSI, MIN, IRM)。	あり
A2	ESN	Electronic Serial Number (電子シリアル番号)。	あり
A3	MEID	Mobile Equipment Identifier (モバイル機器識別情報)。	あり
B ユーザ識別情報			
B1	Source IP Address	MS の IPv4 アドレス。	あり
B2	Network Access Identifier (NAI)	MS のユーザとホーム ネットワークを識別する user@domain 構成。	あり
B3	Framed-IPv6- Prefix	MS IPv6 プレフィクス。	非サポート
B4	IPv6 インターフェイス ID	MS IPv6 インターフェイス識別情報。	非サポート
C セッション識別情報。			
C1	Account Session ID	Account Session ID は、Serving PDSN によって作成された独自の課金 ID です。単一 R-P 接続または P-P 接続からの RADIUS の開始記録や停止記録を一致させることができます。	あり
C2	Correlation ID	Correlation ID は、パケット データ セッションごとに Serving PDSN によって作成された独自の ID です。関連する R-P 接続や P-P 接続ごとの複数の課金イベントに相互に関連付けることができます。	あり

表 7 GPP2 アカウンティング レコード フィールド (続き)

項目	パラメータ	説明	同期化
C3	Session Continue	このアトリビュートが「True」に設定されている場合、セッションが終わりではなく、課金停止の後ただちに Account Start Record が続くことを意味しています。「False」の場合はセッションの停止を示しています。	あり
C4	Beginning Session	このアトリビュートが「True」に設定されている場合、新しいパケット データ セッションが確立されることを意味しています。「False」の場合、以前のパケット データ セッションの継続を示しています。このアトリビュートは RADIUS Accounting-Request (Start) レコードに含まれています。	不可
C5	Service Reference ID	これは、A11 レジストレーション応答メッセージで RN から受信されたサービス インスタンス ID です。	あり
D インフラストラクチャ識別情報			
D1	HA	HA の IPv4 アドレス。	あり
D2	PDSN	PDSN の IPv4 アドレス。	不要：アクティブとスタンバイで同じ設定にする必要があります
D3	Address Serving PCF	サービス側 PCF の IP アドレス (提供 RN) の IP アドレス。	あり
D4	BSID	SID + NID + Cell Identifier タイプ 2。	あり
D5	IPv6 PDSN Address	PDSN の IPv6 アドレス。	サポートされません
D6	Foreign Agent Address	FA-CoA の IPv4 アドレス。	サポートされません
D7	Subnet	HRPD のサブネット情報。	あり
E ゾーン識別情報			
E1	ユーザ ゾーン	Tiered Services ユーザ ゾーン。	あり
F セッション ステータス			
F1	Forward FCH Mux Option	Forward Fundamental Channel 多重オプション。	あり
F2	Reverse FCH Mux Option	Reverse Fundamental Channel 多重オプション。	あり
F5	サービス オプション	RN から受信した CDMA サービス オプション。	あり
F6	Forward Traffic Type	転送方向トラフィック タイプ - Primary または Secondary。	あり
F7	Reverse Traffic Type	反転方向トラフィック タイプ - Primary または Secondary。	あり
F8	FCH Frame Size	FCH フレーム サイズを指定します。	あり
F9	Forward FCH RC	転送 Fundamental Channel での無線チャンネルの形式と構成。データレート、変調、拡大レートに特性を持つ、一組の転送送信形式。	あり
F10	Reverse FCH RC	反転 Fundamental Channel での無線チャンネルの形式と構成。データレート、反転、拡大レートに特性を持つ、一組の転送送信形式。	あり
F11	IP Technology	このコールで使用する IP テクノロジーを、SIP または MIP から指定します。	あり

表 7 GPP2 アカウンティング レコード フィールド (続き)

項目	パラメータ	説明	同期化
F12	Compulsory Tunnel Indicator	単一パケットのデータ接続中のプライベート ネットワークまたは ISP アクセスのための、MS に代わって確立された強制トンネルの呼び出しのインジケータ。	あり
F13	Release Indicator	停止レコードを送信する理由を指定します。	あり
F14	DCCH Frame Size	Dedicated Control Channel (DCCH; 個別制御チャネル) フレーム サイズを指定します。	あり
F15	Always On	常時接続サービスのステータスを指定します。	あり
F16	Forward PDCH RC	転送パケット データ チャネルの無線設定 (このパラメータは、MS が 1xEV DV の性能を持つことを示すものとして使用することができます)。	あり
F17	Forward DCCH Mux Option	転送個別制御チャネル多重オプション。	あり
F18	Reverse DCCH Mux Option	反転個別制御チャネル多重オプション。	あり
F19	Forward DCCH RC	転送個別制御チャネルでの無線チャネルの形式と構成。データ レート、変調、拡大レートに特性を持つ、一組の転送送信形式。	あり
F20	Reverse DCCH RC	反転個別制御チャネルでの無線チャネルの形式と構成。データ レート、反転、拡大レートに特性を持つ、一組の転送送信形式。	あり
F22	Reverse PDCH RC	反転パケット データ チャネルの無線設定。	あり
G セッション アクティビティ			
G1	Data Octet Count (終端)	IP ネットワークから PDSN で受信されたとおり (すべての圧縮やフラグメンテーション前) の、ユーザに送信された IP パケットのオクテットの合計。	あり
G2	Data Octet Count (発生源)	ユーザが送信した IP パケットのオクテットの合計。	あり
G3	Bad PPP フレーム カウント	不正な可能エラーによる PDSN によってドロップされた MS からの PPP フレームの合計。	あり
G4	Event Time	次のいずれかを示す、イベント タイムスタンプです。 <ul style="list-style-type: none"> <li>RADIUS 開始メッセージの一部の場合の課金セッションの開始。</li> <li>RADIUS 停止メッセージの一部の場合の課金セッションの停止。</li> <li>RADIUS Interim-Update メッセージの一部の場合の Interim-Update 課金イベント。</li> </ul>	あり
G5	Remote IPv4 Address Octet Count	1 つ以上のリモート IPv4 アドレスに関連付けられたオクテット カウントを含みます。発信元または送信先の課金に使用されます。	あり
G6	Remote IPv6 Address Octet Count	1 つ以上のリモート IPv6 アドレスに関連付けられたオクテット カウントを含みます。発信元または送信先の課金に使用されます。	サポートされません
G8	Active Time	トラフィック チャネルでのアクティブな接続時間の合計秒。	あり
G9	Number of Active Transitions	ユーザによる非アクティブからアクティブへ移行の合計。	サポートされません
G10	SDB Octet Count (終端)	ショート データ バーストを使用した MS への送信オクテットの合計。	あり
G11	SDB Octet Count (発生源)	ショート データ バーストを使用した MS による送信オクテットの合計。	あり

表 7 GPP2 アカウンティング レコード フィールド (続き)

項目	パラメータ	説明	同期化
G12	SDB の数 (終端)	MS とのショート データ バースト トランザクションの合計数です。	あり
G13	Number of SDBs (Originating)	MS とのショート データ バースト トランザクションの合計数です。	あり
G14	Number of HDLC layer octets received	PDSN の HDLC レイヤによって反対方向で受信したすべてのオクテットの数です。	あり
G15	Inbound MIP Signaling Octet Count	MS から送信されるレジストレーション要求と請求のオクテットの合計数です。	あり
G16	Outbound MIP Signaling Octet Count	任意の圧縮またはフラグメンテーションの前に、MS に送信されたレジストレーション応答およびエージェント アドバタイズメントのオクテットの合計数です。	あり
G17	Last User Activity Time	ユーザが最後に実行した既知のアクティビティのタイムスタンプ (UTC 1970 年 1 月 1 日からの秒数) です。	あり
I.Quality of Service			
I1	IP Quality of Service (QoS)	このアトリビュートは非推奨です。	サポートされません
I2	Airlink Priority	ユーザと関連付けられた Airlink Priority を識別します。パケット データ サービスと関連付けられたユーザの優先度です。	サポートされません
Y.Airlink Record Specific Parameters			
Y1	Airlink Record Type	3GPP2 Airlink Record Type。	不可
Y2	R-P Connection ID	R-P Connection の識別子。PCF および PDSN 間の R-P 接続 (A10 接続) を一意に識別する GRE キーです。	あり
Y3	Airlink Sequence Number	Airlink レコードのシーケンス番号。R-P 接続の Airlink レコードのシーケンスを示します。	あり
Y4	Mobile Originated / Mobile Terminated Indicator	SDB Airlink レコードでだけ使用されます。SDB がモバイル発信かモバイル終端かを示します (0=Mobile Originated および 1=Mobile Terminated)。	あり
Z.Container			
Z1	Container	3GPP2 Accounting Container アトリビュート。このアトリビュートは、3GPP2 AVP を埋め込むために使用されます。	サポートされません

### RADIUS Server Group Support

選択した AAA サーバの IP アドレスは同期されません。

### Mobile IP Signaling

MIP サービスの場合、各 MIP フローの同期されるパラメータには、次のデータが含まれます。

- MIP レジストレーション ライフタイム
- レジストレーション要求に示される MIP フラグ
- AAA サーバから受信する MN-AAA 削除指示
- HA IP アドレス
- モバイルの IP アドレス
- リバース トンネル指示

- MIP レジストレーション要求の Care of Address
- FA-Challenge (モバイル ノード レジストレーション中に使用されます)

### モバイル IP トンネル トラフィック

このトラフィックは、GRE トンネルまたは IP-in-IP トンネルで送信されます。同期する必要がある唯一の情報は、ピアのトンネル エンドポイントです。

### ローカル設定の IPsec

Catalyst 76xx シリーズ上の PDSN の場合、IPsec トンネルは VPN Acceleration Module で終端します。PDSN の役割は、AAA サーバからパラメータを取得、それらのパラメータに基づいて、IPsec トンネルの確立を「トリガ」することです。これらのパラメータの同期は、シャーシ内設定に対する PDSN フェールオーバーの場合に、IPsec トンネルを保持するために十分です。PDSN のフェールオーバーは、VPN Acceleration Module/SUP のフェールオーバーと併用できません。現在のところ、シャーシ間設定およびシャーシ内 SUP フェールオーバーは、ステートフル IPsec をサポートしていません。

### FA-HA IPsec

シャーシ内設定の場合に 7600 上の PDSN のフェールオーバーが発生した場合、FA-HA IPsec トンネルは保持されます。シャーシ間設定の場合は保持されません。

## AAA サーバ アカウンティング

### 定期的なアカウンティングの同期

アカウンティング情報はアクティブ イメージおよびスタンバイ イメージ間でオプションで同期されます。この同期は、設定した定期的なアカウンティング間隔で発生します。同期されるカウンタは、g1、g2、およびパケット数です。Interim Accounting レコードの送信によって、バイト数およびパケット数の同期がトリガされます。オペレータ定義の定期的なアカウンティング間隔を設定すると、PDSN フェールオーバーの影響を受けるときのユーザ課金レコードの精度が決まります。過少課金が発生する可能性はありますが、課金過多が発生することはありません。

### VSA アプローチによるアカウンティング

スイッチオーバーが発生した後に、(必要に応じて) 最初の interim または stop アカウンティング レコードに、スイッチオーバーが発生したことを示す Vendor Specific Attribute (VSA; ベンダー固有アトリビュート) を含めます。この VSA を含める処理は、`cdma pdsn redundancy accounting send vsa swact` コマンドを発行することで制御できます。



(注) G1 カウンタおよび G2 カウンタは同期しません。

次に、vsa によるアカウンティングのデバッグ例を示します。

```
Sep 13 18:23:10.179: RADIUS:   Cisco AVpair          [34] 16
Sep 13 18:23:10.179: RADIUS:   63 64 6D 61 2D 72 66 73 77 61 63 74 3D 31
[cdma-rfswact=1]
```

### システム アカウンティング

セッション冗長性セットアップの場合、セットアップ全体が提示されたときにだけ、アクティブ ユニットからアカウンティング ON が送信されます (フェールオーバー後に、新しいアクティブ ユニットからアカウンティング ON は送信されません)。どのようなシナリオでも、スタンバイ ユニットからシステム アカウンティング イベントが送信されることはありません。ただし、スタンドアロン モードでイベントが送信されます。

アクティブ ユニットでリロードが発行されると、sys-off が送信されます。



## このリリースの新機能

ここでは、Cisco PDSN リリース 5.1 の新機能について説明します。

- 「簡易 IP クライアントの IP アカウンティングのサポート」
- 「PCF 単位の SNMP の新規 MIB オブジェクト」
- 「一般的な NAI のサポート」
- 「最新の IS-835 に合わせたプロキシ MIP の変更」
- 「簡易 IPv6 サポート」
- 「Access-Request アトリビュート」
- 「新しい PCF カウンタ単位の PPP」
- 「VPDN 条件付きデバッグ」
- 「Revocation メッセージの GRE CVSE および MN NAI 拡張」

### 簡易 IP クライアントの IP アカウンティングのサポート

Cisco PDSN では、簡易 IP カスタマーが IP アドレス割り当てのホーム ネットワークで L2TP Network Server (LNS) に接続できるようにサポートされています。Cisco PDSN は、MS および LNS 間の PPP ネゴシエーション中に LNS から返される IPCP 設定の ACK を監視します。次に、IP アドレスを抽出し、以降のすべての AAA パケットで 0.0.0.0 ではなくこのアドレスを使用します。



(注) 簡易 IP アカウンティングは、LNS が割り当てる IPv6 アドレスをサポートしません。

Cisco PDSN リリース 5.1 で、新しいコマンド `cdma pdsn accounting vpdn address [include renegotiation]` が導入されました。以前のリリースの Cisco PDSN では、L2TP トンネルが確立するとすぐに、`accounting-start` (MN IP にすべてゼロを使用) が送信されます。`cdma pdsn accounting vpdn address [include renegotiation]` コマンドをイネーブルにすると、Cisco PDSN がモバイルに有効な IP アドレスを取得するまで `accounting-start` は遅延します。IP アドレスがネゴシエーションされる前にコールが中断した場合、アカウンティング メッセージは送信されません。



(注) 拡張機能 (再ネゴシエーションを含む) 付きで CLI コマンドをイネーブルにすると、VPDN のすべてのパケットがスヌーピングされます。そのため、Cisco PDSN のパフォーマンスに影響があります。ネゴシエーション中に LNS が IP アドレスを変更しない場合、CLI の拡張機能 (再ネゴシエーションを含む) を削除できます。そうすることで、モバイル IP アドレスを受信した後に、スヌーピングは停止されます。

### PCF 単位の SNMP の新規 MIB オブジェクト

Cisco PDSN では、PCF 単位の PPP 統計情報に関して SNMP 管理のサポートが必要です。MIB オブジェクトは管理可能なオブジェクトを定義します。表 8 および 9 は、それぞれ Cisco PDSN リリース 5.1 で導入された PCF 単位の新しい MIB オブジェクトおよび VPDN MIB オブジェクトの説明です。

表 8 は、Cisco PDSN リリース 5.1 の PCF 単位の新しい MIB オブジェクトのリストです。

表 8 Cisco PDSN リリース 5.1 の PCF 単位の新しい MIB オブジェクト

オブジェクト	説明
<b>ccpCdmaExtCacEnabled</b>	Cisco PDSN がコール アドミッション制御機能をサポートするかどうかを決定します。
<b>ccpCdmaExtPcfSoPppPreLCPPdsnA10Rls</b>	PPP が LCP ネゴシエーション フェーズを開始する前に Cisco PDSN によって解放される、PCF 単位の A10 接続の合計数を指定します。
<b>ccpCdmaExtPcfSoPppPreLCPPcfA10Rls</b>	PPP が LCP ネゴシエーション フェーズを開始する前に PCF によって解放される、A10 接続の合計数を指定します。
<b>ccpCdmaExtPcfSoPppLcpOptionIssueFailures</b>	LCP オプション ネゴシエーション エラーによって終了する、PCF 単位の PPP 接続要求の合計数を指定します。
<b>ccpCdmaExtPcfSoPppLcpFailuresMaxRetrans</b>	再送信の最大数に達した後に LCP フェーズで失敗する、PCF 単位の PPP 接続要求の合計数を指定します。
<b>ccpCdmaExtPcfSoPppLcpFailuresUnknown</b>	不明な理由によって LCP フェーズで失敗する、PCF 単位の PPP 接続要求の合計数を指定します。
<b>ccpCdmaExtPcfSoPppLcpPhaseRxTermreqs</b>	LCP フェーズ中に PPP が term 要求を受信したために終了する、PCF 単位の PPP ネゴシエーションの合計数を指定します。
<b>ccpCdmaExtPcfSoPppLcpPcfA10Rls</b>	LCP ネゴシエーション フェーズ中に PCF によって解放される A10 接続の合計数を指定します。
<b>ccpCdmaExtPcfSoPppAuthFailures</b>	認証フェーズで失敗した PCF 単位の PPP セットアップ接続の合計数を指定します。
<b>ccpCdmaExtPcfSoPppAuthAAATimeouts</b>	AAA のタイムアウトによる、PCF 単位の PPP 認証エラーの合計数を指定します。
<b>ccpCdmaExtPcfSoPppAuthFailuresUnknown</b>	不明な理由によって認証フェーズで失敗した、PCF 単位の PPP 接続要求の合計数を指定します。
<b>ccpCdmaExtPcfSoPppAuthMaxRetransFailure</b>	再送信の最大数に達した後に認証フェーズで失敗した、PCF 単位の PPP 接続要求の合計数を指定します。
<b>ccpCdmaExtPcfSoPppAuthPhaseRxTermreqs</b>	認証フェーズ中に PPP が term 要求を受信したために終了する、PCF 単位の PPP ネゴシエーションの合計数を指定します。
<b>ccpCdmaExtPcfSoPppAuthPcfA10Rls</b>	PPP 認証フェーズ中に PCF によって解放される A10 接続の合計数を指定します。

表 8 Cisco PDSN リリース 5.1 の PCF 単位の新しい MIB オブジェクト (続き)

<b>ccpCdmaExtPcfSoPppIpcpOptionIssueFailures</b>	IPCP オプション ネゴシエーション エラー (IP アドレスのネゴシエーションなど) によって終了する、PCF 単位の PPP 接続の合計数を指定します。
<b>ccpCdmaExtPcfSoPppIpcpFailuresMaxRetrans</b>	再送信の最大数に達した後に IPCP フェーズで失敗する、PCF 単位の PPP 接続要求の合計数を指定します。
<b>ccpCdmaExtPcfSoPppIpcpFailuresUnknown</b>	不明な理由によって IPCP フェーズで失敗する、PCF 単位の PPP 接続要求の合計数を指定します。
<b>ccpCdmaExtPcfSoPppIpcpPhaseRxTermreqs</b>	IPCP フェーズ中に PPP が term 要求を受信したために終了する、PCF 単位の PPP ネゴシエーションの合計数を指定します。
<b>ccpCdmaExtPcfSoPppIpcpPcfA10Rls</b>	IPCP のネゴシエーション フェーズ中に PCF によって解放される A10 接続の合計数を指定します。
<b>ccpCdmaExtPcfSoPppIpcpIpResourceFail</b>	IP プールのアドレスの枯渇によって終了する、PCF 単位の PPP ネゴシエーションの合計数を指定します。
<b>ccpCdmaExtPcfSoPppRenegTotalReqs</b>	Cisco PDSN または MN によって再ネゴシエーションされる、PCF 単位の PPP の合計数を指定します。
<b>ccpCdmaExtPcfSoPppRenegByPdsnReqs</b>	Cisco PDSN によって開始される、PCF 単位の PPP 接続再ネゴシエーションの合計数を指定します。
<b>ccpCdmaExtPcfSoPppRenegByMobileReqs</b>	MN によって開始される、PCF 単位の PPP 接続再ネゴシエーションの合計数を指定します。
<b>ccpCdmaExtPcfSoPppRenegSuccesses</b>	アクティブな状態へ正常に移行した、PCF 単位の PPP 再ネゴシエーションの合計数を指定します。
<b>ccpCdmaExtPcfSoPppRenegFailures</b>	Cisco PDSN で失敗した、PCF 単位の PPP 再ネゴシエーションの合計数を指定します。
<b>ccpCdmaExtPcfSoPppRenegConnectionsAborted</b>	MN の電源が切られるなどの理由によって中断された、PCF 単位の PPP 再ネゴシエーションの合計数を指定します。
<b>ccpCdmaExtPcfSoPppRenegAddrMismatchReqs</b>	IP アドレスの不一致によって再ネゴシエーションされる、PCF 単位の PPP 接続の合計数を指定します。
<b>ccpCdmaExtPcfSoPppRenegAccessNetworkIdChanges</b>	セッションのハンドオフ中に Access-Network Identification (ANID) の変更によって再ネゴシエーションされる、PCF 単位の PPP 接続の合計数を指定します。
<b>ccpCdmaExtPcfSoPppRenegGreChangeReqs</b>	GRE キーによって MN から受信した要求が変更されたために再ネゴシエーションされる、PCF 単位の PPP 接続の合計数を指定します。

表 8 Cisco PDSN リリース 5.1 の PCF 単位の新しい MIB オブジェクト (続き)

<b>ccpCdmaExtPcfSoPppRenegOtherReasonReqs</b>	IP アドレスの不一致以外の理由によって再ネゴシエーションされる、PCF 単位の PPP 接続の合計数を指定します。
<b>cCdmaClusterRole</b>	Cisco PDSN が controller-member 内で仮定するロールを指定します。 クラスタの種類： <ul style="list-style-type: none"> <li>• <b>notApply</b> は、Cisco PDSN がクラスタ ロールを仮定していないことを示します。 <b>cCdmaClusterType</b> が controller-member ではない場合、Cisco PDSN ではクラスタ ロールを仮定します。</li> <li>• <b>controller</b> は、Cisco PDSN がクラスタのコントローラであることを示します。</li> <li>• <b>member</b> は、Cisco PDSN がクラスタのメンバであることを示します。</li> <li>• <b>collocated</b> は、Cisco PDSN がクラスタのコントローラとメンバの両方であることを示します。</li> </ul>

表 9 は、Cisco PDSN リリース 5.1 の新しい VPDN MIB オブジェクトのリストです。

表 9 Cisco PDSN リリース 5.1 の新しい VPDN MIB オブジェクト

オブジェクト	説明
<b>cvpdnSystemInitialConnReq</b>	このトンネルのすべての VPDN トンネルで試行された接続の合計数を指定します。
<b>cvpdnSystemSuccessConnReq</b>	このトンネルのすべての VPDN トンネルで試行され、成功した接続の合計数を指定します。
<b>cvpdnSystemFailedConnReq</b>	このトンネルのすべての VPDN トンネルで試行され、失敗した接続の合計数を指定します。

## 一般的な NAI のサポート

Cisco PDSN リリース 5.1 で導入された一般的な NAI 機能では、外部エンティティとのすべてのやり取りでグローバル NAI および Calling Station Identification (CLID) が必要です。また、エンティティ (Foreign Agent) 内のローカル識別子 (ローカル NAI) として CLID が必要です。

冗長セットアップの場合、このアトリビュートは、アクティブ モードとスタンバイ モードの両方でフローごとにスタンバイ モードと同期されます。このアトリビュートは、他のフローアトリビュートと共にスタンバイ モードと同期されます。この機能をイネーブルにするために、次の CLI コマンドが使用されます。

```
router(config)# ip mobile foreign-agent mn-identifier calling-station-id
```

設定を削除するには、次のように記述します。

```
router(config)# no ip mobile foreign-agent mn-identifier calling-station-id
```

次の CLI コマンドも設定します。

MIP RRQ で 3GPP2 CLID NVSE を送信する場合 :

```
router(config)# [no] cdma pdsn attribute send al mip-rrq
```

MIP RRQ で CT CLID NVSE を送信する場合 :

```
Router(config)# [no] cdma pdsn attribute vendor 20942 send al mip rrq
```

FA-CHAP で CLID VSA を送信する場合 :

```
Router(config)# [no] cdma pdsn attribute send al fa-chap
```



(注) セッションがない場合にだけ、このコマンドを設定してください。

## 最新の IS-835 に合わせたプロキシ MIP の変更

プロキシ MIP は IS-835 機能に合わせて変わります。IS-835 は Cisco PDSN リリース 5.1 で導入された機能で、「*Network PMIP Support for PMIPv4*」という 3GPP2 X.S0061-0 Version 1.0 のドラフトバージョンをサポートしています。

PMIP のさまざまな機能を示すために AAA サーバ レベルで使用される PMIP 関連のアトリビュートは次のとおりです。

- 「network-PMIP-NAI アトリビュート」
- 「PMIP ベースのモビリティ機能アトリビュート」
- 「PMIP-HA-Info-IPv4-Service アトリビュート」

### network-PMIP-NAI アトリビュート

network-PMIP-NAI VSA には、アクセス ゲートウェイ (AGW) および HA 間のネットワーク PMIP バインディングのために AGW が使用する NAI を指定します。AGW がネットワーク PMIP をサポートし、ネットワーク PMIP ベースのモビリティについて AT が認可されている場合、network-PMIP-NAI アトリビュートは RADIUS access-accept メッセージに含まれます。



(注) network-PMIP NAI アトリビュートを AAA サーバから受信するのは、access-reply メッセージだけです。また、このアトリビュートは、PMIP コールのモバイル ノードの場合に NAI を指定し、NAI として使用されます。

Cisco PDSN がこのアトリビュートを受け入れるのは、CLI からの PMIP ベースのモビリティ機能コマンド **cdma pdsn attribute send 3gpp2 pmip-indicator auth-req** をイネーブルにした場合だけです。それ以外の場合、コールは拒否されます。

### PMIP ベースのモビリティ機能アトリビュート

PMIP ベースのモビリティ機能の VSA は、AGW が AAA サーバに対するネットワーク PMIP をサポートすることを示します。新しい PMIP ベースのモビリティ機能 CLI コマンド **cdma pdsn attribute send 3gpp2 pmip-indicator auth-req** は、Cisco PDSN リリース 5.1 で導入されました。

PMIP ベースのモビリティ機能アトリビュートは、AGW がネットワーク PMIP をサポートしている場合に、AGW から HAAA に送信される RADIUS access-request メッセージに含まれます。Cisco PDSN は、access-request メッセージを使用して RADIUS 経由で AAA サーバにこのアトリビュートを送信す

ることで、Cisco PDSN が PMIP をサポートすること、および PMIP がイネーブルであることを AAA サーバに対して示します。PMIP ベースのモビリティ機能アトリビュートがない場合、Cisco PDSN が PMIP をサポートしないことを示します。

access-request メッセージを送信するとき、Cisco PDSN では CLI コマンド **cdma pdsn attribute send 3gpp2 pmip-indicator auth-req** がイネーブルかどうかチェックされます。CLI コマンドがイネーブルで、さらに FA サービスがイネーブルの場合、値 1 (PMIP4 のサポートを示します) の PMIP ベースのモビリティ機能は、access-request メッセージで AAA サーバに送信されます。



(注)

- アトリビュートを確実に転送するために、**cdma pdsn attribute send 3gpp2 pmip-indicator auth-req** CLI コマンドをイネーブルにする必要があります。
- FA サービスがディセーブルの場合、CLI コマンドがイネーブルでもこのアトリビュートは送信されません。

Cisco PDSN は、値 1 (PMIP4 のサポートを示します) の PMIP ベースのモビリティ機能アトリビュートの送信だけをサポートします。

AAA サーバは PMIPv4 と PMIPv6 の両方をサポートします。AAA サーバは Cisco PDSN に対する access-reply で、値 1 (PMIPv4 をサポートします)、2 (PMIPv6 をサポートします)、または 3 (両方をサポートします) を指定して、このアトリビュートを送信できます。AAA サーバは PMIPv4 および PMIPv6 をサポートしているため、Cisco PDSN も PMIPv4 によるコールの確立をサポートします。

AAA サーバから送信される access-reply メッセージに、PMIP ベースのモビリティ機能アトリビュートが含まれる場合、Cisco PDSN はその値を検証します。アトリビュートの値は常に 1 (PMIP4 のサポート) または 3 (PMIP4 および PMIP6 両方のサポート) です。それ以外の場合、Cisco PDSN はコールを拒否します。

AAA サーバからの access-accept メッセージで PMIP ベースのモビリティ機能アトリビュートと共にカスタマー固有の PMIP インジケータを受信する場合、PMIP ベースのモビリティ機能アトリビュートの方が優先されます。

## PMIP-HA-Info-IPv4-Service アトリビュート

PMIP-HA-Info-IPv4-Service VSA は、IPv4 サービスに使用されるネットワーク PMIP4 HA または PMIP6 Local Mobility Anchor (LMA) 関連の情報を指定します。この VSA は、AGW または Visiting AAA (VAAA) サーバから Home AAA (HAAA) サーバに対して送信される RADIUS access-request メッセージに含まれます。また、HAAA サーバから VAAA または AGW に対して送信される RADIUS access-accept メッセージにも含まれます。



(注)

Cisco PDSN は、HAAA 割り当ておよび VAAA 割り当ての HA IP アドレスのどちらも受信し、HAAA 割り当ての HA IP アドレスを優先します。

このアトリビュートを AAA サーバから受信するのは、access-reply メッセージだけです。



(注)

Cisco PDSN がこのアトリビュートを受け入れるのは、PMIP ベースのモビリティ機能 CLI コマンド (**cdma pdsn attribute send 3gpp2 pmip-indicator auth-req**) をイネーブルにした場合だけです。それ以外の場合、コールは拒否されます。

このアトリビュートには次のサブタイプがあります。

- VAAA-Assigned-HA-IPv4-Service

- HAAA-Assigned-HA-IPv4-Service
- PMN-HA Key
- PMN-HA-SPI



(注) Security Parameter Index (SPI; セキュリティ パラメータ インデックス) キーの Cisco のペアが、PMN HA キーおよび SPI を含むこのアトリビュートと共に受信されると、PMN キーおよび SPI が優先されます。

- VAAA-Assigned-LMA-IPv4-Service
- HAAA-Assigned-LMA-IPv4-Service

AAA サーバからこのアトリビュートを受信すると、サブタイプの有無が検証され、サブタイプ値が取得されます。



(注) Cisco PDSN は次のサブタイプ 5 および 6 をサポートしません。

- VAAA-Assigned-LMA-IPv4-Service
- HAAA-Assigned-LMA-IPv4-Service

また、Cisco PDSN は、このアトリビュートを access-request で HAAA または VAAA に送信することはサポートしていません。

## 簡易 IPv6 サポート

Cisco PDSN は Cisco PDSN 5.0 よりも前のリリースで IPv6 をサポートしていましたが、Cisco PDSN リリース 5.1 では、IPv6 のサポートを単一 IP アーキテクチャまで拡張しました。

Cisco PDSN は、簡易 IP アドレスを持つワイヤレス MS の PPP 終端地点です。現在、MS は IPv4 をサポートし、IPv6 のサポートまで拡張されました。MS は、ネットワークの簡易 IP サービスにアクセスする際に、IPv4、IPv6、または両方を同時に選択できます。Cisco PDSN は簡易 IPv6 アクセスおよび既存の簡易 IPv4 アクセスをサポートしています。

## Access-Request アトリビュート

Cisco PDSN は、必要に応じて、CLI コマンドを設定して AAA サーバの認可要求でアトリビュートを送信します。Cisco PDSN リリース 5.1 では、AAA サーバの access-request で他の既存のアトリビュートをオプションで送信します。これらのオプションは、前払いオンライン access-request および値が 0.0.0.0 の framed-IP で使用できます。

Cisco PDSN から access-request、fa-chap、または online-req を AAA サーバに送信すると、Cisco PDSN は各 CLI コマンドを確認し、それに従ってアトリビュートを更新します。

たとえば、**cdma pdsn attribute send d4 {auth-req | fa-chap | online-req}** がイネーブルの場合、D4 アトリビュートが他のアトリビュートと共に access-request メッセージで送信されます。

次のアトリビュートが AAA サーバの access-request で送信されます。

- 「Base Station Identifier (D4) アトリビュート」
- 「PCF IP Address (D3) アトリビュート」

- 「User Zone (E1) アトリビュート」
- 「NAS Port アトリビュート」
- 「Framed IP Address (B1) アトリビュート」

## Base Station Identifier (D4) アトリビュート

Base Station Identifier (BSID) アトリビュートは、SID (4 オクテット)、NID (4 オクテット)、およびセル識別子 (タイプ 2 の 4 オクテット) を組み合わせて構成される番号である BSID を表します。

access-request を送信すると、Cisco PDSN は必須の CLI コマンド **cdma pdsn attribute send d4 {auth-req | fa-chap | online-req}** がイネーブルかどうかを確認します。この CLI コマンドがイネーブルではない場合、このアトリビュートは authentication-request メッセージで AAA サーバに送信されません。同様に、BSID アトリビュートが前払いオンライン access-request メッセージのために追加されます。

## PCF IP Address (D3) アトリビュート

PCF IP Address アトリビュートは、サービス側 PCF (つまり、サービス側 RAN の PCF) の IP アドレスを表します。access-request メッセージを送信すると、Cisco PDSN は必須の CLI コマンド **cdma pdsn attribute send d3 {auth-req | fa-chap | online-req}** がイネーブルかどうかを確認します。イネーブルの場合、Cisco PDSN から AAA サーバに対して、PCF IP アドレスに設定した PCF IP Address アトリビュートを authentication-request メッセージで送信します。同様に、PCF IP Address アトリビュートが前払いオンライン access-request メッセージのために追加されます。この CLI コマンドがイネーブルではない場合、このアトリビュートは authentication-request メッセージで AAA サーバに送信されません。

## User Zone (E1) アトリビュート

User Zone アトリビュートは、階層的なサービス ユーザゾーンを表します。access-request メッセージを送信すると、Cisco PDSN は必須の CLI コマンド **cdma pdsn attribute send e1 {auth-req | fa-chap | online-req}** がイネーブルかどうかを確認します。イネーブルの場合、Cisco PDSN から AAA サーバに対して、User Zone アトリビュートを authentication-request メッセージで送信します。このアトリビュートは、前払いオンライン access-request とほぼ同じ方法で追加されます。この CLI コマンドがイネーブルではない場合、このアトリビュートは authentication-request メッセージで AAA サーバに送信されません。

## NAS Port アトリビュート

NAS Port アトリビュートは、NAS ポート ID を表します。access-request メッセージを送信すると、Cisco PDSN は必須の CLI コマンドがイネーブルかどうかを確認します。イネーブルの場合、Cisco PDSN から AAA サーバに対して、NAS ポート ID に設定した NAS Port アトリビュートを authentication-request メッセージで送信します。前払いオンライン access-request メッセージの場合、このアトリビュートはデフォルトで送信されます。CLI コマンド **cdma pdsn attribute send nas-port include-in-authen-req** がディセーブルの場合、このアトリビュートは AAA サーバに対する authentication-request メッセージで送信されません。



## Framed IP Address (B1) アトリビュート

Framed IP Address アトリビュートは、MS の IP アドレスを表します。access-request メッセージを送信するとき、Cisco PDSN では必須の CLI コマンド **cdma pdsn attribute send b1 auth-req** がイネーブルかどうかチェックされます。イネーブルの場合、Cisco PDSN から AAA サーバに対して、0.0.0.0 に設定した Framed IP Address アトリビュートを authentication-request メッセージで送信します。前払いオンライン access-request メッセージの場合、このアトリビュートはデフォルトで送信されます。この CLI コマンドがディセーブルの場合、このアトリビュートは authentication-request メッセージで AAA サーバに送信されません。



(注)

- 新しい CLI コマンド **cdma pdsn attribute send b1 auth-req** を使用するには、RADIUS アトリビュート CLI コマンド **radius-server attribute 8 include-in-access-req** をディセーブルにします。
- MIP コールの場合に Framed IP Address (0.0.0.0) を FA-CHAP 要求で送信するには、CLI コマンド **ip mobile foreign-agent send-mn-address** を使用します。

CLI コマンド **cdma pdsn attribute send b1 auth-req** を設定するには、あらかじめ CLI コマンド **ip mobile foreign-agent send-mn-address** を設定しておく必要があります。**ip mobile foreign-agent send-mn-address** CLI コマンドが未設定の場合、**cdma pdsn attribute send b1 auth-req** を設定できません。

同様に、CLI コマンド **ip mobile foreign-agent send-mn-address** および **cdma pdsn attribute send b1 auth-req** の両方がイネーブルの場合、CLI コマンド **ip mobile foreign-agent send-mn-address** をディセーブルにするには、先に **cdma pdsn attribute send b1 auth-req** CLI コマンドをディセーブルにします。

## 新しい PCF カウンタ単位の PPP

Cisco PDSN は PPP 関連のエラーおよび成功のグローバルな統計情報をサポートしています。Cisco PDSN リリース 5.1 から、PCF 単位の PPP エラーの統計情報をサポートするようになりました。

次の PPP エラーの統計情報が PCF 単位で追加されます。

- 「LCP フェーズ障害カウンタ」
- 「認証フェーズ障害カウンタ」
- 「IPCP フェーズ障害カウンタ」

## LCP フェーズ障害カウンタ

表 10 は LCP フェーズ障害カウンタのリストです。

表 10 LCP フェーズ障害カウンタ

障害カウンタ	説明
LCP Timeout(MaxRetry)	システムが最後に再起動してから、再送信の最大数に達した後に LCP フェーズで失敗した PPP 接続要求の合計数。CLI コマンド <b>cdma pdsn mib ignore mn-failures no-lcp-confreq</b> を Cisco PDSN で設定すると、maxretry カウンタは増加しません。

表 10 LCP フェーズ障害カウンタ (続き)

<b>MS Term-Req in LCP Phase (LCP Term Req during LCP nego rcvd)</b>	システムが最後に再起動してから、LCP のネゴシエーション中に MN から受信した LCP term 要求の合計数。
<b>A11 De-Registration in LCP Phase(A10 release during LCP nego by PCF)</b>	システムが最後に再起動してから、PCF による LCP のネゴシエーション中に解放された A10 の合計数。
<b>LCP Negotiation Fail (Failure Reasons Options)</b>	LCP フェーズのオプションのために発生した PPP エラーの合計数。
<b>Other Failures in LCP Phase(Unknown)</b>	システムが最後に再起動してから、不明な理由のために LCP フェーズで失敗した PPP 接続要求の合計数。

## 認証フェーズ障害カウンタ

表 11 は認証フェーズ障害カウンタのリストです。

表 11 認証フェーズ障害カウンタ

障害カウンタ	説明
<b>Username/Password Mis-Match(Auth failure)</b>	システムが最後に再起動してから、ユーザ名またはパスワードが一致しないために発生した認証エラーの合計数。
<b>AAA Timeout(AAA Timeouts)</b>	AAA のタイムアウトのために発生した PPP 認証エラーの合計数。
<b>Timeout in Authentication Phase(Auth timeouts)</b>	認証のタイムアウトのために発生した PPP 認証エラーの合計数。
<b>MS Term-Req in Authentication Phase(LCP Term Req during Auth nego rcvd)</b>	システムが最後に再起動してから、IPCP のネゴシエーション中に MN から受信した LCP term 要求の合計数。
<b>A11 De-Registration in Authentication Phase(A10 release during Auth nego by PCF)</b>	システムが最後に再起動してから、PCF による認証のネゴシエーション中に解放された A10 の合計数。
<b>Other Failures in Authentication Phase(Unknown):</b>	システムが最後に再起動してから、不明な理由のために認証フェーズで失敗した PPP 接続要求の合計数。

## IPCP フェーズ障害カウンタ

表 12 は IPCP フェーズ障害カウンタのリストです。

表 12 IPCP フェーズ障害カウンタ

障害カウンタ	説明
<b>IPCP Timeout(MaxRetry)</b>	システムが最後に再起動してから、再送信試行の最大数に達した後に IPCP フェーズで失敗した PPP 接続要求の合計数。
<b>MS Term-Req in IPCP Phase(LCP Term Req during IPCP nego rcvd)</b>	システムが最後に再起動してから、認証のネゴシエーション中に MN から受信した LCP term 要求の合計数。
<b>A11 De-Registration in IPCP Phase(A10 release during IPCP nego by PCF)</b>	システムが最後に再起動してから、PCF による IPCP のネゴシエーション中に解放された A10 の合計数。
<b>IPCP Negotiation Fail( Failure Reasons Options)</b>	オプションによる PPP IPCP エラーの合計数。
<b>Not enough IP resource for allocation(Not enough IP resource for allocation)</b>	IP プールに不適切な IP リソースが割り当てられたために終了した PPP ネゴシエーションの合計数。IP プールは AAA サーバまたはローカルからダウンロードされます。  ローカル IP プールを設定するか、Cisco PDSN のローカル IP プールが誤っている場合、このカウンタは増加しませんが、グローバル カウンタは増加します。  以前のリリースでは、リモート IP プールが Cisco PDSN で設定される場合、Unknown カウンタとこのカウンタが増加しました。ただし、Cisco PDSN リリース 5.1 では、Unknown カウンタとこのカウンタは増加しません。
<b>Other Failures in IPCP Phase (Unknown)</b>	システムが最後に再起動してから、不明な理由のために IPCP フェーズで失敗した PPP 接続要求の合計数。

## VPDN 条件付きデバッグ

条件付きデバッグ機能を使用すると、特定セッションのデバッグを検証または観察できます。IMSI またはユーザ名に応じて条件付きデバッグをイネーブルにするには、次の CLI コマンドを使用します。

```
PDSN# debug condition ?
called          called number
calling         calling -----> for IMSI
glbp           interface group
interface      interface
ip             IP address
mac-address    MAC address
match-list     apply the match-list
standby        interface group
username       username -----> for username
vcid           VC ID
voice-port     voice-port number
xconnect       Xconnect conditional debugging on segment pair
```

Cisco PDSN リリース 5.1 では、VPDN コールの場合に条件付きデバッグがイネーブルにされます。IMSI-based (ステーション ID の呼び出し) 条件付きデバッグをイネーブルにする場合、セッションの IMSI が、条件付きデバッグ CLI コマンドで設定した IMSI と一致するかどうかを検証する必要があります。一致が存在する場合、VPDN コンテキスト デバッグ フラグが設定されます。一致が存在しない場合、VPDN コンテキストのデバッグ フラグは設定されません。その結果、他のセッションでデバッグの出力は行われません。IMSI ベースのデバッグがイネーブルの場合、IMSI がデバッグ メッセージに追加されます。ユーザ名が条件の場合にも同様です。ユーザ名と IMSI ベースの条件付きデバッグのどちらもセッションでイネーブルにしている場合、IMSI の方が優先して L2TP および VPDN コール イベント デバッグ メッセージで表示されます。

次のコマンドは、L2TP および VPDN コール イベント デバッグの一部として条件を示します。VPDN セッションでユーザ名または IMSI の条件付きデバッグがイネーブルの場合、条件付きデバッグ CLI コマンドで設定されます。

```
lac(config)# vpdn debug ?
    show-conditions  Show Conditions (IMSI/Username) with debug messages
lac(config)# vpdn debug show-conditions ?
```

## Revocation メッセージの GRE CVSE および MN NAI 拡張

Cisco PDSN リリース 5.1 は CDMA 標準 3GPP2 X.S0011-003-D に準拠しています。Cisco PDSN では、CDMA 標準 (3GPP2 X.S0011-003-D) に従って、Revocation メッセージでネゴシエーション済みの GRE カプセル化および GRE キーを送信し、すべての Revocation メッセージで MN-NAI 拡張を送信します。

GRE CVSE および MN NAI 拡張を Revocation メッセージで送信するための条件は次のとおりです。

- GRE CVSE を FA および HA 間でネゴシエーションする場合、FA の割り当てキーを含む GRE CVSE を Revocation メッセージに含める必要があります。
- FA が GRE CVSE および HA の割り当てキーと共に Revocation メッセージを受信した場合、FA から HA に対して、FA の割り当てキーとして GRE CVSE を指定した Revocation の ACK メッセージを送信する必要があります。
- Revocation メッセージまたは Revocation の ACK メッセージに GRE CVSE がある場合、FA-HA 認証拡張の前に GRE CVSE を含める必要があります。
- CLI コマンド `ip mobile foreign-service revocation exclude-nai` をディセーブルにして、MN NAI 拡張を Revocation メッセージに含める必要があります。
- FA が HA から MN NAI 拡張を含む Revocation メッセージを受信した場合、FA は HA に Revocation の ACK メッセージを送信するときに MN NAI 拡張を含める必要があります。
- Revocation メッセージまたは Revocation の ACK メッセージに MN NAI 拡張がある場合、FA-HA 認証拡張の前に MN NAI 拡張を含める必要があります。

## ブレード単位の単一 IP

ここでは、Service Provider PDSN ゲートウェイ アプリケーションのための、単一 IP インフラストラクチャおよび管理性の要件に関連する概念について説明します。このアプリケーションは Cisco 7600 シリーズ ルータの SAMI サービス ブレードに搭載され、Mobile Internet 製品ファミリに含まれています。ここでは、この機能を設定する方法の詳細についても説明します。

このセクションの内容は、次のとおりです。

- 「単一 IP 機能の概要」
- 「単一 IP インターフェイス」

- 「MIP、簡易 IP、VPDN ベースのコール、または A11 レジストレーション用の単一インターフェイス」
- 「設定用の単一インターフェイス」
- 「SNMP 管理用の単一インターフェイス」
- 「トラブルシューティングおよびデバッグのための単一インターフェイス」
- 「AAA 用の単一インターフェイス」
- 「フェールオーバー用の単一インターフェイス」
- 「操作と管理」
  - 「Chassis-Wide MIB for Application-Related Parameters」
  - 「AAA 非応答に対するトラップ生成」
  - 「Show Subscriber」
  - 「シャーシ内設定の同期」
  - 「設定の詳細」
  - 「Monitor Subscriber」
  - 「Show Subscriber Session」
  - 「バルク統計情報の収集」
- 「Cisco PDSN リリース 5.0 の冗長性のサポート」
- 「パフォーマンス要件」
- 「単一 IP のサポート - 再利用および新規の CLI コマンド」
- 「単一 IP PDSN での分散設定、show、および debug コマンド」
- 「サポートされない機能」

## 単一 IP 機能の概要

現在の SAMI 上の Mobile Internet ゲートウェイ ソリューション (WiMax ASNGW、GGSN、および HA を除く PDSN) は、いずれも multiple-routers-on-a-stick モデルを提供しています。このモデルには担当者の管理性と操作の問題があります。PDSN 単一 IP のシステム設計を使用すると、ブレード単位で SAMI 上のゲートウェイを管理できます。その結果、1 ブレードあたり 6 個のプロセッサという以前の提示に比べ、操作の複雑さが 1/6 に減ります。

シャーシ単位モデルの場合に提供される機能の一部を次に示します。ブレード単位モデルの提示は次の領域に適用されます。

- AAA の対話
- MIB 取得のために SNMP を介したネットワーク管理の対話
- 設定、表示、およびデバッグ機能
- ブレードのエラー検出およびフェールオーバー
- AAA サーバの応答時間の決定およびアラームの表示

さらに、シャーシ単位モデルの提示は、次の対象機能に適用されます。

- 多様な出力フィルタリング機能で、シャーシ全体に存在する加入者を表示します。
- シャーシ全体の 1 人または複数の加入者のセッション アクティビティを表示します。

- トラブルシューティングの目的で、1人または複数の加入者について、加入者を監視します（呼トレース）。
- シャーシのバルク統計情報の照合、転送、および保存。

## 単一 IP インターフェイス

次の機能は、ブレード単位の単一 IP で管理できます。

- 「MIP、簡易 IP、VPDN ベースのコール、または A11 レジストレーション用の単一インターフェイス」
- 「設定用の単一インターフェイス」
- 「SNMP 管理用の単一インターフェイス」
- 「トラブルシューティングおよびデバッグのための単一インターフェイス」
- 「AAA 用の単一インターフェイス」
- 「フェールオーバー用の単一インターフェイス」

## MIP、簡易 IP、VPDN ベースのコール、または A11 レジストレーション用の単一インターフェイス

サービス ブレードは、A11 レジストレーション要求に対して 1 つの IP アドレスを提示します。この IP アドレスは、ブレードのすべてのプロセッサで共通です。vaccess インターフェイスの IP アドレスも、ブレード内のすべてのプロセッサで共通です。そのため、ブレードは単一の IP コールに対して 1 つの IP アドレスを提示します。同様に、サービス ブレードは、簡易 IPv6 を含む各サービスに対して、個別の IP アドレス（PDSN IP アドレス）を提示します。これらのアドレスの設定は Cisco PDSN リリース 4.0 で導入されましたが、設定できるのはブレードの 1 プロセッサだけでした。IP アドレスの設定は、コントロールプレーンおよびトラフィック プレーン プロセッサの両方に存在します。

サービス ブレードは、IXP ucode でパケット配信機能を実装します。それによって、ユーザ トラフィック パケットが適切なトラフィック プレーン プロセッサに送信されます。コントロールプレーン トラフィックと識別されるパケット（A11 パケット、接続解除 POD パケットのパケット、MIP レジストレーションの失効パケットなど）は、コントロールプレーン プロセッサに送信されます。その他のコントロールプレーン パケット（PPP ネゴシエーション、AAA 認証、アカウントリング、MIP など）は、適切なトラフィック プレーン プロセッサに送信されます。特定の ID に一致しないパケットは、コントロールプレーン プロセッサに送信されて処理されます。

## 設定用の単一インターフェイス

サービス ブレードには、ブレード機能を設定できる単一のポイントが用意されます。つまり、Cisco PDSN リリース 4.0 と同様に、サービス ブレードに対するセッションを確立できます。サービス ブレード上のコントロール プロセッサに対してセッションが確立されます。サービス ブレードに対する単一セッションから、各コマンドで 1 つの機能のために要求した PDSN 機能を設定できます。この設定は、同じ設定を必要とするすべてのプロセッサに伝播されます。追加の設定は必要ありません。

IOS 設定コマンドのデフォルトの処理は、サービス ブレード上のすべての IOS プロセッサで設定が有効になることです。設定セッションをホストするプロセッサでだけ実行するコマンドセットを定義することもできます。フィルタ処理された設定コマンドには、たとえば、上記のいずれかに関するインターフェイス設定モードの OSPF、SNMP、HSRP、BGP、Eigrp、CDP、およびサブコマンドに関連するコマンドがあります。

## SNMP 管理用の単一インターフェイス

サービスブレードには、SNMP 操作の対象アドレスである個別の設定可能な IP アドレスが用意されています。この IP アドレスはコントロールプレーンプロセッサでホストされます。PDSN 機能に関連するサービスブレード上のすべての MIB には、この IP アドレスを介してアクセスできます。コントロールプレーンプロセッサ以外のプロセッサから要求された情報は、MIB ターゲットに応じて、プッシュまたはプルされます。

プロセッサ単位で情報を提示するプロセッサリソースの使用状況およびメモリの使用状況に関連する MIB は 2 つあります。6 個の個別エントリ (1 プロセッサあたり 1 個) で返される単一のプロセッサリソース MIB の結果があります。メモリの使用状況の場合も同様です。

## トラブルシューティングおよびデバッグのための単一インターフェイス

サービスブレードには、**show** コマンドおよび **debug** コマンドを実行する単一のエントリポイント (コントロールプレーンプロセッサへのセッション) が用意されています。デフォルトで、**show** コマンドはコントロールプレーンプロセッサでだけ実行されます。1 つまたは複数のトラフィックプレーンプロセッサで実行する必要がある各コマンドは個別に実行されます。

**debug** コマンドの場合、PDSN でも単一 IP の HA モデルに従います。トラフィックプレーンプロセッサからの追加情報を必要とし、ユーザ (NAI または IP アドレス) 単位で承認されるコマンドの場合、そのユーザをホストするトラフィックプレーンプロセッサが識別され、そのプロセッサでコマンドが実行されます。

多様なプロセッサの結果が単一の提示に組み合わされてから、コマンドに対する応答が提供されます。

条件付きデバッグコマンドも同様のアプローチを使用します。PDSN でも、HA 用に Osler が提案するモデルに従います。

## AAA 用の単一インターフェイス

サービスブレードは、AAA の対話用に単一の IP アドレスを提示します。この IP アドレスは、RADIUS ベースの対話の両方で 1 つのアドレスの場合と、プロトコルごとに個別の IP アドレス設定の場合があります。

RADIUS ベースの認証および認可は、トラフィックプレーンプロセッサから実行されます。

サービスブレードパケットの配信機能は、宛先 UDP ポートに応じて、RADIUS トラフィックを特定のプロセッサに配信します。

## フェールオーバー用の単一インターフェイス

現在の SAMI 障害モードは、可能な限り、プロセッサ単位の障害用です。単一 IP モデルの場合、ブレードで障害が検出されると、プロセッサレベルのフェールオーバーで十分な場合でも、ブレードレベルのフェールオーバーになります。この機能は、HA の単一 IP の場合と同様です。

## 操作と管理

ここでは、操作と管理に分類される機能について説明し、次の内容についても説明します。

- [「Chassis-Wide MIB for Application-Related Parameters」](#)
- [「AAA Responsiveness Test Tool およびトラップ」](#)
- [「AAA 非応答に対するトラップ生成」](#)

- 「[Show Subscriber](#)」
- 「[シャーシ内設定の同期](#)」
- 「[Monitor Subscriber](#)」
- 「[Show Subscriber Session](#)」
- 「[バルク統計情報の収集](#)」

## Chassis-Wide MIB for Application-Related Parameters

この機能には、すべてのアプリケーション関連パラメータがシャーシ全体でレポートされる単一の MIB が用意されています。PDSN の場合、この機能は PDSN インスタンス ベースで提供されます。

単一サービス ブレード上のすべての PDSN インスタンスでは、単一 IP アドレスに対する SNMP の Get によってこの情報を入手できます。この情報は、CISCO-PDSN-MIB、CISCO-CDMA-PDSN-EXT-MIB、および CISCO-IP-LOCAL-POOL-MIB で使用できます。PDSN インスタンスごとに MIB を取得するために必要な数の SNMP GET 操作を実行するのは、SNMP マネージャの役割です。今回のリリースの単一 IP PDSN 機能は、サービス ブレードごとに 1 つの PDSN インスタンスをサポートしているため、サービス ブレードごとの Get 操作の数が 12 から 2 に減ります。

## AAA Responsiveness Test Tool およびトラップ

この機能には 2 つの側面があります。

- ローカルで開始された AAA 認証によるバインディングを使用した、AAA サーバの可用性を手動で検証する。
- SNMP トラップに基づいて、通常操作中にサーバが応答しないことを表示する。

### AAA Responsiveness Test Tool

今回のリリースでは、AAA Responsiveness Test Tool をサポートしていません。

### AAA 非応答に対するトラップ生成

「[AAA サーバ非応答に対するトラップ生成](#)」を参照してください。

## Show Subscriber

この機能は、シャーシの単一ポイントから、シャーシの PDSN インスタンスがホストする加入者のリストを表示します。今回のリリースでは、サービス ブレード単位で単一の PDSN インスタンスをサポートします。そのため、必要な手順は、サービス ブレードの 1 つまたはすべてに対して IOS CLI コマンドを使用することで、目的の情報を要求することに限定されます。



表 13 は機能のリストです。

表 13 Show Subscriber 機能のリスト

All	シャーンに登録されている全ユーザの要約。	シャーンに登録されている全ユーザの合計数を表示するには、アクティブなサービスブレードごとに TCOP で <b>show cdma pdsn session {summary   brief   detail}</b> コマンドを使用します。各ブレードのユーザ数が合計され、結果が表示されます。  単一のコマンドで加入者の最大数を表示できます。値を 1000 に設定することをお勧めします。登録された加入者がこの値を超える場合、出力はファイルに保存され、ファイルの名前と場所が示されます。
Card	ある特定のカードまたはスロットに登録されている全ユーザの要約。	1 つのサービス ブレードに登録されている全ユーザの合計を表示するには、 <b>show cdma pdsn session {summary   brief   detail}</b> コマンドを使用します。このコマンドはサービス ブレードのコントロール プロセッサで実行され、目的の結果は <b>total</b> 行に示されます。
Member	ある特定のメンバ (CPU) に登録されている全ユーザの要約。	1 つのサービス ブレードの特定のトラフィック プロセッサに登録されている全ユーザの合計を表示するには、コマンドで指定される TCOP に加え、そのサービス ブレードで <b>show cdma pdsn session {summary   brief   detail}</b> コマンドを使用します。
Connect	接続時間が時間値 (AGE の使用) より高い、低い、または等値である全ユーザの要約。	加入者が最後に再登録した時間ではなく、最初に登録した時間を表示するには、次のコマンドを使用します。  <b>show cdma pdsn session lifetime age {lesser   greater   equals} [hh:mm:ss] {detail   brief   summary}</b>
FA-Chassis	PDSN の FA 上の全ビジターの要約。	シャーンの FA からサービスを提供されるビジターの合計数を表示するには、シャーンのサービス ブレードのすべての TCOP で <b>show cdma pdsn session visitor summary</b> コマンドを使用します。
FA-Member	PDSN 内のある特定の FA 上の全ユーザの要約。	サービス ブレードで FA からサービスを提供されるビジターの合計数を表示するには、必要なサービス ブレードで <b>show cdma pdsn session visitor summary</b> コマンドを使用します。
HA-User	特定の HA に登録されている全ユーザの要約。	HA に登録されているビジターの合計数を表示するには、すべての TCOP で <b>show ip mobile visitor ha-addr [ha-ip]</b> コマンドを使用します。

表 13 Show Subscriber 機能のリスト (続き)

Calltype	このコールタイプ (RTT、EVDO rev A、rev 0 など) に関する全ユーザの要約。	特定のコールタイプに関するビジターの合計数を表示するには、すべての TCOP で <b>show cdma pdsn session service-option [so]</b> コマンドを使用します。
NAI または User	この NAI に対するすべてのユーザの要約 (NAI ではワイルドカードをサポート)。たとえば、 <b>show user summary nai *ptt*</b> だと、ボックスの Push to Talk ユーザが検索されます。レルムによるフィルタもサポートされます。	NAI に対するビジターの合計数を表示するには、すべての TCOP で <b>show cdma pdsn session user [nai]</b> コマンドを使用します (正規表現をサポートする NAI 以外の既存の CLI コマンド)。
Address Range CLI	特定のアドレスレンジ内の全ユーザの要約。	特定のアドレスレンジに対するビジターの合計数を表示するには、すべての TCOP で <b>show cdma pdsn flow mn-ip-address range [startIP] [endIP] {brief   summary   detail}</b> コマンドを使用します。

使用できる出力表示フォーマットは次のとおりです。

- **Summary** - セッション、送受信バイト、送受信パケット、ACL による受け入れとドロップの合計数。
- **Brief** - コマンドフィルタに一致するユーザ別の 1 行の出力。出力は、割り当てられた IP アドレス、NAI、休止、および PCF アドレスで構成されます。
- **Verbose** - **show cdma pdsn session** コマンドの出力が提供する詳細な表示。

この機能は SNMP 経由ではサポートされません。

## シャーシ内設定の同期

この機能で自動同期をイネーブルにすることで、アクティブなブレードで実行された設定コマンドは、パートナーのスタンバイブレードで自動的に同期されます。アクティブまたはスタンバイのパートナーモデルの設定コマンド、PDSN の冗長性コマンド、および HSRP のスタンバイコマンドを冗長性のために障害検出モードとして設定する設定コマンドを除き、自動同期はすべてのコマンドに適用されます。

この機能はデフォルトでディセーブルです。設定モードで **auto-sync all** コマンドでイネーブルにできます。「write memory」は、スタンバイから復帰する前に実行する必要があります。



(注)

設定コマンドは、スタンバイの PDSN では実行できません。EXEC コマンドは許可されています。

アクティブまたはスタンバイの PDSN を判断する方法は、Stateful SwitchOver (SSO) のサポートに使用される Radio Frequency (RF; 無線周波数) インフラストラクチャだけでなく、多様な Mobile Severely Errored Frame (mSEF) ゲートウェイに対するセッション冗長性のサポートに基づきます。

## 初期化

SSO 設定の同期は、起動時に自動実行されます。事前の設定は必要ありません。同様の同期は PDSN に適用できません。冗長ユニット間の IP 接続は、RF ネゴシエーションの前に必要なためです。そのため、アクティブおよびスタンバイのブレードで、異なっても関連性がある設定が必要です。

さらに、SSO 設定の同期機能は、各冗長ユニットで固有の設定をサポートしていません。PDSN、HSRP、および RF では、Interdev プロトコルが必要です。そのいずれも、冗長ユニットで固有の設定が必要です。

各ユニットで固有の設定を必要とする既存のコマンドは、ピア ユニットの設定に合わせるために変更されます。新しいコマンドでピア スロットを識別します。これらのコマンドは解析され、設定の同期を自動的にトリガするために、RF ネゴシエーション状態 RF\_PROG\_STANDBY\_CONFIG が使用されます。新しいコマンドについては、「設定の詳細」を参照してください。

## RF Client

SSO 設定の同期の場合と同様に、PDSN 設定の同期も RF Client です。設定の同期機能によって、進行イベントおよび状態イベント用に RF を備えるコールバックが登録されます。RF は、イベントの進行および状態に従ってこれらの登録済みクライアントに通知するため、PDSN は設定ファイルを同期するときに把握できます。

## 設定ファイルと同期

設定の同期機能は、スタートアップ コンフィギュレーションと実行コンフィギュレーションのプロセスから構成されます。

スタートアップ コンフィギュレーションはテキスト ファイルとして NVRAM に保存されます。メモリへの書き込み、起動時にコピーなどの操作を実行すると、このファイルは同期されます。書き込み操作のためにファイルを開いている場合、ファイルを閉じた後に同期は開始されます。

実行コンフィギュレーションの同期は、特定の操作によって動的に生成されるため、同期を実行するときは常に、実行コンフィギュレーションを生成する必要があります。

SSO の実装では、同期プロセスが開始される前にプライマリがロックされます。スタートアップ コンフィギュレーションおよび実行コンフィギュレーションのバルク同期が実行され、次にパーサー モードの同期が実行されます。

両方のプロセスが同期され、プライマリのロックが解除されると、1 行ごとの同期が開始されます。

すべての同期プロセスには、冗長ユニット間で通信できる転送メカニズムが必要です。

PDSN の設定の同期機能では、次の転送メカニズムのいずれかを使用できます。

- CP-TP メッセージングに現在使用されている Reliable IPC メカニズム
- IPC メッセージング向けの RF または CF SCTP ベースのアプローチ
- IPC メッセージング向けの新しい SCTP ベースのアプローチ

1 つ目は、実装の観点からは最速のソリューションですが、シャーシ内ソリューションとしては拡張性が不十分です。今回のリリースでは、2 番目のオプション RF または CF SCTP をサポートしていません。

## バルク同期

バルク同期を開始する前に、2 つのユニット間で RF Interdev 通信を確立する必要があります。各ユニットがスタートアップ コンフィギュレーションを解析します。その結果、ユニットはアクティブまたはスタンバイ状態になります。起動後に、実行またはプライベート設定の変更がある場合、アクティブユニットはスタンバイに対して、実行およびプライベート設定ファイルのバルク同期を実行します。

バルク同期後に、スタンバイは自身をリロードし、変更された設定を反映します。このスタンバイのリロードフェーズ中に、アクティブ ユニットで設定操作は実行できません。

初期化中に同期される設定は次のとおりです。

- プライベート設定
- 実行コンフィギュレーション

SUP のスタートアップ コンフィギュレーション ファイルは常に同期状態なので、スタートアップ コンフィギュレーションは同期されません。

起動後にプライベート設定が変更された場合、アクティブ ユニットのプライベート設定ファイルをバッファにコピーし、RF Interdev SCTP を使用してそのファイルをスタンバイに送信します。

起動後に実行コンフィギュレーションが変更された場合、アクティブ ユニットのその実行コンフィギュレーション ファイルをバッファにコピーし、Interdev SCTP を使用してそのファイルをスタンバイに送信します。これらの手順に従って、アクティブ ユニットのメッセージをスタンバイに送信し、受信バッファの解析を始めます。

スタンバイ ユニットの受信バッファのコンテンツをローカルに保存し、自身をリロードして変更された設定を適用します。



(注)

NVRAM 設定ファイルには、パブリック設定ファイルとプライベート設定ファイルの 2 種類があります。プライベート設定ファイルはコンソールに表示できません。プライベート NVRAM 設定ファイルの使用例として、システムをリブートしても残る永続的な SNMP インターフェイス インデックスを保守して、合法的傍受のユーザ名とパスワードなどを保存する場合があります。

## 1 行ごとの同期

アクティブ ユニットのスタンバイ ユニットのどちらも起動し、実行中の場合、アクティブ ユニットのから入力された CLI コマンドが最初に実行され、そのコマンドはスタンバイに伝播して実行されます。スタンバイでの実行結果はアクティブ ユニットの返されます。

戻りコードが設定された各 CLI コマンドにすべてのパーサー アクション ルーチンを持たせるために、SSO 実装では Parser Return Code (PRC) スキームが使用されます。この戻りコードは、エラー コード、コンポーネント ID、同期ビット、サブコードなどのクラスの組み合わせです。

Parser Mode Synchronization は、同期のためにコマンドをスレーブに送信する前に、アクティブ ユニットのスタンバイ ユニットのと同じパーサー モードを維持します。

SSO 実装の場合、同期は RPC 経由で実行されます。それによって、アクティブ RP がスタンバイ RP から戻りコード メッセージを受信するまで、現在のプロセスはブロックされます。そのため、コマンドは両方のユニットのために実行されます。

スタンバイ ユニットのコマンドが失敗した場合、結果はアクティブ ユニットの返されます。アクティブ ユニットのポリシー メーカーのスタブ レジストリが呼び出され、発信側または上位レイヤに返された結果の処理方法に関する決定が委ねられます。

単一 IP PDSN 設定同期機能では、SSO の 1 行ごとの同期実装がそのまま使用されます。

## スタートアップ コンフィギュレーションの同期

SSO の実装では、バルク同期を実行できる RF 状態の場合、起動中にスタートアップ コンフィギュレーションが同期されます。スタートアップ コンフィギュレーションの同期を開始する前に、ルータをロックする必要があります。

**write memory** または **copy file1 startup-config** を実行される場合、このシナリオを処理する方法は 2 つあります。

- スタートアップ コンフィギュレーション ファイルをバルク同期します。
- EXEC コマンドの 1 行ごとの同期を実行します。

単一 IP PDSN の場合、スタートアップ コンフィギュレーション ファイルのバルク同期が使用されます。これは、アクティブ ユニットのスタンバイの場所に設定の変更を保存できるためです。

## 実行コンフィギュレーションの同期

実行コンフィギュレーションでは、冗長性ユニットが同じ状態の情報を保持しています。

初期状態では、セカンダリ ユニットが RF Interdev 通信を確立した後に、実行コンフィギュレーションファイルがバルク同期されます。起動前にアクティブ ユニットで実行コンフィギュレーションが変更された場合、バルク同期によってスタンバイ ユニットの自己リロードが実行されます。リロードすると、スタンバイ ユニットにはアクティブ ユニットの実行コンフィギュレーションが適用されます。

その後、1 行ごとの同期が 2 つのユニット間で実行されます。各コマンドを設定すると、プライマリでそのコマンドが実行された後に、同じコマンドがセカンダリ側に渡されます。

単一 IP PDSN 機能の場合、実行コンフィギュレーションのバルク同期は、RF Interdev SCTP を使用して実行されます。

## 制約事項

シャーシ内を設定する場合の制約事項は次のとおりです。

- スタンバイ ユニットで設定コマンドは使用できません。設定できるのはアクティブ ユニットだけで、アクティブ ユニットの設定でスタンバイ ユニットの設定が決まります。
- 初めて冗長性同期機能を設定する場合、冗長ユニットの 1 つだけがアップ状態です。他のユニットをアップ状態にする前に、必要な設定を行って、保存してください。こうすることで、初めての場でもスタンバイ ユニットで設定することを回避できます。
- スタンバイ ユニットで **write memory** コマンドは使用できません。
- 自動同期機能がイネーブルの場合、実行する必要がある CLI コマンドは **unit1-unit2 set** だけです。自動同期機能がイネーブルの場合、コマンドの **local-remote set** は使用できません。**local-remote** コマンドを使用できるのは、自動同期機能をディセーブルにした後だけです。

## 設定の詳細

設定は自動同期機能を使用して同期されるため、両方のユニットの CLI は常に同じです。この機能はデフォルトで無効に設定されています。現在、次のコマンドは各冗長ユニットに固有で、変更されました。

- **ipc zone default**
- **association no.**
- **protocol sctp**
- **unit1-port port1**
- **unit1-ip ip1**
- **unit2-port port2**
- **unit2-ip ip2**

次の新しいコマンドは、インターフェイス GigabitEthernet0/0.23 に導入されました。

```
redundancy ip address unit1 ip1 mask1 unit2 ip2 mask2
```

**redundancy ip address** コマンドはインターフェイス単位のコマンドです。HSRP プロトコルでは、ネゴシエーションのために設定されたこの IP アドレスが使用されます。通常の **ip address** コマンドを使用して設定されるアドレスは使用されません。HSRP とピアとのネゴシエーション専用のサブインターフェイスには、**ip address** 設定は必要ありません。

```
redundancy unit1 slot x unit2 slot y
```

**redundancy slot** コマンドはグローバル 設定で、ピア スロットの特定に使用されます。

シャーシ内設定の同期を設定するには、次のタスクを実行します。

```
redundancy unit1 slot x unit2 slot y
```

```
unit1-port portnum , unit2-port portnum
ipc-assoc-protocol-sctp モードで実行します。
```

```
unit1-ip address1 , unit2-ip address2
```

それぞれ、ipc-unit1-port モードおよび ipc-unit2-port モードで実行します。

```
redundancy ip address unit1 address1 mask1 unit2 address2 mask2
interface モードおよび sub-interface モードで実行します。
```

各カードで実行する必要がある一連の設定手順は次のとおりです。

コマンド	目的
<b>ステップ 1</b> Router# <code>show redundancy states</code>	冗長性コマンドを実行する前に、両方の SAMI で次のコマンドを実行します。 <b>my state</b> は両方のカードでアクティブにする必要があります。 <b>(注)</b> 1つのユニットの電源を切ります。設定は1つのユニットだけで実行する必要があります。
<b>ステップ 2</b> Router(config)# <code>auto-sync all</code>	シャーシ内設定の同期をイネーブルにします。
<b>ステップ 3</b> Router(config)# <code>redundancy unit1 slot 9 unit2 slot 6</code>	グローバルな冗長性ユニット-スロットのマッピングを設定します。
<b>ステップ 4</b> Router(config)# <code>redundancy unit1 hostname name1 unit2 hostname name2</code>	同じシャーシ内のピア スロット名を特定および設定します。
<b>ステップ 5</b> Router(config)# <code>interface GigabitEthernet0/0.2 encapsulation dot1Q 20 redundancy ip address unit1 4.0.0.1 255.255.255.0 unit2 4.0.0.2 255.255.255.0 standby 0 ip 4.0.0.4 standby 0 name hsrp</code>	HSRP のインターフェイスを設定します。 HSRP は、スタンバイ ユニットおよびアクティブ ユニットに一意的 IP を必要としているため、 <b>redundancy ip address</b> コマンドを使用する必要があります。 <b>(注)</b> このインターフェイスでは <b>ip address</b> コマンドを設定しないでください。
<b>ステップ 6</b> Router(config)# <code>ipc zone default</code> Router(config-ipczone)# <code>association 1</code> Router(config-ipczone-assoc)# <code>no shutdown</code> Router(config-ipc-protocol-sctp)# <code>protocol sctp</code> Router(config-ipc-protocol-sctp)# <code>unit2-port 5000</code> Router(config-ipc-unit2-sctp)# <code>unit2-ip 4.0.0.2</code> Router(config-ipc-protocol-sctp)# <code>unit1-port 5000</code> Router(config-ipc-unit1-sctp)# <code>unit1-ip 4.0.0.1</code>	RF Interdev のために IPC 情報を設定します。
<b>ステップ 7</b> Router(config)# <code>redundancy inter-device</code> Router(config-red-interdevice)# <code>scheme standby hsrp</code>	HSRP スキーム名を RF Interdev と関連付けます。

自動同期機能をイネーブルにしてセッションの冗長性を初めて設定する場合、1つのユニットだけを設定し、もう一方のユニットの電源は切る必要があります。

設定が完了したら、unit1 で **write memory** を実行してから、unit2 の電源を投入します。

## Monitor Subscriber

この機能を使用すると、シャーシの単一ポイントから、NAI または割り当て済みの IP アドレスに基づいて条件付きデバッグを確立できます。シャーシ内の PDSN インスタンスが加入者セッションをホストしているか、これは、セッションが確立していない場合は加入者セッションをホストするために選択されるかを知らなくても、この処理は可能です。この機能では、IOS コマンドを中央で実行できる Osler ツールを使用します。IOS コマンドには、応答を受信し、その応答をわかりやすく簡潔なフォーマットで提示する機能があります。

出力フォーマットは 2 つあります。**brief** はデバッグ出力が簡潔に提示され、**verbose** は詳細なデバッグ出力が提示されます。

7600 のスーパーバイザにログインしてから、コマンドのデバッグ条件の「qualifier」プロトコルを実行する必要があります。

次の 2 段階のプロセスを実装する必要があります。

1. セッションをホストするシャーシで PDSN インスタンスを決定します。
2. セッションが存在する場合、その PDSN インスタンスで **debug conditional** コマンドを適用してから、要求された特定の **debug** コマンドを適用します。セッションが存在しない場合、デバッグのためのトリガ前条件を確立してから、シャーシに設定されているすべての PDSN インスタンスで、要求された **debug** コマンドを実行します。

条件付きデバッグが適用されるプロトコルのサブシステムを指定することもできます。たとえば、**Session**、**Accounting**、**TFT**、**VPDN**、**MIP**、**PMIP**、**All** などがあります。

同時に実行できるトリガ前条件は 10 個までです。



(注)

PCOP 上のセッションマネージャは、加入者が存在する場合に加入者を特定するために使用されます。加入者が登録済みの場合、セッションマネージャの API は、検索に使用されます。検索は、IMSI、NAI、またはモバイル割り当ての IP アドレスに基づきます。

## Show Subscriber Session

7600 のスーパーバイザにログインし、**show subscriber session** コマンドを実行します。この subscriber は IMSI、NAI、または IP アドレスで識別されます。

次の 2 段階のプロセスを実装する必要があります。

- セッションをホストするシャーシで PDSN インスタンスを決定します。
- **show ip mobile host {ip-address | nai}**、**show ip mobile secure host {ip-address | nai}**、**show {ip mobile violation address | nai string}**、および **show ip mobile host-counters** のコマンドを実行します。

## バルク統計情報の収集

この機能は、単一ポイントで使用できます。

- シャーシのアクティブな各サービス ブレードから、名前が識別可能な、使用できる PDSN 統計情報の定期的な収集を開始します。
- 選択した各サービス ブレードで、IOS Bulk Statistics コレクションをイネーブルにして、指定した統計情報を収集します。このメカニズムを使用して、MIB 引数の統計情報を収集できます。必要な尺度が MIB の一部ではない場合、バルク統計情報コレクション機能の一部として収集できません。
- URL で識別される外部 TFTP サーバにファイルを転送します。

15 分刻みで統計情報コレクションの期間を設定できます。収集期間の最小値は 30 分です。収集期間の最大値は 24 時間です。

このファイルには、ブレードごとに収集される CPU ベースで使用できる CPU の使用状況およびメモリの占有状況を除き、各ブレードの要約の統計情報が含まれます。ブレード単位のファイルは、そのブレード上の各アプリケーションの CPU のエントリがあります。

ファイルフォーマットは、カンマで区切られた一連の「変数名 値」ペアです。

Cisco PDSN リリース 5.0 では、変数名は変数の OID です。OID は、IOS Bulk Statistics Collection CLI コマンドから使用できるサポートのレベルのためです。

PDSN アプリケーションでサポートされ、MIB で使用できる変数など、収集される統計情報の事前に定義されたセットがあります。統計情報に割り当てられた OID は、関連する MIB の OID に直接対応します。

次の該当する変数は MIB にありません。Bulk Statistics Collection 機能の一部としてこれらはサポートされません。

- PDSNRegRevocationsSent
- PDSNRegRevocationsReceived
- PDSNRegRevocationsIgnored
- PDSNRegRevocationAcksSent
- PDSNRegRevocationAcksReceived
- PDSNRegRevocationAcksIgnored

収集が行われる期間は、`yy:mm:dd:hh:mm:ss yy:mm:dd:hh:mm:ss` というフォーマットでファイルに示されます。最初の日付は開始で、2 番目の日付は終了です。

統計情報の収集をイネーブルにするサブシステムのセットを変更する場合、まず進行中の統計情報の収集をキャンセルしてから、新しい収集を開始する必要があります。キャンセルされたセッションで収集した情報は保存されません。

外部サーバを使用できない場合、ファイルはローカルの不揮発性メモリに保存されます。次のファイルの転送に成功するまで、最後に転送されたファイルがローカルに保存されます。新しいファイルの転送に成功すると、現在の保存ファイルは新しいファイルで置き換えられます。

単一 IP PDSN リリース 5.0 でバルク統計情報機能をサポートするために、新しい IOS コマンドは使用されません。

## Cisco PDSN リリース 5.0 の冗長性のサポート

Cisco PDSN リリース 5.0 機能の冗長性のサポートは、リリース 4.0 のサポート内容と同じです。

セッションの冗長性は、単一 IP アーキテクチャのサポートまで拡張されました。SAMI ごとに 1 つのプロセッサ（つまり PCOP）だけが冗長性管理に関係します。その他のすべてのプロセッサ（TCOP など）は、PCOP の状態に従います。アクティブからスタンバイへの設定の同期は、Cisco PDSN リリース 5.0 でサポートされます。

## パフォーマンス要件

単一 IP PDSN は次のパフォーマンス数値をサポートします。

- サービス ブレードごとに 175,000 の加入者。



- 6個の独立したプロセッサを検証するために適用された測定技術を使用する IMIX による 3.0 Gbps のスループット (20% がアップストリームで 80% がダウンストリーム)。このモデルは、このような測定の一部として実績があるスループットの 5/6 を示します。
- リロードされるスタンバイ PDSN サービス ブレード 200,000 の加入者のレジストレーションをホストするアクティブな HA サービス ブレードのバルク同期に必要な時間は、「6個の独立したプロセッサ」モデルで、完全にロードされたアクティブ サービス ブレードからスタンバイ サービス ブレードへバルク同期する場合よりも短時間です。
- Call Per Second (CPS; 1 秒あたりのコール) レートは、「6個の独立したプロセッサ」モデルの単一プロセッサより低速になることはありません。CPS レートは、パフォーマンス検証で測定されるレート (100 CPS) を満たすか、超えます。

## 単一 IP のサポート - 再利用および新規の CLI コマンド

IPC が IXP と通信できる CLI コマンド、および GTP と GTP モジュール上の IPC が、SAMI PPC 間で、信頼できる確認応答済みの通信および確認応答がされていない通信を実行できる次の CLI コマンドが用意されています。

### EXEC モード

- `debug sami ipc gtp processor 3-8`
- `debug sami ipc gtp processor`
- `debug sami ipc gtp any`
- `debug sami ipc detail`
- `debug sami ipc`
- `debug sami ipc stats detail`
- `debug sami ipc stats`
- `test sami tp-config {enable | disable}` (SingleIP イメージの TP で使用可能)

### show コマンド

- `show sami ipcp ipc gtp`
- `show sami ipcp ipc ixp`
- `show sami ipcp ipc processor`

### 設定モード :

- `default sami ipc crashdump`
- `default sami ipc keepalive`
- `default sami ipc retransmit`
- `default sami ipc retries`
- `sami ipc crashdump`
- `sami ipc keepalive`
- `sami ipc retransmit`
- `sami ipc retries`

設定モードの `sami ipc crashdump` コマンドは次のとおりです。

```
pdsn-Stdby-ftb3-73(config)# sami ipc crashdump ?
```

**never** IPC 障害に応答してクラッシュしません。  
**tolerance** IPC リンク障害の許容期間を指定します。

## 単一 IP PDSN での分散設定、show、および debug コマンド

ここでは、単一 IP PDSN での分散設定、show、および debug コマンドについて説明します。

### 分散設定

Distributed CLI エージェントは、IPC プロトコルを使用して、PCOP の設定情報を各 TCOP に分散しています。

デフォルトで、CLI エージェントはすべてのコマンドを許可していますが、TCOP 上で不要な一部の機能をトリガする可能性があるコマンドをフィルタします。

### CDMA 以外（残りの IOS）の設定コマンド

CDMA 以外の CLI コマンドは、PCOP でブロックまたはフィルタされます。

PCOP 上でフィルタされるコマンドは次のとおりです。

- **router ospf**
- **router bgp**
- **router eigrp**
- **router rip**
- **router [any routing protocol]**
- **cdp [related commands]**
- インターフェイス設定で上記に関連するすべてのサブコマンド

ルーティング プロトコルは TCOP に送信されません。SAMI でルーティング プロトコルを設定することはお勧めしません。SAMI と SUP 間で静的なルーティング設定をセットアップする方が望ましい方法です。

SAMI に IP アドレス プールを割り当て、一方で SUP でそれぞれの静的ルーティングを設定することをお勧めします。

### IP Local Pool Command Change

このコマンドは、GGSN Centralized Pools 実装から再利用されます。

### CDMA 関連の設定コマンド

単一 IP モデルの場合、TCOP にログインすると EXEC バナーが表示され、「通常の」メンテナンス アクティビティを PCOP から実行する必要があるという警告が表示されます。

表 14 は、PDSN 単一 IP がサポートするコマンドのリストです。また、PCOP でフィルタされるか、TCOP にも送信されるかを示します。

コマンドが TCOP に送信される場合、各 TCOP で実行されます。

表 14 単一 IP 用の PDSN コマンド

コマンド (設定コマンド)	目的	使用場所
<b>cdma pdsn multiple service-flows [maximum number]</b>	複数フローのサポートをイネーブルにします。maximum number には、PDSN および PCF 間で作成できる補助 A10 の最大数を定義します。使用できる補助 A10 のデフォルト数は 7 です。	TCOP
<b>cdma pdsn multiple service-flows qos subscriber profile</b>	ローカル加入者の QoS プロファイルを設定できます。加入者の QoS プロファイルが AAA サーバからダウンロードされない場合、このプロファイルは MN に使用されます。	TCOP
<b>cdma pdsn multiple service-flows qos remark-dscp [value]</b>	モバイルからインターネットに対するデータ パケットに、そのモバイルが使用できる DSCP 値内の DSCP がいない場合、マーキングに使用される DSCP の remark 値を設定できます。	TCOP
<b>cdma pdsn tft reject include error extension</b>	TFT が拒否される場合に拒否メッセージにエラー拡張を含めます。	TCOP
<b>cdma pdsn cac maximum bandwidth [number]</b> <b>cdma pdsn cac maximum cpu-threshold [number]</b>	コールアドミッション制御をイネーブルにします。帯域幅や CPU など、CAC パラメータを制御するこれらの CLI の 1 つを使用します。	TCOP 上の PCOP 帯域幅の CPU (メモリ)
<b>cdma pdsn attribute send {f16   f17   f18   f19   f20   f22}</b>	アカウントリング メッセージを転送します。	TCOP

#### ローカル加入者の QoS プロファイル用の PDSN コマンド

**cdma pdsn multiple service flows qos subscriber profile** コマンドを実行すると、サブモードに移行します。表 15 は、ローカル加入者の QoS プロファイルで多様なパラメータの設定に使用できるコマンドのリストです。

表 15 ローカル加入者の QoS プロファイル用の PDSN コマンド

コマンド (設定コマンド)	目的	使用場所
<b>Bandwidth [number]</b>	最大集約帯域幅値を設定します。	TCOP
<b>inter-user-priority [value]</b>	ユーザ間の優先順位パラメータを設定します。	TCOP
<b>tft-allowed [value]</b>	永続的な TFT パラメータの許容数を設定します。	TCOP

表 15 ローカル加入者の QoS プロファイル用の PDSN コマンド (続き)

<b>link-flow [value]</b>	サービス オプション プロファイルで最大サービス接続パラメータを設定します。	TCOP
<b>flow-priority [value]</b>	フロー単位の優先順位の最大値を設定します。	TCOP
<b>flow-profile direction {forward   reverse   bi-direction} flow-id [flow-id]</b>	各方向の認可されたフロー プロファイル ID を設定します。	TCOP
<b>dscp {allowed-class {AF   EF   O}   max-class [value]   reverse-marking [value]}</b>	使用できるディファレンシエーテッドサービスのマーキング パラメータを設定します。	TCOP



(注)

設定コマンドがフィルタされる場合、サブ設定コマンドもフィルタされます。

以下の設定タスクについては、「[PDSN イメージの設定](#)」を参照してください。

- PDSN サービスの有効化
- CDMA Ix インターフェイスの作成
- ループバック インターフェイスの作成
- バーチャル テンプレート インターフェイスの作成と PDSN アプリケーションへのアソシエート
- R-P インターフェイス シグナリングの有効化
- ユーザ セッション パラメータの設定
- HSRP の有効化と冗長性の設定
- PDSN-AAA サーバ インターフェイスのループバック インターフェイスの使用
- アクティブ-アクティブな状況进行处理するアプリケーション トラッキングの設定
- PDSN 環境での AAA サーバの設定
- PDSN 環境での RADIUS の設定
- PDSN 環境での 前払い の設定
- PDSN 環境での VPDN の有効化
- モバイル IP FA の設定
- ローカルなプロキシモバイル IP アトリビュートの設定
- モバイル IP SA の設定
- ネットワーク管理の有効化
- 常時接続サービスの設定
- A11 セッションのアップデートの設定
- SDB インジケータ マーキングの設定
- PPP コントロール パケットの SDB インジケータ マーキングの設定
- PDSN での PoD の設定

- PDSN でのモバイル IP リソース失効の設定
- PDSN アカウンティング イベント
- CDMA RADIUS アトリビュートの設定

### ホスト ルートの設定

一般的に、ホスト ルートはモバイルの TCOP に追加されます。SingleIP の場合、MIP アドレスのすべての ARP 要求は PCOP に送信されます。PCOP が ARP 要求に応答できるようにするには、この CLI コマンドをイネーブルにします。この CLI コマンドを実行すると、フローがアップすると、PCOP 上にモバイルのホスト ルートがインストールされ、フローがダウンするとホスト ルートが削除されます。

この CLI コマンドが必要なのは、ホスト ルートが MIP のスーパーバイザで追加されない場合だけです。デフォルトで、この CLI コマンドは設定されません (表 16)。

表 16 ホスト ルートの設定

コマンド	目的	使用場所
[no] <code>cdma pdsn sm add mobile route</code>	PDSN 上のホスト ルートを設定するか、設定を削除します。	TCOP

## clear コマンド

表 17 は clear コマンドのリストです。

表 17 clear コマンド

コマンド	目的	使用場所
Router# <code>clear cdma pdsn session {all   pcf ip-addr   msid octet-stream} {send {all-update   termreq}}</code>	セッションをクリアします。	TCOP
Router# <code>clear cdma pdsn statistics</code>	RAN-to-PDSN インターフェイス (RP) または PDSN の PPP 統計情報をクリアします。	TCOP
Router# <code>clear ip mobile binding {all [load standby-group-name]   ip-address   nai string ip_address}</code>	モビリティ バインディングを削除します。	TCOP
Router# <code>clear ip mobile visitor [ip-address   nai string ip_address]</code>	ビジター情報をクリアします。	TCOP
Router# <code>clear vpdn tunnel l2tp ?</code>	VPDN L2TP Tunnel 情報をクリアします。 <b>all</b> All L2TP tunnels <b>hostname</b> Based on the hostnames <b>id</b> Based on the tunnel ID <b>ip</b> Based on IP address	TCOP

## 分散された show および debug

デフォルトで、すべての debug コマンドは TCOP で実行され、トレースは PCOP から表示されます。PCOP は、分散されたデバッグの集約は行いません。

分散された show - 分散された show コマンドの場合に従う規則は、「既存の show コマンド」に記載されているコマンドの場合、TCOP から収集されたデータについて PCOP で集約が実行されることです。デフォルトで、show コマンドはすべての TCOP で実行されません。

分散された debug - 分散された debug コマンドの場合に従う規則は、デフォルトで、すべての debug コマンドは TCOP で実行され、トレースは PCOP から表示されることです。PCOP は、分散されたデバッグの集約は行いません。

## 単一 IP アーキテクチャでの新しい show コマンド

次のコマンド例は、単一 IP アーキテクチャの新しい show コマンドを示しています。

```
pdsn# show sami sm imsi IMSI
show sami sm imsi 12345678910112
Session Manager User Details
  IMSI: 12345678910112                Location:7(7000000)

Call Details
  IP Address: 12.1.1.31                VRF ID:0
  HA IP Address: 0.0.0.0                NAI: user1

pdsn# show sami sm statistics
Session Manager Statistics
Request Sent:
  Session: 4                          Control: 0
  Control AAA: 0                       Control HA: 0

Request Received:
  Session Create: 5                    Session Delete: 4
  Flow Create: 6                       Flow Delete: 5
  Agg resp: 0

Response Sent:
  Session Create Success: 5            Session Create Failure: 0
  Session Delete Success: 4           Session Delete Failure: 0
  IMSI update: 0                      IMSI delete Generated : 0
  Flow Create Success: 6              Flow Create Failure: 0
  Flow Delete Success: 5              Flow Delete Failure: 0

IXP Update:
  Total: 0                             Success: 0
  Failure: 0

Failure:
  Message parsing: 0                  Internal 1: 0
  Internal 2: 0                       PPC not found: 0
  Timer Expiry: 0                    Pool Manager: 0
  Flow message parse : 0

PDSN-Act-ftb3-83# sh cdma pdsn statistics sm
PPC Stats:
  Imsi Create Request to PPC Success 4, Failure 0
  Imsi Delete Request to PPC Success 4, Failure 0
  Imsi Response from PPC Success 4, Failure 0
  CCB Create Request to PPC Success 0, Failure 0
  CCB Delete Request to PPC Success 0, Failure 0
  CCB HA Create Request to PPC Success 4, Failure 0
  CCB HA Delete Request to PPC Success 4, Failure 0
  CCB Response from PPC Success 4, Failure 0
  IXP A10 Add Send Success 4 Failure 0, Received Success 4 Failure 0
  IXP A10 Delete Send Success 4 Failure 0, Received Success 4 Failure 0
  IXP CCB Add Send Success 0 Failure 0, Received Success 0 Failure 0
  IXP CCB Delete Send Success 0 Failure 0, Received Success 0 Failure 0
```

```
IXP CCB HA Add Send Success 4 Failure 0, Received Success 4 Failure 0
IXP CCB HA Delete Send Success 4 Failure 0, Received Success 4 Failure 0
IXP Nack terminated session 0 flow 0
Ack timer expiry Imsi 0, Ccb 0
```

```
Tunnel PPC Stats:
Tunnel Create Request Rcvd 3, Sent Ack 3 Nack 0
Tunnel Delete Request Rcvd 3, Deleted 3
Invalid Tunnel Request Type Rcvd 0
PDSN-Act-ftb3-83#
PDSN-Act-ftb3-83#
```

表 18 は、分散された **show** コマンドのリストです。

表 18 分散された **show** コマンド

オプション	説明	CLI コマンド	カテゴリ
Connect	接続時間が time 値 (AGE の使用) より高い、低い、または等値である全ユーザの要約。	<b>show cdma pdsn session age {less   greater   equals} time</b>	C
HA-User	特定の HA に登録されている全ユーザの要約。	<b>show ip mobile visitor home-agent ha-ip</b>	C
アドレスレンジ	このアドレスレンジの全ユーザの要約。	<b>show cdma pdsn flow mn-ip start ip end ip</b>	C
Calltype	このコールタイプ (RTT、EVDO rev A、rev 0 など) に関する全ユーザの要約。	<b>show cdma pdsn session service-option so</b>	C
NAI または User	この NAI に対するすべてのユーザの要約 (NAI ではワイルドカードをサポート)。たとえば、 <b>show user summary nai *ptt*</b> だと、ボックスの Push to Talk ユーザが検索されます。レールムによるフィルタもサポートされます。	<b>show cdma pdsn session user nai</b>	C

## 既存の show コマンド

**show** コマンドは、Data Aggregator (DA) /Data Provider (DP) モデルまたは Remote Console And Logging (RCAL) モデルに分類できます。RCAL モデルのコマンドは、SUP または PCOP から TCOP で直接実行されます。execute-on コマンドを使用する集約は実行されません。cdma 以外のすべての関連コマンドは、この方法で実行する必要があります。

DA/DP カテゴリのコマンドは PCOP で実行され、PCOP 自体にある値を表示するか、すべての TCOP から受信した集約された出力を表示します。

これらのコマンドは、さらにプッシュ コマンドおよびプル コマンドと分類されます。

プッシュ コマンド - プッシュ コマンドは、定期的なすべての TCOP から集約を実行し、要求に応じて (つまり、相当する CLI コマンドの実行時に) PCOP に表示します。

既存のプッシュベースの **show** コマンドのリストは次のとおりです。

- **show cdma pdsn statistics**
- **show cdma pdsn statistics qos**
- **show cdma pdsn statistics ahdlc**

- **show cdma pdsn statistics tft**
- **show cdma pdsn statistics traffic**
- **show cdma pdsn statistics prepaid**
- **show cdma pdsn statistics radius disconnect**
- **show cdma pdsn statistics ppp**
- **show cdma pdsn statistics rp**
- **show cdma pdsn statistics rp error**

プル コマンド - プル コマンドは、このカテゴリのコマンドが実行されるときにだけ集約を実行します。CLI コマンドの実行時に、その時点の TCOP からデータまたは統計情報が取得され、表示されます。

既存のプルベースの **show** コマンドのリストは次のとおりです。

- **show cdma pdsn**
- **show cdma pdsn pcf**
- **show cdma pdsn pcf *pcfipaddr***
- **show cdma pdsn pcf brief**
- **show cdma pdsn pcf *pcfip* psi *psivalue***
- **show l2tp counters tunnel**
- **show l2tp counters tunnel authentication**
- **show cdma pdsn statistics rp pcf**
- **show cdma pdsn statistics rp pcf *pcfip***
- **show cdma pdsn statistics ppp pcf**
- **show cdma pdsn statistics ppp pcf *pcfip***
- **show cdma pdsn statistics sm**
- **show cdma pdsn statistics service-option**
- **show cdma pdsn statistics service-option *sovalue* pcf *pcfip***
- **show cdma pdsn statistics prepaid pcf *pcfip***

## クラスタ処理 show コマンドへの変更

クラスタ処理 **show** コマンドへの変更を次に示します。

```
show cdma pdsn cluster controller member 2.1.1.1
PDSN cluster member 2.1.1.1 (local) state      ready, Group NONE <--- New
registered with PDSN controller 11.1.1.50
reported load 1 percent, will be sought in 2 seconds
```

```
Member 2.1.1.1 statistics:
Number of sessions 0
Controller seek rcvd 6122, Member seek reply rcvd 6122
Member state changed 0 time to ready
Member state changed 0 time to Admin prohibited
Session-Up message rcvd 0, Session-Down message received 0
Member seek not replied in sequence 0
```

```
show cdma pdsn cluster controller configuration
cluster interface GigabitEthernet0/0.341 (collocated)
no R-P signaling proxy
timeout to seek member = 10 seconds
```



```

window to seek member is 2 timeouts in a row if no reply (afterwards the member is
declared offline)
default: spi 101, Timestamp +/- 0, key ascii hello
this PDSN cluster controller is configured

```

```

Controller maximum number of load units = 100

```

```

show cdma pdsn cluster member configuration
cluster interface GigabitEthernet0/0.341
IP address of controller is 11.1.1.50 (collocated) <--- New
no prohibit administratively
timeout to resend status or seek controller = 10 sec or less, randomized
resend a msg for 2 timeouts sequentially if no reply, then inform operator
default: spi 101, Timestamp +/- 0, key ascii hello
this PDSN cluster member is configured

```

## show コマンドへの変更

**show** コマンドへの変更を次に示します。

```

show cdma pdsn pcf:
pdsn_act# show cdma pdsn pcf
PCF 2.2.2.4 has 1 session, 1 service flow
Received 382 pkts (9750 bytes), sent 391 pkts (10585 bytes)
pdsn_act#
Displays only the tunnel information. Sessions associated with that tunnel will not be
displayed.

```

```

show cdma pdsn pcf <pcf-ip-addr>:
pdsn_act# show cdma pdsn pcf 2.2.2.4
PCF 2.2.2.4 has 1 session, 1 service flow
Received 382 pkts (9750 bytes), sent 391 pkts (10585 bytes)
pdsn_act#
Displays only the tunnel information. Sessions associated with that tunnel will not be
displayed.

```

```

show cdma pdsn statistics:
san-pdsn# show cdma pdsn statistics
Last clearing of "show cdma pdsn statistics" counters never
Last Update received at 00:12:54 UTC Mar 1 2009 <--- New
RP Interface:
Reg Request rcvd 0, accepted 0, denied 0, discarded 0
Initial Reg Request rcvd 0, accepted 0, denied 0, discarded 0, AuxRequest 0
Re-registration requests rcvd 0, accepted 0, denied 0, discarded 0
Re-registration requests containing Active-Start 0, Active-Stop 0
Re-registration requests containing new connections 0, missing connections 0, remapping
flows 0
Handoff requests rcvd 0, accepted 0, denied 0, discarded 0, AuxRequest 0
De-registration rcvd 0, accepted 0, denied 0, discarded 0
De-registration Reg Request with Active-Stop 0
Registration Request Errors:
Unspecified 0, Administratively prohibited 0
Resource unavailable 0, Authentication failed 0
Identification mismatch 0, Poorly formed requests 0
Unknown PDSN 0, Reverse tunnel mandatory 0
Reverse tunnel unavailable 0, Bad CVSE 0
Max Service Flows 0, Unsupported So 0, Non-Existent A10 0
Bandwidth Unavailable 0
Update sent 0, accepted 0, denied 0, not acked 0
Initial Update sent 0, retransmissions 0
Acknowledge received 0, discarded 0

```

```

Update reason lifetime expiry 0, PPP termination 0, other 0
Registration Update Errors:
Unspecified 0, Identification mismatch 0
Authentication failed 0, Administratively prohibited 0
Poorly formed request 0
Handoff statistics:
Inter PCF handoff active 0, dormant 0
Update sent 0, accepted 0, denied 0, not acked 0
Initial Update sent 0, retransmissions 0
Acknowledge received 0, discarded 0
De-registration accepted 0, denied 0
Handoff Update Errors:
Unspecified 0, Identification mismatch 0
Authentication failed 0, Administratively prohibited 0
Poorly formed request 0
RP Session Update statistics:
Update sent 0, accepted 0, denied 0, not acked 0
Initial Update sent 0, retransmissions 0
Acknowledge received 0, discarded 0
Sent reasons Always On 0, RN-PDIT 0, Subscriber Qos 0
RP Session Update Errors:
Unspecified 0, Identification mismatch 0
Authentication failed 0, Session parameters not updated 0
Poorly formed request 0
Service Option:
Address Stats:
Simple IP: Static 0, Dynamic 0
Mobile IP: Static 0, Dynamic 0
Proxy Mobile IP: Static 0, Dynamic 0
Simple IP VPDN: Static 0, Dynamic 0
Flow Stats:
Simple IP: Success 0, Failure 0
Mobile IP: Success 0, Failure 0
Proxy Mobile IP: Success 0, Failure 0
Simple IP VPDN: Success 0, Failure 0
Unknown Service Failures: 0
PPP:
Current Connections 0
Connection requests 0, success 0, failure 0, aborted 0
Connection enters stage LCP 0, Auth 0, IPCP 0
Connection success LCP 0, AUTH 0, IPCP 0
Failure reason LCP 0, authentication 0, IPCP 0, other 0
Failure reason lower layer disconnect 0
A10 release before LCP nego by PDSN 0, by PCF 0
LCP Stage
Failure Reasons Options 0, MaxRetry 0, Unknown 0
LCP Term Req during LCP nego sent 0, rcvd 0
A10 release during LCP nego by PDSN 0, by PCF 0
Auth Stage
CHAP attempt 0, success 0, failure 0, timeout 0
PAP attempt 0, success 0, failure 0, timeout 0
MSCHAP attempt 0, success 0, failure 0, timeout 0
EAP attempt 0, success 0, failure 0
MSID attempt 0, success 0, failure 0
AAA timeouts 0, Auth timeouts 0, Auth skipped 0
LCP Term Req during Auth nego sent 0, rcvd 0
A10 release during Auth nego by PDSN 0, by PCF 0
IPCP Stage
Failure Reasons Options 0, MaxRetry 0, Unknown 0
Options failure reason MN Rejected IP Address 0
LCP Term Req during IPCP nego sent 0, rcvd 0
A10 release during IPCP nego by PDSN 0, by PCF 0
CCP Stage
Connection negotiated compression 0

```

```

Compression type Microsoft 0, Stac 0, other 0
Connections negotiated MRRU 0, IPX 0, IP 0
Connections negotiated VJ-Compression 0, BAP 0
PPP bundles 0
Connections failed to negotiate compression 0
Renegotiation total 0, by PDSN 0, by Mobile Node 0
Renegotiation success 0, failure 0, aborted 0
Renegotiation reason: address mismatch 0, lower layer handoff 0
GRE key change 0, other 0
Release total 0, by PDSN 0, by Mobile Node 0
Release by ingress address filtering 0
Release reason: administrative 0, LCP termination 0
Idle timeout 0, echo missed 0
L2TP tunnel 0, insufficient resources 0
Session timeout 0, service unavailable 0
De-Reg from PCF 0, lifetime expiry 0, other 0
Echo stats
Request sent 0, resent 0, max retransmit timeout 0
Response rcvd 0
Discarded Packets
Unknown Protocol Errors 0, Bad Packet Length 0
RSVP:
IEs Parsed 0
TFTs Created Success 0, Failure 0
TFTs Updated Success 0, Failure 0
TFTs Deleted Success 0, Failure 0
Other Failure 0
Unknown 0, Unsupported Ie types 0
Tft Ipv4 Failure Stats
Tft Unauthorized 0, Unsuccessful Processing 0
Tft Treatment Unsupported 0
Packet Filter Add 0, Replace 0
Packet Filter Precedence Contention 0, Unavailable 0
Packet Filter Maximum Limit 0, Non-Existent Tft add 0
QoS:
Total Profile Download Success 0, Failure 0
Local Profile selected 0
Failure Reason DSCP 0, Flow Profile ID 0,
Service option profile 0, Others 0
Total Consolidated Profile 0, DSCP Remarked 0
Total policing installed 0, failure 0, removed 0
slot 0:
AHDLC Engine Type: CDMA HDLC SW ENGINE
Engine is ENABLED
total channels: 375000, available channels: 375000
Framing input 0 bytes, 0 paks
Framing output 0 bytes, 0 paks
Framing errors 0, insufficient memory 0, queue overflow 0
Invalid size 0
Deframing input 0 bytes, 0 paks
Defaming output 0 bytes, 0 paks
Deframing errors 0, insufficient memory 0, queue overflow 0
Invalid size 0, CRC errors 0
RADIUS DISCONNECT:
Disconnect Request rcvd 0, accepted 0
Disconnect Request Errors:
Unsupported Attribute 0, Missing Attribute 0
Invalid Request 0, NAS Id Mismatch 0
Session Cxt Not Found 0, Administratively Prohibited

```

**show cdma pdsn statistics** と同様に、**sm** を除く個々の統計情報のいずれかを実行する場合、最初に次の行が表示されます。

```

Last Update received at 00:12:54 UTC Mar 1 2009 <--- New
router# show cdma pdsn statistics ?
ahdlc AHDLC information
ppp CDMA PDSN ppp statistics
prepaid CDMA PDSN prepaid statistics
qos CDMA PDSN QOS statistics
raa      CDMA PDSN RAA statistics
radius CDMA PDSN traffic statistics
rp CDMA PDSN RP statistics
sm      CDMA PDSN SM statistics
tft CDMA PDSN TFT statistics
| Output modifiers
<cr>
router#

show cdma pdsn statistics rp error:

san-pdsn# show cdma pdsn statistics rp error
Last clearing of "show cdma pdsn statistics rp error" counters never
Last Update received at 00:12:54 UTC Mar 1 2009 <--- New
RP Registration Request Error Reasons:
Invalid Packet length 0, Protocol 0, Flags 0
Invalid Connection ID 0, Authentication Key 0, SPI 0, Mismatch SPI 0
Invalid Mobile ID 0, ID type 0, ID length 0
Invalid Extension Order 0, VSE type 0, Vendor id 0
Invalid Application type 0, Sub Application type 0
Missing extension SSE 0, MHAЕ 0
Duplicate Application type 0, GRE Key 0, CVSE 0
Airlink Retransmission with same sequence number 0
Airlink Invalid attribute length 0, sequence number 0, record 0
Airlink Unknown attribute 0, Duplicate attribute 0
Airlink Initial RRQ No Setup 0, Contains Stop 0, Contains SDB 0
Airlink Start before Setup 0, Start in De-Registration 0
Airlink GRE Key change no Setup 0, Rereceive Setup with same GRE Key 0
Airlink Start rcvd during active 0, Stop rcvd during dormant 0
De-Registration received for unknown session 0
Re-Registration received during session disconnect 0
Processing error due to memory failure 0
RP Registration Update Ack Error Reasons:
Invalid Packet length 0, Protocol 0
Invalid Connection ID 0, Authentication Key 0, SPI 0
Invalid Mobile ID 0, ID type 0, ID length 0
Invalid Extension Order 0, VSE type 0
Missing extension SSE 0, RUAЕ 0
Received for unknown session 0, discard memory failure 0
RP Session Update Ack Error Reasons:
Invalid Packet length 0, Protocol 0
Invalid Connection ID 0, Authentication Key 0, SPI 0
Invalid Mobile ID 0, ID type 0, ID length 0
Invalid Extension Order 0, VSE type 0
Missing extension SSE 0, RUAЕ 0
Received for unknown session 0, discard memory failure 0
RP Registration Reply Error Reasons:
Not sent memory allocation failure 0, Internal error 0
Reply not sent to PCF security not found/parse error 0
RP Registration Update Error Reasons:
Not sent memory allocation failure 0, Internal error 0
RP Session Update Error Reasons:
Not sent memory allocation failure 0, Internal error 0
Other Error Reasons:
Maximum configured/limit number of session reached 0

show cdma pdsn cac:

```

```

pdsn_act# show cdma pdsn cac
                Output in Values                Output in percentage
Total configured bandwidth  2000000 b                100%
Allocated bandwidth         100 b                    0%
Available bandwidth         1999900 b                100%

Sessions allocated          1                        0%
Max sessions allowed       175000                 100%
PDSN_ACT#

```



(注) **show cdma pdsn cac** コマンドでは、CPU およびメモリ関連の詳細は表示されません。

## 単一 IP アーキテクチャでの debug コマンド

表 19 は、単一 IP アーキテクチャでの **debug** コマンドのリストです。

表 19 単一 IP アーキテクチャでの debug コマンド

コマンド	集約は必要か	exec コマンドは TCOP に送信されるか
debug cdma pdsn *	いいえ	はい
debug ppp negotiation	いいえ	はい
debug aaa id	いいえ	はい
debug aaa accounting	いいえ	はい
debug aaa authentication	いいえ	はい
debug aaa authorization	いいえ	はい
debug ip mobile	いいえ	はい
debug aaa pod	いいえ	はい
debug radius	いいえ	はい
debug tacacs	いいえ	はい

## ネットワーク管理および MIB

[「Radius disconnect enabled」](#) を参照してください。

## サポートされない機能

シャーシ内設定の同期。

## 他のゲートウェイから再利用される機能の要約

- SAMI または HA 5.0
- Osler - ユーザ インターフェイス、show コマンド、バルク統計情報

- SNMP 単一インターフェイス
- 単一インターフェイスの設定
- GRE/IP、IP/IP、MIP/UDP トンネルの IXP 検索
- トンネルの IXP デフラグメンテーション
- AAA 応答性トラップ
- フェールオーバーのためのクラッシュ情報または単一インターフェイス
- シャーシ内設定の同期

## 他のゲートウェイで再利用できる機能の要約

PDSN 単一 IP の一部として単一 IP サブシステムに含まれる次の機能は、他のゲートウェイから再利用されます。

- L2TP
- MIP RRQ 転送
- TCOP-TCOP 冗長性
- IXP - ユーザ テーブル単位

Cisco PDSN リリース 5.1 の Single IP per Blade 用設定コマンドについて詳しくは、『*Command Reference for Cisco PDSN Release 5.1 in IOS Release 12.4(22)XR1*』を参照してください。

## Osler のサポート

単一 IP PDSN 製品用の Operator Interface for Multiple Service ブレードは、定義済みの機能セットに単一の OAM 視点を提供するために使用されます。このサポートは、シャーシ全体をブラックボックスとして見ることを意味します。複数のプロセッサ、アクティブまたはスタンバイ設定などを持つ複数のサービス ブレードを心配する必要はありません。

この実装では、カスタマー OAM の展開に対する依存が減り、リアルタイムの診断を迅速に行ったり、予防的な問題解決策を講じたりすることができます。また、多面的なパラメータ（つまり、問題の識別に基づくネットワークの予測可能性、修理、または修復）を進行中に検証できます。

このセクションの内容は次のとおりです。

- 「[Osler のインストール](#)」
- 「[show subscriber コマンド](#)」
- 「[Monitor Subscriber コマンド](#)」
- 「[加入者セッションの表示](#)」
- 「[バルク統計情報の収集](#)」

## Osler のインストール

PDSN Osler Package は TCL 実行可能ファイル (psdn\_Osler-Package.tcl) およびアーカイブ ファイル (psdn\_osler.tar) です。実行可能ファイルとアーカイブ ファイルは、PDSN Osler ポリシーを使用するために選択した場所からスーパーバイザのフラッシュにダウンロードする必要があります。

PDSN Osler Package は SAMI イメージの一部としてバンドルされているため、まず各 SAMI LCP (Processor 0) から両方のファイル（つまり、psdn\_Osler-Package.tcl および psdn\_osler.tar）を SUP の disk0: にコピーする必要があります。

## Osler のインストール コマンド

SUP プロンプトで次のコマンドを発行する必要があります。

```
pdsn-osler# copy sami# slot_number-fs:image/scripts/pdsn_Osler-Package.tcl disk0:
```

```
pdsn-osler# copy sami# slot_number-fs:image/scripts/pdsn_osler.tar disk0:
```

両方のファイルを SUP の disk0: にコピーした後に、SUP 上のパッケージ内で使用できるオプションを表示するには、`tclsh disk0:pdsn_Osler-Package.tcl --help` コマンドを実行します。コマンド出力は次のようになります (表 20)。

表 20 Osler のインストール

コマンド	説明
: tclsh disk0:pdsn_Osler-Package.tcl	
-pkg install uninstall	PDSN Osler パッケージをインストールまたはアンインストールします。uninstall を指定する場合、その他の引数を指定する必要はありません。
-f file name	Osler パッケージをインストールするための SUP フラッシュ上のファイル アーカイブ。
-maxP number	同時に実行できるポリシーの最大数。最小値は 5 にし、最大値は 9 を超えないようにする必要があります。
-tftpN IP address	統計情報、トレース、および加入者の情報を保存する TFTP サーバの IP アドレスまたはホスト名。
-statsLD Directory Path	統計情報を一時的に保存する SUP のローカル ディレクトリ パス。
-statRD Directory Path	Osler のバルク統計情報を保存するリモート TFTP サーバのディレクトリ パス。
-statT [Periodicity [min]]	バルク統計情報の分単位のレポート頻度 (デフォルトは 30 分です)。15 分刻みの増分で、30 ~ 1440 の範囲にする必要があります。
-subRD Directory Path	加入者データを保存するリモート TFTP サーバのディレクトリ パス。
-traceLD [Directory Path]	トレースを一時的に保存する SUP のローカル ディレクトリ パス。
-traceRD Directory Path	トレースの加入者データを保存するリモート TFTP サーバのディレクトリ パス。

## Osler のインストール例

PDSN Osler Package をインストールする場合の例を次に示します。

単一シャーシ環境 :

```
tclsh disk0:pdsn_Osler-Package.tcl -pkg install -f disk0:pdsn_osler.tar -maxP 9 -tftpN
1.1.1.19 -statLD disk0:stats -statRD dirname/stats/globalStats -statT 30 -subRD
nishigup/Osler_Lib -traceLD disk0:/traces -traceRD dirname/traces
```

上記の例では、次のように想定しています。

- TFTP アクセスで書き込み可能なディレクトリ **dirname** を持つ IP 1.1.1.19 で実行されている TFTP サーバがあります。
- /tftpboot/utharani/stats/globalStats, /tftpboot/dirname/traces ディレクトリおよび /tftpboot/dirname/Osler\_Lib ディレクトリがあり、1.1.1.19 上のすべてについて書き込み可能です。



#### ヒント

PDSN Osler インストール パッケージが途中で停止した場合、Enter キーを押してインストール スクリプトを次に進めます。

PDSN Osler Package をアンインストールする場合の例を次に示します。

単一シャーシ環境：

```
tclsh disk0:pdsn_Osler-Package.tcl -pkg uninstall
```



#### (注)

- デュアル シャーシ モードは、PDSN Osler パッケージに存在しません。
- PDSN-Osler インストール スクリプトでは、statsRD、subRD、および traceRD の各引数のすべてに指定されているパスが存在すること、および (tftpN 引数の指定に従って) TFTP サーバで書き込み可能であることを想定しています。
- インストール パッケージに含まれるすべてのファイルは、SUP 上の EEM ユーザ ポリシー ディレクトリ設定 (つまり、「イベント マネージャ ディレクトリ ユーザ ポリシー」) のファイルと同じディレクトリ パスにコピーする必要があります。EEM ユーザ ポリシー ディレクトリに関連する設定がない場合、すべてのインストール ファイルを *disk0:/pdsn\_osler* にコピーし、EEM ユーザ ポリシー設定を *disk0:/pdsn\_osler* に設定します。
- PDSN-Osler パッケージをアンインストールする前に、パルク統計情報のレポートを停止します。

## show subscriber コマンド

CLI コマンドは、アクティブ PDSN インスタンスを実行するプロセッサで呼び出され、多様な条件の 1 つまたは複数に一致する加入者をクエリーします。条件は次のとおりです。

- All - シャーシ レベルのユーザの全セッションの要約
- Card - 特定のカード、スロット、またはブレード上の全ユーザ セッションの要約
- CPU - 特定の CPU 上の全ユーザの要約
- Connect - 接続時間が time 値より高い、低い、または等値である全ユーザの要約
- FA - Chassis - PDSN 内の FA 上の全ビジターの要約
- FA - member - 全ユーザの FA (PDSN 内の特定の FA) の要約
- HA - User - 特定の HA に登録されている全ユーザの要約
- Address space - このアドレス レンジの全ユーザの要約
- Calltype - このコール タイプの全ユーザの要約



- NAI/User - この NAI の全ユーザの要約

summary、brief、および verbose という 3 種類の表示フォーマットが用意されています。

- Summary - 送信パケット、受信パケット、送信バイト、受信バイトなど、表示ポリシーと一致する加入者の単純な合計
- Brief - 表示ポリシーと一致する加入者ごとに、「1 加入者あたり 1 行の出力」フォーマット
- Verbose - 表示ポリシーと一致する加入者ごとに、「1 加入者あたり複数行の出力」フォーマット

Osler CLI はプロセッサからコマンドの出力を収集し、結果を照合し、1 つのコマンドが実行されたように提示します。ファイルのデータを収集するか、verbose および brief オプションで画面にデータを表示するオプションを用意する必要があります。

## Show Subscriber Verbose All

このコマンドは、シャース上のすべての加入者を表示します。このコマンドは、内部的に **show cdma pdsn session detail** を使用し、出力を解析します。



### 注意

このポリシーを実行しないことをお勧めします。大容量のデータ（1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数）が SUP カードにあるため、ポリシーがそれを処理するには長時間かかります。完全にロードされたシャースですべての加入者を表示するのに、1 ~ 2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超過している場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**tfpt://tfpt-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上のファイルに収集するために使用されます。



### (注)

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
----- Slot 1/CPU 5, show cdma pdsn session detail-----

Mobile Station ID IMSI 09003000001
PCF IP Address 6.6.6.2, PCF Session ID 1
A10 connection time 02:25:51, registration lifetime 65535 sec
Number of successful A11 reregistrations 0
Remaining session lifetime INFINITE
Always-On not enabled for the user

Current Access network ID 0006-0606-02
Last airlink record received is Active Start, airlink is active
GRE protocol type is 0x8881
GRE sequence number transmit 867, receive 860
Using interface Virtual-Access2.1, status OPN
Using AHDLC engine on slot 0, channel ID 10
Service Option EV-DO Flow Discrimination 0 DSCP Included 0
Flow Count forward 0 reverse 0
This session has 1 flow
This session has 0 service flows
```

```

Session Airlink State Active
This session has 0 TFTs
Qos subscriber profile
  Max Aggregate Bandwidth : 1
Inter User Priority : 1000
  Maximum Flow Priority : 120980
  Forward profile-id : 4660
  Forward profile-id : 9097
  Forward profile-id : 14454
  Reverse profile-id : 6295
  Reverse profile-id : 17185
  Bidirectional profile-id : 22136
  Bidirectional profile-id : 26505

Flow service Simple, NAI osler1
  Mobile Node IP address 4.4.4.1
  Packets in 0, bytes in 0
  Packets out 0, bytes out 0

Qos per flow : osler1
  Max Aggregate Bandwidth : 1
  Inter User Priority : 1000
  Maximum Flow Priority : 120980
  Number of Persistent Tft : 34567

  Forward profile-id : 4660
  Forward profile-id : 9097
  Forward profile-id : 14454
  Reverse profile-id : 6295
  Reverse profile-id : 17185
  Bidirectional profile-id : 22136
  Bidirectional profile-id : 26505

```

## Show Subscriber Brief All

このコマンドは、シャーシ内のすべての加入者を表示するために実装されます。このコマンドは、内部的に **show cdma pdsn session brief** を使用し、出力を解析します。



### 注意

大容量のデータ (1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数) が SUP カードを経由し、ポリシーがこれを処理するのに時間がかかるため、このポリシーを実行しないことをお勧めします。完全にロードされたシャーシですべての加入者を表示するのに、1 ~ 2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**ftp://ftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上のファイルに収集するために使用されます。



### (注)

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
----- Slot 1/CPU 5, show cdma pdsn session brief-----
```

MSID	PCF IP Address	PSI	Age	St	SFlows	Flows	Interface
09003000001	6.6.6.2	1	00:27:02	OPN	0	1	Virtual-Access2.1
09003000053	6.6.6.5	51	00:00:32	OPN	0	1	Virtual-Access2.2

## Show Subscriber Summary All

このコマンドは、シャーシ内のすべての加入者の要約を表示するために実装されます。このコマンドは、内部的に **show cdma pdsn session summary** を使用し、出力を解析します。

次の例は、表示内容の抜粋です。

```
SHOW SUBSCRIBER SUMMARY
-----
Total Number of sessions :121
Total Number of Paks in :83866
Total Number of Paks out :87872
Total Number of bytes in :1341130
Total Number of bytes out :2601436
```

## Show Subscriber Verbose Card

このコマンドは、特定の SAMI カード上のすべての加入者を表示します。このコマンドは特定のカードで内部的に **show cdma pdsn session detail** を使用し、出力を解析します。



**注意**

大容量のデータ (1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数) が SUP カードを経由し、ポリシーがこれを処理するのに時間がかかるため、このポリシーを実行しないことをお勧めします。完全にロードされたシャーシですべての加入者を表示するのに、1 ~ 2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超過している場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**tfpt://tfpt-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上のファイルに収集するために使用されます。



**(注)**

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
>> Now enter the SAMI Card ID ([1-13]): 1
----- Slot 1/CPU 5, show cdma pdsn session detail-----

Mobile Station ID IMSI 09003000003
  PCF IP Address 6.6.6.5, PCF Session ID 1
  A10 connection time 00:08:36, registration lifetime 65535 sec
  Number of successful All reregistrations 0
  Remaining session lifetime INFINITE
  Always-On not enabled for the user
  Current Access network ID 0006-0606-05
  Last airlink record received is Active Start, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 14, receive 0
  Using interface Virtual-Access2.1, status OPN
  Using AHDLC engine on slot 0, channel ID 54
```

```

Service Option EV-DO Flow Discrimination 0 DSCP Included 0
Flow Count forward 0 reverse 0
This session has 1 flow
This session has 0 service flows
Session Airlink State Active
This session has 0 TFTs
Qos subscriber profile
  Max Aggregate Bandwidth : 1
  Inter User Priority : 1000
  Maximum Flow Priority : 120980
  Forward profile-id : 4660
  Forward profile-id : 9097
  Forward profile-id : 14454
  Reverse profile-id : 6295
  Reverse profile-id : 17185
  Bidirectional profile-id : 22136
  Bidirectional profile-id : 26505

Flow service Mobile, NAI scdma_osler3@ark.com
Mobile Node IP address 9.9.9.2

HA IP address 5.5.5.2
Packets in 0, bytes in 0
Packets out 0, bytes out 0

Qos per flow : scdma_osler3@ark.com
  Max Aggregate Bandwidth : 1
  Inter User Priority : 1000
  Maximum Flow Priority : 120980
  Number of Persistent Tft : 34567
  Forward profile-id : 4660
  Forward profile-id : 9097
  Forward profile-id : 14454
  Reverse profile-id : 6295
  Reverse profile-id : 17185
  Bidirectional profile-id : 22136
  Bidirectional profile-id : 26505

```

## Show Subscriber Brief Card

このコマンドは、特定のカード上のすべての加入者を表示します。このコマンドは特定のカードで内部的に **show cdma pdsn session brief** を使用し、出力を解析します。



### 注意

このポリシーを実行しないことをお勧めします。大容量のデータ（1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数）が SUP カードにあるため、ポリシーがそれを処理するには長時間かかります。完全にロードされたシャーシですべての加入者を表示するのに、1～2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**tftp://tftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上のファイルに収集するために使用されます。



(注) 加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
>> Now enter the SAMI Card ID ([1-13]): 1
----- Slot 1/CPU 5, show cdma pdsn session brief-----
MSID                PCF IP Address      PSI      Age  St SFlows Flows Interface
09003000001         6.6.6.2             1 00:28:39 OPN      0    1 Virtual-Access2.1
09003000053         6.6.6.5             51 00:02:09 OPN      0    1 Virtual-Access2.2
```

## Show Subscriber Summary Card

このコマンドは、特定のカード上のすべての加入者の要約を表示します。このコマンドは特定のカードで内部的に **show cdma pdsn session summary** を使用し、出力を解析します。

次の例は、表示内容の抜粋です。

```
>> Now enter the SAMI Card ID ([1-13]): 1
SHOW SUBSCRIBER SUMMARY <-> (All Subscribers on the Card: 1)
-----
Total   Number of sessions :121
Total   Number of Paks in  :84555
Total   Number of Paks out :88561
Total   Number of bytes in :1352154
Total   Number of bytes out :2620915
```

## Show Subscriber Verbose CPU

このコマンドは、SAMI カードの特定の TCOP からの加入者すべてを示しています。このコマンドは特定の {Card, PCOP} で内部的に **execute-on [TCOP] show cdma pdsn session detail** を使用し、出力を解析します。



注意

このポリシーを実行しないことをお勧めします。大容量のデータ（1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数）が SUP カードにあるため、ポリシーがそれを処理するには長時間かかります。完全にロードされたシャーシですべての加入者を表示するのに、1 ~ 2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超過している場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**ftftp://ftftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。



(注) 加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
>> Now enter the ',' separated SAMI Card & CPU ID (e.g. 4,5): 1,5
----- Slot 1/CPU 5, show cdma pdsn session detail-----

Mobile Station ID IMSI 09003000051
```

```

PCF IP Address 6.6.6.2, PCF Session ID 51
A10 connection time 00:08:24, registration lifetime 65535 sec
Number of successful A11 reregistrations 0

Remaining session lifetime INFINITE
Always-On not enabled for the user
Current Access network ID 0006-0606-02
Last airlink record received is Active Start, airlink is active
GRE protocol type is 0x8881
GRE sequence number transmit 62, receive 55
Using interface Virtual-Access2.2, status OPN
Using AHDLC engine on slot 0, channel ID 53
Service Option EV-DO Flow Discrimination 0 DSCP Included 0
Flow Count forward 0 reverse 0
This session has 1 flow
This session has 0 service flows
Session Airlink State Active
This session has 0 TFTs
Qos subscriber profile
  Max Aggregate Bandwidth : 1
  Inter User Priority : 1000
  Maximum Flow Priority : 120980
  Forward profile-id : 4660
  Forward profile-id : 9097
  Forward profile-id : 14454
  Reverse profile-id : 6295
  Reverse profile-id : 17185
  Bidirectional profile-id : 22136
  Bidirectional profile-id : 26505

Flow service Simple, NAI osler1
  Mobile Node IP address 4.4.4.5
Packets in 0, bytes in 0
  Packets out 0, bytes out 0

Qos per flow : osler1
  Max Aggregate Bandwidth : 1
  Inter User Priority : 1000

  Maximum Flow Priority : 120980
  Number of Persistent Tft : 34567
  Forward profile-id : 4660
  Forward profile-id : 9097
Forward profile-id : 14454
  Reverse profile-id : 6295
  Reverse profile-id : 17185
  Bidirectional profile-id : 22136
  Bidirectional profile-id : 26505

```

## Show Subscriber Brief CPU

このコマンドは、SAMI カードの特定の TCOP からの加入者すべてを示しています。このコマンドは特定の {Card, PCOP} で内部的に **execute-on [TCOP] show cdma pdsn session brief** を使用し、出力を解析して略式で提示します。



### 注意

このポリシーを実行しないことをお勧めします。大容量のデータ（1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数）が SUP カードにあるため、ポリシーがそれを処理するには長時間かかります。完全にロードされたシャーシですべての加入者を表示するのに、1～2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**tftp://tftp-ip/user/[dir]/PPC3-SLOTNumber-sub-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。



(注) 加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
>> Now enter the ',' separated SAMI Card & CPU ID (e.g. 4,5): 1,5
>> Large number of records to process. Should I tftp it (y/n): y
Redirected the file PPC3-SLOT1-04_33_58.19_Feb_2009
*****
===== Total OP-REDIRECTED Records Found =====
```

## Show Subscriber Summary CPU

このコマンドは、SAMI カードの特定の TCOP からの加入者を示します。このコマンドは特定の {Card, PCOP} で内部的に **execute-on [TCOP] show cdma pdsn session summary** を使用し、出力を解析します。

次の例は、表示内容の抜粋です。

```
>> Now enter the ',' separated SAMI Card & CPU ID (e.g. 4,5): 1,5
SHOW SUBSCRIBER SUMMARY <-> (All Subscribers on the Slot,CPU: [1,5])
-----
Total Number of sessions :121
Total Number of Paks in :120771
Total Number of Paks out :124777
Total Number of bytes in :1931750
Total Number of bytes out :3648760
```

## Show Subscriber Verbose with Connect

このコマンドは、パラメータ内にライフタイムを hh:mm:ss 形式で持つ加入者を示しています。このコマンドは、内部的に **show cdma pdsn session lifetime age {greater | less | equals} [time] detail** を使用し、出力を解析します。

SUP カードに大量のデータが送信されるため、基準が大量の加入者に一致する場合、ポリシーがデータを処理するには長時間かかります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**tftp://tftp-ip/user/[dir]/PPC3-SLOTNumber-sub-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。



(注) 加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
>> Now enter the lifetime (hh:mm:ss format): 0:2:29
>> Enter the value type for Life Time Record (e.g: greater|lesser|equals): greater
----- Slot 1/CPU 5, show cdma pdsn session lifetime age greater 0:2:29
detail-----
```

```
Mobile Station ID IMSI 09003000051
PCF IP Address 6.6.6.2, PCF Session ID 51
A10 connection time 00:04:25, registration lifetime 65535 sec
Number of successful All reregistrations 0
Remaining session lifetime INFINITE
Always-On not enabled for the user
Current Access network ID 0006-0606-02

Last airlink record received is Active Start, airlink is active
GRE protocol type is 0x8881
GRE sequence number transmit 38, receive 31
Using interface Virtual-Access2.2, status OPN
Using AHDLC engine on slot 0, channel ID 55
Service Option EV-DO Flow Discrimination 0 DSCP Included 0
Flow Count forward 0 reverse 0
This session has 1 flow
This session has 0 service flows
Session Airlink State Active
This session has 0 TFTs
Qos subscriber profile
  Max Aggregate Bandwidth : 1
  Inter User Priority : 1000
  Maximum Flow Priority : 120980
  Forward profile-id : 4660
  Forward profile-id : 9097
  Forward profile-id : 14454
  Reverse profile-id : 6295
  Reverse profile-id : 17185
  Bidirectional profile-id : 22136
  Bidirectional profile-id : 26505

Flow service Simple, NAI osler1
  Mobile Node IP address 4.4.4.5
  Packets in 0, bytes in 0
  Packets out 0, bytes out 0

Qos per flow : osler1
  Max Aggregate Bandwidth : 1
  Inter User Priority : 1000
  Maximum Flow Priority : 120980
  Number of Persistent Tft : 34567
  Forward profile-id : 4660

  Forward profile-id : 9097
  Forward profile-id : 14454
  Reverse profile-id : 6295
  Reverse profile-id : 17185
  Bidirectional profile-id : 22136
  Bidirectional profile-id : 26505
```

## Show Subscriber Brief with Connect

このコマンドは、パラメータ内にライフタイムを *hh:mm:ss* 形式で持つ加入者を示しています。このコマンドは、内部的に **show cdma pdsn session lifetime age {greater | less | equals} [time] brief** を使用し、出力を解析します。

SUP カードに大量のデータが送信されるため、基準が大量の加入者に一致する場合、ポリシーがデータを処理するには長時間かかります。



ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**ftftp://ftftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。



(注)

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
>> Now enter the lifetime (hh:mm:ss format): 0:2:59
>> Enter the value type for Life Time Record (e.g.: greater|lesser|equals): greater

----- Slot 1/CPU 5, show cdma pdsn session lifetime age greater 0:2:59
brief-----
MSID                PCF IP Address          PSI      Age  St SFlows Flows Interface
09003000051         6.6.6.2                 51 00:05:10 OPN      0    1 Virtual-Access2.2
```

## Show Subscriber Summary with Connect

このコマンドは、パラメータ内にライフタイムを *hh:mm:ss* 形式で持つ加入者を示しています。このコマンドは、内部的に **show cdma pdsn session lifetime age {greater | less | equals} [time] summary** を使用し、出力を解析します。

次の例は、表示内容の抜粋です。

```
>> Now enter the lifetime (hh:mm:ss format): 1:23:0
>> Enter the value type for Life Time Record (e.g: greater|lesser|equals): greater

SHOW SUBSCRIBER SUMMARY <-> (With specified lifetime: 1:23:0)
-----
Total Number of sessions with lifetime greater than the given time :120
Total Number of Paks in :121117
Total Number of Paks out :125114
Total Number of bytes in :1937152
Total Number of bytes out :3657995
```

## Show Subscriber Verbose from FA-Chassis

このコマンドは、シャーシ内で FA が提供するビジターの合計数を示しています。このコマンドは、内部的に **show ip mobile visitor** を使用し、出力を解析します。



注意

このポリシーを実行しないことをお勧めします。大容量のデータ (1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数) が SUP カードにあるため、ポリシーがそれを処理するには長時間かかります。完全にロードされたシャーシですべての加入者を表示するのに、1 ~ 2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**ftftp://ftftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。

**(注)**

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
----- Slot 1/CPU 5, show ip mobile visitor-----

Mobile Visitor List:
Total 1
scdma_osler3@ark.com:
  Home addr 9.9.9.2
  Interface Virtual-Access2.1, MAC addr 0000.0000.0000
  IP src 0.0.0.0, dest 5.5.5.1, UDP src port 434
  HA addr 5.5.5.2, Identification CD1EB19A.10000
  Lifetime 00:10:00 (600) Remaining 00:03:05
  Tunnel0 src 5.5.5.1, dest 5.5.5.2, reverse-allowed
  Routing Options
```

## Show Subscriber Brief From FA-Chassis

このコマンドは、シャーシ内で FA が提供するビジターの合計数を示しています。このコマンドは、内部的に **show ip mobile visitor brief** を使用し、出力を解析して略式で提示します。

シャーシの特定の FA に多数の加入者がいる場合、ポリシーがすべての加入者を表示するには長時間かかります。このような場合、このコマンドを頻繁に実行することをお勧めします。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**tftp://tftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。

**(注)**

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
----- Slot 1/CPU 5, show ip mobile visitor brief-----

Mobile Visitor List:
Total 1
scdma_osler3@ark.com:
  Home addr 9.9.9.1
  MAC addr 0000.0000.0000
  HA addr 5.5.5.2
  FA addr 5.5.5.1
  Lifetime 00:10:00 (600) Remaining 00:08:03
```

## Show Subscriber Summary from FA-Chassis

このコマンドは、シャーシ内で FA が提供するビジターの合計数を示しています。このコマンドは、内部的に **show ip mobile visitor summary** を使用し、出力を解析します。

次の例は、表示内容の抜粋です。

```
SHOW SUBSCRIBER SUMMARY <-> (FA-Chassis Visitors)
-----
```

```
FA-Chassis visitors List:
Total 1
```

## Show Subscriber Verbose from FA-Member

このコマンドは、指定したサービス カード内で FA が提供するビジターの合計数を示しています。このコマンドは、内部的に **show ip mobile visitor [Card]** を使用し、出力を解析します。



### 注意

このポリシーを実行しないことをお勧めします。大容量のデータ（1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数）が SUP カードにあるため、ポリシーがそれを処理するには長時間かかります。完全にロードされたシャーシですべての加入者を表示するのに、1～2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超過している場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**ftftp://ftftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。



### (注)

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
>> Now enter the Card number for FA-Member visitors: 1
----- Slot 1/CPU 5, show ip mobile visitor-----

Mobile Visitor List:
Total 1
scdma_osler3@ark.com:
  Home addr 9.9.9.2
  Interface Virtual-Access2.3, MAC addr 0000.0000.0000
  IP src 0.0.0.0, dest 5.5.5.1, UDP src port 434
  HA addr 5.5.5.2, Identification CD229382.10000
  Lifetime 00:10:00 (600) Remaining 00:02:39
  Tunnel0 src 5.5.5.1, dest 5.5.5.2, reverse-allowed
  Routing Options
```

## Show Subscriber Brief from FA-Member

このコマンドは、指定したサービス カード内で FA が提供するビジターの合計数を示しています。このコマンドは、内部的に **show ip mobile visitor [card] brief** を使用し、出力を解析します。

カードの特定の FA に多数の加入者がいる場合、ポリシーがすべての加入者を表示するには長時間かかります。このような場合、このコマンドを頻繁に実行することをお勧めします。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超過している場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**ftftp://ftftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。

**(注)**

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
>> Now enter the Card number for FA-Member visitors: 1
----- Slot 1/CPU 5, show ip mobile visitor brief-----
Mobile Visitor List:
Total 1
scdma_osler3@ark.com:
  Home addr 9.9.9.2
  MAC addr 0000.0000.0000
  HA addr 5.5.5.2
  Lifetime 00:10:00 (600) Remaining 00:04:57
```

### Show Subscriber Summary from FA-Member

このコマンドは、指定したサービス カード内で FA が提供するビジターの合計数を示しています。このコマンドは、内部的に **show ip mobile visitor [card] summary** を使用し、出力を解析します。

次の例は、表示内容の抜粋です。

```
SHOW SUBSCRIBER SUMMARY <-> (FA-Member Visitors: 1)
-----
FA-Member Visitors List:
Total 1
```

### Show Subscriber Verbose from HA-User

このコマンドは、特定の HA で登録されたユーザの合計数を示しています。このコマンドは、すべての TCOP で内部的に **show ip mobile visitor ha-addr [ha-ip]** を使用し、出力を解析します。

**注意**

このポリシーを実行しないことをお勧めします。大容量のデータ（1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数）が SUP カードにあるため、ポリシーがそれを処理するには長時間かかります。完全にロードされたシャーシですべての加入者を表示するのに、1～2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**tftp://tftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。

**(注)**

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
>> Now enter the HA-User address (HA IP): 5.5.5.2
----- Slot 1/CPU 5, show ip mobile visitor ha-addr 5.5.5.2-----
Mobile Visitor List:
Total 1
scdma_osler3@ark.com:
```

```

Home addr 9.9.9.2
Interface Virtual-Access2.3, MAC addr 0000.0000.0000
IP src 0.0.0.0, dest 5.5.5.1, UDP src port 434
HA addr 5.5.5.2, Identification CD228505.10000
Lifetime 00:10:00 (600) Remaining 00:07:33
Tunnel0 src 5.5.5.1, dest 5.5.5.2, reverse-allowed
Routing Options

```

## Show Subscriber Brief from HA-User

このコマンドは、特定の HA で登録されたユーザの合計数を示しています。このコマンドは、内部的に **show ip mobile visitor ha-addr [ha-ip] brief** を使用し、出力を解析します。

カードの特定の HA に多数の加入者がいる場合、ポリシーがすべての加入者を表示するには長時間かかります。頻繁に実行することは推奨されません。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**tftp://tftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。



(注)

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```

>> Now enter the HA-User address (HA IP): 5.5.5.2
----- Slot 1/CPU 5, show ip mobile visitor ha-addr 5.5.5.2 brief-----
Mobile Visitor List:
Total 1
scdma_osler3@ark.com:
  Home addr 9.9.9.2
  MAC addr 0000.0000.0000
  HA addr 5.5.5.2
  Lifetime 00:10:00 (600) Remaining 00:04:07

```

## Show Subscriber Summary from HA-user

このコマンドは、特定の HA で登録されたユーザの合計数を示すために実装されます。このコマンドは、内部的に **show ip mobile visitor ha-addr [ha-ip] summary** を使用し、出力を解析します。

次の例は、表示内容の抜粋です。

```

>> Now enter the HA-User address (HA IP): 5.5.5.2
SHOW SUBSCRIBER SUMMARY <-> (HA-User IP: 5.5.5.2)
-----
HA User Subscriber List:
Total 1

```

## Show Subscriber Verbose within Address Space

このコマンドは、特定のアドレス レンジ内のすべての加入者を示しています。このコマンドは、内部的に **show cdma pdsn flow mn-ip-address range [mn-ip] detail** を使用し、出力を解析します。

**注意**

このポリシーを実行しないことをお勧めします。大容量のデータ（1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数）が SUP カードにあるため、ポリシーがそれを処理するには長時間かかります。完全にロードされたシャーシですべての加入者を表示するのに、1～2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**ftftp://ftftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。

**(注)**

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
>> Now enter the ',' separated starting IP address & end IP address(e.g.
10.114.200.49,10.114.200.180) : 4.4.4.1,4.4.4.10
----- Slot 1/CPU 5, show cdma pdsn flow mn-ip-address range 4.4.4.1 4.4.4.10
detail-----
```

```
Flow service Simple, NAI osler1@cisco.com
```

```
Mobile Node IP address 4.4.4.1
Packets in 0, bytes in 0
Packets out 0, bytes out 0
```

```
Qos per flow : osler1@cisco.com
Max Aggregate Bandwidth : 1
Inter User Priority : 1000
Maximum Flow Priority : 120980
Number of Persistent Tft : 34567
Forward profile-id : 4660
Forward profile-id : 9097
Forward profile-id : 14454
Reverse profile-id : 6295
Reverse profile-id : 17185
Bidirectional profile-id : 22136
Bidirectional profile-id : 26505
```

```
Flow service Simple, NAI osler1@cisco.com
Mobile Node IP address 4.4.4.2
Packets in 1, bytes in 108
Packets out 1, bytes out 76
```

```
Qos per flow : osler1@cisco.com
Max Aggregate Bandwidth : 1
Inter User Priority : 1000
Maximum Flow Priority : 120980
Number of Persistent Tft : 34567
Forward profile-id : 4660
Forward profile-id : 9097
Forward profile-id : 14454
Reverse profile-id : 6295
Reverse profile-id : 17185
Bidirectional profile-id : 22136
```

Bidirectional profile-id : 26505

## Show Subscriber Brief within Address Space

このコマンドは、特定のアドレス レンジ内のすべての加入者を示しています。このコマンドは、内部的に **show cdma pdsn flow mn-ip-address range <mn-ip> brief** を使用し、出力を解析します。



### 注意

このポリシーを実行しないことをお勧めします。大容量のデータ（1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数）が SUP カードにあるため、ポリシーがそれを処理するには長時間かかります。完全にロードされたシャーシですべての加入者を表示するのに、1～2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**tftp://tftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。



### (注)

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
>> Now enter the ',' separated starting IP address & end IP address (e.g.
10.114.200.49,10.114.200.180) : 4.4.4.1,4.4.4.10
----- Slot 1/CPU 5, show cdma pdsn flow mn-ip-address range 4.4.4.1
4.4.4.10-----
MSID           NAI                               Type           MN IP Address  St
09003000001    osler1@cisco.com                  Simple         4.4.4.2       ACT
```

## Show Subscriber Summary within Address Space

このコマンドは、特定のアドレス レンジ内のすべての加入者の要約を示しています。このコマンドは、内部的に **show cdma pdsn flow mn-ip-address range [mn-ip] summary** を使用し、出力を解析します。

次の例は、表示内容の抜粋です。

```
>> Now enter the ',' separated starting IP address & end IP address (e.g.
10.114.200.49,10.114.200.180) : 4.4.4.1,4.4.4.10
SHOW SUBSCRIBER SUMMARY <-> (Subscriber in address range: 4.4.4.1 4.4.4.10)
-----
Number of flows having mn-ip-adress between 4.4.4.1 4.4.4.10 : 8
Total Number of Packs in :0
Total Number of Packs out :0
Total Number of bytes in :0
Total Number of Packs out :0
```

## Show Subscriber Verbose for Calltype

このコマンドは、特定のコールタイプのユーザの合計数を示しています。このコマンドは、内部的に **show cdma pdsn session service-option [so] detail** を使用し、出力を解析します。

**注意**

このポリシーを実行しないことをお勧めします。大容量のデータ（1 ブレードあたり 500,000 の加入者を SAMI ブレードの数だけ乗じた数）が SUP カードにあるため、ポリシーがそれを処理するには長時間かかります。完全にロードされたシャーシですべての加入者を表示するのに、1～2 時間かかることがあります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**ftp://tftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。

**(注)**

加入者の合計数が、1 PCOP あたり 1000 を超えた場合、ポリシーは加入者を画面に表示しません。ただし、ファイルへ出力をリダイレクトすることにより、加入者のリストを表示できます。

次の例は、表示内容の抜粋です。

```
Select Service type:
1.  EVDO
2.  1xRTT
3.  Quit
Enter the service Type choice from the above menu (1/2/3): 1
----- Slot 1/CPU 5, show cdma pdsn session service-option 59 detail-----

Mobile Station ID IMSI 09003000051
PCF IP Address 6.6.6.2, PCF Session ID 51
A10 connection time 00:11:13, registration lifetime 65535 sec
Number of successful All reregistrations 0
Remaining session lifetime INFINITE
Always-On not enabled for the user
Current Access network ID 0006-0606-02
Last airlink record received is Active Start, airlink is active
GRE protocol type is 0x8881
GRE sequence number transmit 78, receive 71
Using interface Virtual-Access2.2, status OPN
Using AHDLC engine on slot 0, channel ID 55
Service Option EV-DO Flow Discrimination 0 DSCP Included 0
Flow Count forward 0 reverse 0
This session has 1 flow
This session has 0 service flows

Session Airlink State Active
This session has 0 TFTs
Qos subscriber profile
  Max Aggregate Bandwidth : 1
  Inter User Priority : 1000
  Maximum Flow Priority : 120980
  Forward profile-id : 4660
  Forward profile-id : 9097
  Forward profile-id : 14454
  Reverse profile-id : 6295
  Reverse profile-id : 17185
  Bidirectional profile-id : 22136
  Bidirectional profile-id : 26505

Flow service Simple, NAI osler1
Mobile Node IP address 4.4.4.5
```



```
Packets in 0, bytes in 0
Packets out 0, bytes out 0
```

```
Qos per flow : osler1
Max Aggregate Bandwidth : 1
Inter User Priority : 1000
Maximum Flow Priority : 120980
Number of Persistent Tft : 34567
Forward profile-id : 4660
Forward profile-id : 9097
Forward profile-id : 14454
Reverse profile-id : 6295
Reverse profile-id : 17185
Bidirectional profile-id : 22136
Bidirectional profile-id : 26505
```

## Show Subscriber Brief for Calltype

このコマンドは、特定のコールタイプのユーザの合計数を示しています。このコマンドは、内部的に **show pdsn session service-option [so] brief** を使用し、出力を解析します。

特定のカードに多数の加入者がいる場合、ポリシーがすべての加入者を表示するには長時間かかります。頻繁に実行することは推奨されません。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超過している場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**ftftp://ftftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。



(注)

このポリシーは、1 PCOP あたりの加入者の合計数が 1000 を超える場合は、加入者を画面に表示できません。しかし、このファイル オプションは機能しています。

次の例は、表示内容の抜粋です。

```
Select Service type:
1.  EVDO
2.  1xRTT
3.  Quit
Enter the service Type choice from the above menu (1/2/3): 1

----- Slot 1/CPU 5, show cdma pdsn session service-option 59 brief-----
MSID          PCF IP Address      PSI      Age  St SFlows  Flows Interface
09003000051   6.6.6.2             51 00:12:00 OPN    0    1 Virtual-Access2.2
09003000003   6.6.6.5             1 00:04:33 OPN    0    1 Virtual-Access2.1
```

## Show Subscriber Summary for Calltype

このコマンドは、特定のコールタイプのユーザの合計数を示しています。このコマンドは、内部的に **show pdsn session service-option [so] summary** を使用し、出力を解析します。

次の例は、表示内容の抜粋です。

```
Select Service type:
1.  EVDO
2.  1xRTT
3.  Quit
Enter the service Type choice from the above menu (1/2/3): 1
```

```
SHOW SUBSCRIBER SUMMARY <-> With CallType Option 59
-----
Total Number of sessions with service option 59:121
Total Number of Paks in :124122
Total Number of Paks out :128128
Total Number of bytes in :1985366
Total Number of bytes out :3744118
```

## Show Subscriber Verbose with NAI

このコマンドは、NAI 内の特定のストリングを持つ加入者を示しています。たとえば、NAI に「ptt」がある、push to talk の加入者を表示することができます。このコマンドは、内部的に **show cdma pdsn session user \*ptt\* detail** を使用し、出力を解析します。この場合、NAI で「ptt」ストリングが一致するバインディングだけを返します。

SUP カードに大量のデータが送信されるため、一致する基準に応じて、ポリシーがデータを処理するには長時間かかります。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超えている場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**ftftp://ftftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。



(注)

このポリシーは、1 PCOP あたりの加入者の合計数が 1000 を超える場合は、加入者を画面に表示できません。しかし、このファイル オプションは機能しています。

次の例は、表示内容の抜粋です。

```
>> Now enter the NAI (wild-carded or specific): *_osler*
----- Slot 1/CPU 5, show cdma pdsn session user *_osler* detail-----
```

```
Mobile Station ID IMSI 09003000053
  PCF IP Address 6.6.6.5, PCF Session ID 51
  A10 connection time 00:01:37, registration lifetime 65535 sec
  Number of successful A11 reregistrations 0
  Remaining session lifetime INFINITE
  Always-On not enabled for the user
  Current Access network ID 0006-0606-05
  Last airlink record received is Active Start, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 14, receive 0
  Using interface Virtual-Access2.3, status OPN
  Using AHDLC engine on slot 0, channel ID 11
  Service Option EV-DO Flow Discrimination 0 DSCP Included 0
  Flow Count forward 0 reverse 0
  This session has 1 flow
  This session has 0 service flows
  Session Airlink State Active
```

```
This session has 0 TFTs
Qos subscriber profile
  Max Aggregate Bandwidth : 1
  Inter User Priority : 1000
  Maximum Flow Priority : 120980
  Forward profile-id : 4660
  Forward profile-id : 9097
  Forward profile-id : 14454
```

```

Reverse profile-id : 6295
Reverse profile-id : 17185
Bidirectional profile-id : 22136
Bidirectional profile-id : 26505

Flow service Mobile, NAI scdma_osler3@ark.com
Mobile Node IP address 9.9.9.2
HA IP address 5.5.5.2
Packets in 0, bytes in 0
Packets out 0, bytes out 0

Qos per flow : scdma_osler3@ark.com
Max Aggregate Bandwidth : 1
Inter User Priority : 1000
Maximum Flow Priority : 120980
Number of Persistent Tft : 34567
Forward profile-id : 4660
Forward profile-id : 9097
Forward profile-id : 14454
Reverse profile-id : 6295
Reverse profile-id : 17185
Bidirectional profile-id : 22136
Bidirectional profile-id : 26505

```

## Show Subscriber Brief with NAI

このコマンドは、NAI 内の特定のストリングを持つ加入者を示しています。たとえば、NAI に「ptt」がある、push to talk の加入者を表示することができます。このコマンドは、内部的に **show cdma pdsn session user \*ptt\* brief** を使用し、出力を解析します。この場合、NAI で「ptt」ストリングが一致するバインディングだけを返します。

ポリシーは、初めに **summary** コマンドを実行し、PCOP ごとにユーザをチェックします。加入者数が端末ディスプレイの推奨数を超過している場合、このファイル オプションを選択する必要があります。このファイル オプションを選択しない場合、PCOP は無視されます。

IOS CLI コマンドの **show cdma pdsn session detail** を、この目的で使用することができます。**ftftp://ftftp-ip/user/[dir]/PPC3-SLOTNumber-subs-[date-time].txt** が、すべてのデータを TFTP サーバ上にあるファイルに収集するために使用されます。



(注)

このポリシーは、1 PCOP あたりの加入者の合計数が 1000 を超える場合は、加入者を画面に表示できません。しかし、このファイル オプションは機能しています。

次の例は、表示内容の抜粋です。

```

>> Now enter the NAI (wild-carded or specific): osler*

----- Slot 1/CPU 5, show cdma pdsn session user osler* brief-----
MSID          PCF IP Address      PSI      Age  St SFlows Flows Interface
09003000051   6.6.6.2             51 00:01:35 OPN      0    1 Virtual-Access2.2

```

## Show Subscriber Summary With NAI

このコマンドは、NAI 内の特定のストリングを持つ加入者を示しています。たとえば、NAI に「ptt」がある、push to talk の加入者を表示することができます。このコマンドは、内部的に **show cdma pdsn session user \*ptt\* summary** を使用し、出力を解析します。この場合、NAI で「ptt」ストリングが一致するバインディングだけを返します。

次の例は、表示内容の抜粋です。

```

>> Now enter the NAI (wild-carded or specific): osler1*

```

```

SHOW SUBSCRIBER SUMMARY <-> (Matching NAI: osler1*)
-----
Total   Number of sessions with user osler1* :121
Total   Number of Paks in :124644
Total   Number of Paks out :128650
Total   Number of bytes in :1993718
Total   Number of bytes out :3759382

```

## Monitor Subscriber コマンド

Osler は、加入者のトレースのためにすべてのタスクを実行するトレース コマンドを実装しています。加入者は NAI または IMSI に基づいて識別されます。

加入者をトレースするために、ポリシーは、アクティブまたはスタンバイ PDSN を実行するプロセッサ上で複数の CLI コマンドを呼び出し、その加入者の既存の IOS CLI を使用して、条件付きデバッグを設定します。

条件付きデバッグのセットは、セッション、アカウントリング、MIP、PMIP、VPDN、および TFT に基づいています。その結果、プロセッサ上で複数のコマンドが呼び出されます。すべてのプロセッサでデバッグ条件を設定する必要はありません。

monitor コマンドは、各 SAMI プロセッサ モード コマンド **debug condition [username | calling] {NAI | IMSI}** を設定して、自分の名前または NAI をトレースに含める処理をイネーブルにする必要があります。



**(注)** VPDN および PDSN の場合、IMSI ベースの条件付きデバッグは、Osler version 1.0 ではサポートされません。

次のコマンドには、NAI または IMSI に基づいて加入者のトレースを開始するオプションがあります。



**(注)** 加入者のトレースを開始するには、すべてのアクティブおよびスタンバイ PDSN インスタンスで **start subscriber tracing** コマンドでトレース条件を設定します。フラッドを回避するには、まずすべての PDSN インスタンスでトレース条件を設定してから、PDSN 固有のトレースを設定します。

SUP-7600#traces

NAI ベースのトレースでは、トレース コマンドに次のコマンドを使用してトレース条件を設定します。

**trace condition**

**debug condition username [NAI]**

IMSI ベースのトレースでは、トレース コマンドに次のコマンドを使用してトレース条件を設定します。

**trace condition**

**debug condition calling [IMSI]**

show debug condition を設定するには、設定モードで **cdma pdsn debug show-conditions** コマンドを使用します。デバッグ条件を表示する MIP および PMIP デバッグの場合、設定モードで **ip mobile debug include username** コマンドを使用します。

アプリケーション固有のトレースは次のように設定します。:

**application specific traces**

Session

**debug cdma pdsn a11**

**debug cdma pdsn session**  
**debug ppp negotiation**  
**debug radius authentication**  
 Accounting  
**debug radius accounting**  
**debug cdma pdsn accounting**  
 TFT  
**debug cdma pdsn rsvp**  
**debug cdma pdsn tft**  
 VPDN  
**debug vpdn l2x-errors**  
**debug vpdn l2x-events**  
 MIP  
**debug ip mobile**  
 PMIP  
**debug ip mobile proxy**

PDSN インスタンスのデバッグ後に、トレース コマンドで、スーパーバイザ カードのローカル ディスクにトレース ログ ファイルを作成し、トレースをダンプします。また、端末にもトレースが表示されます。

トレース コマンドは、**trace stop** 要求を受信するか、トレース コマンドのレジストレーション時間が期限切れ（デフォルトは 1 時間）になるまで、加入者のトレースを継続的に収集します。**trace stop** 要求を受信すると、加入者のトレースは停止し、加入者のトレースを開始するときに設定されたトレース条件はリセットされます。

## 加入者トレースの停止

トレースを停止するときに、単一の加入者に **trace stop** 要求を送信してトレースを停止できます。**trace stop** 要求には、トレース ログ ファイルの外部ホストへに転送に関する情報が含まれるため、PDSN が **trace stop** 要求を対応するトレース セッションに送信する前に、この情報を確認する必要があります。

**trace stop** 要求でトレース ログ ファイルを外部ホストに転送する必要がある場合、トレース コマンドでトレース ログ ファイルを外部ホストに転送し、スーパーバイザ カードのローカル ディレクトリからトレース ログを削除します。

**trace stop** 要求でトレース ログ ファイルを外部ホストに転送する必要がある場合、トレース コマンドはスーパーバイザ カードのローカル ディレクトリにトレース ログ ファイルを保持します。

## 加入者トレース セッションの表示

トレース コマンドを使用して、システムのすべての既存トレース セッションに関する情報を表示できます。

このオプションは、既存トレース セッションの数と、トレースをイネーブルにしている加入者のリストを表示します。Osler トレース条件に関する情報を表示するには、すべての PDSN インスタンス上で、このオプションから CLI コマンド **show debugging** を呼び出します。

## すべての加入者トレース セッションのクリア

既存のトレース セッションをすべてクリアすることもできます。

トレース セッションをクリアする前に、このオプションでシステムのすべての既存トレース セッションに関する情報を表示します。

`trace clear session` 要求には、トレース ログ ファイルの外部ホストへの転送に関する情報も含まれるため、PDSN が `trace clear session` 要求を送信する前に、この情報を確認する必要があります。

`clear trace session` 要求の送信後に、特定の NAI または割り当てられた IP アドレスについて、すべてのアクティブおよびスタンバイ PDSN インスタンスからポリシーの条件付きデバッグを削除します。

デバッグ条件が 1 つしか存在しない場合、まずアプリケーション固有のトレースを削除してトレースのフラッディングを回避してから、条件を削除します。

システムにアクティブなトレース セッションがない場合、PDSN インスタンスにクリアされていない Osler トレース条件があれば、それをリセットするメカニズムがこのオプションに用意されています。



(注)

このオプションには、アクティブなトレース セッションまたはクリアされていないトレース セッションをすべてクリアするメカニズムが用意されています。そのため、このオプションで、シャーマシ上の Osler トレース ファシリティ全体がリセットされます。

## トレースの表示

加入者のトレースを開始した後、トレース コマンドは継続してシステム ログからトレースを読み取ります。トレース コマンドは、トレース ログ ファイルのトレースをロギングし、端末にトレースを表示する一方で、タイムスタンプとプルに基づいてトレースを再フォーマットして分類します。プロトコル内では、加入者からの特定の要求の処理段階に基づいて、トレースが下位分類されます。

## トレース モード

Osler は `brief` モードと `verbose` モードの加入者のトレース機能を実装しています。この `brief` モードには重要なトレースだけが含まれ、`verbose` モードにはすべての加入者のトレースが含まれます。すべての `brief` モード トレースは、1 つの個別のデータベース ファイルに保守されます。さらに多くのトレースを取得する場合、データベース ファイルにトークンを追加できます。事前に定義されたトークンは、`brief` トレースのデフォルト トークンです。新しいトークンを追加するには、特定のトピックの新しい行に追加します。

## プロトコルの選択

Osler には、`Session`、`Accounting`、`TFT`、`MIP`、`PMIP`、および `VPDN` の各プロトコルに対する加入者のトレース機能があります。そのため、特定のプロトコルについてだけ加入者をトレースできます。

トレース コマンドでトレースを開始するときに、`Session`、`Accounting`、`TFT`、`MIP`、`PMIP`、および `VPDN` から 1 つまたは複数のプロトコルを選択することもできます。また、選択したプロトコルについてだけ、トレース条件をイネーブルにし、ロギングし、条件を表示することができます。

## その他の条件

トレースは継続的なプロセスなので、CPU リソースが消費されます。そのため、CPU 要件を満たすには、トレース コマンドで次のチェックを実行します。

- スーパーバイザ カードの空きディスク容量が 20% 未満になると、警告を返します。空きディスク容量が 20% 未満の場合、トレース コマンドはトレースを開始しません。

- スーパーバイザカードのローカルトレースディレクトリに 51 個以上のトレースログファイルがあると、トレースコマンドは最も古いトレースログファイルが外部ホストに転送され、ローカルスーパーバイザトレースディレクトリからファイルが削除されてから、加入者のトレースが開始されます。
- スーパーバイザカードで重大度 7 でロギングコンソールがイネーブルにされている場合、トレースコマンドはトレースを開始しません。
- **debug all** がスーパーバイザカードでイネーブルの場合、トレースコマンドはトレースを開始しません。
- トレースを開始する前に、トレースコマンドはロギングコンソールコマンドを追跡するアプレットを設定する必要があります。そのため、ロギングコンソールコマンドでスーパーバイザカードを設定する場合は常に、アプレットから **trace stop** 要求をすべての既存トレースセッションに送信します。
- トレースを開始する前に、トレースコマンドで、**debug all** コマンドを追跡するようにアプレットを設定します。そのため、**debug all** をイネーブルにするときは常に、アプレットから **trace stop** 要求をすべての既存トレースセッションに送信します。

## 加入者セッションの表示

CLI コマンドまたはスクリプトコマンドがこのモジュールの一部として実装され、加入者をホストしているサービスブレードを決定し、そのサービスブレード上で IOS CLI を実行してから、結果を照合し、単一の一貫した出力フォーマットで提示できます。

このモジュールは、すべてのアクティブな SAMI カードで次の CLI を実行し、セッションを保持しているカードからセッションとアカウントの詳細を取得します。

条件としての NAI の CLI コマンドは次のとおりです。

```
pdsn# show cdma pdsn session user NAI detail
```

```
pdsn# show cdma pdsn accounting user NAI
```

条件としての IMSI の CLI コマンドは次のとおりです。

```
pdsn# show cdma pdsn session msid IMSI_value detail
```

```
pdsn# show cdma pdsn accounting session IMSI_value
```

条件としての Mobile Node (MN) IP アドレスの CLI コマンドは次のとおりです。

```
pdsn# show cdma pdsn session mn-ip-address IP-Address detail
```

```
pdsn# show cdma pdsn accounting mn-ip-addr IP-Address
```

次の例は、コマンド **showSession** の表示内容の抜粋です。

```
pdsn-osler# showSession
Subscriber IP Address/NAI/IMSI: osler1@cisco.com

##### SUBSCRIBER SESSION FOUND #####

User ID: osler1@cisco.com      [Slot:1 CPU:3]
Session Details:
  Mobile Station ID IMSI 09003000001
  PCF IP Address 6.6.6.2, PCF Session ID 1
  A10 connection time 00:00:12, registration lifetime 65535 sec
```

```

Number of successful All reregistrations 0
Remaining session lifetime INFINITE
Always-On not enabled for the user
Current Access network ID 0006-0606-02
Last airlink record received is Active Start, airlink is active
GRE protocol type is 0x8881
GRE sequence number transmit 14, receive 7
Using interface Virtual-Access2.1, status OPN
Using AHDLC engine on slot 0, channel ID 3
Service Option EV-DO Flow Discrimination 0 DSCP Included 0
Flow Count forward 0 reverse 0
This session has 1 flow
This session has 0 service flows
Session Airlink State Active
This session has 0 TFTs
Qos subscriber profile
Max Aggregate Bandwidth : 1
Inter User Priority : 1000
Maximum Flow Priority : 120980
Forward profile-id : 4660
Forward profile-id : 9097
Forward profile-id : 14454
Reverse profile-id : 6295
Reverse profile-id : 17185
Bidirectional profile-id : 22136
Bidirectional profile-id : 26505
Flow service Simple, NAI osler1@cisco.com
Mobile Node IP address 4.4.4.1
Packets in 0, bytes in 0
Packets out 0, bytes out 0
Qos per flow : osler1@cisco.com
Max Aggregate Bandwidth : 1
Inter User Priority : 1000
Maximum Flow Priority : 120980
Number of Persistent Tft : 34567
Forward profile-id : 4660
Forward profile-id : 9097
Forward profile-id : 14454
Reverse profile-id : 6295
Reverse profile-id : 17185
Bidirectional profile-id : 22136
Bidirectional profile-id : 26505

```

Accounting Details:

```

UDR for session
session ID: 1
Mobile Station ID IMSI 09003000001
A - A1:09003000001 A2: A3:
C - C3:0
D - D3:6.6.6.2 D4:000000000000
E - E1:0000
F - F1:00F1 F2:00F2 F5:003B F6:F6 F7:F7 F8:F8
F9:F9 F10:FA F14:00 F15:0
F16:00 F17:00 F18:00
F19:00 F20:00 F22:00
G - G3:0 G8:0 G9:1 G10:0 G11:0 G12:0
G13:0 G14:245 G15:0 G16:270 G17:0
I - I1:0 I4:0
Y - Y2:1
UDR for flow
Mobile Node IP address 4.4.4.1
B - B1:4.4.4.1 B2:osler1@cisco.com
C - C1:000F C2:7 C4:0
D - D1:0.0.0.0

```



```
F - F11:01 F12:00 F13:00
G - G1:0 G2:0 G4:1232699771
G22:0 G23:0 G24:0 G25:0
Packets- in:0 out:0
```



(注) **showSession** コマンドの実行後に、特定の加入者に関するセッション情報を検索するには、NAI、IP アドレス、または IMSI を入力する必要があります。

## バルク統計情報の収集

統計情報は、シスコ製ルータで使用できる SNMP MIB バルク統計情報機能で収集されます。コントロール プロセッサの SNMP MIB オブジェクトリストは、Osler スクリプトを利用して設定します。バルク統計情報機能をイネーブルにした後は、指定した間隔で統計情報を収集し、設定した TFTP サーバに送信します。FTP ファイル転送が失敗する場合、統計情報はセカンダリ URL に指定された SUP ディスクに送信されます。

### Start Bulk Statistics

このコマンドは、すべてのコントロール プロセッサ上で SNMP MIB オブジェクトを設定します。このコマンドを実行しているときは、Telnet 接続は使用しないでください。使用すると、各 PCOP 上で SNMP MIB を設定できません。このコマンドでアクティブな各 PCOP に対して Telnet セッションを確立し、転送パラメータ、オブジェクトリスト、スキーマ定義など、多様な SNMP オプションを設定します。最後に、統計情報の収集をイネーブルにします。

バルク統計情報の定期的なレポートをイネーブルにするには、**startStats** コマンドを実行する必要があります。次の例は、表示内容の抜粋です。

```
pdsn-osler# startStats
mwtcp-PDSN_SUP-ftb6#startStats
Address or name of remote host to dump statistics[9.11.44.1]?
Directory path on remote host[raseshad/stats]?
Directory path on local host[disk0:/stats]?
Statistics dumping periodicity (in minutes)[30]?
Add MIP object names for statistics reporting? [y/n]y <<<<<
Add VPDN object names for statistics reporting? [y/n]y <<<<<
Collecting Cisco Object Names for Statistics Reporting ....

#####
Configuring Slot:1, Processor:3...
#####

Successfully enabled bulk stats reporting for Slot:1, Processor:3

#####
Configuring Slot:2, Processor:3...
#####

Successfully enabled bulk stats reporting for Slot:2, Processor:3

#####
```

## Stop Bulk Statistics

このコマンドは、すべてのコントロール プロセッサ上にある SNMP MIB オブジェクトの設定を削除します。このコマンドを実行しているときは、どのプロセッサに対しても **telnet** を使用しないでください。使用すると、プロセッサから SNMP MIB オブジェクトの設定を削除できません。アクティブな各 PCOP に対する **telnet** セッションは、統計情報の収集をディセーブルにし、コントロール プロセッサからすべての設定を削除します。

バルク統計情報の定期的なレポートをディセーブルにするには、**stopStats** コマンドを実行する必要があります。次の例は、表示内容の抜粋です。

```
pdsn-osler# stopStats
Stopping periodic bulk statistics collection and dumping...

#####
Configuring Slot:1, Processor:3...
#####

Successfully stopped the periodic bulk stats reporting for Slot:1, Processor:3

#####
Configuring Slot:2, Processor:3...
#####

Successfully stopped the periodic bulk stats reporting for Slot:2, Processor:3

#####

Successfully stopped the periodic reporting of bulk statistics for all active CPs!
```



### ワンポイントアドバイス

スーパーバイザ モジュールから **Osler** をアンインストールする前に、統計情報のレポートを停止してください。そうしないと、すべてのアクティブな PCOP からの統計情報のレポートを手動で停止する必要があります。

## Update Statistics Mapping File

新しい OID をマッピング ファイルに追加します。マッピング ファイルには、そのシスコ オブジェクト名、ベンダー オブジェクト名、およびオブジェクト ID が指定されたすべての OID が含まれます。グローバル統計情報に含める必要がある新しい OID でマッピング ファイルを更新するには、**upStatsMap** コマンドを実行します。

次に、**upStatsMap** コマンドの出力例を示します。

```
pdsn-osler# upStatsMap
Enter the Cisco Object Name: cCdmaServiceOptionSucesses
Enter the SNMP OID: 1.3.6.1.4.1.9.9.157.1.7.6.2.1.3
Enter the Vendor Object Name: ServiceOptionSucesses
Updating the mapping file disk0:/pdsn_osler/pdsn_Mappings.txt...
Done !!
```

Cisco PDSN リリース 5.1 の Osler Support 用設定コマンドについて詳しくは、『*Command Reference for Cisco PDSN Release 5.0 in IOS Release 12.4(22)XR1*』を参照してください。

## 改善されたスループットとトランザクション処理

今回のリリースでは、スループットが改善され、PDSN で 3 Gbps の配信が可能になりました。次の条件の場合にスループットを 3 Gbps に改善できます。

- セッションの 80% が 1 セッションだけで、1xRTT トラフィックを示しています。
  - このトラフィックの CPS は 20 です。
  - 平均スループットまたはユーザは 12.5 kbps です。
  - 平均パケット サイズは 1440 バイトです。
- セッションの 20% は平均して 2 フローか Point-to-Point Protocol (PPP; ポイントツーポイントプロトコル) セッションで、Rev A トラフィックを示しています。
- Rev A トラフィックの 10% は QoS がイネーブルです。
  - このトラフィックの CPS は 5 です。
  - 平均スループットまたはユーザは 100 kbps です。
  - 平均パケット サイズは 384 バイトです。

すべてのスループット パラメータは **No Drop Rate (NDR)** で、10,000 分の 1 パケットのドロップが許容されています。

## 単一 IP ブレードのクラスタ コントローラのサポート

今回のリリースで、単一 IP ブレードのクラスタ コントローラがサポートされました。クラスタ コントローラによって PDSN クラスタ メンバのリソース使用量が減るため、クラスタの容量が改善されます。

次の章では、以下の内容について説明します。

- [「PDSN のクラスタ処理アーキテクチャ」](#)
- [「クラスタ コントローラの機能」](#)
- [「クラスタ コントローラのメトリック」](#)
- [「メンバとコントローラ間のメトリック」](#)
- [「クラスタ コントローラの下位互換性」](#)
- [「コントローラの冗長性」](#)
- [「クラスタ コントローラ サポートの設定」](#)

## PDSN のクラスタ処理アーキテクチャ

次のフローは、PDSN のクラスタ処理アーキテクチャを示しています。

- シャーシ上の PCOP の 1 つは、PDSN メンバとして機能し、さらにコントローラとして動作するように設定されます。この PCOP 単体に、コントローラとメンバの機能が共存しています。単一 IP は、メンバの機能のためだけです。
- コロケーション コントローラまたはメンバの場合、コントローラおよびメンバは同じ CDMA-Ix 1 IP アドレスを共有します。
- コントローラ IP アドレス宛てのすべてのパケットは、コロケーション メンバ上でセッションがホストされていなければ、IXP 上のデフォルト ケースに従い、PCOP に送信されます。このような場合、IXP は A11 RRQ を適切な TCOP に直接転送します。コントローラはセッション マネージャの IMSI データベースを共有します。
- セッション マネージャは、保存している各 IMSI に対して、メンバ IP アドレスおよび TCOP アドレスの両方、または TCOP アドレスを持っています。セッション マネージャは、他のメンバの IMSI について、メンバの IP アドレスを保存します。同じブレードでホストされている IMSI の場

合、セッション マネージャには TCOP アドレスがあります。レコードはコントローラおよびコロケーション メンバのために再利用されるため、コロケーション メンバを禁止しても、レコードはクリアされません。ただし、負荷の選択でコロケーション メンバは考慮されません。

- コロケーション メンバからのセッションのアップまたはセッションのダウンは、個別のメッセージではなく、コントローラに直接通知されます。そのため、定期的な更新は、コロケーション メンバおよびコントローラに対して影響がありません。
- 単一 IP セッション マネージャが処理時にパケットをキュー処理するため、メンバのキュー処理は必要ありません。
- コロケーション メンバおよびコントローラは同じインターフェイスを共有します。コロケーション メンバがあるスタンドアロン コントローラでは、コントローラ IP はオプションです。コントローラ IP は、コントローラの冗長性では HSRP アドレスで、以前のリリースでは必須でした。
- シャーシの他の PCOP は、メンバとしてだけ動作します。

## クラスタ コントローラの機能

クラスタ コントローラのコール フローは、PCF から A11 RRQ を受信することから始まります。コントローラは、A11 RRQ を受信すると、IMSI に関してセッションが存在するかどうかをチェックします。セッションが存在しない場合、コントローラは負荷に基づいてメンバを選択します。負荷テーブルはコントローラによって保守され、すべての登録済みメンバの負荷が含まれます。

選択したメンバが別のブレードにある場合、コントローラはセッション マネージャで一時的なキューに IMSI を追加し (controller-periodic が設定されている場合)、A11 を拒否します。

次に、PCF は A11 RRQ を提案されたメンバに再送信します。選択したメンバでセッションがアップ状態になると、メンバは IMSI に session-up を送信します。コントローラは、メンバからの session-up を処理するときに、セッション マネージャで IMSI を永続化します。負荷に基づいて選択されたメンバは共存するメンバであり、A11 RRQ がセッション マネージャに送信されます。

ハンドオフ中に、新しい PCF がコントローラに A11 RRQ を送信し、コントローラは IMSI を検索します。

セッション マネージャは、ホストされるメンバ IP アドレスと共に IMSI を返します。

IMSI がメンバに存在する場合、コントローラは、ホストされているメンバの IP アドレスと共に reject メッセージを送信します。セッション マネージャが TCOP アドレスを返す場合、コントローラは A11 RRQ をセッション マネージャに転送し、セッション マネージャは選択した TCOP に転送します。

## クラスタ コントローラのメトリック

PCOP および TCOP 間に使用されるロード バランシング メトリックは、Dynamic Feedback Protocol (DFP; ダイナミック フィードバック プロトコル) に沿っています。TCOP は、TCOP 全体の重み付けを計算し、PCOP に送信します。PCOP はその重み付けに基づいてロード バランシングを実行します。

また、同じメトリックがメンバとコントローラにも拡張されます。

$$\text{Weight} = \frac{(\text{MaxSessions} - \text{NumberOfSessions})}{\text{MaxSessions}} (\text{cpu} + \text{mem}) * \frac{\text{dfp\_max\_weight}}{32}$$

dfp\_max\_weight のデフォルト値は 100 です。これはリリース 4.0 がパーセントに基づいているためです。そのため、報告される重み付けは、dfp\_max\_weight (負荷がない場合) からゼロ (負荷が最大の場合) です。

CPU およびメモリ使用率は 0 ~ 16 の範囲に変換され、重み付けの計算に含まれます。CPU が 100% の使用率に達すると、報告される重み付けはゼロになり、その期間はメンバに対するリダイレクトは発生しなくなります。パフォーマンス テストが完了した後に、DFP パラメータが調整されます。

使用できる帯域幅が合計の設定帯域幅に達すると、ゼロという重み付けが送信されます。TCOP はこのメトリックを PCOP に送信します。



(注) 最大の CPU 値は、100% まで設定できます。デフォルト値は 90% です。デフォルト値 (90%) を設定しても、実行コンフィギュレーションでは表示されません。

## メンバとコントローラ間のメトリック

コントローラはパーセントに基づいており (Cisco PDSN リリース 4.0 に基づきます)、0 が軽く、100 が最大の重さと想定しています。コントローラに送信されるときにこのロジックを保持するために、統合された重み付けは反転され、パーセントに変換されます。そのため、メンバがデータを送信するとき、0 については軽い負荷がかけられ、100 については重い負荷がかけられます。

統合された重み付けは、最も負荷が少ない TCOP の重み付けです。セッションの最大数またはブレードの最大帯域幅に達すると、負荷は 100 (重い負荷) とレポートされます。

コントローラとメンバ間で使用されるメトリックは、Cisco PDSN リリース 3.0 と リリース 4.0 で異なります。下位互換性を維持するために、新しいメンバは負荷の拡張も使用します。また、セッションカウントおよび最大セッション カウントは「短い」(2 バイト) フィールドです。メンバはブレード全体を扱うようになったため、セッション カウントと最大セッション カウントは、メンバの制限を超えます。そのため、拡張を再利用し、さらに新しく定義された重み付けで置換する必要があります。

負荷の拡張のアトリビュートは次のとおりです。

- セッション カウントは重み付けです。
- 最大セッション カウントは、メンバ上の最大 DFP 重み付け (100) です。
- パーセントは、重み付けのパーセントです。

## クラスタ コントローラの下位互換性

PDSN\_LOAD 拡張の最大の重み付け (または以前の最大セッション カウント) は 2 バイトだけでした。また、ブレードの容量はほぼ 200,000 セッションです。以前のバージョンの PDSN では、セッション カウント拡張を使用できません。

セッション負荷の CVSE を再利用すると、Cisco PDSN リリース 3.0 または リリース 4.0 のコントローラはそれをセッション カウントと仮定します。そのため、メンバセッション カウントがゼロになると、コントローラはセッション レコードをフラッシュします。Cisco PDSN リリース 5.1 では、メンバセッション カウントは重み付けです。また、サービス セッションでは PDSN メンバの初期フェーズの重み付けがゼロになる可能性があります。レポートされる重み付けがゼロのときに、以前のリリースのコントローラによるクリア処理を回避するには、計算される重み付けがゼロで、まだセッションのサービスがある場合に、新しい PDSN リリース 5.0 メンバから 1 の重み付けを送信します。

ここでは、コントローラおよびメンバの多様な組み合わせのシナリオについて説明します。

### ケース 1 : 3.0 コントローラと 5.0 メンバ

セッション カウント CVSE で負荷が送信されると、Cisco PDSN リリース 3.0 コントローラは、セッション カウントに基づいて処理を進めます。しかし、ラウンドロビンを選択することをお勧めします。

**ケース 2 : 4.0 コントローラと 5.0 メンバ**

Cisco PDSN リリース 3.0 コントローラと同様に、セッション カウント CVSE が考慮され、コントローラの処理が継続されます。しかし、ラウンドロビンを選択することをお勧めします。

**ケース 3 : 5.0 コントローラと 3.0 メンバ**

メンバはセッションに関してだけ負荷を報告します。負荷はパーセントとして計算され、使用されます。

**ケース 4 : 5.0 コントローラと 4.0 メンバ**

Cisco PDSN リリース 4.0 コントローラはデータを解釈し、パーセントで重み付けを収集します。この重み付けをメンバに使用する必要があります。

**コントローラの冗長性**

単一 IP の場合、コントローラの冗長性に影響はありません。スタンバイ コントローラを設定する場合、ブレード全体が冗長性のために使用されます。単一 IP では、ブレードのプロセッサがリロードされると、ブレード全体がリロードされます。そのため、単一 IP では、ブレードでもセッションの冗長性を設定する必要があります。この設定で、アクティブ ブレード上のすべてのメンバ機能が、スタンバイ ブレードに同期されます。

**クラスタ コントローラ サポートの設定**

次の例は、クラスタ コントローラ設定の抜粋を示しています。

```
pdsn# show cdma pdsn cluster controller configuration
cluster interface GigabitEthernet0/0.341 (collocated)
no R-P signaling proxy
timeout to seek member = 10 seconds
window to seek member is 2 timeouts in a row if no reply (afterwards the member is
declared offline)
default: spi 101, Timestamp +/- 0, key ascii hello
this PDSN cluster controller is configured
```

Controller maximum number of load units = 100

次の例は、クラスタ コントローラ メンバ設定の抜粋を示しています。

```
pdsn# show cdma pdsn cluster member configuration
cluster interface GigabitEthernet0/0.341
IP address of controller is 11.1.1.50 (collocated)
no prohibit administratively
timeout to resend status or seek controller = 10 sec or less, randomized
resend a msg for 2 timeouts sequentially if no reply, then inform operator
default: spi 101, Timestamp +/- 0, key ascii hello
this PDSN cluster member is configured
```

**クラスタ コントローラ メンバ設定**

次の例は、クラスタ コントローラ メンバ設定の抜粋を示しています。

```
cdma pdsn cluster controller interface GigabitEthernet0/0.20
cdma pdsn cluster controller standby PDSN-ssp2-43-RP
cdma pdsn cluster controller timeout 120
cdma pdsn cluster controller member periodic-update
cdma pdsn cluster member controller 20.2.43.254
cdma pdsn cluster member interface GigabitEthernet0/0.20
cdma pdsn cluster member timeout 120
```

```
cdma pdsn redundancy
```

コントローラでメンバの選択のために **round-robin** メソッドをイネーブルするには、**cdma pdsn cluster controller member selection-policy round-robin** コマンドをイネーブルする必要があります。

次の例は、クラスタ メンバ設定の抜粋を示しています。

```
cdma pdsn cluster member controller 20.2.43.254
cdma pdsn cluster member interface GigabitEthernet0/0.20
cdma pdsn cluster member timeout 120
cdma pdsn cluster member periodic-update 300
```

また、上記のように設定されている場合の **show** コマンドの出力内容を示します。

コントローラの場合：

```
PDSN-controller-member# show cdma pdsn cluster controller configuration
cluster interface GigabitEthernet0/0.20 (collocated)
no R-P signaling proxy
timeout to seek member = 10 seconds
window to seek member is 2 timeouts in a row if no reply (afterwards the member is
declared offline)
default: spi 300, Timestamp +/- 0, key ascii cisco
this PDSN cluster controller is configured
```

コントローラの冗長性の場合：

```
database in-sync or no need to sync
group: PDSN-ssp2-43-RP
Controller maximum number of load units = 100
```

コロケーション メンバの場合：

```
PDSN-controller-member# show cdma pdsn cluster member configuration
cluster interface GigabitEthernet0/0.20
IP address of controller is 20.2.43.254 (collocated)
no prohibit administratively
timeout to resend status or seek controller = 120 sec or less, randomized
resend a msg for 2 timeouts sequentially if no reply, then inform operator
default: spi 300, Timestamp +/- 0, key ascii cisco
this PDSN cluster member is configured
```

リモート メンバの場合：

```
PDSN-cluster-member# show cdma pdsn cluster member configuration
cluster interface GigabitEthernet0/0.20
IP address of controller is 20.2.43.254
no prohibit administratively
timeout to resend status or seek controller = 120 sec or less, randomized
resend a msg for 2 timeouts sequentially if no reply, then inform operator
default: spi 300, Timestamp +/- 0, key ascii cisco
this PDSN cluster member is configured
```

## IMSI および PCF のリダイレクション

今回のリリースでは、クラスタ コントローラとスタンドアロン PDSN の両方で、International Mobile Subscriber Identifier (IMSI) および Packet Control Function (PCF; パケット制御機能) のリダイレクションをサポートしています。トラブルシューティングの場合にこの機能を使用すると、コールを特定の PDSN 宛てに送信できます。また、この機能を使用して、IMSI の特定の行範囲を異なる PDSN セットに送信できます。

次の章では、以下の内容について説明します。

- 「IMSI ベースのリダイレクション」
- 「PCF ベースのリダイレクション」
- 「IMSI および PCF ベースのリダイレクション」
- 「コントローラ PDSN の機能」
- 「IMSI および PCF ベースのリダイレクションの制限」

## IMSI ベースのリダイレクション

クラスタ コントローラに IMSI ベースのリダイレクションをクラスタ コントローラ、メンバ、またはスタンドアロン PDSN に追加すると、特定の IMSI またはある範囲の IMSI から、設定済みのメンバまたはメンバ以外の PDSN IP に、A11 レジストレーション要求 (RRQ) がリダイレクトされます。

## PCF ベースのリダイレクション

PCF ベースのリダイレクション機能を、クラスタ コントローラ、メンバ、またはスタンドアロン PDSN に追加できます。PCF ベースのリダイレクションを追加すると、特定の PCF またはある範囲の PCF から、設定済みのメンバまたはメンバ以外の PDSN IP に A11 RRQ がリダイレクトされます。

## IMSI および PCF ベースのリダイレクション

ここでは、IMSI および PCF ベースのリダイレクションに共通の機能について説明します。どちらのリダイレクションも、ストレージと検索について同じ機能に従います。ただし、IMSI ベースの検索は、PCF ベースのリダイレクションの前に実行されます。そのため、IMSI ベースのリダイレクションの方が、PCF ベースのリダイレクションよりも優先されます。

IMSI および PCF ベースのリダイレクションのワークフローは、A11 RRQ の受信から始まります。PDSN は A11 RRQ を受信すると、その IMSI についてセッションが存在するかどうかをチェックします。セッションが存在する場合、パケットは通常の A11 処理で扱われます。セッションが存在しない場合、A11 RRQ から派生した IMSI で設定された IMSI リダイレクション テーブルで一致が検索されます。一致を特定すると、未知の HA のもとで 0x88H (小数点以下 136 桁) のコードを満たす、一致した PDSN IP を使用して、11 RRQ が拒否されます。

一致が見つからない場合、A11 RRQ の PCF IP アドレスで設定された PCF リダイレクション テーブルで一致が検索されます。一致を特定すると、未知の HA のもとで 0x88H (小数点以下 136 桁) のコードを満たす、一致した PDSN IP を使用して、11 RRQ が拒否されます。IMSI および PCF リダイレクション テーブルに一致が見つからない場合、または PCF または IMSI リダイレクションが設定されていない場合、A11 RRQ は通常の A11 処理で扱われます。

IP アドレスの範囲または IMSI の範囲の設定を削除する場合、範囲全体を削除するには、IP または IMSI の開始値だけを指定できます。設定を削除する場合、IP または IMSI の範囲の上限値を指定していても、PDSN は上限値を無視します。

## IMSI および PCF ベースのリダイレクションの制限

IMSI および PCF ベースのリダイレクションの機能に影響がある制限は次のとおりです。

- IMSI Mobile Identification Number (MIM) と同等の番号をイネーブルにした場合、IMSI リダイレクションの検索中に、PDSN は入力された 10 桁だけを使用します。設定の残りの桁は無視されます。ただし、**show run** コマンドを使用する場合、IMSI MIN と同等の存在に関係なく、このコマンドで入力されたものが示されます。内部で検索に使用される 10 桁の出力は行いません。



- PCF リダイレクション設定で、PCF の範囲で 2 番目の IP アドレスを 0.0.0.0 と指定すると、2 番目の IP アドレスは破棄され、最初の IP アドレスだけが考慮されます。ただし、最初の IP アドレスを 0.0.0.0 と指定すると、CLI コマンドの設定は失敗します。
- IMSI または PCF リダイレクション設定で、CDMA-Ix 1 インターフェイスまたは IP アドレスを設定せずに CLI コマンドを設定しようとすると、リダイレクションは失敗します。ただし、CLI コマンドを使用してリダイレクションを設定した後に、CDMA-Ix 1 インターフェイスを削除すると、CLI コマンドからのリダイレクションは、エラーまたは警告をスローせずに保持されます。
- IMSI または PCF リダイレクション設定で、CDMA-Ix 1 インターフェイスの IP アドレスと等しいメンバ値で CLI コマンドを設定しようとすると、リダイレクション設定は失敗します。ただし、CLI コマンドのリダイレクションを、リダイレクション CLI コマンドで設定したメンバ IP と等しい値で設定した後に、CDMA-Ix 1 インターフェイスの IP アドレスを変更する場合、CLI コマンドからのリダイレクションは、エラーまたは警告をスローせずに保持されます。

## コントローラ PDSN の機能

コントローラ PDSN のワークフローは、A11 RRQ の受信から始まります。PDSN は A11 RRQ を受信すると、その IMSI についてセッションが存在するかどうかをチェックします。セッションが存在する場合、パケットは通常の A11 処理で扱われます。セッションが存在しない場合、PDSN は A11 RRQ から派生した IMSI で設定された IMSI リダイレクション テーブルで一致をチェックします。IMSI リダイレクション テーブルで一致が見つかった場合、A11 RRQ の PCF アドレスが、異なる PCF グループで設定された IP アドレスの範囲内に含まれるかどうかを PDSN がチェックします。PCF グループとの一致がない場合、A11 RRQ はコントローラ ロード バランサに渡され、クラスタで使用できるすべてのメンバからメンバ PDSN が選択されます。

一致を特定すると (IMSI または PCF)、コントローラは PDSN グループを取得します。次に、コントローラは「force」オプションが設定されているかどうかをチェックします。「force」が設定されている場合、コントローラは PDSN で設定されたプライマリ IP と共に A11 Reject を送信します。「force」が設定されていない場合、コントローラは一致した PDSN グループで最も負荷が少ないメンバを使用できるかどうかをチェックします。

グループのすべてのメンバ PDSN がロードされている場合、コントローラは理由「Insufficient Resources」と共に A11 Reject を送信します。コントローラが PDSN グループの最も負荷が少ないメンバを返す場合、その最も負荷が少ないメンバと共に、A11 Reject が送信されます。

IMSI および PCF リダイレクションを設定する前に、次の点に注意してください。

- IP アドレスの範囲を設定せずに PDSN グループを設定すること、および IMSI または PCF リダイレクションの一部として PDSN グループを設定することができます。任意の A11 RRQ がこのリダイレクションに一致する場合、コントローラは理由「Insufficient Resources」と共に A11 Reject を送信します。そのため、PDSN グループを設定する場合、IP アドレスの範囲を指定することをお勧めします。



**注意**

リダイレクションが二重になるため、IMSI または PCF リダイレクションをコントローラおよびメンバの両方で設定しないでください。

- リダイレクション用に設定した PDSN グループで、IP アドレスの範囲を設定した場合、その IP アドレスの範囲は削除しないでください。PCF または PDSN グループをリダイレクション用に設定し、同じ PDSN グループを削除する場合、その PDSN グループに関連付けられたすべての IMSI または PCF リダイレクション設定は設定から削除されます。

- 「force」オプションをイネーブルにしたリダイレクションを PDSN グループに設定し、グループのプライマリ アドレスを削除する場合、リダイレクション設定の対応する「force」オプションは削除されます。PDSN グループでプライマリ アドレスを指定せずに、リダイレクション CLI コマンドで「force」オプションを設定すると、リダイレクション CLI コマンド設定は失敗します。



(注)

「force」オプションが機能するには、PDSN グループにプライマリ アドレスを選択する必要があります。

- プライマリ IP をコントローラ CDMA-Ix 1 アドレスに設定し、メンバとして設定しない場合、A11 RRQ はセッション マネージャを介してローカルの PDSN に対してキュー処理されます。プライマリ IP をコントローラ CDMA-Ix 1 アドレスに設定し、メンバとして設定する場合、A11 RRQ はローカル メンバに対してキュー処理されます。
- PDSN または PCF グループで設定された IP アドレスの範囲が、異なるグループで設定された範囲と一致する場合、設定は失敗し、エラー メッセージが示されます。PDSN または PCF グループで設定された IP アドレスの範囲が同じグループで設定された範囲と一致する場合、古い設定が保持されます。
- あるグループの IP アドレスの範囲の設定を削除するときに、特定の IP アドレスが異なるグループの範囲に一致する場合、異なるグループの IP アドレスの範囲は削除できないため、設定は削除されません。IP アドレスの範囲または IMSI の範囲の設定を削除する場合、範囲全体を削除するには、IP または IMSI の開始値だけを指定できます。設定を削除する場合、IP または IMSI の範囲の上限値を指定していても、PDSN は IP または IMSI の上限値を無視します。
- IMSI MIM と同等の番号をイネーブルにした場合、IMSI リダイレクションの検索中に、PDSN は入力 of 10 桁だけを使用します。設定の残りの桁は無視されます。ただし、**show run** コマンドを使用する場合、IMSI MIN と同等の存在に関係なく、このコマンドで入力そのものが示されます。内部で検索に使用される 10 桁の出力は行いません。

CLI コマンドからスタンドアロン PDSN の IMSI リダイレクションを設定できる設定例を次に示します。

```
pdsn# cdma pdsn redirect imsi {Single-bound IMSI | Lower-bound IMSI} [Upper Bound IMSI]
member [Member IP]
```

```
cdma pdsn redirect ?
imsi - IMSI Redirection
pcf - PCF Redirection
```

```
cdma pdsn redirect imsi ?
Single or Start IMSI - 15 digit IMSI address
```

```
cdma pdsn redirect imsi 123456789012345 ?
Ending IMSI - 15 digit IMSI address
```

```
cdma pdsn redirect imsi 123456789012345 123456789012400 ?
member - PDSN member
```

```
cdma pdsn redirect imsi 123456789012345 123456789012400 member ?
PDSN IP address - IP address of PDSN where A11 need to be redirected
```

CLI コマンドからスタンドアロン PDSN の IMSI リダイレクションを削除するには次のように記述します。

```
pdsn# no cdma pdsn redirect imsi {Single-bound IMSI | Lower-bound IMSI}
```



(注)

下限の IMSI は、IMSI 範囲の低い値を示します。IMSI 範囲の上限値を指定する必要はありません。

CLI コマンドからスタンドアロン PDSN の PCF リダイレクション CLI コマンドを設定するには、次のように記述します。

```
pdsn# cdma pdsn redirect pcf {Single or Lower-bound PCF IP_address | Upper-bound PCF IP_address} member Member_IP
```

```
pdsn# cdma pdsn redirect ?  
imsi - MSID Redirection  
pcf - PCF Redirection
```

```
pdsn# cdma pdsn redirect pcf ?  
PCF IP address - Single or Start of the range of PCF IP address
```

```
pdsn# cdma pdsn redirect pcf 11.11.11.11 ?  
PCF IP address - Last PCF address in the range
```

```
pdsn# cdma pdsn redirect pcf 11.11.11.11 11.11.11.200 ?  
member - PDSN member
```

```
pdsn# cdma pdsn redirect pcf 11.11.11.11 11.11.11.200 member ?  
PDSN IP address - IP address of PDSN where All need to be redirected
```

CLI コマンドからスタンドアロン PDSN の PCF リダイレクションを削除するには、次のように記述します。

```
pdsn# no cdma pdsn redirect pcf Single or Lower-bound PCF IP address
```



**(注)** 単一 PCF IP または設定されている PCF IP の範囲を削除するには、範囲の下限値だけを指定できます。

Cisco PDSN リリース 5.0 で導入された次のコマンドを使用すると、クラスタ コントローラ PDSN を設定できます。

PCF グループのクラスタ コントローラを設定するには、次のように記述します。

```
pdsn# cdma pdsn cluster controller pcf group number  
description group name  
pcf ip [end_ip]  
pcf ip [end_ip]
```

PDSN グループのクラスタ コントローラを設定するには、次のように記述します。

```
pdsn# cdma pdsn cluster controller pdsn group number  
description group name  
pdsn ip [end_ip]  
pdsn ip [end_ip]  
primary ip
```

IMSI または PCF リダイレクションのクラスタ コントローラを設定するには、次のように記述します。

```
pdsn# cdma pdsn cluster controller redirect  
imsi IMSI_range pdsn pdsn_group_number [force]  
pcf pcf_group_number pdsn pdsn_group_number [force]
```

## China Telecom 用モバイル IP および AAA アトリビュート

今回のリリースで、China Telecom (CT) に必要な MIP および AAA アトリビュートがサポートされました。

次の章では、以下の内容について説明します。

- 「MIP RRQ の発信ステーション ID」
- 「MIP RRQ の関連 ID」
- 「プロキシ モバイル IP インジケータ アトリビュート」 (P.124)
- 「プロキシ モバイル IP インジケータ アトリビュート」
- 「プロキシ モバイル IP 機能インジケータ アトリビュート」
- 「PDSN サービス アドレス」
- 「課金タイプ」

### MIP RRQ の発信ステーション ID

Normal Vendor Specific Extension (NVSE) としての発信ステーション ID は、FA および HA 間の MIP レジストレーション要求 (RRQ) のキャリアです。

発信ステーション ID の設定 :

```
router(config)# cdma pdsn attribute vendor 20942 send a1 mip_rrq
```

### MIP RRQ の関連 ID

NVSE としての関連 ID は、FA および HA 間の MIP RRQ のキャリアです。PDSN の関連 ID は、MIP RRQ で HA に送信されます。この ID は HA で生成されたアカウント記録すべてで送信されます。

関連 ID の設定 :

```
router(config)# cdma pdsn attribute vendor 20942 send c2 mip_rrq
```

### プロキシ モバイル IP インジケータ アトリビュート

PMIP インジケータは VSA です。PMIP インジケータは、access-accept パケットとして、Remote Authentication Dial-In User Service (RADIUS) 経由で PDSN に返されます。そのため、PDSN は加入者の代理で PMIP を開始します。

### プロキシ モバイル IP 機能インジケータ アトリビュート

PMIP 機能インジケータは VSA です。PDSN は、機能インジケータを access-request パケットとして RADIUS 経由で AAA サーバに送信し、PDSN が PMIP をサポートしており、イネーブルであることを AAA サーバに示します。機能インジケータ アトリビュートがない場合、PDSN は PMIP をサポートしません。

PMIP 機能インジケータの設定 :

```
router(config)# cdma pdsn attribute vendor 20942 send pmip_capability access_request
```

## PDSN サービス アドレス

PDSN サービス アドレスは VSA です。このサービス アドレスは、accounting-start メッセージで AAA に送信されます。

PDSN サービス メッセージの設定 :

```
pdsn-stby-ftb4-73(config)# cdma pdsn attribute vendor 20942 send pdsn-src-addr ?
pdsn-stby-ftb4-73(config)# acct_reqs Send pdsn-src-addr attribute in acct-reqs ?
pdsn-stby-ftb4-73(config)# cdma pdsn attribute vendor 20942 send pdsn-src-addr ac ?
pdsn-stby-ftb4-73(config)# cdma pdsn attribute vendor 20942 send pdsn-src-addr acct_reqs
```

## 課金タイプ

課金タイプは、AAA サーバから access-accept メッセージでダウンロードされる CT VSA です (課金タイプが特定ユーザの AAA 加入者プロファイルで設定される場合)。Cisco PDSN は、accounting-start メッセージを使用して、このダウンロードされたアトリビュート値を AAA サーバに送信します。

この課金タイプには、次の 3 種類があります。

- 0x00000001 - 後払い
- 0x00000002 - 前払い
- 0x00000003 - 後払いと前払い

課金タイプをダウンロードするには、次の CLI コマンドをイネーブルにする必要があります。

```
pdsn_active(config)# cdma pdsn attribute vendor 20942
```

設定を削除するには、次のように記述します。

```
pdsn_active(config)# no cdma pdsn attribute vendor 20942
```

次の例は、各フローのダウンロードした課金タイプの抜粋を示しています。

```
pdsn_active# show cdma pdsn session
Mobile Station ID MIN 2000000003
  PCF IP Address 10.1.1.1, PCF Session ID 1
  A10 connection time 00:00:05, registration lifetime 500 sec
  Number of successful A11 re-registrations 0
  Remaining session lifetime 494 sec
  Always-On not enabled for the user
  Current Access network ID 000A-0101-01
  Last airlink record received is Connection Setup, airlink is active
  GRE protocol type is 0x8881
  GRE sequence number transmit 14, receive 22
  Using interface Virtual-Access2.1, status OPN
  Using AHDLC engine on slot 0, channel ID 6
  Service Option EV-DO Flow Discrimination 0 DSCP Included 0
  Flow Count forward 0 reverse 0
  This session has 1 flow
  This session has 0 service flows
  Session Airlink State Setup
  This session has 0 TFTs
  Qos subscriber profile
  Max Aggregate Bandwidth : 200
  Inter User Priority : 1000
```

```

Flow service Mobile, NAI mwts-mip-np-user11@ispxyz.com
Mobile Node IP address 12.1.1.10
Home Agent IP address 4.1.1.2
Packets in 0, bytes in 0
Packets out 0, bytes out 0
Charge Type 1
Radius disconnect enabled

```

## MIB のサポート

今回のリリースで、単一 IP およびシャーシ全体の MIB に関連するいくつかの新しい MIB がサポートされました。多くの MIB は、Key Performance Indicator (KPI) のソースとして使用されます。

次の章では、以下の内容について説明します。

- 「[KPI のソースとしての MIB](#)」
- 「[MIB 用モデル](#)」

## KPI のソースとしての MIB

KPI のソースとして使用される MIB は次のとおりです。

- RFC 2006 MIB
- CISCO-CDMA-PDSN-MIB
- CISCO-CDMA-PDSN-EXT-MIB
- CISCO-VPDN-MGMT-MIB
- CISCO-VPDN-MGMT-EXT-MIB
- CISCO-AAA-SERVER-MIB
- RFC 2618 RADIUS Authentication Client MIB
- IF-MIB
- CISCO-IP-LOCAL-POOL-MIB
- CISCO-PROCESS-MIB
- CISCO-MEMORY-POOL-MIB (ENHANCED-MEMPOOL-MIB で置き換えられます)
- CISCO-ENHANCED-MEMPOOL-MIB

### CISCO-PROCESS-MIB

(<http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&mibName=CISCO-PROCESS-MIB>)

および CISCO-MEMORY-POOL-MIB

(<http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-MEMORY-POOL-MIB>) は、サービス ブレード PDSN-SIP-50 単位で単一の MIB レポートを提供するための要件の影響を受けます。



(注)

- SNMP を介した SNMPSET を使用して値を設定できません。つまり、read-write または read-create オブジェクトに書き込み権限は許可されません。
- CPU、I/O、およびプロセス メモリは単一 IP でサポートされないため、TCOP レベルのトラップ (MN 認証エラー、レジストレーション ID の不一致) および高負荷のトラップはありません。

- CPU、I/O、およびプロセス メモリは単一 IP でサポートされていないため、CDMA PDSN MIB 用の SNMP SET、TCOP レベルのトラップ (MN 認証エラー、レジストレーション ID の不一致)、および高負荷のトラップはありません。
- SNMP SET、および CISCO-VPDN-MGMT MIB と CISCO-AAA\_-SERVERS-MIB 用のトラップはありません。

どちらの MIB にも、プロセッサ単位のコンテンツが含まれます。6 個のアプリケーション プロセッサすべてに関する情報は、1 つの SNMP GET でレポートされ、各 MIB には 6 個のエントリが含まれます (1 アプリケーション プロセッサあたり 1 個)。

IF-MIB には、コントロールプレーン プロセッサのインターフェイスに加え、トラフィック プレーン プロセッサのインターフェイスに関する情報が含まれます。

CISCO-PROCESS-MIB には、1 つまたは複数の CPU に関する情報を提供するファシリティが含まれます。CSG2 プロジェクトは、ENTITY-MIB と CISCO-PROCESS-MIB の併用に必要なソリューションを開発しました。

CISCO-MEMORY-POOL-MIB はこの機能をサポートしていません。ただし、CSG2 プロジェクトはソリューションを開発し、CISCO-ENHANCED-MEMPOOL-MIB (<http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&submitClicked=true&mbName=CISCO-ENHANCED-MEMPOOL-MIB#dependencies>) を組み込みました。これは今回のリリースで再利用されます。

現在、CISCO-CDMA-PDSN-MIB と CISCO-CDMA-PDSN-EXT-MIB のどちらも、グローバル統計情報および PCF ベースの統計情報だけをサポートしています。これらのアトリビュートはすべて、複数 CPU には依存しません。そのため、PCOP で値が集約されます。

現在、CISCO-VPDN-MGMT-MIB と CISCO-VPDN-MGMT-EXT-MIB のどちらも、VPDN 情報、VPDN トンネル情報、VPDN トンネル ユーザ情報、およびユーザごとの障害履歴だけをサポートしています。これらのアトリビュートはすべて、複数 CPU には依存しません。PCOP で値が集約されます。

現在、CISCO-AAA-SERVER-MIB は、各 AAA 機能の個別の統計情報、サーバが提供する AAA 機能の状態、および AAA サーバを設定するテーブルだけをサポートしています。これらのアトリビュートはすべて、複数 CPU には依存しません (ただし、設定テーブルを除きます)。PCOP で値が集約されます。

## MIB 用モデル

ここでは、各 MIB に従うモデルについて説明します。TCOP には、SNMP MIB に必要なデータを定期的に PCOP へプッシュするメカニズムがあります。PCOP 上のプロセスは、このデータを定期的に受信し、TCOP インデックスが指定された適切な一時的構造に配置します。

SNMP GET が PCOP に到達すると、PCOP はデータを集約します。また、TCOP ごとに個別エントリの場合はデータを集約しません。また、GET 要求に関連する SNMP 変数の合計値または非合計値に格納されます。以降のコードで、応答の PDU の SNMP 変数に格納し、GET を要求したエンティティに返信します。

集約カウンタは PCOP で使用できます。または、各カウンタはテーブルに変換され、TCOP インデックスが指定されます。PCOP は、SNMP GET で SNMP 応答 PDU に格納する時点でデータをプルするか、SNMP 変数に格納する一時的構造のプッシュ済みデータの値を使用します。それから、SNMP 応答 PDU に格納して、マネージャ エンティティに戻します。PCOP 上のデータを取得するための MIB のモデルは、プッシュ モデルまたはオンデマンドプル モデルです。

表 21 で、今回のリリースでサポートされる各 MIB について説明します。

表 21 PDSN でサポートされる MIB

MIB	説明	TCOP からの情報が必要か	必要な場合、メカニズム
RFC 2006-MIB	SMIPv2 を使用する IP モビリティサポートの場合、管理対象オブジェクトの RFC 2006 定義を使用します。	不要：トラフィックカウンタはありません	-
Cisco-CDMA-PDSN-MIB / CISCO-CDMA-PDSN-EXT-MIB	CDMA PDSN 機能をサポートします。	必要	PDSN グローバル統計情報は、毎分定期的に集約されます。 レジストレーションおよび PCF ベースの統計情報は、プルメカニズムに基づいています。 PCOP でのデータ集約と TCOP でのデータ提供。
RFC 2618 RADIUS Authentication Client MIB	RFC 2618 に定義されている定義を使用します。	不要：トラフィックカウンタはありません	HA 5.0 から再利用されます。
IF-MIB	コントロールプレーンプロセッサのインターフェイスに加え、トラフィックプレーンプロセッサのインターフェイスに関する情報が含まれます。	必要	PCOP でのデータ集約と TCOP でのデータ提供。プッシュパラダイムに従います。 仮想アクセスインターフェイスの場合、多くのリソースを消費します。そのため、これらのインターフェイスはクエリーに応答しません。他のインターフェイスは HA 5.0 と同様です。
CISCO-IP-LOCAL-POOL-MIB	ローカル IP プールに関連する設定および監視機能を定義します。	不要：トラフィックカウンタはありません	-
CISCO-ENHANCED-MEMPOOL-MIB	管理対象システム上にあるすべての物理エンティティのメモリプールを関しする場合。	必要	PCOP でのデータ集約と TCOP でのデータ提供。プッシュパラダイムに従います。各 TCOP は毎秒 PCOP に更新を送信します。
CISCO-PROCESS-MIB	IOS を実行するプロセッサ（2 枚のドーターカード上の 6 プロセッサ）上で、アクティブなシステムプロセスの統計情報を記述します。	必要	PCOP でのデータ集約と TCOP でのデータ提供。プッシュパラダイムに従います。TCOP の CPU 統計情報は毎秒送信されます。他の統計情報は毎分 PCOP に送信されます。
CISCO-ENTITY-MIB	単一の SNMP エージェントがサポートする複数の論理エンティティを表すための MIB モジュール。	必要	CP でのデータ集約と TP でのデータ提供。



表 21 PDSN でサポートされる MIB (続き)

MIB	説明	TCOP からの情報が必要か	必要な場合、メカニズム
CISCO-VPDN-MGMT-MIB/CISCO-VPDN-MGMT-EXT-MIB	<p>Cisco IOS の VPDN 機能をサポートします。次のエンティティが管理対象です。</p> <ul style="list-style-type: none"> <li>グローバル VPDN 情報</li> <li>VPDN トンネル情報</li> <li>VPDN トンネル ユーザ情報</li> <li>ユーザごとの障害履歴</li> </ul>	必要	グローバル情報、トンネル情報、ユーザ情報、およびユーザごとの障害履歴の統計情報は、プルメカニズムに基づいています。PCOP でのデータ集約と TCOP でのデータ提供。
CISCO-AAA-SERVER-MIB	<p>デバイス内の AAA サーバ運用の状態を反映して、設定と統計情報を提供します。</p> <p>AAA サーバの MIB は次の情報を提供します。</p> <ul style="list-style-type: none"> <li>AAA サーバを設定するためのテーブル</li> <li>各 AAA 機能の個別の統計情報</li> <li>AAA 機能を提供するサーバの状態</li> </ul>	必要	PCOP でのデータ集約と TCOP でのデータ提供。プルパラダイムに従います。

## AAA サーバ非応答に対するトラップ生成

今回のリリースで、PDSN が MN の認証中に AAA サーバの非応答を認識したときに、SNMP トラップの送信または NMS サーバに対する通知を行う機能がサポートされました。

各 RADIUS サーバで、パーセントのしきい値（通常しきい値または上限しきい値）を設定できます。PDSN および AAA サーバ間の RADIUS メッセージのラウンドトリップ時間が、しきい値を超えるか下回ると、AAA サーバの応答または非応答を示す SNMP トラップまたは通知が NMS サーバに送信されます。同様に、RADIUS 再送信メディアセッションの数が、しきい値を超えるか下回ると、AAA サーバの応答または非応答を示す SNMP トラップまたはメッセージが NMS サーバに送信されます。ラウンドトリップ時間と再送信のしきい値のデフォルト値は次のとおりです。

- Normal : 0
- High : 100

たとえば、ラウンドトリップ時間または再送信の回数が増えしきい値を超えると、AAA サーバの状態が BUSY または DOWN であることを示す SNMP トラップまたは通知が NMS サーバに送信されます。同様に、ラウンドトリップ時間または再送信の回数が増えしきい値を下回ると、AAA サーバの状態が NORMAL であることを示す SNMP トラップまたは通知が NMS サーバに送信されます。ラウンドトリップ時間および再送信によって、それらに設定されるしきい値に個別のトラップが生成されます。

通知の条件は次のとおりです。

- ラウンドトリップ時間に関する AAA サーバの状態が BUSY と通知され、ラウンドトリップ時間に関する AAA サーバの状態が NORMAL になるまで、その AAA サーバに関するトラップまたは通知は NMS サーバに送信されなくなります。
- 再送信の BUSY トラップが送信された後は、再送信のサーバの状態が NORMAL になるまで、再送信の BUSY トラップは同じサーバに送信されません。

- ラウンドトリップ時間に関する AAA サーバの状態が **NORMAL** と通知された後は、ラウンドトリップ時間に関するサーバの状態が **BUSY** と特定されない限り、ラウンドトリップ時間の **NORMAL** トラップまたは通知は NMS サーバに送信されません。
- 再送信の **NORMAL** トラップが送信された後は、再送信のサーバの状態が **BUSY** になるまで、再送信の **NORMAL** トラップは同じサーバに送信されません。

この機能をイネーブルにするには、次のタスクを実行します。

	コマンド	目的
ステップ 1	Router(config)# <b>radius-server snmp-trap timeout-threshold normal high</b>	AAA の非応答を示す SNMP トラップを生成できます。  <i>normal</i> は通常しきい値 (50 ~ 75% の通常値) で、トラップの生成に使用されます。  <i>high</i> は上限しきい値 (60 ~ 100% の高い値) で、トラップの生成に使用されます。
ステップ 2	Router(config)# <b>radius-server snmp-trap retrans-threshold normal high</b>	ラウンドトリップ時間または再送信値が上限しきい値を超え、通常しきい値を下回る場合、トラップ (SNMP 通知) を生成します。ラウンドトリップ時間または再送信回数に関するトラップが生成されます。  <i>normal</i> は通常しきい値 (%) で、トラップの生成に使用されます。  <i>high</i> は上限しきい値 (%) で、トラップの生成に使用されます。
ステップ 3	Router(config)# <b>snmp-server enable traps aaa_server</b> snmp-server host [ip address] version [1   2c   3] [community-string]	AAA の非応答および IP アドレスを示す SNMP トラップを生成できます。



(注) この機能がサポートされるのは 7600 上の Cisco SAMI カードだけです。

RADIUS-CLIENT-AUTHENTICATION-MIB は、PDSN インスタンスごとに実装され、その各インスタンスがトラップを生成します。

RADIUS-CLIENT-AUTHENTICATION-MIB には、AAA アクセスのタイムアウトに関するエンティティが含まれます。このタイムアウトの発生に基づいて、トラップが追加されます。また、ラウンドトリップ遅延 (最大応答時間のパーセントとして定義されます) に対してしきい値を設定し、そのしきい値を超えたときにトラップを生成することもできます。ラウンドトリップ遅延が 2 番目のしきい値を下回る場合、追加のトラップが生成されます。これで、トラップ生成に関して遅延のレベルを実現できます。

## スーパーバイザのサポート

今回のリリースで、SUP32、SUP720、および RSP720 バリエントがサポートされました。

スーパーバイザは、Cisco Catalyst 6500 Supervisor Engine 32 (WS-SUP32-GE-3B および WS-SUP32-10GE-3B)、Cisco Catalyst 6500 Supervisor Engine 720 (WS-SUP720-3B および WS-SUP720)、および新しい Cisco Route Switch Processor 720 (RSP720-3C-GE、RSP720-3CXL-GE、および RSP720-3CXL-10GE) でサポートされるようになりました。

## Data Over Signaling

今回のリリースで、Data Over Signaling (DOS) がサポートされました。DOS はショート データ パースト機能とも呼ばれ、空いているシグナリング チャンネルを使用して、モバイル ステーション (MS) との間でショート データ パーストを送受信できます。

IOS は、Modular QoS CLI (MQC) コマンドセットおよび Common Classification Engine (CCE) API を使用して、ポリシー処理のフローベース インフラストラクチャをサポートします。CCE は、分類および特性の関連付け機能を IOS アプリケーションに提供する汎用的なフレームワークです (QoS、ACL など)。IOS フローは CCE で、クラスの一意的インスタンスとして、また送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、プロトコル全体あるいはサブセットとして定義されます。

1 MIP セッションあたり 1 つの **vaccess** だけが使用できる場合、フローは複数あり、各フローは異なるポリシー名をダウンロードします。従って、**vaccess** はターゲットではありません。フローベースの QoS を PDSN で有効にするため、仮想オブジェクトが PDSN に作成されます。この仮想オブジェクトはインターフェイスとして機能し、サービス ポリシーをアタッチします。この仮想オブジェクトは、QoS へのフローとマーキング パラメータを識別します。

DOS パケットは、ルータに設定されているポリシー マップ (フローベース ポリシー) に基づいて識別されます。このポリシー マップは、各方向の **access-accept** 中に AAA サーバからダウンロードする必要があります。ダウンロードしたポリシーは、その方向の仮想インターフェイス上で PDSN にインストールされます。

QoS は、DOS マーキングに適格としてパケットにマークが付けられます。PDSN は、分類基準だけにに基づき、またセッションが休止状態の場合にだけ、ダウストリームまたは転送方向の GRE ヘッダーに含まれる DOS アトリビュートでパケットにマークを付ける必要があります。



(注) DOS 機能をイネーブルにするには、**cdma pdsn dos** を設定する必要があります。



(注) このポリシーを、**vaccess** とフローのいずれかとしてインストールできます。両方同時のインストールはサポートされません。**vaccess** ベースのインストールを使用する場合、**no cdma pdsn QoS policy flow-only** コマンドを使用して、CDMA PDSN QoS policy flow-only をディセーブルにする必要があります。

次の章では、以下の内容について説明します。

- 「DOS のフロー トリガ分類」
- 「DOS の分類基準に基づくフロー マーキング」
- 「AT 終端の DOS」
- 「AT 生成の DOS」
- 「1xRTT PCF から送信される SDB アカウンティング レコード」
- 「DOS に関する制限」
- 「DOS の設定」

### DOS のフロー トリガ分類

フローに基づいてパケットが PDSN に到達すると、その仮想インターフェイスに関連付けられたサービス ポリシーが特定され、データ パケットに適用する必要がある QoS 機能も特定されます。IOS QoS は、仮想オブジェクトのためにフローの分類をトリガします。これは各フローに固有で、分類基準は PDSN フローであることを示します。

## DOS の分類基準に基づくフロー マーキング

PDSN では、分類基準に基づいて各パケットが分類され、マークが付けられます。現在、PDSN は **set marking** だけをサポートしています。**set dos** は分類基準に基づいて SDB パケットにマークを付ける場合に使用されます。



(注) DOS マーキングは、ダウンストリーム方向でだけ実行されます。

## AT 終端の DOS

PDSN が休止セッションでダウンストリーム トラフィックを送信しているとき、SDB トラフィックであることを示すために、PDSN は GRE ヘッダーに SDB または DOS アトリビュートを追加します。このアトリビュートで PCF に対してシグナリングし、Access Network (AN; アクセス ネットワーク) に送信するときに、トラフィックを適切に処理する必要があることを示します。

### 1x SDB/HRPD DoS インジケータ

PDSN によって、1x SDB または High Rate Packet Data (HRPD) DoS 送信に適しているというタグがパケットに付けられる場合、次のように定義されるアトリビュートで識別されます。

Type '000 0001' : Short Data Indication

Length 02H

SDI/DoS 0 : 予約済み

1 : 1x SDB または HRPD DoS の送信に適したパケット

## AT 生成の DOS

AT 生成の DOS の場合、PDSN は受信パケットの特殊な処理を実行しません。

## 1xRTT PCF から送信される SDB アカウンティング レコード

1xRTT PCF はエアリンク レコードを送信して、SDB トランザクションが発生したことを PDSN に示します。4 に設定した **airlink-record Y1** を送信することでこの処理が実行されます。モバイル発信 (y4) またはモバイル終端がゼロの場合、PDSN は G10 の値ずつ G11 を増分し、1 ずつ G13 を増分します。モバイル発信 (y4) またはモバイル終端が 1 の場合、PDSN は G10 の値ずつ G10 を増分し、1 ずつ G12 を増分します。

## DOS に関する制限

DOS の実行には、次の制限があります。

- 再レジストレーション時に新しいポリシーをダウンロードする場合、この新規ポリシーは処理されず、最初のレジストレーション時にダウンロードされたポリシーだけがインストールされます。ポリシーは、**vaccess** とフロー (デフォルト) のいずれかとしてインストールできます。**vaccess** を使用してインストールする場合、**no cdma pdsn qos policy flow-only** コマンドを使用して、必ずフローベース ポリシーを無効にしてください。
- 特定のポリシー マップをインストールした場合、ポリシー マップ、関連するクラス マップ、およびアクション グループは変更できません。

- フローベース ポリシーを使用する DOS マーキングは、Virtual Private dial-up Network (VPDN; バーチャル プライベート ダイアルアップ ネットワーク) コールでサポートされません。

## DOS の設定

PDSN で DOS をイネーブルにするには、次のように記述します。

### cdma pdsn dos

フローベースの DOS 分類およびマーキングの場合、次のように記述します。

```
class-map class-pdsn
  Match any
policy-map policy-pdsn
  Class class-pdsn
    set dos
```

次の、Exec モードでの CLI コマンドは、特定のフローでフローベースの分類が有効になっている場合の、フローベースの QoS マーキング統計情報を示しています。統計情報には、DOS マーキングされたパケットの数などの詳細が含まれます。統計情報は特定の NAI に基づいて示されます。

```
pdsn_active# show policy-map apn realm user1

MSID           NAI           Type           MN IP Address   St  HA IP
01002647325    user1         Simple         3.1.1.5         ACT 0.0.0.0
```

Service-policy output: SIP-POLICY

```
Class-map: SIP-CLASS (match-all)
  5 packets, 520 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any
  QoS Set
    dos
    Packets marked 5

Class-map: class-default (match-any)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any
```

Exec モードの次の CLI コマンドで、フローベースの QoS ポリシーのインストールおよびダウンロード統計情報が表示されます。

```
pdsn_active-4# show cdm pds stat qos

QoS:
  Total Profile Download Success 10, Failure 0
  Local Profile selected 1
  Failure Reason DSCP 0, Flow Profile ID 0,
  Service option profile 0, Others 0
  Total Consolidated Profile 5, DSCP Remarked 5
  Total policing installed 5, failure 0, removed 3

Flow based QoS:
  Input policy:
    Total policy download success 2, failure 0
    Failure reason policy not configured 0, policy downloaded already 0
    Total policy installed 1, failure 0, removed 1
  Output policy:
    Total policy download success 2, failure 0
    Failure reason policy not configured 0, policy downloaded already 0
    Total policy installed 1, failure 0, removed 1
```

Exec モードの次の CLI コマンドで、フローベースの QoS を使用するフロー数が表示されます。

```
pdsn_active-4# show cdm pds
PDSN software version 5.0, service is enabled

All registration-update timeout 5 sec, retransmissions 5
All session-update timeout 5 sec, retransmissions 3
Mobile IP registration timeout 10 sec
A10 maximum lifetime allowed 65534 sec
GRE sequencing is on
Maximum PCFs limit not set
Maximum sessions limit not set (default 35000 maximum)
SNMP failure history table size 100
MSID Authentication is disabled
Ingress address filtering is disabled
Sending Agent Adv in case of IPCP Address Negotiation is enabled
Allow CI_ADD option during IPCP Phase is disabled
Aging of idle users disabled
Radius Disconnect Capability enabled
Multiple Service flows enabled
Maximum number of service-flows per MN allowed is 7
Call Admission Control disabled
Police Downstream enabled
Data Over Signaling disabled
Flow based policy enabled

Number of pcfs connected 1,
Number of pcfs 3GPP2-RP 1,
Number of sessions connected 1,
Number of sessions 3GPP2-RP 1,
Number of sessions Active 1, Dormant 0,
Number of sessions using HDLCoGRE 1, using PPPoGRE 0
Number of sessions using Auxconnections 0, using Policing 1, using DSCP 1
Number of service flows 0
Number of flows using flow based qos 1
Number of sessions connected to VRF 0,
    Simple IP flows 1, Mobile IP flows 0,
    Proxy Mobile IP flows 0, VPDN flows 0
```

## Differentiated Services Code Point マーキングのサポート

今回のリリースで、Differentiated Services Code Point (DSCP) マーキングがサポートされました。このマーキングはフローベース ポリシーを使用します。

IOS は、Modular QoS CLI (MQC) コマンドセットおよび Common Classification Engine (CCE) API を使用して、ポリシー処理のフローベース インフラストラクチャをサポートします。CCE は、分類および特性の関連付け機能を IOS アプリケーションに提供する汎用的なフレームワークです (QoS、ACL など)。IOS フローは CCE で、クラスの一意的インスタンスとして、また送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、プロトコル全体あるいはサブセットとして定義されます。

1 MIP セッションあたり 1 つの vaccess だけが使用できる場合、フローは複数あり、各フローは異なるポリシー名をダウンロードします。従って、vaccess はターゲットではありません。フローベースの QoS を PDSN で有効にするため、仮想オブジェクトが PDSN に作成されます。この仮想オブジェクトはインターフェイスとして機能し、サービス ポリシーをアタッチします。この仮想オブジェクトは、QoS へのフローとマーキング パラメータを識別します。

DSCP パケットは、ルータに設定されているポリシー マップ (フローベース ポリシー) に基づいて識別されます。このポリシー マップは、各方向の access-accept 中に AAA サーバからダウンロードする必要があります。ダウンロードしたポリシーは、その方向の仮想インターフェイス上で PDSN にインストールされます。

PDSN は、分類基準に基づいて、アップストリーム (reverse) およびダウンストリーム (forward) の両方で、DSCP を使用してパケットにマークを付ける必要があります。



(注)

このポリシーを、`vaccess` とフローのいずれかとしてインストールできます。両方同時のインストールはサポートされません。`vaccess` ベースのインストールを使用する場合、**no cdma pdsn qos policy flow-only** コマンドを使用して、CDMA PDSN QoS policy flow-only をディセーブルにする必要があります。

次の章では、以下の内容について説明します。

- 「DSCP のフロー トリガ分類」
- 「DSCP の分類基準に基づくフロー マーキング」
- 「DSCP に関する制限」
- 「DSCP の設定」

## DSCP のフロー トリガ分類

フローに基づいてパケットが PDSN に到達すると、その仮想インターフェイスに関連付けられたサービス ポリシーが特定され、データ パケットに適用する必要がある QoS 機能も特定されます。IOS QoS は、「`apn_qos_info_t`」のためにフローの分類をトリガします。これは各フローに固有で、分類基準は PDSN フローであることを示します。

## DSCP の分類基準に基づくフロー マーキング

PDSN では、分類基準に基づいて各パケットが分類され、マークが付けられます。PDSN は、`set` マーキングだけをサポートします。たとえば、**set dos**、**set dscp**、および **set qos-group** です。**qos-group** および **set dos** は互いに矛盾するため、**qos-group** または **set dos** を使用する必要があります。



(注)

リバース トンネルをイネーブルにする場合、DSCP マーキングは内側のパケットでだけ発生します。

## DSCP に関する制限

DSCP の実行には、次の制限があります。

- 再レジストレーション時に新しいポリシーをダウンロードする場合、この新規ポリシーは処理されず、最初のレジストレーション時にダウンロードされたポリシーだけがインストールされます。ポリシーは、`vaccess` とフロー (デフォルト) のいずれかとしてインストールできます。`vaccess` を使用してインストールする場合、**no cdma pdsn qos policy flow-only** コマンドを使用して、必ずフローベース ポリシーを無効にしてください。
- フローベース ポリシーを使用する DOS マーキングは、VPDN コールの場合はサポートされません。
- 特定のポリシー マップをインストールした場合、ポリシー マップ、関連するクラス マップ、およびアクション グループは変更できません。

## DSCP の設定

フローベースの DSCP 分類およびマーキングの場合、次のように記述します。

```
Class-map class-pdsn
```

```

Match any
Policy-map policy-pdsn-out
  Class class-pdsn
    set dscp 1

Policy-map policy-pdsn-in
  Class class-pdsn
    set dscp 1

```

次の、Exec モードでの CLI コマンドは、特定のフローでフローベースの分類が有効になっている場合の、フローベースの QoS マーキング統計情報を示しています。統計情報には、DSCP マーキングされたパケットの数などの詳細が含まれます。統計情報は特定の NAI に基づいて示されます。

```
pdsn_active# show policy-map apn realm user1
```

MSID	NAI	Type	MN IP Address	St	HA IP
01002647325	user1	Simple	3.1.1.5	ACT	0.0.0.0

```
Service-policy input: policy-pdsn-in
```

```

Class-map: class-pdsn (match-all)
  5 packets, 520 bytes
  30 second offered rate 0 bps, drop rate 0 bps
Match: any
QoS Set
  dscp 1
  Packets marked 5

```

```

Class-map: class-default (match-any)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
Match: any

```

```
Service-policy output: policy-pdsn-out
```

```

Class-map: class-pdsn (match-all)
  5 packets, 520 bytes
  30 second offered rate 0 bps, drop rate 0 bps
Match: any
QoS Set
  dos
  Packets marked 5

```

```

Class-map: class-default (match-any)
  0 packets, 0 bytes
  30 second offered rate 0 bps, drop rate 0 bps
Match: any

```

Exec モードの次の CLI コマンドで、フローベースの QoS ポリシーのインストールおよびダウンロード統計情報が表示されます。

```
pdsn_active-4# show cdm pds stat qos
```

```

QoS:
Total Profile Download Success 10, Failure 0
Local Profile selected 1
Failure Reason DSCP 0, Flow Profile ID 0,
Service option profile 0, Others 0
Total Consolidated Profile 5, DSCP Remarked 5
Total policing installed 5, failure 0, removed 3

```

```

Flow based QoS:
Input policy:
  Total policy download success 2, failure 0

```



```

Failure reason policy not configured 0, policy downloaded already 0
Total policy installed 1, failure 0, removed 1
Output policy:
Total policy download success 2, failure 0
Failure reason policy not configured 0, policy downloaded already 0
Total policy installed 1, failure 0, removed 1

```

Exec モードの次の CLI コマンドで、フローベースの QoS を使用するフロー数が表示されます。

```

pdsn_active-4# show cdm pds
PDSN software version 5.0, service is enabled

All registration-update timeout 5 sec, retransmissions 5
All session-update timeout 5 sec, retransmissions 3
Mobile IP registration timeout 10 sec
A10 maximum lifetime allowed 65534 sec
GRE sequencing is on
Maximum PCFs limit not set
Maximum sessions limit not set (default 35000 maximum)
SNMP failure history table size 100
MSID Authentication is disabled
Ingress address filtering is disabled
Sending Agent Adv in case of IPCP Address Negotiation is enabled
Allow CI_ADD option during IPCP Phase is disabled
Aging of idle users disabled
Radius Disconnect Capability enabled
Multiple Service flows enabled
Maximum number of service-flows per MN allowed is 7
Call Admission Control disabled
Police Downstream enabled
Data Over Signaling disabled
Flow based policy enabled

Number of pcfs connected 1,
Number of pcfs 3GPP2-RP 1,
Number of sessions connected 1,
Number of sessions 3GPP2-RP 1,
Number of sessions Active 1, Dormant 0,
Number of sessions using HDLCoGRE 1, using PPPoGRE 0
Number of sessions using Auxconnections 0, using Policing 1, using DSCP 1
Number of service flows 0
Number of flows using flow based qos 1
Number of sessions connected to VRF 0,
Simple IP flows 1, Mobile IP flows 0,
PMIP flows 0, VPDN flows 0

```

## Nortel Aux A10 のサポート

今回のリリースで、Nortel Aux A10 がサポートされました。その結果、PDSN は 0x88D2 に設定されたプロトコルタイプの Aux A11 Request を受信できるようになりました。0x88D2 に設定されたプロトコルタイプを持つ Aux A10 接続は、AHDLC エンコーディングでパケットを送信します。この新しいサポートによって PDSN は、0x88D2 のプロトコルタイプを持つ Aux A10 宛てのパケットについて、AHDLC エンコーディングおよびデコーディングを処理できるようになります。

## IMSI プレフィックスのマスキング解除

今回のリリースで、IMSI プレフィックスのマスキング解除がサポートされました。IMSI プレフィックスのマスキング解除は、テクノロジー間のハンドオフに必要です (1xRTT と EVDO 間のやり取り)。テクノロジー間のハンドオフでは、加入者の IMSI が 15 桁から 10 桁に変更される場合やその逆の場合、またはすべて 1 またはすべて 0 に設定されている上位 5 桁を国コードを使用する EVDO に変更する場合やその逆の場合、同じ PPP セッションが保持されます。

この機能で、上位 5 桁のマスキングは解除され、PDSN 上の一致するセッションが検索されます。1xRTT から EVDO へのハンドオフ、またはその逆は、同じセッションとして扱われます。

次の章では、以下の内容について説明します。

- 「[単一 IP アーキテクチャに関する変更](#)」
- 「[単一 IP アーキテクチャでの機能フロー](#)」
- 「[IMSI プレフィックスのマスキング解除に関する制限](#)」
- 「[IMSI プレフィックスのマスキング解除の設定](#)」

### 単一 IP アーキテクチャに関する変更

IMSI MIN と同等の機能を持つ新しいフラグ「strict」が、TCOP および IXP 間で通信されるメッセージに導入されました。IMSI MIN と同等の機能をイネーブルにすると、「strict」フラグは false に設定されます (デフォルトは true です)。着信 IMSI の場合、IXP はすべての桁を IMSI エントリ (strict または非 strict) とマッチングします。一致しない場合、IXP は末尾 10 桁をチェックし、非 strict の IMSI エントリでマッチングを試行します。

### 単一 IP アーキテクチャでの機能フロー

単一 IP アーキテクチャの機能フローは次のとおりです。

- MN は PCF1 経由でコールを開始します。PCF1 は A11 RRQ の一部として 10 桁の IMSI を送信します。SAMI の IXP は 10 桁の IMSI を受信し、検索を実行します。この A11 RRQ は新しいため、検索は失敗し、A11 RRQ は PCOP に送信されます。
- PCOP は 10 桁に基づいて IMSI の検索を実行し、検索は失敗します。次に、PCOP は A11 RRQ をロード バランサ (LB) が選択した TCOP に転送します。
- TCOPx は A11 RRQ を処理し、セッションを作成します。セッションの作成時に、「PCF1 IP + GRE + 10 digits of IMSI with strict = FALSE」というデータを含むメッセージを送信することで、IXP にエントリがインストールされます。
- PCF1 を再登録します。数分後に、同じ 10 桁の A11 RRQ が送信されます。
- モバイルが異なる PCF2 にローミングすると、プレフィックスの 5 桁のゼロまたは異なる桁 (国コードおよびローミングのための他のデータ) が 10 桁の IMSI に追加され、A11 RRQ の 15 桁の IMSI として送信されます。
- IXP は 15 桁のテーブルを検索し、検索は失敗します。今回も、受信した 15 桁の IMSI の下位 10 桁を使用して 10 桁のテーブルを検索し、有効なエントリを取得します。有効なエントリの strict フラグは false に設定されているため、検索に成功し、IXP は A11 RRQ を同じ TCOPx に転送します。
- TCOPx が A11 RRQ を受信します。異なる PCF から受信すると、ハンドオフを実行します。ハンドオフが正常に完了すると、IXP は「PCF2 IP + GRE + 10 digits IMSI with strict = FALSE」というメッセージで更新されます。
- PCF2 を再登録します。数分後に、PCF2 は同じ 15 桁の A11 RRQ を送信します。

- PDSN は A11 RRQ を受信すると、上位 5 桁をマスキングし、下位 10 桁の IMSI について既存のセッションがあるかどうかをチェックします。
  - 既存のセッションがあり、受信した要求も同じ PCF から送信された場合、PDSN はセッションを再登録します。
  - 既存のセッションがあり、受信した要求が異なる PCF から送信された場合、PDSN はハンドオフを実行します。
- セッションが存在しない場合、PDSN は IMSI を使用して新しいセッションを開きます。
- この機能がイネーブルの場合、PDSN は IMSI の下位 10 桁に基づいてすべてのセッションを保持します。そのため、セッションが PDSN に存在する場合、この機能の設定や設定の削除は行わないことをお勧めします。
- 下位 10 桁を 15 桁の MSID に指定しても、表示コマンド **show cdma pdsn session msid** は同じセッション結果を出力します。show の出力には最後に受信した IMSI が含まれます。**clear cdma pdsn session msid** コマンドにも同じ状況が当てはまります。
- 上位 10 桁から 15 桁で表示コマンド **show cdma pdsn session msid** を実行すると、セッション情報は一切出力されません。**clear cdma pdsn session msid** コマンドにも同じ状況が当てはまります。

## IMSI プレフィックスのマスキング解除に関する制限

- クラスタ コントローラ アーキテクチャでは、コントローラとメンバの両方で、IMSI プレフィックス機能のマスキング解除をイネーブルにする必要があります。
- セッションがない PDSN でこの機能をイネーブルにする必要があります。PDSN にセッションが存在する場合、この機能の設定または削除を行うことはできません。
- この機能をイネーブルにする場合、アカウントング レコードは 10 桁の IMSI になります。
- AAA サーバで POD IMSI を設定します。PDSN は下位 10 桁と比較し、セッションが存在するかどうかを確認します。
- 3.0 または 4.0 メンバを使用して、5.0 コントローラでこの機能をイネーブルにします。この場合、コントローラは下位 10 桁を記録し、メンバに 15 桁で返信します。

## IMSI プレフィックスのマスキング解除の設定

次の CLI コマンドで、PDSN の IMSI プレフィックスのマスキング解除を設定します。この CLI コマンドは、新しいウィンドウで（セッションがない状態で）設定することをお勧めします。

```
Router(config)# cdma pdsn imsi-min-equivalence
```

設定を削除するには、次のように記述します。

```
Router(config)# no cdma pdsn imsi-min-equivalence
```

次の例は、**show cdma pdsn session msid** コマンドに対する下位 11 桁がある出力の抜粋を示しています。

```
pdsn-act# show cdma pdsn session msid 45678987655
```

```
Mobile Station ID IMSI 112345678987655
PCF IP Address 4.0.0.1, PCF Session ID 1
A10 connection time 00:02:33, registration lifetime 20000 sec
Number of successful A11 reregistrations 0
Remaining session lifetime 19846 sec
Always-On not enabled for the user
Current Access network ID 0004-0000-01
```

```

Last airlink record received is Active Start, airlink is active
GRE protocol type is 0x8881
GRE sequence number transmit 13, receive 0
Using interface Virtual-Access3, status OPN
Using AHDLC engine on slot 0, channel ID 2
Service Option 1xRTT Flow Discrimination 0 DSCP Included 0
Flow Count forward 0 reverse 0
This session has 1 flow
This session has 0 service flows
Session Airlink State Active
This session has 0 TFTs
Qos subscriber profile
    
```

次の例は、**show cdma pdsn session msid** コマンドに対する下位 10 桁がある出力の抜粋を示しています。

```

pdsn-act# show cdma pdsn session msid 5678987655
Mobile Station ID IMSI 112345678987655
PCF IP Address 4.0.0.1, PCF Session ID 1
A10 connection time 00:02:48, registration lifetime 20000 sec
Number of successful A11 reregistrations 0
Remaining session lifetime 19831 sec
Always-On not enabled for the user
Current Access network ID 0004-0000-01
Last airlink record received is Active Start, airlink is active
GRE protocol type is 0x8881
GRE sequence number transmit 13, receive 0
Using interface Virtual-Access3, status OPN
Using AHDLC engine on slot 0, channel ID 2
Service Option 1xRTT Flow Discrimination 0 DSCP Included 0
Flow Count forward 0 reverse 0
This session has 1 flow
This session has 0 service flows
Session Airlink State Active
This session has 0 TFTs
Qos subscriber profile
    
```

次の例は、**show cdma pdsn accounting** コマンドに対する出力を抜粋して示しています。

```

pdsn1# show cdma pdsn accounting
UDR for session
session ID: 1
Mobile Station ID IMSI 112345678987655

A - A1:5678987655 A2: A3:
C - C3:0
D - D3:11.1.1.12 D4:000000000000
E - E1:0000
F - F1:0000 F2:0000 F5:003B F6:00 F7:00 F8:00
  F9:00 F10:00 F14:00 F15:0
  F16:00 F17:00 F18:00
  F19:00 F20:00 F22:00
G - G3:0 G8:0 G9:0 G10:0 G11:0 G12:0
  G13:0 G14:176 G15:0 G16:0 G17:0
I - I1:0 I4:0
Y - Y2:1

UDR for flow
Mobile Node IP address 9.1.1.9
B - B1:9.1.1.9 B2:g7SIP1@xxx.com
C - C1:0025 C2:98 C4:0
D - D1:0.0.0.0
F - F11:01 F12:00 F13:00
G - G1:0 G2:0 G4:1243836799
    
```

```
G22:0 G23:0 G24:0 G25:0
Packets- in:0 out:0
```

次の例は、**show cdma pdsn accounting detail** コマンドに対する出力を抜粋して示しています。

```
pdsn1# show cdma pdsn accounting detail
UDR for session
session ID: 1
Mobile Station ID IMSI 112345678987656

Mobile Station ID (A1) IMSI 5678987656
ESN (A2)
MEID (A3)
Session Continue (C3) ' ' 0
Serving PCF (D3) 11.1.1.12 Base Station ID (D4) 000000000000
User Zone (E1) 0000
Forward Mux Option (F1) 0 Reverse Mux Option (F2) 0
Service Option (F5) 59 Forward Traffic Type (F6) 0
Reverse Traffix type (F7) 0 Fundamental Frame size (F8) 0
Forward Fundamental RC (F9) 0 Reverse Fundamntal RC (F10) 0
DCCH Frame Format (F14) 0 Always On (F15) 0
Forward PDCH RC (F16) 0 Forward DCCH Mux (F17) 0
Reverse DCCH Mux (F18) 0 Forward DCCH RC (F19) 0
Reverse DCCH RC (F20) 0 Reverse PDCH RC (F22) 0

Bad PPP Frame Count (G3) 0 Active Time (G8) 0
Number of Active Transitions (G9) 0
SDB Octet Count Terminating (G10) 0
SDB Octet Count Originating (G11) 0
Number of SDBs Terminating (G12) 0
Number of SDBs Originating G13 0
Number of HDLC Layer Bytes Received (G14) 290
In-Bound Mobile IP Signalling Octet Count (G15) 0
Out-bound Mobile IP Signalling Octet Count (G16) 0
Last User Activity Time (G17) 0
IP Quality of Service (I1) 0
Airlink Quality of Service (I4) 0
R-P Session ID (Y2) 1

UDR for flow
Mobile Node IP address 9.1.1.1
IP Address (B1) 9.1.1.1, Network Access Identifier (B2) g7SIP1@xxx.com
Account Session ID (C1) 2
Correlation ID (C2) ' ' 18
Beginning Session (C4) ' ' 0
MIP Home Agent (D1) 0.0.0.0
IP Technology (F11) 01 Compulsory Tunnel indicator (F12) 00
Release Indicator (F13) 00
Data Octet Count Terminating (G1) 0
Data Octet Count Originating (G2) 0 Event Time G4:1243950581
Rsvp Signaling Inbound Count (G22) 0 Outbound Count (G23) 0
Rsvp Signaling Packets In (G24) 0 Packets Out (G25) 0
Packets- in:0 out:0
```

## 永続的な TFT のサポート

今回のリリースで、Traffic Flow Template (TFT) のインストールがサポートされました。TFT は、AAA サーバアトリビュートに依存する必要があります。PDSN は、access-accept の一部として AAA サーバから 3GPP2 アトリビュート タイプ 89 (cdma-num-persistent) アトリビュートを受信しない場

合、Resource reSerVation Protocol (RSVP; リソース予約プロトコル) メッセージを拒否し、TFT のインストールに失敗します。AAA サーバアトリビュートへの依存関係を削除するために、今回のリリースでは AAA サーバとローカル QoS のプロファイルをマージしました。

次の新しいコマンドを使用すると、TFT をインストールする前に、AAA からダウンロードした 3rd Generation Partnership Project 2 (3GPP2; 第 3 世代パートナーシップ プロジェクト 2) アトリビュート タイプ 89 (cdma-num-persistent) をチェックできます。

```
router(config)# cdma pdsn tft persistent-check
```

設定によっては、PDSN は次のように動作します。

- 新しいコマンドがデフォルトで設定されていない場合、PDSN は RSVP パケットの受信時に TFT をインストールします。
- 新しいコマンドが設定されている場合
  - かつ永続的 TFT アトリビュートが AAA サーバからダウンロードされる場合、PDSN は TFT をインストールします。
  - かつ PDSN が AAA サーバが cdma-num-persistent アトリビュートをダウンロードしていない場合、PDSN はローカル QoS プロファイルを適用します。
  - かつ AAA がタイプ 89 (cdma-num-persistent) 以外の値を返す場合、PDSN は TFT をインストールしません。
  - かつ AAA サーバがアトリビュートを返さず、PDSN がローカル加入者プロファイルで設定されていない場合、PDSN は TFT をインストールしません。
  - かつ AAA サーバがアトリビュートを返さず、PDSN が tft-allowed コマンドを使用してローカル加入者プロファイルでイネーブルにされていない場合、PDSN は TFT をインストールしません。
- CLI コマンドが設定されている場合、Cisco PDSN リリース 4.0 の動作が保持されます。

設定を削除するには、次のコマンドを使用します。

```
router(config)# no cdma pdsn tft persistent-check
```

## FA-HA IP-in-IP トンネルの場合の一意的な IP-ID の保存

今回のリリースで PDSN は、パケットに断片化の機会がある場合に、IP ヘッダーに一意的な ID を保存することで、IP ヘッダーの ID フィールドに有効な値を設定できます。この機能を使用すると、短時間で ID 番号を繰り返すことを回避できるため、パケットの重複も回避できます。

次の新しいコマンドを使用すると、パケットサイズのしきい値を設定できます。

```
Router(config)# ip mobile tunnel ip-ip conserve-ip-id threshold value
```

この *value* は、パケットのしきい値を示します。また、*ip-id* は以下の値になります。

- パケット サイズがしきい値を上回る場合はゼロ以外の数字
- パケット サイズがしきい値を下回る場合はゼロ

次の例は、**ip mobile tunnel ip-ip conserve-ip-id threshold** コマンドに対する出力を抜粋して示しています。

```
pdsn_active(config)# ip mobile tunnel ip-ip conserve-ip-id threshold ?
<576-1500> length in bytes

pdsn_active(config)# ip mobile tunnel ip-ip conserve-ip-id threshold 600
pdsn_active(config)# end
```

```
pdsn_active#
```

設定を削除するには、次のように記述します。

```
pdsn_active(config)# no ip mobile tunnel ip-ip conserve-ip-id threshold 600
pdsn_active(config)# end
pdsn_active#
```

## GRE CVSE Support in FA-HA Tunnel

今回のリリースでは、PDSN と HA が Generic Routing Encapsulation (GRE) キーをネゴシエーションできますが、以前のリリースでは、GRE 対応のリバース トンネルを経由して渡されるパケット (FA-to-HA) は、ゼロのデフォルト キー値を持ちます。このネゴシエーションは、Foreign Agent-Home Agent (FA-HA) トンネルで GRE Critical Vendor-Specific Extension (CVSE) のサポートを使用して行うことができます。

FA および HA は各自固有のキーを生成できます。または、FA および HA は FA が生成したキーを使用できます。GRE キーの CVSE を HA に送信するには、次のコマンドを設定します。

- すべての MIP RRQ ですべての HA に GRE CVSE を送信するには、次のように記述します。  
**Router(config)# cdma pdsn attribute send gre\_cvse mip\_rrq**
- HA 単位で GRE CVSE を送信するには、次のように記述します。  
**Router(config)# ip mobile foreign-agent extension gre home-agent address range or a single address**

次の例は、**show ip mobile visitor** コマンドに対する出力を抜粋して示しています。

```
pdsn_active# show ip mobile visitor
Mobile Visitor List:
Total 1
mwts-mip-np-user11@ispxyz.com:
  Home addr 12.1.1.10
  Interface Virtual-Access2.1, MAC addr 0000.0000.0000
  IP src 0.0.0.0, dest 4.1.1.1, UDP src port 434
  HA addr 4.1.1.2, Identification CDF2DC2A.10000
  Lifetime 00:01:00 (60) Remaining 00:00:45
  Tunnel0 src 4.1.1.1, dest 4.1.1.2, reverse-allowed
  gre cvse enable
  FA provided key 1253037210, HA returned key 2926312514
  Routing Options - (G)GRE (T)Reverse Tunneling
```

次の例は、**show ip mobile proxy registration** コマンドに対する出力を抜粋して示しています。

```
pdsn_active# show ip mobile proxy registration

Proxy Mobile Node Registrations:

userpmip1@ispxyz.com:
  Registration accepted 06/29/09 06:27:11
  Next Re-registration 00:00:13
  Registration sequence number 1
  Care-of addr 4.1.1.1, HA addr 4.1.1.2, Home addr 12.1.1.12
  gre cvse enable
  FA provided key 1527991487, HA returned key 3076709629
  Flags sbdmG-T-, Identification CDF2DD3F.8CB49CB8
  Lifetime requested 00:01:00 (60), granted 00:01:00, remaining 00:00:43
```

次の例は、**show ip mobile tunnel** コマンドに対する出力を抜粋して示しています。

```
pdsn_active# show ip mobile tunnel
```

```

Mobile Tunnels:
Total mobile ip tunnels 1
Tunnel0:
  src 4.1.1.1, dest 4.1.1.2
  encaps GRE/IP, mode reverse-allowed, tunnel-users 1
Multiple GRE keys supported
  Input ACL users 0, Output ACL users 0
  IP MTU 1472 bytes
  Path MTU Discovery, mtu: 0, age: 10 mins, expires: never
  outbound interface Ethernet1/0
  FA created, CEF switching enabled, ICMP unreachable enabled
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 drops
  0 packets output, 0 bytes

```

**cdma pdsn attribute send gre\_cvse mip\_rrq** コマンドを設定するには、次のように記述します。

```

pdsn_active# conf term
pdsn_active(config)# cdma pdsn attribute send gre_cvse mip_rrq
pdsn_active(config)# end

```

**ip mobile foreign-agent extension gre home-agent** コマンドを設定するには、次のように記述します。

```

pdsn_active# conf term
pdsn_active(config)# ip mobile foreign-agent extension gre home-agent 4.1.1.2
pdsn_active(config)# end

```

設定を削除するには、次のように記述します。

```

pdsn_active# conf term
pdsn_active(config)# no cdma pdsn attribute send gre_cvse mip_rrq

pdsn_active# conf term
pdsn_active(config)# no ip mobile foreign-agent extension gre home-agent 4.1.1.2

```

## リモート アドレス アカウンティング

今回のリリースでは、PDSN が Remote Address-based Accounting (RAA) をサポートできるようになりました。RAA を使用すると、パケットデータ セッション中に、モバイル ステーション (MS) とリモート IP アドレスの間で交換されたオクテット数をカウントできます。PDSN は、認証手続き中に Home RADIUS サーバから受信したユーザ プロファイルに従って、このアカウンティング機能をユーザ単位でイネーブルにします。PDSN は、AAA サーバからの Remote Address Table Index アトリビュートをサポートして、セッションで RAA をイネーブルにします。PDSN は IP アドレスを認識できる場合にだけ RAA をサポートします。たとえば、Virtual Packet Data Network (VPDN; 仮想パケットデータ ネットワーク) では、IP パケットはないため、PDSN は VPDN コールのために RAA をサポートしません。

次の章では、以下の内容について説明します。

- 「セッションのセットアップ」
- 「G5 アトリビュートについて」
- 「RADIUS からダウンロードした 835B 準拠の RAA テーブルインデックスのサポート」



## セッションのセットアップ

ここでは、セッションをセットアップするワークフローについて説明します。最初のコール設定時に、PDSN は AAA サーバで認証し、**access-accept** の一部としてリモートテーブル インデックス アトリビュートをダウンロードします。**access-accept** 中に RAA テーブル インデックスのダウンロードすると、ダウンロードされた RAA テーブルのインデックスは、PDSN 上に設定されたテーブル インデックスに対してマッチングが実行されます。一致したインデックスはセッションに関連付けられ、一致しないインデックスはドロップされてセッションに関連付けられません。**force index match** が設定され、ダウンロードされたインデックスが設定された RAA テーブル インデックスと一致しない場合、セッションはドロップされます。

## G5 アトリビュートについて

G5 カウンタには、**forward octet count**、**reverse octet count**、RAA インデックスまたは **remote-network-and-mask** のペア、**forward octet overflow count**、および **reverse octet overflow count** のカウンタが含まれます。



(注)

G5 には、監視対象である RAA テーブル インデックスまたはネットワークかマスクの組み合わせが含まれます。

**remote address mask** は、リモート アドレス アカウンティングのアドレス範囲を示すために使用されます。PDSN は、そのマスクのすべてのリモート IP アドレスのオクテット カウントを集約し、1 つの **remote IPv4 octet-count** アトリビュートを生成します。

G5 アトリビュートは、**accounting stop** および **accounting interim** に含まれます。アトリビュートには次のような機能があります。

- G5 アトリビュートのインスタンスは、**accounting stop** の送信後に削除されます。マッチングに基づいて、新しいインスタンスが作成されます。
- パケットのマッチングは、セッションとフローの両方で行われます。
- **summarize** オプションが設定されていない場合、G5 カウンタには **network-and-mask** ペア（つまり、単一の IP アドレスを示すために使用される一意のホスト マスク）が含まれます。この時点でテーブル インデックスは存在しません。**summarize** オプションがテーブル インデックスのために設定された場合にだけ、インデックスは存在します。
- 冗長性の場合、テーブル パラメータと G5 コンテナは、スタンバイに同期されます。このとき、アクティブ PDSN で設定する場合、テーブル パラメータはスタンバイに同期されます。G5 コンテナが存在する場合、**accounting** 要求が送信されるたびに同期されます。
- バイト カウントがオーバーフローしていない場合でも、**accounting** 要求の一部として **octet overflow** アトリビュートは存在します。

次のワークフローで、トラフィック フロー中の G5 アトリビュートに対する更新について説明します。

1. ダウンストリーム トラフィックの場合で、そのセッションで RAA がイネーブルで、有効なインデックスがセッションに関連付けられている場合、発信元 IP アドレスが、関連付けられたインデックスの IP アドレスと一致するかどうかを PDSN はチェックします。アップストリーム トラフィックの場合、送信先 IP アドレスが、関連付けられたインデックスの IP アドレスと一致するかどうかを PDSN はチェックします。
2. 一致が検出された場合、次のように処理されます。
  - a. G5 インスタンスが存在する場合、PDSN はバイトまたはオクテット カウントがカウントされます。トラフィックが既存の G5 コンテナに一致する場合、PDSN はそのコンテナで使用されるバイトをカウントします。

- b. `summarize` がイネーブルの場合、PDSN は単一の G5 インスタンスの packets をカウントします。Remote Table Index AAA サーバアトリビュートを使用して、`summarize` オプションをイネーブルまたはディセーブルにすることができます。
- c. 一致および対応する G5 インスタンスが存在しない場合（つまり、作成済みの場合）、PDSN は G5 インスタンスを作成し、それをカウントします。

## RADIUS からダウンロードした 835B 準拠の RAA テーブル インデックスのサポート

AAA サーバからダウンロードした IS835B 準拠の RAA テーブル インデックスをサポートするには、新しい `cdma pdsn accounting remote address compliance 835b` コマンドをグローバル コンフィギュレーション モードで使用します。

次の点に注意してください。

- CLI コマンドの設定時に、835B に準拠するテーブル インデックスだけが受け入れられます。他のフォームは拒否され、対応するセッションは終了します。
- CLI コマンドがディセーブルの場合、835C または D および B に準拠するテーブル インデックスが受け入れられます。他のフォームは拒否され、対応するセッションは終了します。デフォルトでは、このコマンドはディセーブルです。
- IS835B および IS835C に準拠する RAA テーブル インデックスの場合、`remote address octet count` は IS835C フォーマットだけです。
- RADIUS からダウンロードした IS835B 準拠の RAA テーブル インデックスがデフォルトでサポートされます。このコマンドは、ダウンロードしたテーブル インデックス (IS835B フォーマット) を必須にするように設定されます。



(注) RAA がイネーブルの場合は次のとおりです。

- IP flow accounting はイネーブルになりません。
- IPv6 アドレス指定はサポートされません。
- Prepaid exempt はサポートされません。
- RAA 対応のセッションが存在する場合、RAA テーブルを削除できません。ただし、RAA テーブルのコンテンツは変更できます。その変更は、以降のセッションおよび再登録されたセッションで有効になります。
- `access-accept` 中に AAA サーバからダウンロードされたリモート アドレスはサポートされません。リモート テーブル インデックスだけがサポートされます。

## リモート アドレス アカウンティングの設定

リモート アドレス アカウンティングのために次のコマンドが導入されました。

リモート アドレス テーブルを設定するには、次のように記述します。

```

psdn(config)# cdma pdsn accounting remote address table
psdn(config-raa)# index number
psdn(config-raa-table)# description string
psdn(config-raa-table)# remote address ip-addr ip-addr mask

```

テーブルに設定されたリモートアドレスを削除するには、次のように記述します。

```
pdsn(config)# cdma pdsn accounting remote address table
pdsn(config-raa)# index number
pdsn(config-raa-table)# no remote address ip-addr
```

インデックスを削除するには、次のように記述します。

```
pdsn(config)# cdma pdsn accounting remote address table
pdsn(config-raa)# no index number
```

リモートアドレス テーブルを削除し、リモートアドレス アカウンティング機能をディセーブルにするには、次のように記述します。

```
pdsn(config)# no cdma pdsn accounting remote address table
```



(注) RAA 対応のセッションが存在する場合、設定はディセーブルにできません。

リモートアドレス アカウンティングを強制するには、次のように記述します。

```
pdsn(config)# cdma pdsn accounting remote address table index match
```



(注) このコマンドは、ダウンロードした RAA インデックスと、PDSN に設定されているインデックスとの照合を強制的に行うように設定されます。そのセッションでダウンロードされたテーブル インデックスのいずれも PDSN で設定されていない場合、セッションは作成されません。

force remote address accounting を削除するには、次のように記述します。

```
pdsn(config)# no cdma pdsn accounting remote address table index match
```

次の例は、リモートアドレス アカウンティングがイネーブルの場合の **show run** コマンドに対する出力を抜粋して示しています。

```
cdma pdsn accounting remote address table
index 1
  description test1
  remote address 1.1.1.1 255.255.255.255
  remote address 2.2.2.0 255.255.255.0
  remote address 10.10.10.5 255.255.255.255
index 2
  description test2
  remote address 3.3.3.3 255.255.255.255
  remote address 4.4.4.0 255.255.255.255
cdma pdsn accounting remote address index match
```

次のコマンドで、すべての RAA 関連の統計情報がクリアされます。

```
pdsn# clear cdma pdsn statistics
```

次のコマンドで、AAA サーバからダウンロードされた 835B 準拠の RAA テーブル インデックスのサポートがイネーブルになります。

```
pdsn(config)# cdma pdsn accounting remote address compliance 835b
```

このコマンドを使用すると、PDSN は AAA サーバからダウンロードした IS835B 準拠の AAA テーブル インデックスだけを受け入れます。このコマンドをディセーブルにすると、PDSN は、IS835C または D および B に準拠する AAA サーバからダウンロードした RAA テーブル インデックスを受け入れます。その他のフォームは拒否されます。このコマンドはデフォルトでディセーブルに設定されています。

次のコマンドで、AAA サーバからダウンロードされた 835B 準拠の RAA テーブル インデックスの場合にだけ、サポートがディセーブルになります。

```
pdsn(config)# no cdma pdsn accounting remote address compliance 835b
```

次の新しいコマンドで、リモート アドレス アカウンティングをデバッグできます。

```
pdsn# debug cdma pdsn accounting raa errors
```

CDMA PDSN Remote address based accounting errors debugging はオンです。

```
pdsn#debug cdma pdsn accounting raa events
```

CDMA PDSN Remote address based accounting events debugging はオンです。

Cisco PDSN リリース 5.1 のリモート アドレス アカウンティングのデバッグについて詳しくは、『Cisco Packet Data Serving Node Release 5.0 for Cisco IOS Release 12.4(22)XR1』のデバッグ コマンドを参照してください。

## デフォルトのサービス オプション実装

アカウンティング レコードの一部として、PDSN は次のいずれかの場合に AAA サーバにゼロを送信します。

- F5 Service Option の値としてゼロを受信した場合。  
または
- airlink start を受信しなかった場合。

F5 Service Option 値を制御された方法でゼロ以外の値に設定する場合、次の新しいコマンドを使用し、アカウンティングにデフォルトの SO 値を設定できるようになりました。

```
Router(config)# [no] cdma pdsn a11 default-service-option value
```

この新しいコマンドを使用すると、アカウンティングにデフォルトの SO 値を設定できます。

この設定を削除するには、このコマンドの **no** フォームを使用します。



(注)

F5 アトリビュート値が受信した airlink start レコードに存在せず、ゼロ以外の値がすでにある場合、Usage Data Record (UDR) の F5 を変更しないでください。UDR の F5 値がゼロの場合、A10 サービス オプション値で F5 を更新します。A10 サービス オプション値が使用できない場合、新しいコマンドを使用して設定された値でアトリビュートを更新します。

## Configurable Per-Flow アカウンティング オプション

現在、PDSN はフローごとのアカウンティングをサポートしています。つまり、アカウンティング レコードはフローごとに送信されます (IP フロー)。今回のリリースでは、PDSN が configurable per-flow アカウンティングをオプションでサポートできるようになりました。これは、CLI コマンドの設定か、アカウンティング オプションのダウンロードによって決まります。

次の章では、以下の内容について説明します。

- 「Per-Flow アカウンティング オプションの設定」
- 「per-flow アカウンティング オプションを設定する機能フロー」
- 「configurable per-flow アカウンティング オプション用のセッションとフローのセットアップ」
- 「per-flow アカウンティング オプション設定の制限」

## Per-Flow アカウンティング オプションの設定

次のコマンドは、PDSN の per-flow アカウンティング オプションの設定に使用されます。

メイン フローで CDMA PDSN アカウンティングを設定するには、次のように記述します。

```
pdsn_act(config)# cdma pdsn accounting [main flow] ?
```

この **main flow** にはオプションでアカウンティングのメイン フローを設定します。

IPlows など、CDMA PDSN アカウンティング メイン フローを設定するには、次のように記述します。

```
pdsn_act(config)# cdma pdsn accounting [main flow include ipflows]
```

この **main flow include ipflows** には、オプションでアカウンティング メイン フローの IP フローを含めます。

CDMA PDSN アカウンティングの設定を削除するには、次のように記述します。

```
pdsn_act(config)# no cdma pdsn accounting ?
```

```
local-timezone Enable local timezone values for accounting
```

```
main flow Accounting on Main Flow
```

```
prepaid Prepaid related configurations
```

```
remote Configure Remote Accounting
```

```
send Accounting option
```

```
time-of-day Generate accounting record at specified time
```

```
pdsn_act(config)# no cdma pdsn accounting main flow ?
```

アカウンティング オプションの設定オプションは、次のとおりです。

### オプション 1 - メイン フロー専用のアカウンティング オプションの設定 :

アカウンティング オプション (Cisco VSA 全般) が AAA サーバから 2 としてダウンロードされるか、**cdma pdsn accounting main flow** コマンドがイネーブルの場合。

### オプション 2 - メイン フローに Ipflow を含める場合のアカウンティング オプションの設定 :

アカウンティング オプション (Cisco VSA 全般) が AAA サーバから 3 としてダウンロードされるか、**cdma pdsn accounting main flow include ipflows** コマンドがイネーブルの場合、アカウンティング レコードはメイン フローに単独で送信され、IP フローの詳細が含まれます。

## デフォルトのオプション - per-flow アカウンティング :

オプション 1 が設定されると、per-flow アカウンティングが実行されます。AAA サーバからダウンロードしたアカウンティング オプション (Cisco VSA 全般) がオプション 1 でもオプション 2 でもない場合、または `cdma pdsn accounting main-flow` コマンドも `cdma pdsn accounting main-flow include ipflows` コマンドもイネーブルではない場合、デフォルトのオプションが設定されます。

## per-flow アカウンティング オプションを設定する機能フロー

この設定の機能フローには 3 つのオプションがあります。Only Main Flow、Include IP flow in Main Flow、および Per-Flow Accounting (デフォルト) です。

### オプション 1 - Only Main Flow :

アカウンティングはメインフローだけで行われます。IPflow のアカウンティング レコードは送信されません。しかし、TFT が一致する場合、アップストリームとダウンストリーム トラフィックは、それぞれ IPflow と aux A10 だと見なされます。ただし、アカウンティング レコード (start または stop または interim) は IPflow 用に送信されません。メインフローのアカウンティング レコード (interim および stop) が送信されるとき、G1 または G2 用のカウンタ、IPflow の送受信パケットは含まれません。

### オプション 2 - Include IP Flow in Main Flow :

アカウンティングはメインフローだけで行われます。IPflow のアカウンティング レコードは送信されません。しかし、TFT が一致する場合、アップストリームとダウンストリーム トラフィックは、それぞれ IPflow と aux A10 だと見なされます。ただし、アカウンティング レコード (start または stop または interim) は IPflow 用に送信されません。メインフローのアカウンティング レコード (interim および stop) が送信されるとき、G1 または G2 用のカウンタ、IPflow の送受信パケットは G1 または G2 とメインフローの送受信パケットに追加されます。

### デフォルトのオプション - Per Flow Accounting :

per-flow (IP フロー) ベースのアカウンティングが行われます。アカウンティング レコードは、メインフローと IPflow 用に送信されます。

## configurable per-flow アカウンティング オプション用のセッションとフローのセットアップ

最初のコール設定時に、PDSN は AAA サーバで認証し、access-accept の一部としてアカウンティング オプションをダウンロードします。アトリビュートのダウンロード時、PDSN はダウンロード オプションが有効かどうか確認します。有効なオプションであれば、セッションにコピーされます。有効でない場合、PDSN は CLI コマンドの設定をチェックします。アカウンティング オプションが設定されている場合、セッションにコピーされます。アカウンティング オプションが設定されていない場合、アカウンティング オプションはありません。

IPflow 用に `airlink` レコードが受信された場合、レコードは解析され更新されます。アカウンティング オプションが有効な場合、IPflow 用のアカウンティング レコードは送信されません。アップストリームおよびダウンストリーム トラフィックは、TFT のチェック後、それぞれの IPflow と aux A10 を介して送信されます。

アカウンティング レコード (interim および stop) を送信する前、PDSN はアカウンティング オプションと依存するアカウンティング オプション値を確認します。メインフローのそれぞれのアトリビュートに、G1 または G2、送信または受信パケットを含めるかどうか決定できます。アカウンティング オプションが有効な場合は、メインフロー用の IPflow をフラッシュするとき、G1 または G2、IPflow の送受信パケットをリセットできます。

## per-flow アカウンティング オプション設定の制限

per-flow アカウンティング オプション設定には、次の制限があります。

- アカウンティング オプションが 2 回ダウンロードされた場合、最初のダウンロードだけが有効と見なされます。
- ダウンロードされたアトリビュートは、設定された値よりも優先されます。
- アカウンティング オプションはセッション ベースです。フロー ベースではありません。
- アカウンティング オプションは単一フローにだけ有効と見なされます。複数の MIP フロー、または SIP、MIP フローが開かれている場合、同じアカウンティング オプションがそれぞれのフローに適用されます。
- **cdma pdsn accounting main flow** または **cdma pdsn accounting main flow include ipflows** 設定コマンドを削除すると、アカウンティング オプション設定は削除されます。
- 冗長性を維持するため、アカウンティング オプションはスタンバイに同期されます。

## IP フロー識別子の PCF 下位互換性サポート

PDSN は GRE ヘッダーに 4 バイトの IPflow 識別子を追加します。ただし、PCF には、標準 A.S0008 v3.0 (IPflow 識別子を、より小さい値である予約バイトなしの 3 バイトに定義している) に基づいているものもあります。

今回のリリースは、IPflow 識別子について、グローバル コンフィギュレーション モードで次の新しいコマンドを使用することで、PCF の下位互換性をサポートしています。

**pdsn# cdma pdsn compliance hrpd ipflow-discriminator**

このコマンドの設定で、IPflow 識別子は 3 バイトの新しいフォーマットで定義されます。A10 は予約バイトなしの 3 バイトの IPflow 識別子を保持します。デフォルトでは、このコマンドはディセーブルです。

## max-class 値に対する DSCP のコメントのサポート

PDSN は、不正な Differentiated Services Code Point (DSCP; DiffServ コード ポイント) の値を持つアップストリーム パケットを認識して、ゼロ、またはグローバル設定コマンド **cdma pdsn multiple service-flows qos remark-dscp remark\_value** で指定された値でコメントします。すべての不正パケットは、0、またはこのコマンドで指定されたグローバル値だけでコメントされます。



(注) DSCP は、AAA サーバからダウンロードされるかローカルで設定された max-class 値より大きい値です。

不正パケットの DSCP 値に、ユーザ単位で DSCP 値にコメントするため、今回のリリースでは新しいコマンドが導入されました。

パケットの DSCP 値に、AAA サーバからダウンロードされるかローカルで設定された max-class 値をコメントするには、次のように記述します。

**pdsn# cdma pdsn multiple service-flows qos remark-maxclass**

今回のリリースから、PDSN は次の 3 つの方法で DSCP 値にコメントできます。

- 新しいコマンド **cdma pdsn multiple service-flows qos remark-maxclass** が設定されておらず、また **cdma pdsn multiple service-flows qos remark-dscp remark\_value** だけが設定されているとき、着信パケットの DSCP 値が max-class 値より大きい場合に、PDSN は DSCP 値を **cdma pdsn multiple service-flows qos remark-dscp remark\_value** コマンドで指定された *remark\_value* でコメントします。
- 2つのコマンド **cdma pdsn multiple service-flows qos remark-max-class** および **cdma pdsn multiple service-flows qos remark-dscp remark\_value** が設定されているとき、着信パケットの DSCP 値が max-class 値より大きい場合に、PDSN は DSCP 値を max-class 値でコメントします。
- 2つのコマンド **cdma pdsn multiple service-flows qos remark-maxclass** および **cdma pdsn multiple service-flows qos remark-dscp remark\_value** が設定されていないとき、着信パケットの DSCP 値が max-class 値より大きい場合に、PDSN は DSCP 値を 0x00 でコメントします。

## フラグメンテーション サイズのコマンド サポート

今回のリリースで、1次パケットのフラグメンテーション サイズを設定できる新しいコマンドが導入されました。それによって、ネットワークでの2次フラグメントによる以降のフラグメンテーションが回避されます。IPフラグメンテーションでは、1次フラグメントは、内側のパケットのレイヤ4ヘッダー情報を含まない場合があります。そのため、レイヤ4までの広範な検査を実行するネットワーク上のファイアウォールは、1次フラグメントをドロップする場合があります。

1次フラグメント サイズを設定してネットワークが最初のセグメントをドロップしないようにするため、グローバル コンフィギュレーション モードでの次の新しいコマンドを使用して、1次パケットのフラグメンテーション サイズを `Offset = 0` と設定することができます。

```
pdsn# ip fragment first minimum size ?
```

この *size* は 8 ~ 560 バイトの数値を示します。

*size* は、8 バイトの倍数で、ペイロードだけを含み、他のヘッダーを含まないようにする必要があります。それ以外の場合、コマンドは拒否され、次のエラー メッセージが表示されます。

```
%% First fragment payload size is not in multiples of 8.
```

## China Telecom 向けの新しい統計カウンタ

今回のリリースで、China Telecom 向けの新しい統計カウンタがサポートされました。

現在、CLI の PDSN 関連の統計情報だけがサポートされており、Exhaustion of Prepaid Quota は CLI で提供されます。今回のリリースは PCF カウンタ単位の A11 レジストレーション更新をサポートします。

新しいメトリックのリストは、PDSN の SNMP 経由で China Telecom から利用できるようになりました。次の統計カウンタがサポートされています。

- 「PCF レベル単位の前払い統計情報」
- 「PCF 間のハンドオフ RRQ」
- 「受け入れられた PCF 間のハンドオフ」
- 「EVDO ネットワーク初期 aux A10 接続要求」
- 「成功した PPP 接続要求」
- 「成功した PPP 初期要求」
- 「失敗した PPP 接続要求」
- 「LCP 段階前に PCF が A10 を終端」



- 「L2TP トンネル用の初期接続要求」
- 「成功した L2TP トンネル用の要求」
- 「失敗した L2TP トンネル用の要求」
- 「RP インターフェイスのアウトバウンドおよびインバウンドバイト」

## PCF レベル単位の前払い統計情報

EXEC モードの CLI コマンド **show cdma pdsn statistics prepaid** は、PCF レベル単位に強化されています。更新されたコマンドで、PCF レベル単位の前払い統計情報が得られます。

PCF レベル単位の前払い統計情報カウンタには、Total Online Access Response Received カウンタおよび Discarded カウンタはありません。ただし、これらのカウンタは、グローバル レベルの前払い統計情報で利用できます。オンライン応答を処理しているときにセッションが削除された場合、カウンタの PCF レベル単位は増加できません。

次の例は、**show cdma pdsn statistics prepaid pcf** コマンドに対する出力を抜粋して示しています。

```
pdsn1_act# show cdma pdsn statistics prepaid pcf 2.2.2.1
PCF 2.2.2.1, Service Option 59
Total prepaid flows opened: 0
  Volume-based 0, Duration-based 0
  Simple IP 0, VPDN 0, Proxy Mobile IP 0, Mobile IP 0
Total online Access Requests sent 0
Total online Access Response
Accepted 0, Timeout 0
Online Access Requests sent with Update Reason:
Pre-Initialization          0
Initial Request             0
Threshold Reached           0
Quota Reached               0
Remote Forced Disconnect    0
Client Service Termination  0
Main SI Released            0
SI not established          0
Tariff Switch Update        0
```

## PCF 間のハンドオフ RRQ

現在、CLI の PDSN 関連の統計情報だけがサポートされています。今回のリリースは、PCF 間のハンドオフ RRQ をサポートします。PDSN には、PCF 単位に基づく PCF 間のハンドオフ用のカウンタがあります。

## 受け入れられた PCF 間のハンドオフ

現在、CLI の PDSN 関連の統計情報だけがサポートされています。今回のリリースは、承認済み PCF 間のハンドオフをサポートします。PDSN には、PCF 単位に基づく、承認済み PCF 間のハンドオフ用のカウンタがあります。

## EVDO ネットワーク初期 aux A10 接続要求

現在、CLI の PDSN 関連の統計情報だけがサポートされています。今回のリリースは、EVDO ネットワーク初期 aux A10 接続要求をサポートします。今回のリリースでは、aux A10 接続の合計数が要求され、「statistics rp」の下に新しいカウンタが追加され、PCF レベル単位がサポートされます。

## EVDO ネットワークの承認済み初期 aux A10 接続

今回のリリースは、EVDO ネットワークの承認済み初期 aux A10 接続をサポートします。今回のリリースでは、aux A10 接続の合計数が正常に作成され、「statistics rp」の下に新しいカウンタが追加され、PCF レベル単位がサポートされます。

### 新しい aux 接続の要求および承認

2つの新しいカウンタ、New Aux Connection Requested および New Aux Connection Accepted が EXEC モードの CLI コマンド **show cdma pdsn statistics rp** の下に追加されました。これらのカウンタは、PCF レベル単位でも使用できます。

PDSN が新しい aux 接続数を  $n$  作成するレジストレーションやレジストレーション要求を受信すると、New Aux Connection Requested カウンタは  $n$  ずつ増加します。すべての aux 接続が正常に作成された場合、New Aux Connection Accepted カウンタは  $n$  ずつ増加します。要求された aux 接続の作成に問題が生じた場合、New Aux Connection Accepted カウンタは増加しません。

次の例は、**show cdma pdsn statistics rp pcf pcf IP address** コマンドに対する出力を抜粋して示しています。

```
pdsn1_act# show cdma pdsn statistics rp pcf 2.2.2.1

PCF 2.2.2.1, Service Option 59
  Reg Request rcvd 2, accepted 2, denied 0, discarded 0
  Initial Reg Request rcvd 1, accepted 1, denied 0, discarded 0, AuxRequest 0
  Re-registration requests rcvd 1, accepted 1, denied 0, discarded 0
  Re-registration requests containing Active-Start 1, Active-Stop 0
  Re-registration requests containing new connections 0, missing connections 0,
remapping flows 0
  New Aux Connection Requested 4, New Aux Connection Accepted 4
  Handoff requests rcvd 0, accepted 0, denied 0, discarded 0, AuxRequest 0.
```

## 成功した PPP 接続要求

現在、成功した PPP 接続要求カウンタは China Telecom に準拠していません。今回のリリースでは、このカウンタは更新されると、MIB および PCF 単位に基づくカウンタにも追加されます。

IPCP は、ネゴシエーションと再ネゴシエーションのときに、PPP 接続要求カウンタで更新されます。VPDN では、PDSN は AAA サーバから認証応答成功メッセージを受信して、このカウンタを更新します。成功した PPP 接続要求総数の計算方法は、次のとおりです。

成功した PPP 接続要求総数 = (接続成功 + 再ネゴシエーション成功)。

VPDN コールの PPP 再ネゴシエーションは、PDSN に透過的です。VPDN コールに対しては、初期 PPP 接続ステータスだけが更新されます。

## 成功した PPP 初期要求

現在、成功した PPP 初期要求カウンタは China Telecom 定義に準拠していません。今回のリリースでは、このカウンタは更新されると、PCF 単位に基づくカウンタにも追加されます。

IPCP は、初期段階では PPP 初期要求カウンタで更新されます。VPDN の場合、PDSN は AAA から認証応答成功メッセージを受信して、このカウンタを更新します。

### PPP 統計情報接続成功カウンタ

VPDN コールでは、認証取得成功が受信されるとすぐに、L2TP トンネルの状態にかかわらず接続成功カウンタが増加します。

次の例は、**show cdma pdsn statistics ppp** コマンドに対する出力を抜粋して示しています。

```
pdsn1_act# show cdma pdsn statistics ppp
Last clearing of "show cdma pdsn statistics ppp" counters never
PPP:
  Current Connections 2
  Connection requests 2, success 2, failure 0, aborted 0
```

## 失敗した PPP 接続要求

コード障害の理由の 1 つに、割り当て用の IP リソースがないことがあります。現在、この障害の理由はサポートされておらず、CLI コマンドの PDSN 関連統計情報だけがサポートされています。今回のリリースで、この障害の理由がサポートされ、失敗した PPP 接続要求が MIB および PCF 単位に基づくカウンタに追加されます。

### 割り当て用の IP リソースがない場合の PPP 統計情報の新しいカウンタ

現在、IP プールが枯渇しているとき、IP プール名が AAA サーバからダウンロードされる場合、IPCP 段階で使用できる不明なカウンタが増加します。プール名がローカルで設定されている場合、リリースされているその他のカウンタは増加します。**show cdma pdsn statistics PPP** コマンドには、プール名が AAA サーバからダウンロードされたか、ローカルで設定されたかに関係なく、IP プールの枯渇によって IPCP 段階で失敗したセッション数を反映するための新しいカウンタが導入されています。

IP アドレス枯渇に関連する以前のカウンタの動作は変更されていません。ローカルの IP プール枯渇は IPCP 障害と見なされないため、新しいカウンタの値は、IPCP 段階の障害合計とは一致しません。

次の例は、**show cdma pdsn statistics ppp** コマンドに対する出力を抜粋して示しています。

```
pdsn_act# show cdm pdsn statistics ppp
Last clearing of "show cdma pdsn statistics ppp" counters 00:09:33
Last update received at 02:51:38 UTC Mar 1 2002
PPP:
  Current Connections 2
  Connection requests 11, success 2, failure 9, aborted 0
  Connection enters stage LCP 11, Auth 11, IPCP 11
  Connection success LCP 11, AUTH 11, IPCP 2
  Failure reason LCP 0, authentication 0, IPCP 9, other 0
  Failure reason lower layer disconnect 0

  A10 release before LCP nego by PDSN 0, by PCF 0

  IPCP Stage
  Failure Reasons Options 0, MaxRetry 0, Unknown 9
  Options failure reason MN Rejected IP Address 0
  LCP Term Req during IPCP nego sent 9, rcvd 0
  A10 release during IPCP nego by PDSN 0, by PCF 0
  No enough IP resource for allocation 9
```

## LCP 段階前に PCF が A10 を終端

現在、CLI の PDSN 関連の統計情報だけがサポートされています。今回リリースは、LCP 段階前に PCF が A10 を終端させた回数カウンタをサポートします。

### PCF レベル単位での PPP 統計情報

「LCP 段階前に PCF が A10 を終端」させた PPP 統計情報がわかるカウンタと、再ネゴシエーションの詳細は、PCF レベル単位で利用できるようになりました。

次の例は、**show cdma pdsn statistics ppp pcf pcf ip address** コマンドに対する出力を抜粋して示しています。

```
pdsn1_act# show cdma pdsn statistics ppp pcf 2.2.2.1

PCF 2.2.2.1, Service Option 59
Current Connections 1
Connection requests 1, success 1, failure 0, aborted 0

A10 release before LCP nego by PDSN 0, by PCF 0

Renegotiation total 0, by PDSN 0, by Mobile Node 0
Renegotiation success 0, failure 0, aborted 0
Renegotiation reason: address mismatch 0, lower layer handoff 0
GRE key change 0, other 0
```

## L2TP トンネル用の初期接続要求

現在、CLI の PDSN 関連の統計情報だけがサポートされています。今回のリリースは、L2TP トンネル用の初期接続要求をグローバルカウンタとしてサポートします。**show l2tp counters tunnel** コマンドを実行すると、XMIT からの Start-Control-Connection-Reply (SCCRQ) カウンタによって、L2TP トンネル用の初期接続要求の詳細がわかります。

## 成功した L2TP トンネル用の要求

現在、CLI の PDSN 関連の統計情報だけがサポートされています。今回のリリースは、成功した L2TP トンネル用の要求をグローバルカウンタとしてサポートします。**show l2tp counters tunnel** コマンドを実行すると、XMIT からの Start-Control-Channel-Connected (SCCCN) カウンタによって、成功した L2TP トンネル用の接続要求の詳細がわかります。

## 失敗した L2TP トンネル用の要求

現在、CLI の PDSN 関連の統計情報だけがサポートされています。今回のリリースは、失敗した L2TP トンネル用の要求をグローバルカウンタとしてサポートします。**show l2tp counters tunnel** コマンドを実行すると、XMIT からの SCCRQ、SCCCN カウンタによって、失敗した L2TP トンネル用の接続要求の詳細がわかります。

## アクティブおよび休止セッション カウンタ

アクティブカウンタ (PCF レベル単位でも利用可能)、および休止セッションカウンタで、休止状態のメイン接続の合計の詳細がわかります。

次の例は、**show cdma pdsn statistics pcf pcf ip address** コマンドに対する出力を抜粋して示しています。

```
pdsn1_act# show cdma pdsn pcf 2.2.2.1
PCF 2.2.2.1 has 1 session
Received 6 pkts (185 bytes), sent 15 pkts (640 bytes)

PCF Session ID 1, Mobile Station ID IMSI 09884708943
A10 connection age 01:40:24
A10 registration lifetime 65535 sec, time since last registration 6024 sec
Number of sessions Active 2, Dormant 0,
```

## RP インターフェイスのアウトバウンドおよびインバウンド バイト

今回のリリースで、RP インターフェイスのアウトバウンドおよびインバウンド バイト (SO=33,SO=59,SO=64,SO=67) が、PCF 単位に基づくカウンタに追加されました。

### サービス オプションによる RP インターフェイスのアウトバウンドおよびインバウンド バイト カウンタ

EXEC モードに新しい CLI コマンドが導入され、サービス オプションに基づく RP インターフェイスのアウトバウンドおよびインバウンド バイト合計数がわかるようになりました。このコマンドは、PCF レベル単位でも利用できます。

次の例は、**show cdma pdsn statistics service-option** コマンドに対する出力を抜粋して示しています。

```
san-pdsn# show cdma pdsn statistics service-option 33 ?
  pcf  give pcf ip for faster response!!
  |    Output modifiers
  <cr>

san-pdsn# show cdma pdsn statistics service-option 33 pcf ?
  A.B.C.D  PCF IP address

san-pdsn# show cdma pdsn statistics service-option 33 pcf 41.1.1.2
Service Option: 50 PCF: 41.1.1.2
  Bytes in: 0                      Bytes out: 0
  Packs in: 0                      Packs out: 0

san-pdsn# show cdma pdsn stat serv 59
Service Option: 59
  Bytes in: 184                    Bytes out: 506
  Packs in: 30                     Packs out: 1

san-pdsn# show cdma pdsn stat serv 59 pcf 41.1.1.3
Service Option: 59 PCF: 41.1.1.3
  Bytes in: 0                      Bytes out: 0
  Packs in: 0                      Packs out: 0
```

## 以前のリリースの機能

ここでは、Cisco PDSN リリース 5.1 よりも前のリリースで導入された機能について説明します。

### ユーザ間の優先度

PCF は、MN へのパケットをスケジューリングするために、ユーザ間の優先度アトリビュートを使用します。PDSN は、AAA サーバからの RADIUS access-accept メッセージでこのアトリビュートを受信します。

### ローマー ID

ローマー ID はルーセント社によって定義されたホーム エリア アトリビュートで、PDSN は AAA サーバからの RADIUS access-accept メッセージでこのアトリビュートを受信します。

## Served MDN

Served MDN は China Telecom によって定義されたベンダー固有アトリビュートです。これは Class IETF アトリビュートと似ています。PDSN は、AAA サーバからの RADIUS access-accept t メッセージで Served MDN アトリビュートを受信します。Served MDN は、セッションまたは IPflow のために AAA サーバに送信されるすべてのアカウントング要求メッセージに含まれます。

Served-MDN アトリビュートは China Telecom の VSA で、ユーザ単位の RADIUS access-accept メッセージの一部として AAA サーバからダウンロードされます。

**cdma pdsn attribute vendor 20942** コマンドを設定すると、PDSN は Served MDN アトリビュートを解析して、アカウントング メッセージでそのアトリビュートを送信します。解析が成功すると、アトリビュート値は、RADIUS access-accept メッセージを受信したユーザのフロー構造の一部として保存されます。

ダウンロードされた場合、このアトリビュートは、対応するフローおよび関連する IPflow のすべてのアカウントング要求メッセージ (start、stop、および interim-update) で送信されます。PDSN が単一の access-accept メッセージでこのアトリビュートの複数の値を受信して、その解析が成功すると、ダウンロードされたアトリビュートのリストに含まれる最後のインスタンスがフロー構造に保存されません。

Served-MDN VSA が不正なフォーマットや不適切な長さの場合、PDSN は access-accept をドロップします。また、対応する障害カウンタが増加します。PPP 再ネゴシエーションまたは MIP 再レジストレーションの際に access-accept でアトリビュートの新しい値を受信されると、最後にダウンロードされた値で既存の値が更新されます。以降の access-accept がこの値をダウンロードしない場合、既存の値が保持されます。

PCF 間のハンドオフの場合、accounting stop および accounting start メッセージの両方でこのアトリビュートが送信されます。PPP 再ネゴシエーションの場合、PDSN が新しい値を受信すると、フロー構造に新しい値が保存されます。セッションが休止され、accounting start stop がイネーブルでないときに新しいアトリビュート値がダウンロードされると、accounting stop には古い Served MDN アトリビュート値が含まれ、accounting start には新しい Served MDN アトリビュート値が含まれます。

不明な China Telecom アトリビュートを受信した場合、それらのアトリビュートは無視されます。

IETF class アトリビュートと CT VSA served MDN アトリビュートの両方が access-accept の一部としてダウンロードされた場合、両方のアトリビュートはセッションのアカウントング メッセージで AAA サーバに送信されます。

アカウントング、表示、デバッグで Served MDN アトリビュートをサポートするには、次のコマンドを実行します。

```
router (config)# cdma pdsn attribute vendor 20942
```

この新しいコマンドで、PDSN は Served MDN アトリビュートを解析し、アカウントング メッセージでアトリビュートを送信できるようになります。

## Framed Pool

Framed Pool アトリビュートは、PDSN が AAA サーバから RADIUS access-accept メッセージでダウンロードする IETF アトリビュートです。このアトリビュート値は、PDSN で設定された IP プールとマッチングするために PDSN が使用し、PPP IPCP ネゴシエーションを介して選択されたプールから IP アドレスを割り当てます。PDSN は、AAA サーバからプール名をダウンロードするための Cisco VSA をサポートします。この機能は、IETF VSA としてプール名をダウンロードするために必要です。

PDSN は、ユーザ フロー単位の **access-accept** メッセージの一部として、AAA サーバから IETF **framed-pool** アトリビュートをダウンロードします。ローカル プール名がダウンロードしたプール名と一致し、さらにプールに割り当て可能な IP アドレスがある場合、MN に IP アドレスが割り当てられ、その IP アドレスは MN への IPCP CONFNAK メッセージの一部として送信されます。

**access-accept** のときに、MN が固定 IP アドレスを要求し、IETF プール名もダウンロードされる場合、MN から要求された固定 IP アドレスは、その IP アドレスが PDSN で設定されたプールの範囲に含まれる場合に限り、優先されます。それ以外の場合、ダウンロードされたプールから IP アドレスが割り当てられます。

ローカルプールが PDSN で設定されたプール名と一致しない場合、または一致したプール名に割り当て可能なアドレスがない場合、PPP IPCP ネゴシエーションは失敗し、コールは終了します。**framed IP pool** アトリビュートおよび **Cisco av pair pool name** アトリビュートがダウンロードされる場合、IP アドレスはフレーム化プールから割り当てられます。複数の **framed IP pool** 名がダウンロードされると、IP アドレスはダウンロードされたプールの最初から割り当てられます。**framed IP pool** の IP アドレスが枯渇した場合、セッションは終了します。

IETF プール名は、AAA サーバ サブシステムによってスタンバイ ユニットに同期されます。このアトリビュートの解析と検証は、AAA サーバ サブシステムによって実行されます。

#### その他の考慮事項

SIP コールがサポートされます。他のすべてのコールについては、IP アドレス割り当ては HA が行い、VAAA のプール設定は PDSN から無視されます。

PMIP コールでは、HA に割り当てられるアドレスは、IETF プール名アトリビュート値がダウンロードされた場合でも、IPCP の一部として MN とネゴシエーションされます。

## 3GPP2 DNS サーバ IP

DNS サーバ IP アドレスアトリビュートは、RADIUS **access-accept** メッセージで PDSN が AAA サーバからダウンロードする 3GPP2 VSA です。AAA サーバからダウンロードされるこれらの IP アドレスは、IPCP ネゴシエーション中に要求された場合は MN に送信する必要があります。

PDSN は、**access-accept** メッセージの一部として AAA サーバからベンダー ID 117 と共に 3GPP2 DNS IP アドレス VSA をダウンロードします。ダウンロードしたアトリビュートは、プライマリおよびセカンダリ IP アドレスについて解析され、ユーザセッションの AAA サーバリストに保存します。**sub-type 3** および **4** で送信される値は、PDSN からは使用されません。このアトリビュート（要求された場合）は、AAA サーバリストからの IPCP ネゴシエーション中に MN へ送信されます。

PPP IPCP ネゴシエーション中に、MN は、**0.0.0.0** のプライマリ DNS IP アドレスおよび **0.0.0.0** のセカンダリ DNS IP アドレスを送信することで、IPCP CONFREQ メッセージで IP アドレスを要求します。DNS IP アドレスについてユーザが認可されると、AAA サーバからダウンロードされたアドレスは、IPCP CONFNAK メッセージを介して MN に送信されます。

無効なアトリビュートが DNS VSA にダウンロードされると（例えば、無効な長さや無効なサブタイプ）、PDSN は **access-accept** をドロップし、対応する障害カウンタが増加されます。PDSN は **primary** および **secondary** フィールドの IP アドレスの内容をチェックしません。また、受信した値がそのまま MN に送信されます。

ユーザ要求が DNS IP アドレスに送信され、PDSN が DNS IP アドレス VSA をダウンロードしない場合、IPCP CONFREQ メッセージが送信され、MN から送信された DNS 要求が拒否されます。MN は、新しい CONFREQ にプライマリ DNS アドレスまたはセカンダリ DNS アドレスを指定せずに送信します。

SIP コールの場合、VAAA で設定されると、ダウンロードされたアトリビュートは MN に送信されず。SIP コールおよび PMIP コールの場合、ダウンロードされたフラグは PDSN で無視されます。MIP コールの場合、DNS は MIP RRP を介して HA から送信されます。VAAA での設定は必要ありません。

PMIP コールの場合、HA からダウンロードされた DNS アドレスが優先されます。PMIP セッション コールで、DNS IP アドレスが AAA サーバからダウンロードされた場合、MN が DNS サーバの IP アドレスを要求した場合でも、MN にアドレスは提案されません。

複数の 3GPP2 アトリビュートまたは 3GPP2 アトリビュートの組み合わせ、および CISCO VSA DNS アトリビュートがダウンロードされる場合、最後にダウンロードしたアトリビュート値が考慮されま す。3GPP2 DNS サーバの IP アドレス アトリビュートがダウンロードされ、ただし MN どネゴシエー ションしていない場合、そのアトリビュートはセッションに表示されます。

## サブインターフェイスがある仮想ルート フォワーディング

Virtual Route Forwarding (VRF; 仮想ルート フォワーディング) アトリビュートはシスコ固有のベン ダーアトリビュートであり、RADIUS access-accept メッセージで AAA サーバからダウンロードされ ます。vaccess (PDSN 上のセッションごとに作成されるサブインターフェイス) は、AAA サーバから ダウンロードされる VRF アトリビュート値と一致する VRF に追加されます。PDSN は、 access-accept メッセージの一部として、AAA サーバからシスコのベンダー固有の VRF アトリビュ ートをダウンロードします。この VSA がユーザ認可で受信される場合、および RADIUS から返される VRF 名が PDSN でグローバルに設定される場合、PDSN はこの VRF 情報をセッションに適用します。

IOS の現在のサポートによって、このユーザセッションが VRF をサポートできる全 vaccess インター フェイスが作成されます。VRF は、セッション数を 8,000 (8K のソフトウェア IDB だけが存在しま す) に制限するフルアクセス インターフェイスを強制的に作成します。

VRF が PDSN で設定されている場合、ルーティング テーブルのインスタンスが作成されます。VRF が、作成される vaccess に適用されると、PPP IPCP ネゴシエーションの後に、挿入されるルートは、 グローバル ルーティング テーブルではなく、VRF ルーティング テーブルに保存されます。現在の実装 は LCP ベースの設定要求として VRF をサポートします。

### Basic Functionality

- PDSN は、access-accept メッセージの一部として、AAA サーバからシスコのベンダー固有の VRF アトリビュートをダウンロードします。VRF のサブインターフェイス サポートの場合、VRF 値は IP レベルアトリビュートとしてダウンロードされます。
- VRF が機能するには、IP CEF をイネーブルにする必要があります。
- ユーザの認可でこの VSA を受信した場合、および RADIUS から返される VRF 名が PDSN でグ ローバルに設定される場合、PDSN は、このユーザ セッションで作成された vaccess インターフェ イスにこの VRF 情報を適用します。
- VRF で「ip unnumbered」アトリビュートをダウンロードして、セッションの VRF アトリビュ ートを適用する必要があります。
- VRF アトリビュートが IP レベルアトリビュートとしてダウンロードされる場合、セッションで作 成される vaccess はサブインターフェイスです。また、このサブインターフェイスは、ダウンロー ドした VRF アトリビュート値と一致する PDSN 上の VRF に追加されます。ダウンロードした VRF 名が設定されていない場合、そのコールはドロップされます。
- VRF で「ip unnumbered」アトリビュートをダイアログし、VRF ルーティング テーブルにサブイ ンターフェイスのサポートを作成する必要があります。AAA サーバからの access-accept メッセー ジに、ダウンロードされた LCP および IP VRF アトリビュートの両方がある場合、常に完全な vaccess インターフェイスを作成します。ユーザ プロファイルの LCP VSA の順序は重要ではあり ません。これはすべての VRF-ID VSA 指定を上書きします。
- AAA サーバからの access-accept メッセージに、ダウンロードされた複数の IP VRF アトリビュ ートがある場合、セッションはドロップされます。



- VRF アトリビュートが順番どおり (VRF ID の次に付番されていないインターフェイス) にダウンロードされない場合、セッションはドロップされます。
- virtual-template で VRF アトリビュートが設定される場合、および AAA サーバから VRF がダウンロードされない場合、ローカルで設定された VRF アトリビュートはセッションで更新されます。
- virtual-template で VRF アトリビュートが設定される場合、および AAA サーバから異なる VRF アトリビュートがダウンロードされる場合、AAA サーバからダウンロードされた VRF アトリビュートはセッションで更新されます。
- AAA サーバの VRF アトリビュート処理時のエラーは、AAA サーバサブシステムで処理されます。
- VRF を使用するユーザセッションの場合、PDSN は重複する IP アドレスをサポートします。
- PPP ネゴシエーションの場合、VRF 名をダウンロードすると、セッションで作成される vaccess は新しい VRF と関連付けられるようになります。
- PPP ネゴシエーションで VRF 名がダウンロードされない場合、セッションの vaccess は VRF に関連付けられません。
- MIP および VPDN コール中に VRF アトリビュートがダウンロードされる場合、VRF アトリビュートは使用されません。
  - PMIP コールの場合、VRF アトリビュートはダウンロードされ、Virtual Access は VRF ルーティングテーブルに関連付けられ、リバーストラフィックは VRF エンタープライズだけを介して送信されます。
  - SIP+MIP コールで、VRF と関連付けて SIP コールが確立される場合、および SIP コールが VRF と関連付けられているときに MIP コールが要求される場合、MN からの MIP RRQ が VRF エンタープライズに送信される時、MIP コールはアップ状態になりません。
- VRF が適用された V-Access で受信されたトラフィックは、常に VRF エンタープライズに転送されます。これは通常の IOS の動作です。
- PDSN は VRF の一部として IPv4 アドレスだけをサポートします。IPv6 の動作は定義されていません。
- (MN に対する) 転送方向の vaccess のデータトラフィックは、エンタープライズの外部から受信され、パケットは IOS によってドロップされます。
- PDSN のパケットのアカウンティングは、通常どおりに発生します。
- 同じ VRF に関連付けられている場合に MN から MN ヘルパーティングするパケットは、エンタープライズに送信され、発信元 MN にルーティングされます。PDSN はこのトラフィックを切り替えません。
- トラフィックが MN から PDSN 宛ての場合、パケットは VRF にルーティングされませんが、PDSN で処理されます。
- セッションの作成時にだけ、VRF アトリビュートはスタンバイユニットに同期されます。PPP ネゴシエーション中の VRF の変更は、スタンバイに同期されません。

#### その他の考慮事項

- PDSN の VRF 情報が適用されるのは、確立したコールが SIP セッションの場合だけです。
- Mobile-IP ユーザおよび Proxy Mobile-IP ユーザの場合、重複する IP アドレスを処理できるため、このサポートは必要ありません。
- SIP の重複する IP アドレスは、vaccess および設定されている VRF インターフェイスで区別されます。VRF ルーティングテーブルには、対応する MN を識別する vaccess エントリがあります。

- PDSN での VRF のサポートによって、常にエンタープライズごとに個別のルーティング テーブルがあり、エンタープライズ/コーポレート ネットワークにアクセスするユーザに個別のルーティング テーブルを持たせることができます。ユーザから発信されたパケットは、セキュリティ リスクを回避するため、このルーティング テーブルから外れて転送できません。

### パフォーマンス

- VRF ルーティング テーブルを作成するには、追加のメモリが必要です。

### スケーラビリティ

- この機能は、最大 175,000 PDSN セッションをサポートします。
- セッションあたりのプロセスは増えるため、CPS に影響が及ぶ可能性があります。

## PDSN セッション冗長性の設定

PDSN セッション冗長性のために、次の新しいコマンドが導入されました。

### PDSN セッション冗長性の有効化

冗長性機能がイネーブルの場合、アクティブ PDSN はセッションおよびフロー関連のデータをスタンバイ ピアに同期できます。デフォルトで、この機能はディセーブルです。

コマンドの構文は次のとおりです。

**[no] cdma pdsn redundancy**

基礎となる冗長性インフラストラクチャが設定されている状態で、上記の CLI コマンドが設定されると、セッション冗長性はイネーブルになります。上記のコマンドが **no** を指定して実行されると、PDSN の冗長性機能はディセーブルになります。

### 定期的なアカウントिंग カウンタの同期

デフォルトで、アクティブ PDSN はアカウントिंग カウンタの同期を定期的に試行しません。定期的なアカウントिंग カウンタの同期をイネーブルにするには、次のコマンドを設定します。

**[no] cdma pdsn redundancy accounting update-periodic**

デフォルトの動作に戻すには、このコマンドの **no** フォームを使用します。設定すると、各フローのバイト カウントおよびパケット カウントは、(**aaa accounting update periodic xxx**. を使用して) 設定した定期的なアカウントिंग間隔で、アクティブ ユニットからスタンバイ ユニットに同期されます (変更が発生した場合に限定されます)。定期的なアカウントिंगが設定されない場合、バイト カウントとパケット カウントは同期されません。

### PDSN セッション冗長性のための debug コマンド

PDSN のハイ アベイラビリティの問題領域を特定しやすくするために、次の debug コマンドが導入されました。これらすべての debug は、必要に応じて **undebug all** または **no debug all** を使用して無効にすることができます。

**[no] debug cdma attribute**

**[no] debug cdma pdsn redundancy packets**

PDSN-SR に関するデータをデバッグおよび収集するには、上記のコマンドを実行します。結果として、冗長データに関する詳細がコンソールに送信されます。

**[no] debug cdma pdsn redundancy errors**

PDSN-SR 冗長性エラーをデバッグするには、上記のコマンドを実行します。結果として A11 データに関する詳細がコンソールに送信されます。

### [no] debug cdma pdsn redundancy events

PDSN セッション冗長性イベントに関するイベントをデバッグするには、上記のコマンドを実行します。結果として、PDSN に関する詳細 (RP など) データがコンソールに送信されます。

### 冗長性統計情報の表示

PDSN のペアがアクティブ モードおよびスタンバイ モードで動作しているときに、スタンバイに同期されたセッションおよび関連フローについての多様な情報を表示できる機能は重要です。次のコマンドを使用すると、PDSN のセッション冗長性データを表示できます。

#### show cdma pdsn redundancy statistics

上記のコマンドを実行すると、複数のデータ アイテムが表示されます。その一部を次に示します。

- 同期されたセッション数
- SIP フロー数
- MIP フロー数
- switch-over 後に同期されたセッション数
- 同期に失敗したセッション数



(注) **show cdma pdsn redundancy statistics** を実行すると、**service internal** が設定されるまで非表示になります。

#### show cdma pdsn redundancy

このコマンドを実行すると、表示されている既存のデータに加え、PDSN の冗長性機能が有効かどうかに応じて、「psdn redundancy is enabled」または「redundancy is not enabled」も出力されます。

### PDSN セッション冗長性統計情報のクリア

#### clear cdma pdsn redundancy statistics

このコマンドを実行すると、PDSN セッション冗長性に関連付けられたすべてのデータ カウンタは、初期値に設定されます。

### その他の debug コマンド

上記の PDSN-SR debug コマンドの他に、ハイ アベイラビリティに関連する次のコマンドもデバッグ時に役立ちます。

```
debug redundancy inter-device
```

```
debug ccm
```

### その他の show コマンド

上記の PDSN-SR show コマンドの他に、ハイ アベイラビリティに関連する次のコマンドも役立ちます。

```
show redundancy inter-device
```

## PDSN セッション冗長性インフラストラクチャの設定

PDSN-SR 機能は、Cisco IOS Check-point Facility (CF) を使用して、ステートフル データを Stream Control Transmission Protocol (SCTP) を通じて冗長 PDSN へ送信します。さらに、Cisco IOS HSRP と共に、PDSN は Cisco IOS Redundancy Facility (RF) を使用してアクティブ PDSN とスタンバイ PDSN のトランシジョンを監視、報告します。

PDSN-SR を設定する前に、デバイス間の冗長性インフラストラクチャを設定する必要があります。

## HSRP の設定

HSRP で、IP トラフィックを単一ルータの可用性に依存せず、ネットワーク上のホストからルーティングするため、高いネットワーク可用性を実現できます。HSRP は、アクティブなルータやスタンバイのルータを選択する際に、ルータのグループで使用されます。インターフェイスのいずれかがダウンした場合にデバイス全体がダウンしたと見なされ、スタンバイのデバイスがアクティブになってアクティブなデバイスの役割を引き継げるよう、HSRP は内部と外部両方のインターフェイスを監視します。

HSRP の設定の際は、次の推奨事項と制約事項が適用されることに注意してください。

- 少なくとも、HSRP を有効にし、1 つの PDSN インスタンスに対し 1 つのインターフェイスで定義された HSRP 「master」グループである必要があります。「follow」グループは、すべての他の PDSN インターフェイスで、**follow** キーワード オプションを指定した **standby** インターフェイス設定コマンドを使用して設定できます。**follow** グループを使用することにより、次の利点があります。
  - **follow** グループ機能は、**master** グループの HSRP パラメータを共有するよう設定されているすべてのインターフェイスで有効です。
  - 同じグループを共有しているインターフェイスは、マスター インターフェイスの状態に従い、マスター インターフェイスと同じプライオリティを使用します。これにより、すべてのインターフェイスが必ず同じ HSRP 状態になります。それ以外の場合、マスター HSRP インターフェイスではなく別のロールと見なされるインターフェイスが 1 つまたは複数ある可能性があります。
  - この処理で HSRP グループ数が最適化されるため、多数の設定があるときに設定とメンテナンスのオーバーヘッドが最小限に抑えられます。
  - 設定されている場合、不必要なネットワーク トラフィックを、HSRP Hello メッセージを **follow** グループから削除することで、インターフェイス全体から除外します。
- スタンバイ PDSN で、**standby preempt** インターフェイス設定コマンドを使用してプリエンプト遅延を設定しないでください。
- 最適化のため、ブリッジやゲートウェイの仮想 MAC アドレスの学習を許可する目的で **standby use-bia** コマンドを使用しない場合、メイン インターフェイス (gig0/0) で **standby mac-refresh** コマンドにデフォルトより大きな値 (hello メッセージは 10 秒ごとに送信されます) を設定します。この値は、hello メッセージの送信間隔に使用されます。



**(注)** **standby use-bia** が設定される場合、**follow** グループ インターフェイスから **no hello** メッセージが送信されます。明確に使用しない理由がない限り、HSRP ありのデフォルトの仮想 MAC アドレスを使用することをお勧めします。

- ARP マルチキャスト パケットは、アクティブに変わった HSRP 状態がある場合に送信されます。**follow** グループの仮想 IP アドレス に対する ARP 要求には、HSRP 状態がアクティブの場合に応答します。また、ARP マルチキャストは、スレーブ仮想 IP アドレスの設定時で、**master** グループがアクティブの場合に **follow** グループの VLAN で送信されます。

各 PDSN **follow** グループと同じグループ番号を、プライマリ グループで定義した番号のまま使用してください。プライマリ グループと **follow** グループで同じグループ番号を使用すると、多数の PDSN インターフェイスと HSRP グループがある環境で、HSRP グループを簡単に設定やメンテナンスできます。

HSRP 設定と HSRP グループの詳細情報については、次の URL を参照してください：

[http://www.cisco.com/en/US/partner/tech/tk648/tk362/tk321/tsd\\_technology\\_support\\_sub-protocol\\_home.html](http://www.cisco.com/en/US/partner/tech/tk648/tk362/tk321/tsd_technology_support_sub-protocol_home.html)

および

[http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies\\_configuration\\_example09186a0080094e90.shtml](http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies_configuration_example09186a0080094e90.shtml)

## HSRP の有効化と HSRP マスター グループの設定

インターフェイスで HSRP を有効にし、プライマリ グループを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

---

**ステップ 1** Router(config-if)# **standby [group-number] ip [ip-address [secondary]]**

インターフェイスで HSRP を有効にします。

**ステップ 2** Router(config-if)# **standby [group-number] priority priority**

アクティブ ルータの選択に使用するホット スタンバイ プライオリティを設定します。プライオリティ値の範囲は 1 ~ 255 です。1 はプライオリティが最低、255 は最高を表します。ローカルなルータのプライオリティが、現在のアクティブなルータよりも高い場合、ローカルなルータがアクティブなルータの代わりになるよう指定してください。

**ステップ 3** Router(config-if)# **standby [group-number] name name**

スタンバイ グループの名前を指定します。

**ステップ 4** Router(config-if)# **standby use-bia [scope interface]**

(オプション) HSRP を、割り当て済みの MAC アドレスの代わりに仮想 MAC アドレスとしてインターフェイスのバーンドイン アドレスを使用するよう設定します。

---

## follow グループの設定

HSRP follow グループを、follow キーワード オプションが指定された standby インターフェイス設定コマンドを使用してインターフェイスの follow グループを定義することにより、プライマリ グループの HSRP パラメータを共有するよう設定します。グループ トラッキング状態を共有し、同じプライオリティを持つインターフェイスです。

プライマリ グループに従うインターフェイスを設定するには、インターフェイス設定モードで次のコマンドを使用します。

---

**ステップ 1** Router(config-if)# **standby group-number follow group-name**

follow グループの番号と、follow および共有ステータスに対するプライマリ グループの名前を指定します。



(注) 指定されたグループ番号をプライマリ グループ番号と同じにすることをお勧めします。

---

**ステップ 2** Router(config-if)# **standby group-number ip virtual-ip-address**

follow グループのグループ番号と仮想 IP アドレスを指定します。



(注) 上記で指定されたグループ番号は、マスター グループ番号と同じである必要があります。

---

## デバイス間冗長性の有効化

デバイス間冗長性をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

---

### ステップ 1 Router(config)# **redundancy inter-device**

冗長性が設定され、デバイス間設定モードになります。

すべてのデバイス間設定を削除するには、このコマンドの **no** フォームを使用します。

### ステップ 2 Router(config-red-interdevice)# **scheme standby standby-group-name**

使用する冗長性スキームを定義します。現在、「standby」だけがサポートされているスキームです。

*standby-group-name* – **standby name** インターフェイス設定コマンドで指定されたスタンバイ名と一致する必要があります（「HSRP の設定」の項を参照してください）。また、スタンバイ名は両方の PDSN で同じでなければなりません。

### ステップ 3 Router(config-red-interdevice)# **exit**

グローバル コンフィギュレーション モードに戻ります。

---

## デバイス間通信トランスポートの設定

デバイス間の冗長性には、冗長 PDSN 間の通信を行うトランスポートが必要です。このトランスポートは、Interprocess Communication (IPC) コマンドを使用して設定します。

デバイス間通信トランスポートを、2 つの PDSN 間で設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

---

### ステップ 1 Router(config)# **ipc zone default**

Inter-device Communication Protocol (IPC) を設定し、IPC ゾーン コンフィギュレーション モードにします。

このコマンドを使用して、アクティブ デバイスとスタンバイ デバイス間の通信リンクを開始します。

### ステップ 2 Router(config-ipczone)# **association /**

2 つのデバイスのアソシエーションを設定し、IPC アソシエーション コンフィギュレーション モードにします。

IPC アソシエーション コンフィギュレーション モードで、トランスポート プロトコル、ローカル ポート、ローカル IP アドレス、リモート ポートとリモート IP アドレスなどのアソシエーションの詳細を設定します。

有効なアソシエーション ID の範囲は 1 ~ 255 です。デフォルト値はありません。

### ステップ 3 Router(config-ipczone)# **no shutdown**

無効なアソシエーションと関連するトランスポート プロトコルを再起動します。トランスポート プロトコル パラメータを変更した場合はアソシエーションのシャットダウンが必要です。

### ステップ 4 Router(config-ipczone-assoc)# **protocol sctp**

Stream Control Transmission Protocol (SCTP) をこのアソシエーションのトランスポート プロトコルとして設定し、SCTP プロトコル設定モードを有効にします。

### ステップ 5 Router(config-ipc-protocol-sctp)# **local-port local\_port\_num**

冗長ピアとの通信に使用するローカル SCTP ポート番号を定義し、IPC トランスポート-SCTP ローカル設定モードを有効にします。

IPC ゾーン設定は TCOP に配信されます。TCOP がピアとの SCTP 接続を確立するため、設定済みの SCTP ポート番号から隣接する 12 個のポート番号のセットが RF または CF のために使用されます。

Router(config-ipc-protocol-sctp)# **local-port 5000**

上記の場合、5000 ~ 5011 のポートは SCTP 通信のために使用されます。

自動同期機能をイネーブルにした場合、次のように SCTP ポートを設定します。

Router(config-ipc-protocol-sctp)# **unit1-port port\_num**

有効なポート番号の範囲は 1 ~ 65535 です。デフォルト値はありません。



(注) ローカル ポート番号は、ピア ルータのリモート ポート番号と一致する必要があります。

**ステップ 6** Router(config-ipc-local-sctp)# **local ip ip\_addr**

冗長ピアとの通信に使用されるローカル IP アドレスを定義します。ローカル IP アドレスは、ピア ルータのリモート IP アドレスと一致する必要があります。

Router(config-ipc-unit1-sctp)# **unit1-ip ip\_addr**

自動同期機能がイネーブルの場合、冗長ペアとの通信に使用される IP アドレスを示します。

**ステップ 7** Router(config-ipc-local-sctp)# **keepalive [period [retries]]**

キープアライブ パケットを有効にし、インターフェイスまたは特定のインターフェイスのトンネル プロトコルが停止する前に Cisco IOS ソフトウェアがキープアライブ パケットを応答つきで送信を試みる回数を指定します。

この回数の有効値は 0 より大きい整数で、秒単位です。デフォルトは 10 です。リトライの有効値は 1 より大きく 355 より小さい整数です。デフォルトは、事前に使用した値です。事前に値を指定していない場合は、5 になります。

**ステップ 8** Router(config-ipc-local-sctp)# **retransmit-timeout interval**

メッセージ再送信時間を設定します。有効範囲は 300 ~ 60000 ミリ秒です。最小値のデフォルトは 1000 です。最大値のデフォルトは 60000 です。

**ステップ 9** Router(config-ipc-local-sctp)# **path-retransmit number**

対応する宛先アドレスが非アクティブになる前のキープアライブ リトライの最大回数を設定します。有効範囲は 2 ~ 10 です。デフォルトは 5 です。

**ステップ 10** Router(config-ipc-local-sctp)# **assoc-retransmit number**

アソシエーションが失敗を宣言する前の、宛先アドレスすべてへの再送信の最大回数を定義します。有効範囲は 2 ~ 20 です。デフォルトは 10 です。

**ステップ 11** Router(config-ipc-local-sctp)# **exit**

IPC トランスポート - SCTP ローカル設定モードを終了します。

**ステップ 12** Router(config-ipc-protocol-sctp)# **remote-port port\_num**

冗長ピアとの通信に使用されるリモート SCTP ポートを定義し、IPC Transport-SCTP リモート設定モードをイネーブルにします。有効なポート番号の範囲は 1 ~ 65535 です。デフォルトはありません。



(注) リモート ポート番号は、ピア デバイスのローカル ポート番号と同じにする必要があります。

**ステップ 13** Router(config-ipc-protocol-sctp)# **unit2-port port\_num**

自動同期がイネーブルの場合、unit2 の SCTP ポートを定義します。

```
Router(config-ipc-remote-sctp)# remote-ip ip_addr
```

ローカル デバイスとの通信に使用する冗長ピアのリモート IP アドレスを定義します。すべてのリモート IP アドレスは、同じデバイスを参照する必要があります。すべてのアソシエーション設定を削除するには、このコマンドの **no** フォームを使用します。

```
Router(config-ipc-unit2-sctp)# unit2-ip ip_addr
```

unit1 デバイスとの通信に使用する冗長ピアの unit2 IP アドレスを定義します。

## PDSN-AAA サーバインターフェイスのループバック インターフェイスの使用

AAA サーバでアクティブなユニットとスタンバイのユニットを単一の NAS として表示するには、同じ NAS IP アドレスを両方のユニットに使用する必要があります。現在、NAS IP アドレスは **ip radius source-interface** コマンドを使用して、PDSN に設定できます。設定すると、このインターフェイスの IP アドレスが NAS IP アドレスとして使用されます。

ただし、このコマンドは仮想 IP アドレス (HSRP) をサポートしません。結果、両方のユニットが単一 NAS として表示されるようにするには、ループバック インターフェイスを設定し、このインターフェイスを発信元インターフェイスとして使用するのが唯一の方法です。つまり、CLI コマンドは次のようになります。

```
ip radius source-interface Loopback1
```

## アクティブ-アクティブな状況进行处理するアプリケーション トラッキングの設定

**ステップ 1** Router(config) # **track object-id application pdsn**

PDSN アプリケーションのトラッキング オブジェクトを定義します。

**ステップ 2** Router(config-if) # **standby track object-id [decrement priority]**

PDSN に定義したトラッキング オブジェクトを、HSRP コンフィグに関連付けます。HSRP が、このオブジェクトの状態のトラッキングを開始します。設定された **decrement priority** は、トラッキング オブジェクトの状態に基づいて HSRP プライオリティの変更で使用されます。トラッキング オブジェクトが「アップ」の場合、HSRP にはプライオリティが設定されます。トラッキング オブジェクトが「ダウン」の場合、HSRP は、**standby track** コマンドに指定された **decrement priority** 分、プライオリティを減らします。



(注) プリエンプトが設定されている場合、**priority** 値はアクティブおよびスタンバイ PDSN のプライオリティの差よりも大きい必要があります。

# プロトコルのレイヤ処理と RP 接続

各モバイル ステーションには PDSN との間に単一の PPP 接続があります。また、各 PPP 接続には、PDSN とベース ステーション/PCF 間に対応する R-P 接続があります。R-P 接続の関連情報は、PPP 接続期間は維持されます。



また、PPP 接続および関連する HDLC、LCP、CCP、および IPCP の状態情報も、パケット データ セッションの有効期間は維持されます。単一の PPP 接続で 1 つの SIP フローおよびいくつかの MIP フローをサポートできます。



(注)

Closed-RP は Cisco PDSN リリース 4.0 でサポートされていません。

## Open-RP インターフェイス接続

R-P 接続は、PDSN およびベース ステーション/PCF 間の論理トンネルを示します。R-P 接続によって、PPP 接続のベアラ データを PDSN およびベース ステーション/PCF 間で送信できます。R-P 接続の状態情報は、PPP 接続期間は PDSN で維持されます。ハンドオフ中に、モバイル ステーションは別のベース ステーション/PCF を介して PDSN に接続できます。その結果、PDSN および新しいベース ステーション/PCF 間に別の R-P 接続が確立します。また、PDSN および古いベース ステーション/PCF 間の R-P 接続は解放されます。

R-P 接続の状態情報は、セッションの休止フェーズ中でも PDSN で維持されます。モバイル ステーションがアクティブ状態に移行すると、PDSN は状態情報によってモバイル ステーションと既存の使用できる PPP 接続を関連付けることができます。R-P 状態情報が失われると、PDSN から PPP 接続が解放されます。R-P 接続が失われた後、パケット データ サービスにアクセスするモバイル ステーションは、新しい PPP 接続を確立し、ユーザ アプリケーションのリセットと再起動が行われます。そのため、PDSN は R-P 接続の状態情報を保持して、アクティブおよび休止セッション フェーズ間の遷移時に発生するユーザ アプリケーションの中断を最小限に抑えます。

## PPP 接続

PPP 接続は、モバイル ステーションおよび PDSN 間のリンク層接続を示します。この情報には HDLC の状態、ネゴシエーションされた LCP パラメータ、ネゴシエーションされた IP アドレスおよび CCP 圧縮状態テーブルなどが含まれます。ピア PPP エンティティは、ユーザ セッションの接続性を損なうことなく、アクティブセッション中に LCP および CCP パラメータを再ネゴシエーションできます。ただし、ユーザ ID、認証関連情報、およびネゴシエーションされた IP アドレスは保持されるため、SimpleIP フロー上で確立したアプリケーションは、再ネゴシエーションが発生したことを認識しません。PPP 接続の状態情報はセッションの休止フェーズ中に PDSN で保持されます。それによって、アクティブおよび休止セッション フェーズ間の遷移時に発生するユーザ アプリケーションの中断が最小限に抑えられます。

## アプリケーション フロー

単一の PPP 接続で 1 つの SIP およびいくつかの MIP フロー インスタンスをサポートできます。各 SIP フローの状態情報には、関連する IP アドレス、NAI、および課金関連のユーザ データ レコード (UDR)、および他の関連情報が含まれます。各 MIP フローの状態情報には、MIP ビジター リスト情報、NAI、UDR、および他の関連情報が含まれます。

## PPPoGRE RP インターフェイス

PDSN と無線ネットワーク/ベースステーションとのインターフェイスによって、パケットネットワークおよび無線アクセスネットワーク間にユーザデータストリームの伝送パスができます。PDSN は、PPPoGRE RP インターフェイスを使用して、Packet Control Function (PCF; パケット制御機能) を介して無線ネットワークに接続します。

次のリストで、無線ネットワークおよび PDSN オンの伝送パスについて説明します。

- PDSN には、IP パケットの転送機能をサポートする、メディアから独立した物理リンクがあります。
- PPPoGRE RP インターフェイスは、シグナリングチャンネルおよびベアラデータ転送機能の両方をサポートします。

PPPoGRE RP インターフェイスは、制御データおよびベアラデータの転送機能について 3GPP2 TIA/EIA/IS-835 標準に基づいています。次のリストで、3GPP2 標準と、PDSN パースペクティブからの PPPoGRE RP インターフェイスとの違いについて説明します。

- PPPoGRE 機能をサポートする PDSN に接続している PCF は、GRE Protocol Type フィールドを 0x880B に設定した A11 レジストレーション要求を送信します。
- PDSN と MN のどちらも、PPPoGRE セッションについて AHDLC フレーミングまたはデフレーミングを必要としません。
- A10 ベアラデータパケットは、0x880B (PPPoGRE) に設定された GRE Protocol フィールドで送受信します。

## A11 Session Update

この機能は、「Interoperability Specification (IOS) for *cdma 2000 Access Network Interfaces (Part 7 (A10 and A11 Interfaces))* (3G-IOSv4.3) Version 2.0.1 Date: July 2003)」および「Interoperability Specification (IOS) for *cdma 2000 Access Network Interfaces (Part 3 Features)* (3G-IOSv4.3) Version 2.0.1 Date: July 2003 standard)」に基づいています。A10 接続に関するセッションパラメータを追加、変更、または更新するために、A11 Session Update メッセージが PDSN から PCF に送信されます。次のパラメータは、Application Type 08H (Session Parameter) のセッションパラメータ NVSE 拡張の A11 Session Update メッセージで、PDSN から PCF に送信されます。また、これらのセッションパラメータ NVSE 拡張は、A11 レジストレーション応答メッセージで PDSN から送信されます。

- Radio Network Packet Data Inactivity Timer [01H]
  - Application Sub-Type 01H である Application Data フィールドには、Radio Network Packet Data Inactivity Timer (RN-PDIT) 値が秒単位で含まれます。このフィールドの長さは 1 オクテットで範囲は 01H ~ FFH です。これはタイマー値 1 ~ 255 秒に相当します。
  - サービスタイプ SIP、MIP、PMIP、MSID、および VPDN でサポートされます。
- Always On Indicator [02H]
  - Application Sub Type 02H (Always-on indicator) である Application Data のフィールドの長さはゼロです。
  - サービスタイプ SIP および MSID でサポートされます。

PDSN は標準「*cdma 2000® Wireless IP Network Standard TIA-835-C, AUGUST 2003*」に従い、認証フェーズ中に RADIUS サーバ (Visited/Home RADIUS) から Always On Indicator VSA および RN-PDIT VSA をダウンロードします。1 ユーザが複数のパケットデータセッションを開始すると、PDSN は複数のホームドメインから複数の RN PDIT VSA を受信する可能性があります。この場合、複数のホームドメインから受信した最大の RN PDIT 値が、PDSN から RN に送信されます。この更新は、進行中のパケットデータセッション中で、以前に RN に送信された RN PDIT 値よりも大きい新し

い RN PDIT 値を PDSN が受信したときに発生する可能性があります。ハンドオフ シナリオの場合、Airlink が休止状態ではない場合、A11 レジストレーション応答で RN-PDIT および Always-On indicator が送信されます。

## SDB インジケータ マーキング

この機能は、SIP signaling for PTT アプリケーションなどの Short Data Burst (SDB; ショート データ バースト) アプリケーションをサポートし、PDSN とのやり取りを提案します。SIP は PTT アプリケーションで使用され、PTT コールを伝えます。メッセージは短く、エンドユーザに配信する必要があります。RAN でショート データ バースト サポートを使用して、これらをエンドユーザ、特にモバイルで終了する必要があるメッセージの場合に送信できます。これは特に、ユーザが実際に休止している場合に重要です。

提案は次の 2 つの部分から構成されます。

- PDSN および PC 間にある GRE リンク上の SDB 指示または他の指示のシグナリング。
- ペイロードに適したデータ パケットの指示。



(注) SDB マーキングはサービス タイプ SIP でだけサポートされます。

## SDB 指示のシグナリング

SDB 指示は 3GPP2 Proposal Contribution (Ericsson/SKT) A30-20030818-006 に基づいています。この規定に従い、休止セッションの場合に PDSN から送信される SDB パケットを示すために、GRE ヘッダーの予約済みビットの 1 つが使用されます。休止の PDSN の定義は、A11 レジストレーション要求が PCF から受信され、A11 レジストレーションの成功応答が PDSN から送信された Airlink Stop レコードです。

Data Burst Message のエア インターフェイスでの転送に適した IP アドレスが GRE フレームに含まれる場合、PDSN は B ビットを「1」に設定できます。PCF から PDSN 方向で A8 インターフェイスの場合、B ビットは「0」に設定されます。

## SDB 指示の場合のデータ パケットの識別

SDB 指示は、特定のデータ型の場合にだけ必要です。モバイルが休止モードの場合、ポリシー基準に一致するモバイル宛てのパケットが SDB 指示のために選択されます。

サーバまたはシグナリング プロトコルの選択が限られている場合、初期フェーズのためにローカル ポリシーを考慮できます。たとえば、SIP シグナリング メッセージを送信する SIP サーバが 1 つだけの場合、ポートとソース IP の組み合わせを使用できます。さらに、PDSN に最小 IP 長および最大 IP 長を設定できます。

PDSN で IOS MQC を使用して、SDB 分類を必要とする一致パケットに分類規則を適用できます。たとえば、単純な分類基準に、サーバのポート番号およびソース IP アドレスの範囲を含めることができます。より複雑な分類基準であれば、カスタムのプロトコル検査を含めることができます。

パケットが分類基準に合格し、ユーザが休止の場合、PDSN は SDB 指示を PCF にシグナリングします。

SDB 指示機能に関してデータ パケットの識別をイネーブルにするには、次のコマンドを使用します。

```
cdma pdsn compliance ios4.1 sdb
```

このコマンドで、PDSN は、IOS4.1 標準に従って PCF から送信された SDB レコードを処理できるようになります。

RTP やカスタム アプリケーションなど、特定の種類のペイロードに詳細な分類が必要な場合、IOS NBAR を使用してそのパケットを検査できます。IOS NBAR を設定する方法について詳しくは、NBAR に関するドキュメントを参照してください。

分類機能の設定例を次に示します。

```
class-map match-all sdb-packets
  match packet length min 100 max 300
  match protocol <protocol>
  match access-group <access-group-number>
ip access-list <access-group-number> permit ip 192.0.2.0 0.0.0.255 any
```

(この **access-list** の例では、アドレス範囲が 192.0.2.0/24 のサーバからの特定のプロトコルをマッチングできます)

プロトコルおよびアクセス グループは、目的のパケット ストリームに合わせて設定できます。一致基準には、次のようにカスタム プロトコル検査を含めることもできます。

**ip nbar custom media\_new 8 hex 0x60 dest udp 3001**

この文で、ポート番号 3001 の UDP 宛先が指定されたすべてのパケットが分類され、オフセット 8 に値 0x60 が含まれます。プロトコル **media\_new** は、**match protocol protocol** 文で使用できるようになりました。

```
policy-map sdb-policy
  class sdb-packets
  set qos-group group-number
```

次に、ポリシー マップが入力インターフェイスに適用されます。**group-number** は、分類された一致基準を表します。特定の **group-number** に設定されたすべてのパケットは、PCF と PDSN 間での SDB 使用のフラグが付きます。この処理は次のコマンドで実行されます。

**cdma pdsn a11 dormant sdb-indication gre-flags group-number**

B ビット (SDB インジケータ) は **sdb-indication group-number** に一致するパケットに対し設定されません。

## PPP コントロール パケットの SDB インジケータ マーキング

データ パケットは前述のように SDB を使用してモバイルに送信できますが、PPP 制御パケットの配信にも SDB を使用できます。これは特に、セッションが休止している常時接続セッションで有効です。基本的に、常時接続が設定されていると、PDSN はセッションを有効にしておくために LCP エコー要求を送信 (および LCP エコー応答を待機) します。反対に、このようなセッションが休止している場合、これらの LCP エコー要求を MN に送信するためのデータ チャネルを設定する必要があります。その他のオプションは、SDB を使用して LCP エコー要求をデータ チャネルを設定せずに送信するためのものです。

この機能をイネーブルにするには、上記の CLI と共に次の CLI コマンドを設定します。

**cdma pdsn a11 dormant sdb-indication match-qos-group group-number ppp-ctrl-pkts**

## 複数サービス接続

現在、PDSN は、1 つの A10 接続および 1 つの関連セッションを保守し、複数のフロー (1 つの SIP フローおよび複数の MIP フロー) をサポートしています。この新しい実装では、「サービス接続」という用語は、IS-835-D に定義されている A10 接続を示します。特定の MS に対するすべての A10 サービス接続は、単一の A10 セッションに関連付けられます。特定インスタンスの IETF プロトコル レイヤを共有する一連のパケットは、「IP フロー」と呼ばれます。複数の IP フローが単一のサービス接続を使

用することもあります。現在は1つのメインサービスインスタンスだけで、すべてのSIPおよびMIPフローはその単一のサービスインスタンスを使用します。複数のフロー（SIPまたはMIP）上のIPフローは、複数のA10に拡散する可能性があります。

各A10接続は、A11メッセージングのRANに従って、複数のIPフローをサポートできます。MSがシグナリングするTFTは、どのアプリケーションがどのIPフローにマッピングされるかを示します。

A10セッションに対するIPフローのマッピングがPCFから送信されます。各IPフローはフローIDを使用して識別されます。

Cisco PDSN リリース 4.0 は、2つの補助A10で最高25,000のセッション、および1 aux A10あたり各方向で2つのIPフローをサポートします。

## セッションの作成 - A11 レジストレーション要求

### 接続確立コールフロー

PCFはメインサービス接続のために、Service Option 59を指定した最初のA11レジストレーション要求を送信します。このSR IDはA11レジストレーション要求で常にメインサービスインスタンスです。このサービスフローはデフォルトのA10接続であり、forwardおよびreverseの両方向で、ID FFHが指定されたApplication Flowによって使用されます。MNが複数のフローを必要とする場合、PCFは、Additional Session Information NVSE（作成される追加のA10接続の詳細を含みます）を含め、ライフタイムがゼロ以外のA11レジストレーション要求を送信します。現在の実装はSO 64だけをサポートします。SO 67はサポートしません。補助接続SO 64にはPPPoAHDLCが必要です。

RRQには、R\_QOS\_SUBBLOBとAdditional Session Info（GREキー情報）が含まれます。これでA10からフローIDがマッピングされます。

すべてのPPPネゴシエーションは、メインサービス接続上で発生します。

### A11 レジストレーション応答

PDSNは、PCFから受信したライフタイムがゼロ以外の要求に基づいて、レジストレーション応答を送信します。PDSNは、有効なA11レジストレーション要求を受信すると、要求されたA10接続を作成し、PCFに対してACKを送信します。A11要求に新しい補助接続が含まれる場合、新しいA10接続が作成されます。PDSN上にある補助接続のいずれかの情報が、A11レジストレーション要求にならない場合、そのA10接続はPDSNから削除されます。補助接続のいずれかをPDSNで作成できなかった場合、PDSNはInsufficient Resourcesというメッセージで応答します。

各A10接続は、Additional Session Information NVSE（Application Type 0CH）のGREキーに基づいて作成されます。QoS NVSE（Application Type 0DH）（ForwardおよびReverse）に定義されているアプリケーションフローは、（GRE information NVSE）SR IDに基づいて対応するA10接続にリンクされます。また、このレジストレーション応答には、認証（認証中にAAAサーバからアトリビュートをダウンロードするとき）および休止のハンドオフ中の加入者QoSポリシーが含まれます。

追加のセッション情報に64以外のSOが含まれる場合は、常に8BH（Registration Denied - service option not supported）で拒否されます。

FlowからA10へのマッピングが受信され、SRIDが存在しない場合は、常に8EH（Registration Denied - nonexistent A10 or IP flow）で拒否されます。

### セッションの更新

すべてのA11レジストレーション（ライフタイムがゼロ以外のA11レジストレーション要求）には、このレジストレーション後に存在するAdditional Session NVSEにすべてのA10接続が含まれます。Additional Session NVSEに追加のA10接続がある場合、それらの接続が作成されます。既に存在するA10接続で、要求にはない場合、その接続は解放されます。

レジストレーション中に、フロー ID から A10 へのマッピングは変わる可能性があります。MN および PCF はマッピングをネゴシエーションし、同じマッピングを PDSN に転送します。PDSN はそれに従ってフロー ID を新しくマッピングされた A10 に再マッピングします。

## セッションの削除

PCF からのすべての接続を解放するには、PCF からライフタイム値がゼロの A11 レジストレーション要求を送信します。メイン サービス接続を解放すると、その補助接続もすべて解放されます。

PDSN 側がセッションを終了する場合、A11 Registration Update を送信します。この処理は、すべての接続を切断する必要がある場合に発生します。PDSN は特定の接続の解放を開始できません。このメッセージの.packet フォーマットは変更されません。SRID は、複数の HRPD セッションに対して常に 1 つ指定されます。

## A11 Session Update

A11 Session Update は、新しくダウンロードまたはアップデートした加入者 QoS プロファイルを PCF に渡すときに使用されます。PDSN は QoS 情報をアップデートしないため、PDSN には QoS アップデート情報が含まれません。

設定された場合、1 つ以上の加入者 QoS アトリビュートが認証中にダウンロードされると、A11 Session Update が送信されます。ハンドオフ中は、セッションが休止中の場合を除き、このアトリビュートが RRP で送信されます。セッションが休止中の場合、セッションがアクティブになったときに、session-update が送信されます。

## 複数サービス接続の設定

PDSN で複数サービス接続機能を設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	<code>router# cdma pdsn multiple service-flows [maximum number]</code>	複数フローのサポート機能をイネーブルにします。 maximum number には、PDSN および PCF 間で作成できる補助 A10 の最大数を定義します。デフォルト値は 7 です。

## 例

設定例を示します。

```
router#cdma pdsn multiple service-flows ?
      maximum Maximum limit
      qos       Configure qos parameters
      <cr>

router# cdma pdsn multiple service-flows
router# cdma pdsn multiple service-flows maximum 8
```

## 設定の確認

PDSN で複数サービス接続機能がイネーブルであることを確認するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	router# <b>Show cdma pdsn</b>	Cisco PDSN リリース 4.0 では、次の情報を表示するように show output が強化されました。 <ul style="list-style-type: none"> <li>複数のサービス フロー機能がイネーブルまたはディセーブルです。</li> <li>複数の補助 A10 を使用できます。</li> <li>サービス フローでアクティブなセッション数。</li> <li>システムで現在アクティブなサービス フローの合計数。</li> </ul>
ステップ 2	router# <b>show cdma pdsn session</b> [{ <b>service-flows</b>   <b>detail</b> }]	Cisco PDSN リリース 4.0 では、次の情報を表示するように出力が強化されました。 <ul style="list-style-type: none"> <li>新しいサービス フローの詳細。</li> <li><b>forward</b> および <b>reverse</b> の両方向に関する新しい IP フローの詳細。</li> </ul>
ステップ 3	router# <b>Show cdma pdsn statistics</b>	Cisco PDSN リリース 4.0 では、次の情報を表示する新しいカウンタが導入されました。 <ul style="list-style-type: none"> <li>追加のセッション情報 NVSE および QoS 情報 NVSE が含まれた要求の数（新規要求およびレジストレーション要求の両方）。</li> <li>補助接続の詳細を含む要求に対する新しい拒否理由は、サポートされないサービス オプション、存在しない A10 のようになります。</li> <li>見つからない接続の数および再マッピング フローの数。</li> </ul>
ステップ 4	router# <b>show cdma pdsn session brief</b>	Cisco PDSN リリース 4.0 では、セッションのサービス フローの数を表示するために新しい列が導入されました。
ステップ 5	router# <b>Show cdma pdsn pcf</b>	Cisco PDSN リリース 4.0 では、存在する補助 A10 の数を表示するために新しいカウンタが導入されました。
ステップ 6	router# <b>Show cdma pdsn pcf brief</b>	Cisco PDSN リリース 4.0 では、現在 PCF に存在する補助 A10 の数を表示するため新しい列が導入されました。

## 例

次に、Cisco PDSN リリース 4.0 の例を示します。

```
router# show cdma pdsn
PDSN software version 4.0, service is enabled

All registration-update timeout 1 sec, retransmissions 5
All session-update timeout 3 sec, retransmissions 3
Mobile IP registration timeout 300 sec
A10 maximum lifetime allowed 65535 sec
```

```

GRE sequencing is on
Maximum PCFs limit not set
Maximum sessions limit set to 10 (default 9950 maximum)
SNMP failure history table size 100
MSID Authentication is disabled
Ingress address filtering is disabled
Sending Agent Adv in case of IPCP Address Negotiation is enabled
Allow CI_ADD option during IPCP Phase is disabled
Aging of idle users disabled
Radius Disconnect Capability disabled
Multiple Service flows enabled
Maximum number of service-flows per MN allowed is 8
Call Admission Control enabled
Police Downstream enabled

Number of pcfs connected 1,
Number of pcfs 3GPP2-RP 1,
Number of sessions connected 1,
Number of sessions 3GPP2-RP 1,
Number of sessions Active 1, Dormant 0,
Number of sessions using HDLCoGRE 1, using PPPoGRE 0
Number of sessions using Auxconnections 1, using Policing 1, using DSCP 1
Number of service flows 1
    Simple IP flows 1, Mobile IP flows 0,
    PMIP flows 0, VPDN flows 0

```

サービス フローおよびセッションの詳細に関する情報を含む場合の例を示します。

#### router#show cdm pds session service-flows

```

Mobile Station ID IMSI 09884708942
PCF IP Address 2.2.2.4, PCF Session ID 1

GRE protocol type is 0x8881
GRE sequence number transmit 17, receive 0
Using interface Virtual-Access2.1
Using AHDLC engine on slot 0, channel ID 1
Service Option EV-DO Flow Discrimination 0 DSCP Included 0
Flow Count forward 0 reverse 0
This session has 1 flow
This session has 1 service flow

Service Flow PCF IP Address 2.2.2.4 SR ID 0x2
    Service Option 0x40 Flow Discrimination 0 DSCP Included 0
    Flow Count forward 2 reverse 2
    GRE protocol type is 0x8881, key 2
    GRE sequence number transmit 0, receive 0
    Using AHDLC engine on slot 0, channel ID 0

```

次に、Cisco PDSN リリース 4.0 の **show cdma pdsn statistics** コマンドの出力例を示します。

```

router# show cdma pdsn statistics
Last clearing of "show cdma pdsn statistics" counters never
RP Interface:
    Reg Request rcvd 1524, accepted 1405, denied 2, discarded 117
    Initial Reg Request rcvd 18, accepted 17, denied 1, discarded 0, AuxRequest 1
    Re-registration requests rcvd 1380, accepted 1374, denied 0, discarded 6
    Re-registration requests containing Active-Start 15, Active-Stop 16, updated QoS Blob 5
    Re-registration requests containing new connections 10, missing connections 12, remapping
    flows 1

Handoff requests rcvd 2, accepted 2, denied 0, discarded 0, AuxRequest 1
    De-registration rcvd 13, accepted 12, denied 1, discarded 0
    De-registration Reg Request with Active-Stop 9
    Registration Request Errors:

```



Unspecified 0, Administratively prohibited 0  
 Resource unavailable 0, Authentication failed 0  
 Identification mismatch 1, Poorly formed requests 1  
 Unknown PDSN 0, Reverse tunnel mandatory 0  
 Reverse tunnel unavailable 0, Bad CVSE 0  
**Max Service Flows 0, Unsupported SO 0, Non-existent A10 0,**  
 Bandwidth unavailable 0

Update sent 52, accepted 9, denied 8, not acked 35  
 Initial Update sent 14, retransmissions 38  
 Acknowledge received 17, discarded 0  
 Update reason lifetime expiry 0, PPP termination 11, other 3  
 Registration Update Errors:  
 Unspecified 0, Identification mismatch 8  
 Authentication failed 0, Administratively prohibited 0  
 Poorly formed request 0

Handoff statistics:  
 Inter PCF handoff active 2, dormant 0  
 Update sent 5, accepted 2, denied 2, not acked 1  
 Initial Update sent 2, retransmissions 3  
 Acknowledge received 4, discarded 0  
 De-registration accepted 2, denied 0  
 Handoff Update Errors:  
 Unspecified 0, Identification mismatch 2  
 Authentication failed 0, Administratively prohibited 0  
 Poorly formed request 0

RP Session Update statistics:  
 Update sent 0, accepted 0, denied 0, not acked 0  
 Initial Update sent 0, retransmissions 0  
 Acknowledge received 0, discarded 0  
 Sent reasons Always On 0, RN-PDIT 0, **Subscriber QoS 0**  
 RP Session Update Errors:  
 Unspecified 0, Identification mismatch 0  
 Authentication failed 0, Session parameters not updated 0  
 Poorly formed request 0

Service Option:  
 Unknown (0) success 1405, failure 2

PPP:  
 Current Connections 0  
 Connection requests 17, success 17, failure 0, aborted 0  
 Connection enters stage LCP 17, Auth 6, IPCP 13  
 Connection success LCP 17, AUTH 6, IPCP 13  
 Failure reason LCP 0, authentication 0, IPCP 0, other 0  
 Failure reason lower layer disconnect 0

A10 release before LCP nego by PDSN 0, by PCF 0

LCP Stage  
 Failure Reasons Options 0, MaxRetry 0, Unknown 0  
 LCP Term Req during LCP nego sent 0, rcvd 0  
 A10 release during LCP nego by PDSN 0, by PCF 0

Auth Stage  
 CHAP attempt 2, success 2, failure 0, timeout 0  
 PAP attempt 4, success 4, failure 0, timeout 0  
 MSCHAP attempt 0, success 0, failure 0, timeout 0  
 EAP attempt 0, success 0, failure 0  
 MSID attempt 0, success 0, failure 0  
 AAA timeouts 0, Auth timeouts 0, Auth skipped 11

```

LCP Term Req during Auth nego sent 0, rcvd 0
A10 release during Auth nego by PDSN 0, by PCF 0

IPCP Stage
Failure Reasons Options 0, MaxRetry 0, Unknown 0
Options failure reason MN Rejected IP Address 0
LCP Term Req during IPCP nego sent 0, rcvd 0
A10 release during IPCP nego by PDSN 0, by PCF 0

CCP Stage
Connection negotiated compression 0
Compression type Microsoft 0, Stac 0, other 0
Connections negotiated MRRU 0, IPX 0, IP 13
Connections negotiated VJ-Compression 0, BAP 0
PPP bundles 0
Connections failed to negotiate compression 0

Renegotiation total 0, by PDSN 0, by Mobile Node 0
Renegotiation success 0, failure 0, aborted 0
Renegotiation reason: address mismatch 0, lower layer handoff 0
GRE key change 0, other 0

Release total 16, by PDSN 14, by Mobile Node 2
Release by ingress address filtering 0
Release reason: administrative 4, LCP termination 2
Idle timeout 3, echo missed 0
L2TP tunnel 0, insufficient resources 0
Session timeout 0, service unavailable 0
De-Reg from PCF 0, lifetime expiry 0, other 7

Echo stats
Request sent 0, resent 0, max retransmit timeout 0
Response rcvd 0

Discarded Packets
Unknown Protocol Errors 424, Bad Packet Length 0

RSVP
IEs Parsed 0
TFTs Created Success 0, Failure 0
TFTs Updated Success 0, Failure 0
TFTs Deleted Success 0, Failure 0

Other Failure 0
Unknown 0, Unsupported Ie types 0
Tft Ipv4 Failure Stats
Tft Unauthorized 0, Unsuccessful Processing 0
Tft Treatment Unsupported 0, Persistency reached 0
Packet Filter Add 0, Replace 0
Packet Filter Precedence Contention 0, Unavailable 0
Packet Filter Maximum Limit 0, Non-Existent Tft add 0

QoS:
Total Profile Download Success 10, Failure 10,
Local Profile selected 4
Failure Reason DSCP 1, Flow Profile ID 1,
Service Option Profile 1, Others 1
Total Consolidated Profile 4, DSCP Remarkd 0
Total Policing installed 4, failure 5, removed 4

slot 0:
AHDLC Engine Type: CDMA HDLC SW ENGINE
Engine is ENABLED

```

```
total channels: 20000, available channels: 20000
```

```
Framing input 5306 bytes, 169 paks
Framing output 7008 bytes, 169 paks
Framing errors 0, insufficient memory 0, queue overflow 0
  Invalid size 0
```

```
Deframing input 1371683974 bytes, 4005798483 paks
Defaming output 4948 bytes, 142 paks
Deframing errors 0, insufficient memory 0, queue overflow 0
  Invalid size 64, CRC errors 117817589
```

#### RADIUS DISCONNECT:

```
Disconnect Request rcvd 0, accepted 0
Disconnect Request Errors:
  Unsupported Attribute 0, Missing Attribute 0
  Invalid Request 0, NAS Id Mismatch 0
  Session Cxt Not Found 0, Administratively Prohibited 0
```

## データ プレーン

### ダウンストリーム (Forward) パケット処理

PDSN の forward 方向でパケットが受信される場合、フロー アカウンティングが発生します。この時点で、まず PDSN は、宛先 IP アドレスに基づいて適用できる TFT を識別します。このパケットは、アプリケーション フローを識別するパケット フィルタを経由します。A11 RRQ には、アプリケーション フローからサービス フローへのマッピングが含まれます。このマッピングを使用してサービス フローが識別され、パケットは A10 接続情報でマークされます。パケットが PPP 制御パケットの場合、パケットはメイン A10 接続でマークされます。後で、このパケットによって PPP カプセル化の後に AHDLC カプセル化が完了すると、対応する A10 接続が選択され、トンネルに転送されます。

A11 RRQ (より具体的には QoS アップデート) では、PCF はフロー識別を使用するように指定できません。つまり、すべてのベアラ パケットには、GRE 用の 3GPP2 ヘッダー拡張でエンコーディングされたフロー ID が含まれます。

### アップストリーム (Reverse) パケット処理

reverse 方向でパケットを受信すると、PPP カプセル化が削除された後に、フロー アカウンティングのために PDSN によってパケットが選択されます。DSCP のためにまずパケットが評価され、それに従ってアクションが実行されます。パケットが転送できる場合、パケットは TFT を介して渡されます (TFT にはフロー ID を識別するパケット フィルタがあります)。GRE ヘッダーのパケットに「IP フロー」の詳細が含まれる場合、そのフロー ID に関して、TFT 経由ではなくパケットが直接アカウンティングされます。フローが識別されると、アカウンティングが実行され、転送されます。フローを識別するパケット フィルタがない場合、デフォルト フロー ID FF が想定されます。

## QoS シグナリング

ここでは、Quality of Service (QoS) シグナリングと次の概念について説明します。

- トラフィック フロー テンプレートの処理
  - TFT メッセージを送信する RSVP メッセージの処理

- TFT 解析およびパケット フィルタのインストールの処理
- 加入者 QoS プロファイルの処理
  - 加入者 QoS プロファイルのダウンロード、またはローカルで設定した加入者 QoS プロファイルの使用
  - セッションまたはフローに対する加入者 QoS プロファイルの適用
- データ プロファイルの処理
  - IP フローは、TFT を使用して識別され、アカウンティングされます。
  - (必要に応じて) データ トラフィックのポリシングは、最大集約帯域幅に基づいています。
  - 両方向のパケットに対する DSCP マーキングの適用は、適用されるプロファイルに基づきます。

## トラフィック フロー テンプレート

Traffic Flow Template (TFT; トラフィック フロー テンプレート) で IP フローを定義します。TFT には、各 IP フローを定義するパケット フィルタ セットが含まれます。1 つの IP フローで複数のアプリケーション フローが送信されることがあります。各フローは、パケット フィルタを使用して識別されます。

MN はフローを決定し、RSVP メッセージとして TFT でパケット フィルタを送信します。RSVP メッセージには、TFT を定義する 3GPP2 オブジェクトが含まれます。1 つの RSVP メッセージには、送信された複数の TFT を持つ 1 つの 3GPP2 だけが含まれます。HRPD には、1 つの MS IP アドレスあたり 1 つの永続的 TFT だけが含まれます。TFT には、フロー、パケット フィルタ、およびパケットの扱いが記述されます。MN は、1 つのフロー方向の 1 IP アドレスあたり 1 TFT を送信します。これらのパケット フィルタは、優先順位レベルに関連付けられます。パケット フィルタはソートされ、セッションに関連付けられます。これらのパケット フィルタのフロー ID (IP フロー ID) は、A11 RRQ に指定された IP フロー ID とマッチングされ、使用する対応の A10 接続が決定されます。マッピングがない場合、PDSN はメイン サービス インスタンス (デフォルトの A10 で、フロー ID は FF) を介してパケットを転送します。

この場合、RSVP メッセージはセッション上のデータ トラフィックとしてアカウンティングされます。

### その他の考慮事項

forward および reverse の両方向で、HRPD MS だけが Non-Specific TFT を使用します。

各 TFT IE には、forward 方向または reverse 方向に対してマッチングされる 1 つまたは複数のパケット フィルタが含まれます。PDSN は 1 つの TFT の 1 方向あたり 255 個のパケット フィルタをサポートします。

PPP 再ネゴシエーション中に、同じ宛先に更新要求が送信されると、(TFT と同様に) すべての接続の詳細が解放され、再確立されます。

### パケット フィルタ

パケット フィルタには、特定の方向に関する IP フローが記述されます。パケット フィルタにはサブタイプ PF0 および PF1 が含まれます。PF0 は、Outer IP Header にフィルタが適用されることを示し、PF1 は、拡張ヘッダーまたは転送ヘッダーにフィルタが適用されることを示します。PDSN の初期のサポートは、IPv4 アドレス /Port/ToS/Protocol だけです。初期フェーズでサポートされる唯一のプロトコルは、IP および GRE です。各パケット フィルタは、優先順位レベルに関連付けられます。(データ トラフィック中の) パケットがこの TFT に渡され、IP フローが識別されるとき、パケットははその優先順位の順序でこれらのフィルタを経由します。

## TFT のインストール

更新の TFT をインストールする必要がある場合、MS は「新しい TFT の作成」をアタッチして TFT を送信します。次の TFT は、「既存の TFT へのパケットフィルタの追加」、「既存の TFT の削除」、「既存の TFT に含まれるパケットフィルタの置換」、「既存の TFT からのパケットフィルタの削除」などの適切なアクティブでマークされます。

TFT が適切に解析され、正常にインストールされると、PDSN は肯定応答します。

PDSN はシナリオの状況に応じて、次のエラーのいずれかをレポートします。

**表 22** TFT エラー メッセージ

Packet filter add failure	PDSN は何らかの理由で要求されたパケットフィルタを追加できませんでした。
Packet filter unavailable	MS は、PDSN にインストールされていないパケットフィルタを置換または削除しようとした。
Unsuccessful TFT processing	PDSN は、何らかの理由（TFT のフォーマットが不適切など）で TFT を解決できませんでした。
Channel not available	対応する A10 が確立していないときに、MS は非永続的な TFT (P=0) をインストールしようとした。
Evaluation precedence contention	評価の優先順位の値に競合が検出されました。
Treatment not Supported	MS に、PDSN でサポートされないフローまたはチャネルの処理値が含まれていました。
Packet filter replace failure	パケットフィルタの置換要求に、何らかの不明なエラーが含まれます。
Unauthorized TFT	MS は、MSIP アドレスフィールドの認可されていない IP アドレスを使用して TFT をインストールしようとした。
Max number of Packet Filters for the TFT has been reached	MS は、いずれかの方向の TFT について 255 を超えるパケットフィルタをインストールしようとした。
Attempted to add Packet Filters to non	MS は、TFT を作成する前に、パケットフィルタを TFT に追加しようとした。

PDSN は、3GPP2 OBJECT に含まれる IE の順序で要求を処理します。すべての IE の処理が正常に終了すると、PDSN はその MS の IP アドレスを含む ResvConf メッセージを返します。IE の処理に失敗すると、PDSN は Resv メッセージの以降の処理を停止します。PDSN は、エラーコードと処理に失敗した IE のインデックスを含む ResvErr メッセージを MS に返します。TFT IE インデックスは 1 から始まります。IE の処理に失敗すると、PDSN は Resv メッセージの以降の処理を停止しますが、そのメッセージの以前の IE で実行されたアクションの結果は保持されます。

## TFT のアップデート

MS は任意の時点で TFT をアップデートできます。たとえば、パケットフィルタの内容が変わったときや、MS の IP アドレスが変わったときなどです。

TFT は IP アドレスに基づいて MS と関連付けられているため、MS の IP アドレスが変わると、MS か RSVP メッセージが送信されて古い IP アドレスが削除され、新しい IP アドレスの新しい TFT が作成されます。

セッションの TFT が削除されるのは、MS が TFT メッセージを削除した場合、セッションが終了した場合、または PPP の再ネゴシエーション時だけです。

## TFT の設定

TFT エラー拡張を含むように PDSN を設定するには、次のタスクを実行します。

router# **cdma pdsn tft reject include error extension**

TFT が拒否された場合は常に **reject** メッセージにエラー拡張を含めるように、この CLI コマンドを設定します。

### 例

次に、**cdma pdsn tft reject include error extension** コマンドの例を示します。

```
cdma pdsn tft ?
  reject      Configure CDMA PDSN TFT reject

cdma pdsn tft reject ?
  include     Configure CDMA PDSN TFT reject include

cdma pdsn tft reject include ?
  error       Configure CDMA PDSN TFT reject include error

cdma pdsn tft reject include error ?
  extension   Configure CDMA PDSN TFT reject include error extension

cdma pdsn tft reject include error extension ?
```

## 設定の確認

TFT 機能がイネーブルであることを確認し、TFT に関する情報を収集するには、次のタスクを実行します。

コマンド	目的
<b>ステップ 1</b> router# <b>show cdma pdsn session {qos tft detail}</b>	Cisco PDSN リリース 4.0 では、 <b>show cdma pdsn session command</b> で、次の情報を表示する拡張機能が追加されました。 <ul style="list-style-type: none"> <li>• 加入者 QoS プロファイル</li> <li>• 既存の内容に加えてこのセッションにインストールされた TFT</li> </ul>

コマンド	目的
<b>ステップ2</b> router# <code>show cdma pdsn statistics</code>  router# <code>show cdma pdsn statistics tft</code>	Cisco PDSN リリース 4.0 では、次の情報を表示する新しいカウンタが導入されました。 <ul style="list-style-type: none"> <li>• 解析に成功した TFT と失敗した TFT の数</li> <li>• TFT 解析が失敗した理由を特定する新規カウンタ</li> <li>• AAA サーバからダウンロードしたか、ローカルにインストールされている、加入者 QoS プロファイルの数</li> <li>• 加入者 QoS プロファイルの統合</li> <li>• インストールされた、またはアンインストールされたポリシー</li> <li>• インストールされたポリシーに基づいて DSCP がコメントされたパケット</li> </ul>
<b>ステップ3</b> router# <code>show cdma pdsn redundancy</code>	Cisco PDSN リリース 4.0 では、スタンバイに同期される TFT 数の詳細について表示するように、このコマンド出力が強化されました。

例

次に設定例をいくつか示します。

```

router#show cdma pdsn session tft
Mobile Station ID IMSI 123456789011122
  PCF IP Address 10.1.1.1, PCF Session ID 1
  This session has 1 flow
  This session has 1 Tft
  TFT IP Address 3.1.1.1
  Number of Packet Filters Forward 2, Reverse 1
  Forward Packet Filters
    Packet Filter 1
      Flow Id 10, Precedence 255, PF Type 0
      Source Port 125

    Packet Filter 2
      Flow Id 10, Precedence 255, PF Type 0
      Source Port 125

  Reverse Packet Filters
    Packet Filter 1
      Flow Id 10, Precedence 10, PF Type 0
      Source Port 125

Mobile Station ID IMSI 123456789011123
  PCF IP Address 10.1.1.1, PCF Session ID 2
  This session has 1 flow
  This session has 1 Tft

  TFT
  IP Address 3.1.1.2
  Number of Packet Filters Forward 2, Reverse 3
  Forward Packet Filters
    Packet Filter 1
      Flow Id 2, Precedence 2, PF Type 0
      Source Ip 5.5.5.5 Mask 255.255.255.0
    
```

```

Packet Filter 2
Flow Id 5, Precedence 5, PF Type 0
Source Ip 1.1.1.1 Mask 255.255.255.0

Reverse Packet Filters
Packet Filter 1
Flow Id 10, Precedence 255, PF Type 0
Source Port 125

Packet Filter 2
Flow Id 10, Precedence 255, PF Type 0
Source Port 125

Packet Filter 3
Flow Id 10, Precedence 255, PF Type 0
Source Port 125

router#show cdma pdsn statistics
Last clearing of "show cdma pdsn statistics" counters never
RP Interface:
  Reg Request rcvd 1524, accepted 1405, denied 2, discarded 117
  Initial Reg Request rcvd 18, accepted 17, denied 1, discarded 0, AuxRequest 1
  Re-registration requests rcvd 1380, accepted 1374, denied 0, discarded 6
  Re-registration requests containing Active-Start 15, Active-Stop 16, updated QoS Blob 5
  Re-registration requests containing new connections 10, missing connections 12
  Handoff requests rcvd 2, accepted 2, denied 0, discarded 0, remapping flows 1
  De-registration rcvd 13, accepted 12, denied 1, discarded 0
  De-registration Reg Request with Active-Stop 9
  Registration Request Errors:
    Unspecified 0, Administratively prohibited 0
    Resource unavailable 0, Authentication failed 0
    Identification mismatch 1, Poorly formed requests 1
    Unknown PDSN 0, Reverse tunnel mandatory 0
    Reverse tunnel unavailable 0, Bad CVSE 0
    Max Service Flows 0, Unsupported SO 0, Non-existent A10 0,
    Bandwidth unavailable 0

  Update sent 52, accepted 9, denied 8, not acked 35
  Initial Update sent 14, retransmissions 38
  Acknowledge received 17, discarded 0
  Update reason lifetime expiry 0, PPP termination 11, other 3
  Registration Update Errors:
    Unspecified 0, Identification mismatch 8
    Authentication failed 0, Administratively prohibited 0
    Poorly formed request 0

  Handoff statistics:
    Inter PCF handoff active 2, dormant 0
    Update sent 5, accepted 2, denied 2, not acked 1
    Initial Update sent 2, retransmissions 3
    Acknowledge received 4, discarded 0
    De-registration accepted 2, denied 0
  Handoff Update Errors:
    Unspecified 0, Identification mismatch 2
    Authentication failed 0, Administratively prohibited 0
    Poorly formed request 0

  RP Session Update statistics:
    Update sent 0, accepted 0, denied 0, not acked 0
    Initial Update sent 0, retransmissions 0
    Acknowledge received 0, discarded 0
    Sent reasons Always On 0, RN-PDIT 0, Subscriber QoS 0
  RP Session Update Errors:
    Unspecified 0, Identification mismatch 0

```



Authentication failed 0, Session parameters not updated 0  
 Poorly formed request 0

Service Option:

Unknown (0) success 1405, failure 2

PPP:

Current Connections 0  
 Connection requests 17, success 17, failure 0, aborted 0  
 Connection enters stage LCP 17, Auth 6, IPCP 13  
 Connection success LCP 17, AUTH 6, IPCP 13  
 Failure reason LCP 0, authentication 0, IPCP 0, other 0  
 Failure reason lower layer disconnect 0

A10 release before LCP nego by PDSN 0, by PCF 0

LCP Stage

Failure Reasons Options 0, MaxRetry 0, Unknown 0  
 LCP Term Req during LCP nego sent 0, rcvd 0  
 A10 release during LCP nego by PDSN 0, by PCF 0

Auth Stage

CHAP attempt 2, success 2, failure 0, timeout 0  
 PAP attempt 4, success 4, failure 0, timeout 0  
 MSCHAP attempt 0, success 0, failure 0, timeout 0  
 EAP attempt 0, success 0, failure 0  
 MSID attempt 0, success 0, failure 0  
 AAA timeouts 0, Auth timeouts 0, Auth skipped 11  
 LCP Term Req during Auth nego sent 0, rcvd 0  
 A10 release during Auth nego by PDSN 0, by PCF 0

IPCP Stage

Failure Reasons Options 0, MaxRetry 0, Unknown 0  
 Options failure reason MN Rejected IP Address 0  
 LCP Term Req during IPCP nego sent 0, rcvd 0  
 A10 release during IPCP nego by PDSN 0, by PCF 0

CCP Stage

Connection negotiated compression 0  
 Compression type Microsoft 0, Stac 0, other 0  
 Connections negotiated MRRU 0, IPX 0, IP 13  
 Connections negotiated VJ-Compression 0, BAP 0  
 PPP bundles 0  
 Connections failed to negotiate compression 0

Renegotiation total 0, by PDSN 0, by Mobile Node 0  
 Renegotiation success 0, failure 0, aborted 0  
 Renegotiation reason: address mismatch 0, lower layer handoff 0  
 GRE key change 0, other 0

Release total 16, by PDSN 14, by Mobile Node 2  
 Release by ingress address filtering 0  
 Release reason: administrative 4, LCP termination 2  
 Idle timeout 3, echo missed 0  
 L2TP tunnel 0, insufficient resources 0  
 Session timeout 0, service unavailable 0  
 De-Reg from PCF 0, lifetime expiry 0, other 7

Echo stats

Request sent 0, resent 0, max retransmit timeout 0  
 Response rcvd 0

Discarded Packets

Unknown Protocol Errors 424, Bad Packet Length 0

```

RSVP
TFTs Parsed 0
TFTs Created Success 0, Failure 0
TFTs Updated Success 0, Failure 0
TFTs Deleted Success 0, Failure 0
TFT Failure Stats
  Tft Unauthorized 0, Unsuccessful Parsing 0
  Tft Treatment Unsupported 0, Persistency reached 0
  Packet Filter Add 0, Replace 0
  Packet Filter Precedence Contention 0, Unavailable 0
  Packet Filter Maximum Limit 0, Non-Existent Tft add 0

```

```
router#show cdma pdsn redundancy
```

```
CDMA PDSN Redundancy is enabled
```

```
CDMA PDSN Session Redundancy system status
```

```
PDSN state = ACTIVE
```

```
PDSN-peer state = STANDBY HOT
```

```
CDMA PDSN Session Redundancy Statistics
```

```
Last clearing of cumulative counters never
```

	Synced to standby since peer up	Current Connected
Sessions	0	0
SIP Flows	0	0
MIP Flows	0	0
PMIP Flows	0	0
TFT	0	0

## 加入者 QoS ポリシー

PDSN とのセッションを確立する間、認証時に加入者 QoS アトリビュートは AAA サーバからダウンロードされます。次に、加入者 QoS プロファイルの一部として AAA サーバからダウンロードされたアトリビュートを示します。

- 許可されたディファレンシエーテッド サービス マーキング
- 許可された永続的 TFT の数
- ベストエフォート トラフィックでの最大認可集約帯域幅
- 各方向の認可済みフロー プロファイル ID
- フロー優先順位あたりの最大値
- サービス オプション プロファイル
- ベスト エフォート トラフィックでのユーザ間の優先順位

最大認可集約帯域幅は、PDSN 上のポリシングおよび帯域幅の割り当てに使用されます。

この一覧に記載されている最初の 2 つの項目は、PDSN がベアラ トラフィックで認可および適用するために使用されます。残りの 5 個のアトリビュートは、A11 レジストレーション応答および A11 Session-Update の一部として PCF に保存および転送されます。

単一の NAI で異なるポリシーが MN にダウンロードされる場合、PDSN のプロファイルが更新されません。

1 つの MN あたり複数の NAI がある場合、上記の属性の複数バージョンが受信されます。PDSN はその属性を統合し、PCF に転送します。この統合プロセスで、次の詳細情報が提供されます。

- 許可されたサービス オプションの合計数
- サービス インスタンスの最大値中の最大値
- すべての許可されている Authorized Flow Profile ID の合計セット
- ベスト エフォート トラフィックでの最大認可集約帯域幅の最大値
- フローの優先順位あたりの最大値中の最大値
- ベスト エフォート トラフィックでのユーザ間の優先順位の最大値

加入者 QoS プロファイルが AAA サーバからダウンロードされていない場合、ローカルで設定された QoS プロファイルが適用されます。

## Allowed Differentiated Services Marking

許可されたディファレンシエーテッド サービス マーキング 属性は、3 つのサブタイプから構成されます。

- A、E、O ビット フラグ
- Max-class
- RT マーキング

MS はパケットにマークし、トラフィックを送信することがあります。PDSN はそれを監視し、マークされた値が許可されたマーキングに含まれるかどうかを確認します。パケットに許可された値よりも大きな DSCP が含まれる場合、コメントの DSCP が設定される場合は、PDSN はそのパケットにコメントできます。このコメントの DSCP が設定されない場合、ベスト エフォート DSCP を使用してパケットが転送されます。

PDSN は次の方法で DSCP を確認します。

- max-class が設定されている場合、すべての定義済みクラスの処理は昇順で (AF リスト、EF、および Selector Class の順)、PDSN はパケット内の DSCP が Max-class の範囲内かどうかを確認します。
- max-class が存在せず、A、E、および O ビット フラグが存在する場合、設定されているビットに従って、PDSN は DSCP を確認します。
- max-class およびビット フラグの両方が存在する場合、PDSN はデフォルト クラスでコメントを付けます。
- この属性に RT マーキングが設定される場合、リバース トンネル処理されるパケットは、ローカルで設定した値でもマーキングされます。

## 許可された永続的 TFT の数

HRPD には、1 つの MS IP アドレスあたり 1 つの永続的 TFT だけを含めることができます。この属性は PCF に転送されません。

永続的 TFT 属性の数がダウンロードされないか、ローカルで設定されない場合、TFT は「Unsuccessful TFT Processing」エラーで拒否されます。

## 最大認可集約帯域幅

最大認可集約帯域幅はダウンストリーム ポリシングに使用されます。この値は、そのセッションのそのモバイルに保証された帯域幅と見なされます。これは PCF に転送されます。

## 加入者 QoS プロファイルの設定

PDSN で加入者 QoS プロファイル機能を設定するには、次のタスクを実行します。

	コマンド	目的
ステップ 1	<code>router# cdma pdsn multiple service-flows qos subscriber profile</code>	ローカル加入者の QoS プロファイルを設定できます。加入者 QoS プロファイルが AAA サーバからダウンロードされない場合、このプロファイルは MN に使用されます。
ステップ 2	<code>router# cdma pdsn multiple service-flows qos remark-dscp value</code>	モバイルからインターネットに送信されるデータ パケットに、そのモバイルに許可されている dscp 値内の DSCP が含まれるとき、マーキングに使用する DSCP の remark 値を設定できます。

`cdma pdsn multiple service flows qos subscriber profile` を実行すると、サブモードに移行します。次のコマンドを使用して、ローカルの加入者 QoS プロファイルで多様なパラメータを設定できます。

	コマンド	目的
ステップ 1	<code>router# cdma pdsn multiple service-flows qos subscriber profile</code>	最大集約帯域幅値を設定します。有効な範囲：8000 ~ 2000000000。
	<code>Bandwidth number</code>	ユーザ間の優先順位パラメータを設定します。有効な範囲：1 ~ 4294967295。
	<code>inter-user-priority value</code>	永続的な TFT パラメータの許容数を設定します。有効な範囲：1 ~ 255。
	<code>tft-allowed value</code>	サービス オプション プロファイルで最大サービス接続パラメータを設定します。有効な範囲：1 ~ 4294967295。
	<code>link-flow value</code>	HRPD で確立できる Configures Service オプション。有効な範囲：1 ~ 255。HRPD の場合、SDB レコードはサポートされません。
	<code>service-option value</code>	フロー単位の優先順位パラメータの最大値を設定します。有効な範囲：1 ~ 65535。
	<code>flow-priority value</code>	各方向の認可されたフロー プロファイル ID を設定します。
	<code>flow-profile direction {forward  reverse  bi-direction} flow-id flow-id</code>	使用できるデフォレンシエータドサービスのマーキング パラメータを設定します。有効な範囲：1 ~ 63。
	<code>dscp {allowed-class {AF EF O}   max-class value  reverse-marking value}</code>	

### 例

次にいくつかの設定例を示します。

```
router(config)#cdma pdsn multiple service-flows qos subscriber profile
router(config-qos-profile)#
Eg:
cdma pdsn multiple service-flows qos subscriber profile

router# cdma pdsn multiple service-flows qos remark-dscp AF11
```

```

router#(config-qos-profile)#bandwidth ?
<8000-2000000000> Value

router#(config-qos-profile)#bandwidth 9000 ?
<cr>

```

## dscp コマンド

次に **dscp** コマンドの例を示します。

```

router#(config-qos-profile)#dscp ?
  allowed-class    allowed dscp's classes with which user can mark
  packets
  max-class        User may mark packets with a class selector code
  point
  reverse-marking  marking level pdsn apply to reverse tunneled packets

```

```

router#(config-qos-profile)#dscp allowed-class ?
  AF  User can send packets with AF dscp (A bit)
  EF  User can send packets with EF dscp (E bit)
  O   User can mark packets for experiment or local use (O bit)

```

```

router#(config-qos-profile)#dscp allowed-class AF ?
<cr>

```

```

AF11      AF11
AF12      AF12
AF13      AF13
AF21      AF21
AF22      AF22
AF23      AF23
AF31      AF31
AF32      AF32
AF33      AF33
AF41      AF41
AF42      AF42
AF43      AF43
Default   Selector Class 0
EF        EF
class1    Selector Class 1
class2    Selector Class 2
class3    Selector Class 3
class4    Selector Class 4
class5    Selector Class 5
class6    Selector Class 6
class7    Selector Class 7

```

```

router(config-qos-profile)#

```

```

router(config-qos-profile)#dscp reverse-marking ?

```

```

AF11      AF11
AF12      AF12
AF13      AF13
AF21      AF21
AF22      AF22
AF23      AF23
AF31      AF31
AF32      AF32
AF33      AF33
AF41      AF41
AF42      AF42
AF43      AF43
Default   Selector Class 0
EF        EF
class1    Selector Class 1

```

```
class2 Selector Class 2
class3 Selector Class 3
class4 Selector Class 4
class5 Selector Class 5
class6 Selector Class 6
class7 Selector Class 7
```

```
router(config-qos-profile)#
```

### flow-priority コマンド

次に、**flow-priority** コマンドの例を示します。

```
router(config-qos-profile)#flow-priority ?
<1-4294967295> Value
```

```
router(config-qos-profile)#flow-priority 100 ?
<cr>
```

### flow-profile direction コマンド

次に、**flow-profile** コマンドの例を示します。

```
router#(config-qos-profile)#flow-profile ?
direction Configure direction for flow of packet
```

```
router#(config-qos-profile)#flow-profile direction ?
<1-3> 1-Reverse 2-Forward 3-Bi-direction
```

```
router#(config-qos-profile)#flow-profile direction 1 ?
flow-id defines qos treatment to apply to a packet flow
```

```
router(config-qos-profile)#flow-profile direction 1 flow-id ?
<1-65535> Value
```

```
router#(config-qos-profile)#flow-profile direction 1 flow-id 100 ?
```

### inter-user-priority コマンド

次に、**inter-user-priority** コマンドの例を示します。

```
router#(config-qos-profile)#inter-user-priority ?
<1-4294967295> Value
```

```
router#(config-qos-profile)#inter-user-priority 200 ?
<cr>
```

### link-flow コマンド

次に、**link-flow** コマンドの例を示します。

```
router(config-qos-profile)#link-flow ?
<1-4294967295> Value
```

```
router(config-qos-profile)#link-flow 40 ?
<cr>
```

```
router(config-qos-profile)#
```

### tft コマンド

次に、**tft** コマンドの例を示します。

```
router(config-qos-profile)#tft-allowed ?
<1-4294967295> Value
```

```
router(config-qos-profile)#tft-allowed 1 ?
<cr>
```

```
router(config-qos-profile)#tft-allowed 1
```

### subscriber redundancy rate コマンド

次に、**subscriber redundancy rate** コマンドの例を示します。

```
router(config)# subscriber redundancy rate 250 1
```

## 設定の確認

PDSN 上の加入者 QoS プロファイルを確認するには、次のタスクを実行します。

コマンド	目的
ステップ1 router# <b>show cdma pdsn session {qos tft detail}</b>	Cisco PDSN リリース 4.0 では、 <b>show cdma pdsn session command</b> で、次の情報を表示する拡張機能が追加されました。 <ul style="list-style-type: none"> <li>加入者 QoS プロファイル</li> <li>既存の内容に加えてこのセッションにインストールされた TFT</li> </ul>
ステップ2 router# <b>Show cdma pdsn qos local profile</b>	このコマンドで、ローカルで設定された加入者 QoS プロファイルが表示されます。
ステップ3 router# <b>show cdma pdsn</b>	Cisco PDSN リリース 4.0 では、QoS がイネーブルにされ、ポリシングがインストールおよびイネーブルにされているセッションの数を表示する新しいカウンタが導入されます。
ステップ4 router# <b>show cdma pdsn statistics</b>	Cisco PDSN リリース 4.0 では、次の情報を表示する新しいカウンタが導入されました。 <ul style="list-style-type: none"> <li>解析に成功した TFT と失敗した TFT の数</li> <li>TFT 解析が失敗した理由を特定する新規カウンタ</li> <li>AAA サーバからダウンロードしたか、ローカルにインストールされている、加入者 QoS プロファイルの数</li> <li>加入者 QoS プロファイルの統合</li> <li>インストールされた、またはアンインストールされたポリシング</li> <li>インストールされたポリシーに基づいて DSCP がコメントされたパケット</li> </ul>

## 例

次に、**show cdma pdsn session tft** コマンドの例を示します。

```
router# show cdma pdsn session tft
Mobile Station ID IMSI 123456789011122
PCF IP Address 10.1.1.1, PCF Session ID 1
This session has 1 flow
This session has 1 Tft
TFT IP Address 3.1.1.1
```

```

Number of Packet Filters Forward 2, Reverse 1
Forward Packet Filters
  Packet Filter 1
    Flow Id 10, Precedence 255, PF Type 0
    Source Port 125

  Packet Filter 2
    Flow Id 10, Precedence 255, PF Type 0
    Source Port 125

Reverse Packet Filters
  Packet Filter 1
    Flow Id 10, Precedence 10, PF Type 0
    Source Port 125

Mobile Station ID IMSI 123456789011123
PCF IP Address 10.1.1.1, PCF Session ID 2
This session has 1 flow
This session has 1 Tft

TFT IP Address 3.1.1.2
Number of Packet Filters Forward 2, Reverse 3
Forward Packet Filters
  Packet Filter 1
    Flow Id 2, Precedence 2, PF Type 0
    Source Ip 5.5.5.5 Mask 255.255.255.0

  Packet Filter 2
    Flow Id 5, Precedence 5, PF Type 0
    Source Ip 1.1.1.1 Mask 255.255.255.0

Reverse Packet Filters
  Packet Filter 1
    Flow Id 10, Precedence 255, PF Type 0
    Source Port 125

  Packet Filter 2
    Flow Id 10, Precedence 255, PF Type 0
    Source Port 125

  Packet Filter 3
    Flow Id 10, Precedence 255, PF Type 0
    Source Port 125

```

次に、**show cdma pdsn qos local profile** コマンドの例を示します。

```

router# show cdma pdsn qos ?
  local          CDMA PDSN local qos information

router# show cdma pdsn qos local ?
  profile        CDMA PDSN local qos profile information

router# show cdma pdsn qos local profile ?
  | Output modifiers
  <cr>

router# show cdma pdsn qos local profile ?
CDMA PDSN LOCAL QOS PROFILE
QoS subscriber profile
  Max Aggregate Bandwidth : 8000
  Inter User Priority : 4321
  Maximum Flow Priority : 4
  Number of persistent TFT : 10
  Total link flow : 2

```



```

Service Option : 59
Service Option : 61
Flow-profile
Forward flow-id : 1
Reverse flow-id : 2
Bi-direction flow-id : 3
DSCP
Allowed-class AF
Max-selector class 4

```

次に、QoS の統計情報を特定する `show cdma pdsn statistics` コマンドの例の抜粋を示します。

```

router #show cdma pdsn statistics

QoS:
Total Profile Download Success 10, Failure 10, Local Profile selected 4
Failure Reason DSCP 1, Bandwidth 1, TFT 1, Flow Profile ID 1,
Max per flow 1, IUP 1, Others 4
Total Consolidated Profile 4, DSCP Remarked 0
Total Policing installed 4, failure 5, removed 4

```

## その他の QoS パラメータ

MS は R\_QOS\_SUB\_BLOB から PCF の IP フローについて QoS パラメータを送信します。PCF は QoS を認めた後で、その詳細を A11 RRQ で PDSN に転送します。この詳細はアカウントティングの間は保存および転送されます。また、この詳細には、A10 接続マッピングに使用される IP フロー (FlowID) の定義のマッピングが含まれます。このプロブには、フロー ID をベアラ パケットに含める必要があるかを示すインジケータも含まれます。設定する場合、PDSN は、そのフローのすべてのベアラ パケットにフロー ID などの新しい GRE ヘッダーを追加します。

## フローの再マッピング

セッションと接続がアップ状態でも、MS が再マッピングを決定することはよくあります。たとえば、アプリケーションの起動時に実行されることがあります。このような場合、QoS が再ネゴシエーションされ、詳細は PDSN に転送されます。PDSN は A10 を作成または削除し、対応する A10 接続にフローを再マッピングします。

## Per-flow アカウンティング

### 接続の確立

HRPD システムでは、複数の A10 接続の確立に単一の A11 レジストレーション要求メッセージが使用される場合、確立される A10 接続ごとに A10 Connection Setup Airlink レコードが含まれます。QoS プロブのフィールドは、アカウントティングのために AAA サーバに転送する以外に、PDSN で使用または処理されません。

### エアリンクの開始

accounting start は次の条件で生成されます。

- ID が FFH の IP フローの場合、メインの A10 接続がトラフィック チャネルに関連付けられるとき、または新しいパラメータが設定されるとき。
- その他すべての IP フローの場合、その IP フローで、
  - IP フローがアクティブな状態であり、さらにその関連するリンク フローがトラフィック チャネルに関連付けられているとき。

- 新しいパラメータが設定される時。



(注) HRPD システムで ID が FFH の IP フローの場合、アカウントリングは双方向です。これは forward および reverse の IP フローの両方に適用されます。

このレコードに許可された QoS パラメータは含まれません。

### エアリンクの停止

accounting stop は次の条件で生成されます。

- メインの A10 接続は、トラフィック チャンネルとの関連付けが解除されるか、パラメータ設定が有効ではなくなります。
- その他すべての IP フローについて、IP フローがアクティブな状態で、その関連するリンク フローがトラフィック チャンネルと関連付けられている場合、次の結果の 1 つ以上が発生します。
  - トラフィック チャンネルの解放、
  - IP フローの非アクティブ化または削除、
  - リンクとトラフィック チャンネルとの関連付けの解除。または、
- パラメータ設定が有効ではなくなった場合。

PCF 間のハンドオフの場合、ソース PCF は、アクティブ化された各 IP フローの Active-Stop Airlink レコードを PDSN に送信します。また、対象の PCF は、各方向のアクティブ化された各 IP フローの Active-Start Airlink レコードを PDSN を送信します。

A11 のレジストレーション中に、いくつかの接続が見つからず、フローが削除された場合、その接続およびフローに accounting stop が送信されます。同様に、新しく追加されたすべての flow-id に、accounting start が送信されます。

受信したアカウントリング レコードを含む IP フローは、それぞれの IP フロー ID および方向を含む許可された QoS で識別されます。IP フローの再マッピングが発生すると、そのフローは、ある A10 から別の A10 にマッピングされます。PDSN は古い A10 に accounting stop を送信し、その IP フローの新しい A10 には accounting start を送信します。このシナリオでは、accounting Start および Stop は、それぞれ active start および active stop の受信でトリガされます。active start および stop が受信されず、セッションが中断された場合でも、古い A10 に対する accounting stop と新しい A10 に対する start のペアは、その IP フローに送信されます。

IP フローで flow status が inactive の active stop を受信すると、フローは非アクティブ状態に移行します。その IP フローで active start を受信すると、フローはアクティブになります。IP フローがアクティブから非アクティブに以降すると、PDSN は stop accounting stop record を生成します。active start を受信した後、および accounting start が送信された非アクティブからアクティブに変更されたときは、IP フローがアクティブに戻ります。

## Per-Flow アカウンティングの設定

PDSN で Per-Flow アカウンティングを設定するには、次のタスクを実行します。

コマンド	目的
ステップ1 router# <b>cdma pdsn attribute send</b> {f16 f17 f18 f19 f20 f22}	Cisco PDSN リリース 4.0 では、既存の CLI コマンドに新しいオプションが導入されました。次の新しいアトリビュートがアカウンティング メッセージで送信されます。  (F16) Forward PDCH RC (F17) Forward DCCH Mux Option (F18) Reverse DCCH Mux Option (F19) Forward DCCH RC (F20) Reverse DCCH RC (F22) Reverse PDCH RC

### 例

次に、Cisco PDSN リリース 4.0 の出力例を示します。

```
cdma pdsn attribute send ?
a1          Attribute Calling Station ID
a2          Attribute ESN, Electronic Serial Number
a3          Attribute MEID, Mobile Equipment Identifier
c5          Service Reference ID
esn-optional Send ESN in Access Req/accounting records only when received
            from PCF

f11         IP Technology
f15         Attribute f15, always-on
f16       Forward PDCH RC
f17         Forward DCCH MUX
f18         Reverse DCCH MUX
f19         Forward DCCH RC
f20         Reverse DCCH RC
f22         Reverse PDCH RC
f5          Attribute Service Option
g1          Attribute Input Octets
g17         Last known user activity
g2          Attribute Output Octets
is835a      is835a specified attributes (g3 and g8 to g16)
```

PCF から受信する場合にだけ、Access 要求/アカウンティング レコードに meid-optional Send MEID があります。

## Per-Flow アカウンティングの確認

Per-Flow アカウンティングが PDSN に設定されていることを確認するには、次のタスクを実行します。

コマンド	目的
ステップ1 router# <b>Show cdma pdsn accounting [detail]</b>	Cisco PDSN リリース 4.0 では、HRPD および IP フローの情報を表示するように出力が強化されました。

### 例

次に、出力例を示します。

```

router#show cdma pdsn accounting detail
UDR for session
session ID: 1
Mobile Station ID IMSI 123456789123457

Mobile Station ID (A1) IMSI 123456789123457
ESN (A2) 000100020003005
MEID (A3)
Session Continue (C3) ' ' 0
Serving PCF (D3) 2.2.1.1 Base Station ID (D4) 000000000000
User Zone (E1) 0000
Forward Mux Option (F1) 1 Reverse Mux Option (F2) 2
Service Option (F5) 59 Forward Traffic Type (F6) 6
Reverse Traffix type (F7) 7 Fundamental Frame size (F8) 8
Forward Fundamental RC (F9) 9 Reverse Fundamental RC (F10) 10
DCCH Frame Format (F14) 14 Always On (F15) 0
Forward PDCH RC (F16) 16 Forward DCCH Mux (F17) 17
Reverse DCCH Mux (F18) 18 Forward DCCH RC (F19) 19
Reverse DCCH RC (F20) 20 Reverse PDCH RC (F22) 22

Bad PPP Frame Count (G3) 0 Active Time (G8) 0
Number of Active Transitions (G9) 1
SDB Octet Count Terminating (G10) 0
SDB Octet Count Originating (G11) 0
Number of SDBs Terminating (G12) 0
Number of SDBs Originating G13 0
Number of HDLC Layer Bytes Received (G14) 225
In-Bound Mobile IP Signalling Octet Count (G15) 0
Out-bound Mobile IP Signalling Octet Count (G16) 0
Last User Activity Time (G17) 0
IP Quality of Service (I1) 0
Airlink Quality of Service (I4) 0
R-P Session ID (Y2) 1

UDR for flow
Mobile Node IP address 20.2.0.0
IP Address (B1) 20.2.0.0, Network Access Identifier (B2) mwtcp-sip-basic-user1
Account Session ID (C1) 4248
Correlation ID (C2) ' ' 240
Beginning Session (C4) ' ' 0
MIP Home Agent (D1) 0.0.0.0
IP Technology (F11) 01 Compulsory Tunnel indicator (F12) 00
Release Indicator (F13) 00
Data Octet Count Terminating (G1) 0
Data Octet Count Originating (G2) 0 Event Time G4:1219295403
Rsvp Signaling Inbound Count (G22) 0 Outbound Count (G23) 0
Rsvp Signaling Packets In (G24) 0 Packets Out (G25) 0
Packets- in:0 out:0

```

次に、Cisco PDSN リリース 4.0 で導入された部分を示します。

```

UDR for IPFlow (new: Yes)
Session ID : 2 Flow ID : 0x01 Direction : Forward
Account Session ID (C1) 1095 Correlation (C2) 0
Service Reference ID (C5) 2 Flow ID (C6) 1
Serving PCF (D3) 2.2.1.1
Forward Mux Option (F1) 1 Reverse Mux Option (F2) 2
Service Option (F5) 59 Forward Traffic Type (F6) 6
Reverse Traffix type (F7) 7 Fundamental Frame size (F8) 8
Forward Fundamental RC (F9) 9 Reverse Fundamntal RC (F10) 10
DCCH Frame Format (F14) 14 Forward PDCH RC (F16) 16
Forward DCCH Mux (F17) 17 Reverse DCCH Mux (F18) 18
Forward DCCH RC (F19) 19 Reverse DCCH RC (F20) 20

```

**Reverse PDCH RC (F22) 22    Flow Status (F24) Active**

Data Octet Count Terminating (G1) 0  
 Data Octet Count Originating (G2) 0    Event Time G4:0  
 Active Time (G8) 0  
 Number of Active Transitions (G9) 1  
 SDB Octet Count Terminating (G10) 0  
 SDB Octet Count Originating (G11) 0  
 Number of SDBs Terminating (G12) 0  
 Number of SDBs Originating G13 0  
**Granted Qos (I5):**  
 Flow direction :0 Flow ID :1  
 Flow Profile ID :0  
 Qos Attribute Set ID :1 Traffic Class :0  
 Peak Rate :1 Bucket Size :100  
 Token Rate :100 Maximum Latency :100  
 Max IP Packet Loss Rate :10  
**Packet Size :10 Delay Variance Sensitive :100**  
 IP Quality of Service (I1) 0  
 Airlink Quality of Service (I4) 0  
 R-P Session ID (Y2) 2

## UDR for session

session ID: 1  
 Mobile Station ID IMSI 987654321098766

Mobile Station ID (A1) IMSI 987654321098766  
 ESN (A2)  
 MEID (A3)  
 Session Continue (C3) ' ' 0  
 Serving PCF (D3) 11.1.1.11 Base Station ID (D4) 123412340000  
 HRPD Subnet (D7) SNL 40  
     SN 0001000100020003000000000000000004  
     SID 0003000400050006000000000000000007  
 User Zone (E1) 0000  
 Forward Mux Option (F1) 241    Reverse Mux Option (F2) 242  
 Service Option (F5) 59    Forward Traffic Type (F6) 246  
 Reverse Traffic type (F7) 247    Fundamental Frame size (F8) 248  
 Forward Fundamental RC (F9) 249    Reverse Fundamntal RC (F10) 250  
 DCCH Frame Format (F14) 0    Always On (F15) 0  
 Forward PDCH RC (F16) 0    Forward DCCH Mux (F17) 0  
 Reverse DCCH Mux (F18) 0    Forward DCCH RC (F19) 0  
 Reverse DCCH RC (F20) 0    Reverse PDCH RC (F22) 0

Bad PPP Frame Count (G3) 0 Active Time (G8) 0  
 Number of Active Transitions (G9) 0  
 SDB Octet Count Terminating (G10) 0  
 SDB Octet Count Originating (G11) 0  
 Number of SDBs Terminating (G12) 0  
 Number of SDBs Originating G13 0  
 Number of HDLC Layer Bytes Received (G14) 177  
 In-Bound Mobile IP Signalling Octet Count (G15) 0  
 Out-bound Mobile IP Signalling Octet Count (G16) 0  
 Last User Activity Time (G17) 0  
 IP Quality of Service (I1) 0  
 Airlink Quality of Service (I4) 0  
 R-P Session ID (Y2) 1

## UDR for flow

Mobile Node IP address 9.1.1.6  
 IP Address (B1) 9.1.1.6, Network Access Identifier (B2) g7SIP1@xxx.com  
 Account Session ID (C1) 11  
 Correlation ID (C2) ' ' 34  
 Beginning Session (C4) ' ' 0

```
MIP Home Agent (D1) 0.0.0.0
IP Technology (F11) 01 Compulsory Tunnel indicator (F12) 00
Release Indicator (F13) 00
Data Octet Count Terminating (G1) 0
Data Octet Count Originating (G2) 0 Event Time G4:1247463520
Rsvp Signaling Inbound Count (G22) 0 Outbound Count (G23) 0
Rsvp Signaling Packets In (G24) 0 Packets Out (G25) 0
Packets- in:0 out:0
```

## ハンドオフ シナリオ

ここでは、多様なハンドオフ シナリオについて説明します。

### PCF 間のハンドオフ - 同じ PDSN (RevA から RevA)

PDSN は、PPP の再ネゴシエーションかどうかに関係なく、古い PCF との既存の A10 接続をすべて解放し、新しい PCF のために補助接続を新しく確立します。

この場合、TFT はクリアされません。フロー ID は保持され、新しい PCF の A10 接続に再マッピングされます。

### 1x から RevA へのハンドオフ

MN が 1x ネットワークから Rev A PCF にハンドオフすると、既存のフローがメイン サービス接続と見なされます。補助サービス フローおよびアプリケーションフローが新しく作成されます。1xRTT から EV-DO へのハンドオフが発生した場合、PDSN は各方向の 1 フローごとに active start を受信すると、accounting start を送信します。この場合、その IP フローの関連する A10 について、connection setup が受信されます。

### Rev A から 1x へのハンドオフ

MN が Rev A PCF から 1x PCF へハンドオフする場合、すべてのサービス フローおよびアプリケーションフローは TFT を除いて削除されます。加入者 QoS プロファイルはそのセッションで保持されません。ポリシングおよび DSCP の確認が実行中の場合は、続行されます。EV-DO から 1xRTT へのハンドオフがある場合、アクティブな IP フローについて、各方向の IP フローごとに accounting stop が送信されます。Start-Stops のペアが非アクティブの IP フローに送信されます。これは、AAA サーバコンテキストからデタッチできる最後の stop のためです。

## コール アドミッション制御

加入者 QoS プロファイルのペアとして、帯域幅は AAA サーバからダウンロードされます。PDSN は、その帯域幅をモバイル ステーションに使用できるようにする必要があります。この帯域幅は、モバイルが何らかのビデオ サービスを使用する場合に役立ちます。

PDSN には、使用可能な最大帯域幅を定義する出力と見なされる特定のインターフェイスはありません。そのため、直接の割り当てはありません。また、PDSN は、割り当てのエラー時に汎用的な IOS QoS 実装を使用できません。

解決策として、ボックスの合計帯域幅を定義する新しい CLI コマンドが導入されました。この帯域幅は、SAMI カード上のギガビット インターフェイスか、ラインカード上の出力インターフェイスの場合があります。使用可能な最大帯域幅は、この 2 つのうち小さい方です。

セッションが PDSN に登録され、PDSN が割り当てる帯域幅をダウンロードすると、常に使用できる帯域幅が確認されます。要求された帯域幅を使用できる場合、セッションが作成され、割り当てられた量が使用可能な帯域幅から差し引かれます。帯域幅がなくなると、コールは拒否されます。

セッションが削除されると、帯域幅は元のプールに戻されます。

レジストレーション中に異なる帯域幅がダウンロードされるたびに、古い帯域幅は返され、新しい帯域幅が差し引かれます。

$$\text{帯域幅要因} = (\text{消費帯域幅} / \text{総帯域幅}) \times 100$$

この他にも、メモリ、CPU、およびセッション負荷要因が含まれることがあります。

#### セッション負荷：

現在、計算されクラスタ コントローラに転送される負荷は、ボックスの総セッション キャパシティに対するアクティブなセッション数の比率です。

$$\text{セッション要因} = (\text{アクティブなセッション数} / \text{総セッション キャパシティ}) \times 100$$

#### メモリ：

メモリ要因は、プロセッサ メモリと IO メモリの 2 つの部分で構成されています。RRQ が受け入れられるのは、メモリの 10% が使用可能な場合（プロセッサ メモリと IO メモリの両方） だけにする必要があります。

$$\text{プロセッサメモリ要因} = (\text{使用メモリ} / \text{総メモリ}) \times 100$$

$$\text{IO メモリ要因} = (\text{使用メモリ} / \text{総メモリ}) \times 100$$

#### CPU 要因：

プロセッサは、重いトラフィック（1 秒あたりに大量のパケット）や大量の要求、重いデータ トラフィックにより負荷がかかることがあります。このパラメータを考慮する場合、計算に最新の CPU 使用率を採用する必要があります。

$$\text{CPU 要因} = (\text{CPU} \%)$$

4 つのパラメータすべてを考慮した新しい負荷要因は 4 つの最大値となります。

最大値がメモリまたは CPU の場合、新しいレジストレーション要求は、設定されたしきい値未満に値が低下するまで拒否されます。

最大値の原因が帯域幅要因で、新しい要求が 1x（帯域幅をダウンロードしない）の場合、要求は許可されます。RevA または 1x（帯域幅をダウンロード）の場合、帯域幅がダウンロードされるまでレジストレーションは処理されます。その後、帯域幅の可用性に基づいて、要求は処理または拒否されます。

セッション数が最も高い値の場合、最大値に達するまで処理されます。

#### コントローラとメンバーの計算

メンバーは新しく計算された負荷をシステムの正確な負荷としてコントローラに送信します。コントローラは、メンバーから送信された負荷値を使用してロード バランシングを行います。関連付けられたすべてのメンバーの負荷パラメータのいずれかがしきい値 100% に達すると、コントローラはコールを拒否します。BW および CPU しきい値が設定されている場合、CAC はメンバーでイネーブルになります。Cisco PDSN リリース 4.0 をサポートするために、コントローラで複数のフローがイネーブルになります。デフォルトのメモリしきい値は 90 % です。

## PDSN でのコール アドミッション制御の設定

PDSN でコール アドミッション制御機能を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>router# cdma pdsn cac maximum [bandwidth number]</code> <code>cdma pdsn cac maximum [cpu number]</code>	コール アドミッション制御機能をイネーブルにします。 <b>bandwidth</b> キーワードを使用して最大 CAC 帯域幅パラメータを制御し、 <b>cpu</b> キーワードを使用して最大 CPU しきい値を制御します。
ステップ 2	<code>router# cdma pdsn cluster controller member</code> <code>reva-support</code>	メンバーが Cisco PDSN リリース 4.0 に基づいている場合、CAC は多くのパラメータに基づいて行われます。このコマンドを使用して、クラスタ コントローラで新しく導入されたすべてのパラメータを活用して負荷を分散させます。



(注) MIP コールのレジストレーション中に RADIUS サーバから帯域幅をダウンロードする方法は、現在 PDSN では処理されません。

### 例

次に、コンフィギュレーション コマンドの例を示します。

```
router# cdma pdsn cac ?
  maximum          Configure Maximum values for CAC Parameters

cdma pdsn cac maximum ?
  bandwidth        Configure Maximum Bandwidth
  cpu              Configure CPU Threshold parameters

cdma pdsn cac maximum bandwidth ?
<8000-2000000000> Value

cdma pdsn cac maximum cpu ?
<30-100> Value
```



(注) デフォルトでは、最大 CPU 値は 90 です。

### 設定の確認

CAC 機能がイネーブルかどうかの確認および CAC 機能に関する情報収集を行うには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>router# show cdma pdsn cac</code>	さまざまなコール アドミッション制御パラメータおよびステータスを表示します。

### 例

`show cdma pdsn cac` コマンドの例を示します。

```
router# show cdma pdsn cac
Router#sh cdma pdsn cac
```



in percentage	Output in Values	Output
Total configured bandwidth	200000000 b	100%
Allocated bandwidth	0 b	0%
Available bandwidth	200000000 b	100%
CPU Threshold		90%
CPU Current		0%
Processor Memory Threshold	813609471	90%
Processor Memory Current	73398292	8%
IO Memory Threshold	60397977	90%
IO Memory Current	45603376	67%
Sessions allocated	0	0%
Max sessions allowed	25000	100%
Router#		

## リソース管理

リソース管理では、PDSN や HA などのネットワーク要素でパケット データ セッションに関連するリソースを解放するメカニズムを定義します。リソースはセッションのハンドオフにより、または管理上の目的で解放されることがあります。

IS-835-C は、リソース管理に次の 2 つのメカニズムを定義しています。

- パケット オブ ディスコネクト (POD)
- MIP リソース失効

Packet of Disconnect (POD; パケット オブ ディスコネクト) に基づくリソース管理は SIP、MIP、および PMIP フローに適用され、MIP リソース失効に基づくリソース管理は、MIP フローだけに適用されます。

PDSN は、パケット オブ ディスコネクトおよび MIP リソース失効の両方に基づくリソース管理をサポートしています。

## モバイル IP のリソース失効

基本的な MIP リソースの失効は、モビリティ エージェント (MIP サービスを MH に提供する) が他のモビリティ エージェントに、管理上の理由または MN ハンドオフによってレジストレーションの終了を通知できる方式を定義する IS-835-C イニシアチブです。

PDSN/FA で設定されている場合、エージェント アドバタイズメントのモビリティ エージェント アドバタイズメント エクステンションには X ビットが設定され、そのリンクでのリソース失効のアドバタイジングがサポートされます。MIPv4 でリソース失効をサポートするように設定されている PDSN には、再レジストレーションを含むすべての MIP RRQ に失効サポート エクステンションが含まれます。HA からの関連 MIP RRP にも有効な失効サポート エクステンションが含まれている場合、PDSN は関連付けられたレジストレーションを取り消し可能と見なします。

取り消し可能なレジストレーションの場合、PDSN/FA が管理上セッションを終了する必要があるときは、PDSN/FA は HA にリソース失効メッセージを送信し、そのレジストレーション用に確保されていたリソースを解放します。

HA から設定可能な時間内にリソース失効 ACK メッセージを受信しない場合、リソース失効メッセージが再送信されます。

HA からリソース失効メッセージが受信され、レジストレーション（ホーム アドレス、気付アドレス、HA アドレスにより識別）が検出されると、そのレジストレーションが確保していたリソースが解放され、リソース失効 ACK メッセージが HA に返されます。取り消されたバインディングに関連付けられた PPP セッションで他にアクティブな MIP レジストレーションがない場合、PDSN は取り消されたレジストレーションに関連付けられていた PPP および R-P セッションを解放します。

## レジストレーション取り消しの制約

PDSN ではレジストレーション取り消しに次の制約が適用されます。

- FA-CHAP および HA-CHAP 中に Access-Accept メッセージで AAA サーバから返された STC VSA は無視され、PDSN および HA のローカル コンフィギュレーションが優先されます。
- 失効のエクステンションとメッセージは、FHAЕ や IPsec で保護されていない場合も、PDSN と HA の両方で受け付けられ、処理されます。ユーザが FA-HA セキュリティの関連付けを設定するか、2 つのエージェント間に IPsec トンネルを提供して、メッセージのセキュリティを提供することを推奨します。
- MobileIP MIB はレジストレーション取り消し情報でアップデートされません。
- PDSN では、すべての **ip mobile foreign-service** コマンドは、インターフェイス レベルではなくグローバル レベルで設定する必要があります。
- PDSN では、I-bit のサポートのために、ローカル ポリシーは I-bit と常にネゴシエートし、失効メッセージで常に 1 に設定します。また、MN データ フローの取り消しを通知しながら、エージェント アドバタイズメント メッセージで B-bit を 1 に設定する方法はサポートされていません。
- リリース失効とバインド アップデートを同時にイネーブルにすることはできません。いずれか 1 つを選択しなければなりません。

## パケット オブ ディスコネクト

RADIUS 切断（または POD）は、RADIUS サーバが Radius Disconnect メッセージを PDSN に送信してリソースを解放できるメカニズムです。リソースはセッションのハンドオフにより、または管理上の目的で解放されることがあります。識別されるリソースには、PPP、RP セッションおよび MIP バインディングが含まれます。PDSN および HA での RADIUS 切断のサポートは TIA835C に準拠します。

PDSN は、Access-Request メッセージ（認証および認可手順のために送信）の中に、3GPP2 ベンダー固有 Session Termination Capability (STC) VSA を含めることでリソース管理機能をホーム AAA サーバに伝えます。STC VSA で送信された値はコンフィギュレーションで取得されます。また、PDSN は Access-Request に Fully Qualified Domain Name (FQDN; 完全修飾ドメイン名) を含む NAS-Identifier アトリビュートも含めます。

ホーム AAA サーバは、ユーザと NAS Identifier/NAS-IP アドレス間の関係を確立して、PDSN 間ハンドオフを検出します。Access-Request で受信した NAS-Identifier/ NAS IP アドレスが前に保存された値（ゼロ以外）と異なる場合、PDSN 間ハンドオフが検出されます。

Disconnect Request には、NAS-ID および Username (NAI) アトリビュートが含まれます。オプションで、セッション識別アトリビュートとして 3GPP2 Correlation ID Calling station ID (IMSI) および Framed IP アドレスが含まれていることもあります。PDSN 間ハンドオフが検出された場合は、Disconnect Reason VSA が含まれます。PDSN でサポートされるセッション識別アトリビュートは、3GPP2 Correlation ID と Calling station ID (IMSI) です。

3GPP2 Correlation ID および Calling station ID (IMSI) アトリビュートが Disconnect Request で受信され、PDSN がそれらに対応するセッションまたはフローを検出できると、PDSN は関連付けられたフローを終了し、Disconnect ACK メッセージを RADIUS サーバに送信します。受信したアトリビュートでセッションが検出されない場合、PDSN はエラー コード "session context not found"（セッション

コンテキストが見つかりませんでした)とともに Disconnect NACK メッセージを返します。Disconnect Request に無効なアトリビュート (8 桁の IMSI など) がある場合、PDSN がエラー コード "Invalid Request" (無効な要求) とともに Disconnect NACK を返します。

PDSN は、NAI アトリビュート (設定されている場合) だけを含む Disconnect Request の処理もサポートします。規格に準拠して、PDSN は受信したユーザ名に対応するすべてのセッションを終了します。

Ballot バージョンは、HA で Disconnect Request を受信する可能性があることに触れていますが、そのようなイベントでとられるアクションについての詳細な説明はありません。そのため、NAI とともに Framed-IP-Address アトリビュートが受信された場合は、そのバインディングを終了し、Disconnect Request で NAI アトリビュートだけが受信された場合は、その NAI のすべてのバインディングを終了するというアプローチを採用します。

この機能には次の制約事項があります。

- 休止 NVSE はどれもサポートされません。

この機能のコマンドライン インターフェイスは、標準 AAA サーバ インターフェイスです。リリース 2.0 以上で推奨される POD の設定方法は、**aaa server radius dynamic-author** コマンドを使用する方法です。この方法により、クライアント、セキュリティ キー、その他の変数の設定オプションのあるサブコンフィギュレーション モードに入ります。

次の NAS グローバル AAA コマンドは、POD パケットのリスニングをイネーブルにするために使用されます。

- **aaa pod server key word**。word は共有キーです。

このコマンドの完全な構文は次のとおりです。

- **aaa pod server [clients ipaddr1 [ipaddr2] [ipaddr3] [ipaddr4]] [port port-number] [auth-type {any | all | session-key}] server-key [encryption-type] string**

次のデバッグ コマンドも使用できます。

- debug aaa pod

## RADIUS 切断の制約事項

- 休止 NVSE はどれもサポートされません。
- MIB サポートは現在計画されていません。
- NAI だけを持つ RADIUS Disconnect メッセージの処理は、IS 835-C に準拠して設定する必要があります。

## RADIUS の機能強化

Cisco PDSN リリース 3.0 は、次の機能強化をサポートします。

- RADIUS サーバのロード バランシング
- レルムに基づく RADIUS サーバの選択

## RADIUS サーバのロード バランシング

RADIUS ロード バランシング (RLB) 機能は、RADIUS サーバ セット全体で RADIUS 認証およびアカウンティング トランザクションの負荷を共有します。RLB がいない場合、すべてのトランザクションは、サーバ グループでアライブ状態であると見なされた最初のサーバに送られます。このサーバから

の応答が停止し、デッドとしてマークされると、PDSN はグループの次のサーバにフェールオーバーします。グループに他に使用可能なサーバが存在するにもかかわらず、1 台のサーバだけを使用すると、コール設定とティアダウンの全体的なスループットが制限されます。

RADIUS サーバのロード バランシングでは、PDSN は、トランザクションの負荷をサーバ グループ内の複数のサーバに分散できます。低速のサーバが追跡され、それらのサーバではトランザクションの負荷は軽減されます。また、サーバがデッドとマークされた場合や再起動された場合にも適応します。

トランザクションはバッチ (サイズは設定可能) にグループ化され、各サーバに 1 つのバッチが割り当てられ、処理されます。この機能では、それらのバッチに基づいて、1 度に 1 つのバッチずつトランザクションの負荷を分散します。最初のトランザクションを受け取ると、アルゴリズムにより最も未処理のトランザクションが少ないサーバが特定され、このサーバに次のトランザクションのバッチが割り当てられます。トランザクションのバッチが割り当てられると、最も未処理のトランザクションが少ないサーバが特定され、このサーバに次のトランザクションのバッチが割り当てられます。こうして、常に最も未処理のトランザクションが少ないサーバに次のバッチが割り当てられます。このロード バランシング スキームは、サーバ グループに基づいて適用できます。つまり IOS プラットフォームで定義された各サーバ グループに独自のロード バランシング スキームを設定できます。

バッチ サイズは慎重に設定する必要があります。バッチ サイズを大きさを決定する場合、スループットと CPU 負荷のバランスを考慮する必要があります。バッチ サイズを大きくすると、計算量が減り、CPU の負荷は小さくなりますが、サーバ グループ内の他のサーバがアイドル状態であるにもかかわらず、特定のサーバにトランザクションが割り当てられる可能性があります。バッチ サイズが非常に小さい場合、サーバ全体で未処理の負荷を頻繁に計算するため、CPU の負荷が大きくなります。研究室でのシミュレーションでは、バッチ サイズを 25 にすると、CPU の負荷に悪影響を与えることなく、適度なスループットが得られることが示されています。

### 高遅延 RADIUS サーバ

アルゴリズムは、応答時間の異なるサーバに十分適応できます。迅速なサーバは未処理のトランザクション数が少なく、大量の着信トランザクションが割り当てられます。低速のサーバは、割り当てられるトランザクションの数は比例して少なくなります。

### サーバのフェールオーバー

フェールオーバー後、トランザクションが次のサーバにフェールオーバーすると、そのサーバの未処理カウントが増えます。こうして、フェールオーバーされたトランザクションもロード バランシングされます。次のトランザクションのバッチが割り当てられると、このサーバの未処理カウントにその負荷が正確に反映され、新規トランザクションとフェールオーバー トランザクションの両方が、未処理トランザクション カウントで説明されます。

### サーバグループの処理

次の 2 つのサーバグループがあるとします。

サーバ S1、S2、S3 で構成されるサーバグループ SG1

サーバ S3、S4、S5 で構成されるサーバグループ SG2

SG1 がロード バランシングに設定され、SG2 は設定されていません。要求が SG2 に送信されると、これらの要求は、グループの最初のサーバである S3 に割り当てられ、このサーバの未処理トランザクション カウントが増加します。要求が SG1 に送信された場合、これらの要求はサーバ間でロード バランシングされます。トランザクションを S3 に送信すると、SG2 のトランザクションは直接このサーバに割り当てられるので、S3 の未処理トランザクション カウントが高くなります。したがって、SG1 でのトランザクションを受け取る割合は低くなります。目的はトランザクションをより高速で大きな負荷を処理できるサーバに送信することなので、これは好ましい動作です。負荷は現在サーバグループが処理しているものだけでなく、1 台のサーバが処理しているトランザクションの合計です。

### 優先サーバ

特定のセッションのすべての要求に同じサーバを使用することが望ましい場合があります。RADIUS サーバのロード バランシングでは、このような処理が行われる保証はありません。このような状況を避けるために、Cisco PDSN リリース 3.0 では優先サーバの指示が導入されています。



(注)

この指示は、単なる優先または推奨です。

デフォルトでイネーブルになる優先サーバの動作では、あるセッションのすべてのアカウントिंग レコード (Start、Stop、および Interim) を同じ RADIUS サーバに送ろうとします。ただし、同じセッションの認証レコードと認可レコードは、依然としてロード バランシング アルゴリズムで決定された異なる RADIUS サーバに送られる可能性があります。

次のイベントでは、同じセッションのアカウントिंग レコードが異なる RADIUS サーバに送られることがあります。

- PPP 再ネゴシエーション
- ハンドオフ

PDSN は、可能な限りそのサーバを使用しようとしませんが、ロードバランシング メカニズムに基づいてグループの他のサーバにフォールバックすることもあります。

このインジケータが使用される場合、使用するサーバの決定にコストは考慮されません。ただし、常に優先サーバを使用できるわけではありません。サーバがデッドとマークされている場合があります。あるいは、サーバが、セッション中に前のトランザクションに使用されたサーバ グループに属していないために使用できないこともあります (たとえば、アカウントिंग サーバ グループは認証サーバ グループとは異なる場合などです)。この場合、アルゴリズムは、ロードバランシング スキームに基づいて代替サーバを選択できます。

### 着信 RADIUS 要求

RADIUS サーバのロード バランシング機能は、着信 RADIUS 要求 (パケット オブ ディスコネクトなど) には適用できません。POD 応答は、サービスを要求したサーバが応答先となる必要があるため、これらの要求はサーバ間でロードバランシングできません。

## ドメインに基づく加入者認可

Cisco IOS には、それぞれのレルムに基づいて加入者を認可する「加入者認可」メカニズムがあります。この機能の詳細については、次の URL にアクセスしてください。

[http://www.cisco.com/en/US/partner/products/ps6350/products\\_configuration\\_guide\\_chapter09186a0080455cf0.html#wp1056463](http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a0080455cf0.html#wp1056463)

## IS-835 前払いのサポート

Cisco PDSN リリース 2.0 は、前払いユーザのリアルタイム モニタリングとデータ コール のレーティングを提供します。PDSN の前払い請求ソリューションは、RADIUS (AAA) サーバに基づき、既存のフローベースのアカウントング機能を利用します。前払い請求機能では、RADIUS サーバが PBS とインターフェイスして、リアルタイムの請求情報を PDSN と PBS 間で中継できるようにする必要があります。サードパーティの PBS がデータ コール のリアルタイム レーティングを制御し、ユーザ アカウントの残高を維持します。シスコは PBS を提供していません。

Cisco PDSN リリース 2.1 では、次の 3 種類の前払いサービスを使用できます。

- ボリュームベースの前払いデータ サービス

- タリフ スイッチングによるボリュームベースの前払いデータ サービス
- 時間ベースの前払いデータ サービス

PDSN では、前払い機能は次のタイプのデータ セッションに対してサポートされています。

- AAA サーバで認証と認可が実行される SIP セッション
- AAA サーバでユーザの認証と認可が実行される VPDN セッション
- AAA サーバでセッションまたは NAI に対して FA-CHAP が実行される MIP セッション
- AAA サーバでユーザの認証と認可が実行される PMIP セッション

前払いサービスは、MSID ベースの認証アクセスで開かれたセッションでも使用できます。



(注)

PDSN では、1 つの前払いフローにボリュームベースまたは時間ベースのいずれかを使用できますが、両方のオプションを使用することはできません。PDSN では、それぞれがボリュームまたは時間ベースのどちらかの前払いサービスをサポートする複数のフローが許容されます。PDSN は、特定の時間に、フローごとにボリュームベースだけ、または時間ベースだけ、あるいはどちらの前払いサービスでもサポートするように設定できます。

VPDN 以外の前払いフローに対するボリュームベースのアカウントティングでは、PPP ペイロードに存在するバイト数をカウントします。VPDN の場合、PPP パケット ヘッダーを含む、PPP パケット内のバイト数をカウントします。複数のフローからなるセッションの場合、一部のフローでボリュームベースまたは時間ベースの前払いデータ サービスがイネーブルになり、他のフローではイネーブルになっていないことがあります。

PDSN では、ボリュームベースの前払いデータ サービスには、タリフベースの前払いサービスもサポートされています。タリフベースの前払いサービスをサポートするには、PBS に次の機能が必要です。

- ボリュームによる請求：時間ごとに異なるタリフを設定します。
- 請求サーバはユーザに異なる割り当て（ボリュームベース）を行います。この割り当ては、各時間に対応するタリフによって決まります（このため、2 つの請求レートはオーバーラップしません）。

## Cisco PDSN リリース 2.1 の前払いサポートの制約事項

- リモート アクセス ベースのアカウントティングの前払いはサポートされていません。
- オンラインの Access-Request メッセージは、"Authorize Only"（認可のみ）ではなく "outbound"（送信）というサービスタイプで送信され、メッセージにユーザ パスワードが含まれます。
- 現在のリリースには、前払い MIB サポートはありません。
- HA に対する前払いはサポートされていません。

## 前払い請求

ユーザが AAA サーバ認証で SIP アクセスを実行するか、FA-CHAP で MIP アクセスを実行すると、前払い対応 PDSN は、認証および認可を受けるための RADIUS Access-Request メッセージを送信します。前払い対応 PDSN は、RADIUS Access-Request メッセージに PPAC VSA を含めることで、請求サーバに PDSN の前払い機能を通知します。

ホーム RADIUS は、通常どおり認証および認可手順を実行します。HAAA は、ユーザのプロファイルからユーザが前払いユーザであることを識別すると、請求サーバとインターフェイスしてそのユーザの前払い関連情報を取得し、Access-Request メッセージで前払い関連情報を渡します。請求サーバは、ユーザの前払い認可を実行します。HAAA と請求サーバでの前払い認可手順は、次のステップで構成されています。

- PPAC VSA のチェック
- ホーム ネットワーク ポリシーのチェック
- ユーザのアカウント残高および状態のチェック

請求サーバがユーザを有効な前払いユーザとして認めた場合、サーバは HAAA に、請求サーバのコンフィギュレーションと PDSN が示す機能に基づいて、ボリュームまたは時間、あるいは両方に基づく前払いサービスをサポートすることを通知します。HAAA は PPAC VSA の情報を PDSN にエンコードし、請求サーバによってボリュームベースまたは時間ベース（または両方）の前払いサービスがサポートされていることを示します。

HAAA は、RADIUS Access-Accept または Access-reject メッセージを使用して、前払い対応 PDSN に認可応答を送信します。認可応答では、同じ RADIUS Access-Accept メッセージに PPAQ VSA が含まれ、ユーザに対応する前払いフローの初期割り当て、割り当て ID、および割り当てのしきい値が表示されます。

PDSN が、前払い関連の機能に関して HAAA にオンライン Access-Request メッセージを送信する場合、メッセージの User-Password (=2) フィールドは設定されず、通常の RADIUS メッセージ認証が設定され、メッセージオーセンティケータで実行されます。現在、User-Password はオンライン Access-Request でデフォルト値の "cisco" に設定されています。

PDSN が HAAA から初回の RADIUS Access-Accept メッセージで PPAC VSA を受信しないか、メッセージは含まれているものの、"Prepaid Accounting not used"（前払いアカウントिंग不使用）となっている場合、RADIUS Access-Accept メッセージに PPAQ VSA が含まれていれば、ユーザの前払いフローを解放します。PDSN は Access-Request を HAAA に送信して、クライアントサービスの終了を示す Update-Reason VSA で指定された割り当てを返します。

PDSN がボリュームまたは時間に基づく前払いサービスをサポートできる場合、PDSN は PPAC のセッションに適用される請求サーバ指定サービスに基づいて、フローに対して前払いサービスをイネーブルにします。請求サーバが、PDSN でボリュームまたは時間の割り当てが可能なことも示している場合、PDSN は、HAAA からの PPAQ に含まれる割り当て（ボリュームまたは時間）のタイプに基づいて前払いサービスをイネーブルにします。PPAQ に両方のタイプの割り当てがある場合、PDSN で前払いフローは開かれませんが、

PDSN がボリュームに基づく前払いサービスをサポートでき、請求サーバが時間に基づく前払いサービスをサポートすることを示した場合、PDSN は前払いフローを閉じます。PDSN は "Client Service Termination"（クライアントサービス終了）という Update-Reason VSA を含む Access-Request メッセージを送信します。同じロジックは、PDSN が時間に基づく前払いをサポートし、請求サーバがボリュームに基づく前払いサービスを返した場合にも当てはまります。

PDSN が、サポート対象の前払いサービスを示す PPAC VSA を含む Access-Accept メッセージを受信したものの、メッセージに初期割り当てが含まれていない場合、PDSN はフローを閉じます。Access-Accept で割り当てを受信しなかったため、PDSN は、その後 HAAA に RADIUS Access-Request メッセージを送信しません。

FA-CHAP の MIP レジストレーション中に PDSN が送信する Access-Request に関する HAAA と請求サーバとの対話を無視する場合、PDSN はオンライン Access-Request メッセージで Session-Continue VSA を "TRUE" に設定します。

前払いフローのホストとなったセッションに複数のフローが存在し、前払いフローが停止して、それがセッションの最後のフローだった場合、セッションは PDSN によって削除されます。MIP フローの 1 つが満了し、それがセッションの最後のフローではない場合、PDSN はそのフローをローカルで閉じます。リソース失効メカニズムが PDSN でイネーブルになっている場合、ここでは関連するリソース失効メカニズムが適用されます。

SIP フローが閉じた場合 (PPP セッションのティアダウンや SIP フローの割り当てをすべて消費したなど)、前払いかどうかに関係なく他のすべての MIP フローも閉じます。SIP フローが割り当てをすべて消費したために閉じた場合、"Quota Reached" (割り当てに到達) という Update-Reason を含む Access-Request メッセージを送信します。他の理由で SIP セッションが閉じた場合、"Client Service Termination" (クライアント サービスの終了) という Update-Reason を含む Access-Request が送信されます。PPP セッションの他の前払いフローもすべて、前払いサービスを閉じる Access-Request メッセージを送信し、未使用の割り当てを返します。これらのフローの Update-Reason には、"Main SI Released" (メイン SI 解放) という値が含まれます。

割り当てのしきい値に達すると、PDSN は HAAA に Access-Request を送信して、フローに追加の割り当てを取得します。割り当てのしきい値と指定された割り当てが同じ場合、割り当てを使い切った時に (割り当て = しきい値の場合)、PDSN はこれをフローの終了として処理し、Update-reason が "Quota reached" (割り当てに到達) の Access-Request を送信します。

フローの割り当てが切れると、PDSN は HAAA に、前払いフローが解放されたことを示すオンライン Access-Request を送信します。この間、PDSN はフローを削除済みとしてマークし、フローのパケット交換を停止します。この Access-Request に対して AAA サーバから Access-Accept を受信すると、PDSN はユーザの前払いフローを削除し、アカウント停止を送信します。

PDSN でリソース失効メカニズムが有効になっている場合、PDSN は HA にリソース失効を送信して、HA でのバインディングをクリアし、フローのビジター情報をクリアします。

RADIUS Disconnect Request (POD) または MIP 失効メッセージを受け取ると、PDSN は、Update-Reason サブタイプが "Remote forced disconnect" (リモート強制切断) に設定された、使用済みの割り当てを含みむオンライン RADIUS Access-Request メッセージを送信します。PDSN はフローを削除し、HA にリソース失効メッセージを送信し、既存の RADIUS Accounting-Stop を送信します。

## ボリュームベースの前払いデータ サービス フロー

アカウントリング ボリュームベースの前払いサービスのメトリックは、アップストリームおよびダウンストリーム方向のユーザ フローを通過する総バイト数です。

**ステップ 1** 前払い対応 PDSN は、RADIUS Access-Request メッセージをホーム RADIUS サーバに送信するには SIP または MIP 設定が必要であると判断します。SIP セッションでは、ユーザはローカルではなく AAA サーバに認証される必要があります。MIP ユーザの場合、FA-CHAP 認証が必要です。

PDSN は、HAAA または請求サーバにその PDSN がボリューム ベースの前払いをサポートすることを通知する PPAC VSA (値 = 1 または 3) を含めます。PDSN でリソース失効がイネーブルになっている場合、PDSN は、MIP セッションのリソース失効をサポートできることを示す SessionTerminationCapability (STC) アトリビュートを送信します。

ホーム RADIUS サーバはユーザから送信された Access-Request を通常の方法で認証および認可します。ユーザ プロファイルからユーザが前払い加入者であることが判明すると、HAAA は請求サーバとインターフェイスし、Access-Request メッセージで受信したユーザの前払い情報を請求サーバに提供します。

**ステップ 2** 請求サーバは、ユーザの前払い情報を受信すると、PDSN の機能をチェックします (PPAC VSA で送信)。請求サーバは、ユーザの残高とアカウント ステータスが有効であるかどうかもチェックします。その後請求サーバは PDSN に、ボリュームに基づく前払いパケット データ サービスをサポートすることを伝えます。さらに、ユーザに初期割り当てを行います。これは、通常ユーザが使用できる総割り当



ての一部です。ユーザに指定された割り当ては、請求サーバが現在の割り当てに対してユーザに指定した Quota ID によって識別されます。請求サーバは HAAA とインターフェイスし、この情報を HAAA に提供します。

HAAA は受信したユーザの前払い情報を RADIUS Access-Accept メッセージに入れて、PDSN に送信します。RADIUS メッセージには次の情報が含まれます。

- 次のパラメータを含む PPAQ VSA
  - VolumeQuota パラメータで指定されたユーザ フローの初期化割り当て
  - 指定された割り当ての Quota ID
  - VolumeThreshold パラメータで指定された割り当てのしきい値
- 前払いサービスがボリュウムに基づくことを示す PPAC VSA

PDSN は AAA サーバから Access-Accept メッセージを受信すると、RADIUS パケットを解析して中のアトリビュートを取得します。PDSN はフローに指定された割り当てと割り当てられたフローに対応するしきい値に関するパケット内の情報を保存します。また、メッセージのユーザ フローに割り当てられた Quota ID も保存します。ユーザのフローが発生すると (SIP に IP アドレスが割り当てられるか、HA から MIP RRP を受信し、MS に送信)、PDSN は割り当てに基づいてフローを流れるユーザのトラフィックの測定を開始します。

**ステップ 3** 各前払いフローを流れるユーザ データ (IP データグラム) は、アップストリームとダウンストリームの両方向で計算されます。消費バイト数は、フローに指定された割り当てに基づいて請求サーバによってチェックされます。

**ステップ 4** 前払いフローの割り当てがボリュウムしきい値に達すると、PDSN は AAA サーバに Access-Request メッセージを送信して、ユーザの割り当てを更新します。この RADIUS パケットには、次のパラメータを含む PPAQ VSA が含まれています。

- "Threshold reached" (しきい値に達した) (= 3) ことを示すように設定される Update-Reason サブタイプ
- 以前受け取った Quota ID
- VolumeQuota Sub-Type に使用量

HAAA は RADIUS パケットを認証し、認証が成功した場合、パケットにある前払い関連情報を請求サーバに転送します。

**ステップ 5** 請求サーバは、ユーザが使用する割り当て量でデータベースをアップデートします。ユーザが割り当ての更新を示すと、請求サーバはユーザの前払い残量の一部を割り当てます。現在割り当てられている割り当ての新しい Quota ID とその割り当てに対応するしきい値も指定します。この情報は HAAA に渡されます。

HAAA は、請求サーバから受け取った情報を、RADIUS の Access-Accept メッセージに入れて PDSN に送信します。PPAQ VSA には次のアトリビュートがカプセル化されます。

- Quota ID
- VolumeQuota パラメータに、割り当てられた割り当て
- 指定された割り当てに対応するしきい値を含む VolumeThreshold パラメータ

PDSN は AAA サーバから Access-Accept メッセージを受信すると、RADIUS パケットを解析して中のアトリビュートを取得します。PDSN は、パケットに含まれる情報を保存し、フローに指定された割り当てと、割り当てられたフローに対応する現在のしきい値をアップデートします。現在の割り当ての新しい Quota-ID も保存します。

**ステップ 6** ユーザ データ (IP データグラム) は前払いフローにより引き続き流れ、アップストリームとダウンストリームの両方向で計算されます。消費バイト数は、フローに割り当てられた割り当てに基づいてチェックされます。

**ステップ 7** PDSN は、次の基準に基づいて、前払いフローを閉じることを決定します。

- 割り当てを更新する Access-Request メッセージが送信されたが、設定可能な時間が経過しても AAA サーバから Access-Accept メッセージを受信しなかった。この時間は、PDSN で設定されている RADIUS メッセージのタイムアウトと同じです。
- 割り当てを取得する Access-Accept が送信されたが、Access-Accept が受信可能になる前に、残りの VolumeQuota が消費された。これは、VolumeQuota 値と VolumeThreshold 値が同じ場合です。この場合、PDSN は次の情報を含む PPAQ VSA が入った Access-Request メッセージを送信します。
  - "Quota reached" (割り当てに達した) (= 4) ことを示す Update-Reason サブタイプ
  - ユーザが使用した割り当て量を含む VolumeQuota アトリビュート

このとき、PDSN は前払いフローを削除済みとしてマークし、その前払いフローではパケット交換を行いません。PDSN は前払いフローを即座に削除せず、Access-Request の応答または Access-Request メッセージのタイムアウトを待ちます。

**ステップ 8** ユーザが前払いフローに対して "Quota reached" (割り当てに達した) ことを示すと、請求サーバは新しい割り当てを行いません。請求サーバは前払いフローを終了し、それを HAAA に示します。HAAA は、PPAQ VSA 内に "Quota is reached" (割り当てに達した) という Update-Reason サブタイプをカプセル化して、前払いパケット データ セッションの終了を確認する Access-Accept メッセージを PDSN に送信します。

PDSN は Access-Accept メッセージの受信後、前払いセッションのユーザ フローを削除します。通常のアカウンティング手順の一環として、PDSN は、該当するリソースの解放時に、オフライン RADIUS Accounting-Stop メッセージを送信します (通常操作)。

## 時間ベースの前払いデータ サービス フロー

時間ベースの前払いサービスのアカウンティング メトリックは、セッションの時間 (秒) です。

**ステップ 1** 前払い対応 PDSN は、RADIUS Access-Request メッセージをホーム RADIUS サーバに送信するには SIP または MIP 設定が必要であると判断します。SIP セッションの場合、ユーザ認証はローカルではなく AAA サーバで行う必要があります。MIP ユーザの場合、認証には FA-CHAP が必要です。

PDSN は、HAAA または請求サーバにその PDSN が時間ベースの前払いをサポートすることを通知する PPAC VSA (値 = 2 または 3) を含めます。PDSN でリソース失効がイネーブルになっている場合、PDSN は、MIP セッションのリソース失効をサポートできることを示す SessionTerminationCapability (STC) アトリビュートを送信します。RADIUS Access-Request メッセージには、Event\_Time アトリビュート (G4、値 = 55) が含まれます。

ホーム RADIUS サーバはユーザから送信された Access-Request を通常の方法で認証および認可します。ユーザ プロファイルからユーザが前払い加入者であることが判明すると、HAAA は請求サーバとインターフェイスし、Access-Request メッセージで受信したユーザの前払い関連情報を請求サーバに提供します。

**ステップ 2** 請求サーバは、ユーザの前払い情報を受信すると、PDSN の機能をチェックします (PPAC VSA で送信)。請求サーバは、ユーザの残高とアカウント ステータスが有効であるかどうかもチェックします。請求サーバは、時間に基づく前払いパケット データ サービスをサポートすることを PDSN に通知します。さらに、ユーザに初期割り当てを行います。これは、通常ユーザが使用できる総割り当ての一部です。ユーザに指定された割り当ては、請求サーバが現在の割り当てに対してユーザに指定した Quota ID によって識別されます。請求サーバは HAAA とインターフェイスし、この情報を HAAA に提供します。

HAAA は受信したユーザの前払い情報を RADIUS Access-Accept メッセージに入れて、PDSN に送信します。RADIUS メッセージには次の情報が含まれます。

次のパラメータを含む PPAQ VSA

- DurationQuota パラメータで指定されたユーザ フローの初期化割り当て
- 指定された割り当ての Quota ID
- DurationThreshold パラメータで指定された割り当てのしきい値

前払いサービスがボリュームに基づくことを示す PPAC VSA。

時間ベースの前払いパケット データ サービスでは、請求サーバによる DurationQuota/DurationThreshold 割り当てには Event\_Time アトリビュートが使用されます。

PDSN は AAA サーバから Access-Accept メッセージを受信すると、RADIUS パケットを解析して中のアトリビュートを取得します。PDSN はフローに指定された割り当てと割り当てられたフローに対応するしきい値に関するパケット内の情報を保存します。また、割り当てに対応する Quota ID も保存します。

ユーザのフローが発生すると (SIP に IP アドレスを割り当て、または HA から MIP RRP を受信し MS に送信、など)、PDSN は時間しきい値と時間割り当て値に対応するタイマーを開始します。

タイマーが、前払いフローの割り当てのしきい値に達すると、PDSN は AAA サーバに Access-Request メッセージを送信して、前払いフローの割り当てを更新します。この Access-Request メッセージには、次のパラメータを含む PPAQ VSA が入っています。

- "Threshold reached" (しきい値に達した) (=3) ことを示すように設定される Update-Reason サブタイプ
- 以前受け取った Quota ID
- 使用時間を含む DurationQuota サブタイプ

HAAA は RADIUS パケットを認可し、認可が成功した場合、パケットにある前払い関連情報を請求サーバに転送します。

**ステップ 3** 請求サーバは、ユーザが使用した割り当て量でデータベースをアップデートします。ユーザが割り当ての更新を示すと、請求サーバはユーザの前払い残量の一部を割り当てます。現在割り当てられている割り当ての新しい Quota ID とその割り当てに対応するしきい値も指定します。この情報は HAAA に渡されます。

HAAA は、請求サーバから受け取った情報を、RADIUS の Access-Accept メッセージに入れて PDSN に送信します。PPAQ VSA には次のアトリビュートがカプセル化されます。

- Quota ID
- 指定された割り当てを含む DurationQuota パラメータ
- 指定された割り当てに対応するしきい値を含む DurationThreshold パラメータ

PDSN は AAA サーバから Access-Accept メッセージを受信すると、RADIUS パケットを解析して中のアトリビュートを取得します。PDSN は、パケットに含まれる情報を保存し、フローに指定された割り当てと、割り当てられたフローに対応する現在のしきい値で情報をアップデートします。PDSN は、Accept-Accept メッセージで受信した新しい値で時間割り当てタイマーを再開し、現在の割り当てに対応する新しいしきい値でしきい値タイマーを開始します。現在の割り当ての新しい Quota-ID も保存します。

**ステップ 4** PDSN は、次の基準に基づいて前払いフローを閉じます。

- 割り当てを更新する Access-Request メッセージが送信されたが、設定可能な時間が経過しても AAA サーバから Access-Accept メッセージを受信しなかった。この時間値は、PDSN で設定されている RADIUS メッセージのタイムアウトと同じです。

- 割り当てを取得する Access-Accept が送信されたが、Access-Accept が受信可能になる前に、残りの VolumeQuota が消費され、対応するタイマーが切れた。これは、DurationQuota 値と DurationThreshold 値が同じ場合です。

このイベントが発生した場合、PDSN は、次のパラメータを含む PPAQ VSA が入った Access-Request メッセージを送信します。

- "Quota reached" (割り当てに達した) (= 4) ことを示す Update-Reason サブタイプ
- ユーザが使用した割り当て量を含む DurationQuota アトリビュート

PDSN は前払いフローに削除のマークを付け、前払いフローからパケットを交換しません。PDSN は前払いフローを即座に削除せず、Access-Request の応答または Access-Request メッセージのタイムアウトを待ちます。

**ステップ 5** ユーザが前払いフローに対して "Quota reached" (割り当てに達した) ことを示すと、請求サーバは新しい割り当てを行いません。請求サーバは前払いフローを終了し、それを HAAA に示します。HAAA は、PPAQ VSA 内に "Quota is reached" (割り当てに達した) という Update-Reason サブタイプをカプセル化して、前払いパケット データ セッションの終了を確認する Access-Accept メッセージを PDSN に送信します。

PDSN は Access-Accept メッセージの受信後、前払いセッションのユーザ フローをクリアします。通常のオフライン アカウンティング手順の一環として、PDSN は、該当するリソースの解放時に、オフライン RADIUS Accounting-Stop メッセージを送信します。

## タリフ スイッチングによるボリュームベースの前払いデータ サービス

PDSN と請求サーバは、タリフ スイッチングによるボリュームベースの前払いパケット データ サービスをサポートします。タリフ スイッチ トリガは、請求サーバで制御されます。この機能をサポートするために、新しいサブタイプ PrepaidTariffSwitch (PTS) VSA アトリビュートが、HAAA から PDSN に送信されます。このアトリビュートには、次の主要サブタイプが含まれます。

- QuotaId : Quota Id は PPAQ のものと同じです。
- VolumeUsedAfterTariffSwitch (VUATS) : タリフ スイッチ後に交換されるボリューム
- TariffSwitchInterval (TSI) : 対応するオンライン RADIUS Access-Request メッセージに対応するタイプスタンプ (g4) と次のタリフ スイッチ条件の間隔 (秒)

次のシーケンスは、タリフ スイッチングがイネーブルになっている場合の前払いデータ サービスの機能を説明しています。

**ステップ 1** 前払い対応 PDSN は、RADIUS Access-Request メッセージをホーム RADIUS サーバに送信するには SIP または MIP 設定が必要であると判断します。SIP セッションの場合、ユーザの認証は、ローカルではなく AAA サーバで行う必要があります。MIP ユーザの場合、FA-CHAP による認証が必要です。

PDSN は、HAAA または請求サーバにその PDSN がボリューム ベースの前払いをサポートすることを通知する PPAC VSA (値 = 1 または 3) を含めます。PDSN でリソース失効がイネーブルになっている場合、PDSN は、MIP セッションのリソース失効をサポートできることを示す SessionTerminationCapability (STC) アトリビュートを送信します。

ホーム RADIUS サーバはユーザから送信された Access-Request を通常の方法で認証および認可します。ユーザ プロファイルからユーザが前払い加入者であることが判明すると、HAAA は請求サーバとインターフェイスし、Access-Request メッセージで受信したユーザの前払い関連情報を請求サーバに提供します。

**ステップ 2** 請求サーバは、ユーザの前払い情報を受信すると、PPAC VSA で送信された PDSN の機能をチェックします。請求サーバは、ユーザの残高とアカウント ステータスが有効かどうかともチェックします。請求サーバは、ボリュームに基づく前払いパッケージ データ サービスをサポートすることを PDSN に通知します。また、請求サーバは、ユーザに初期割り当てを指定します。これは、通常、ユーザが使用できる総割り当ての一部です。ユーザに指定された割り当ては、請求サーバがユーザに指定した Quota ID によって識別されます。請求サーバは HAAA とインターフェイスし、この情報を HAAA に提供します。

タリフ スイッチングをサポートする請求サーバは、次のタリフ スイッチ ポイントまでの残り秒数を示し、情報を HAAA サーバに伝えます。割り当てのしきい値に達していない場合は、PDSN が HAAA に Access-Request を送信するタリフ スイッチ ポイント後の時間を含めることもできます。

HAAA は請求サーバから受信したユーザの前払い情報を RADIUS Access-Accept メッセージに入れて、PDSN に送信します。RADIUS メッセージには次の情報が含まれます。

- 次のパラメータを含む PPAQ VSA
  - VolumeQuota パラメータで指定されたユーザ フローの初期化割り当て
  - 指定された割り当ての Quota ID
  - VolumeThreshold パラメータで指定された割り当てのしきい値
- 次のパラメータを含む PTS VSA
  - QuotaID を含む PPAQ VSA アトリビュート
  - タリフ スイッチの条件がトリガされるまでの残り秒数を示す TariffSwitchInterval
  - しきい値ポイントに達していない場合、PDSN がオンラインの Access-Request を送信するタリフ スイッチ ポイント後の時間を示す TimeIntervalafterTariffSwitchUpdate
- 前払いサービスがボリュームに基づくことを示す PPAC VSA。

PDSN は AAA サーバから Access-Accept メッセージを受信すると、RADIUS パケットを解析して中のアトリビュートを取得します。PDSN はフローに指定された割り当てと割り当てられたフローに対応するしきい値に関するパケット内の情報を保存します。また、メッセージに存在するユーザ フローで割り当てられた Quota ID も保存します。

ユーザのフローが発生すると（SIP に IP アドレスが割り当てられるか、HA から MIP RRP を受信し、MS に送信）、PDSN は割り当てに基づいてフローを流れるユーザのトラフィックの測定を開始します。また、TariffSwitchInterval アトリビュートで受信した値に対応するタイマーを開始して、タリフ スイッチ条件がヒットした場合に認識できるようにします。PDSN は、Access-Request と Tariff Switch Interval のタイムスタンプが Access-Accept メッセージのタイムスタンプより大きい場合だけタイマーを開始します。

PTS アトリビュートの QuotaId は、PPAQ 内の QuotaId と同じである必要があります。2 つの値が異なると、前払いフローは PDSN によって閉じます。

**ステップ 3** 各前払いフローを流れるユーザ データ（IP データグラム）は、アップストリームとダウンストリームの両方向で計算されます。消費バイト数は、フローに指定された割り当てに基づいて請求サーバによってチェックされます。

**ステップ 4** 前払いフローの割り当てが VolumeThreshold 値に達すると、PDSN は AAA サーバに Access-Request メッセージを送信して、ユーザの割り当てを更新します。この RADIUS パケットには、次のパラメータを含む PPAQ VSA が含まれています。

- "Threshold reached"（しきい値に達した）(= 3) ことを示すように設定される Update-Reason Sub-Type
- 以前受け取った Quota ID
- VolumeQuota Sub-Type に使用量

HAAA は RADIUS パケットを認可し、認可が成功した場合、パケットにある前払い関連情報を請求サーバに転送します。

**ステップ 5** 請求サーバは、ユーザが使用した割り当て量でデータベースをアップデートします。ユーザが割り当ての更新を示すと、請求サーバはユーザの前払い残量の一部を割り当てます。現在割り当てられている割り当ての新しい Quota ID とその割り当てに対応するしきい値も指定します。この情報は HAAA に渡されます。

また、請求サーバは HAAA に、次のタリフ スイッチ トリガ ポイントまでの残り秒数を示します。

HAAA は、請求サーバから受け取った情報を、RADIUS の Access-Accept メッセージに入れて PDSN に送信します。PPAQ VSA には次のアトリビュートがカプセル化されます。

- Quota ID
- VolumeQuota パラメータに、割り当てられた割り当て
- VolumeThreshold パラメータに、割り当てられたクォータに対応するしきい値

PTS アトリビュート内部には次のアトリビュートがカプセル化されます。

- QuotaID。PPAQ アトリビュートと同じ
- タリフ スイッチの条件がトリガされるまでの残り時間 (秒) を示す TariffSwitchInterval
- しきい値ポイントに達していない場合に、PDSN がオンラインの Access-Request を送信するときに、タリフ スイッチ ポイント後の期間を示す TimeIntervalafterTariffSwitchUpdate

PDSN は AAA サーバから Access-Accept メッセージを受信すると、RADIUS パケットを解析して中のアトリビュートを取得します。パケット内の情報を保存し、フローに割り当てられた割り当てと、割り当てられたフローに対応する現在のしきい値でアップデートします。現在の割り当ての新しい Quota-ID も保存します。

また、PDSN は、TariffSwitchInterval アトリビュートで示されたタイマーを再起動します。この時間は、次のタリフ スイッチ条件がヒットするまでの残り秒数を示します。

**ステップ 6** ユーザ データ (IP データグラム) は前払いフローにより引き続き流れ、アップストリームとダウンストリームの両方向で計算されます。消費バイト数は、フローに割り当てられた割り当てに基づいてチェックされます。

**ステップ 7** タリフ スイッチ間隔のタイマーが切れ、フローのタリフ スイッチ ポイントにヒットしたことを示します。PDSN は、アップストリームおよびダウンストリーム方向のセッションを通るオクテットの総数と、タリフ スイッチ トリガ ポイント後に PDSN によって切り替えられたバイト数をカウントし続けます。TimeIntervalafterTariffSwitchUpdate が AAA サーバから送信された場合、PDSN は、タリフ スイッチ ポイント到達後は、この値でタイマーを開始します。

**ステップ 8** 各前払いフローを流れるユーザ データ (IP データグラム) は、次のしきい値に他するまで、アップストリームとダウンストリームの両方向で計算されます。PDSN は、最後の割り当てアップデートまで切り替えられた総バイト数と、タリフ スイッチ トリガ ポイントヒット後に PDSN によって切り替えられた総バイト数をカウントします。消費バイト数は、フローに割り当てられた割り当てに基づいてチェックされます。

**ステップ 9** VolumeThreshold 値が、フローの VolumeQuota 値で割り当てられた割り当てに達するか、TimeIntervalafterTariffSwitchUpdate に対応するタイマーが切れると、PDSN は、AAA サーバと請求サーバへの Access-Request メッセージで割り当てアップデート情報を送信します。このオンラインの RADIUS Access-Request メッセージには、PPAQ VSA の次のアトリビュートが含まれます。

- しきい値に達した場合、"Threshold reached" (しきい値に達した) (= 3) ことを示すように設定された Update-Reason Sub-Type。しきい値に達せず、TimeIntervalafterTariffSwitchUpdate が切れた場合は、"Tariff Switch Update" (タリフ スイッチのアップデート) (= 9) を示すように設定されます。
- 以前受け取った Quota ID。

- VolumeQuota Sub-Type に利用量。
- PTS アトリビュートには次のサブタイプが含まれます。
- 以前受け取った Quota ID。
  - VolumeUsedAfterTariffSwitch (VUATS) アトリビュート。タリフ スイッチ トリガ ポイント後に PDSN によって切り替えられた総オクテット数が含まれます。

HAAA は RADIUS パケットを認可し、認可が成功した場合、パケットにある前払い関連情報を請求サーバに転送します。

請求サーバは、ユーザが使用した割り当て量でデータベースをアップデートします。ユーザが割り当ての更新を示すと、請求サーバはユーザの前払い残量の一部を割り当てます。現在割り当てられている割り当ての新しい Quota ID とその割り当てに対応するしきい値も指定します。この情報は HAAA に渡されます。

また、請求サーバは HAAA に、次のタリフ スイッチ トリガ ポイントまでの残り秒数を示します。

HAAA は、請求サーバから受け取った情報を、RADIUS の Access-Accept メッセージに入れて PDSN に送信します。PPAQ VSA には次のアトリビュートがカプセル化されます。

- 現在の割り当ての新しい Quota ID
- VolumeQuota パラメータに、割り当てられた割り当て
- VolumeThreshold パラメータに、割り当てられたクォータに対応するしきい値

PTS アトリビュートには次のサブタイプが含まれます。

- 以前受け取った Quota ID
- タリフ スイッチの条件がトリガされるまでの残り時間（秒）を示す TariffSwitchInterval
- オプションで、しきい値ポイントに達していない場合に、PDSN がオンラインの Access-Request を送信するときに、タリフ スイッチ ポイント後の期間を示す TimeIntervalafterTariffSwitchUpdate

PDSN は AAA サーバから Access-Accept メッセージを受信すると、RADIUS パケットを解析して中のアトリビュートを取得します。PDSN は、パケットに含まれる情報を保存し、フローに割り当てられた割り当てと、割り当てられたフローに対応する現在のしきい値で情報をアップデートします。現在の割り当ての新しい Quota-ID も保存します。

また、PDSN は、TariffSwitchInterval アトリビュートで示されたタイマーを再起動します。PDSN は、Access-Request と Tariff Switch Interval のタイムスタンプが Access-Accept メッセージのタイムスタンプより大きい場合だけタイマーを起動します。この時間は、次のタリフ スイッチ条件がヒットするまでの残り秒数を示します。

## Acct-Stop および暫定レコードでの G17 アトリビュートのサポート

G17 アトリビュートは、ユーザが登録解除した時間ではなく最後のアクティビティが検出された時間に基づいてユーザに請求するために必要です。次のシナリオでは、アトリビュートの使用方法および AAA サーバが最後のユーザ アクティビティを識別する方法について簡単に説明します。

G17 は、ユーザによって最後のアクティビティが検出された時間を示す最後のユーザ アクティビティとして定義されます。G17 アトリビュートは、acct-stop および暫定アカウントリング アップデート メッセージで送信されます。次の使用ガイドラインがあります。

- G17 アトリビュートのサポートは、`cdma pdsn attribute send g17` コマンドを発行して設定します。
- アトリビュートは、`acct-start` レコードには含まれず、`accounting stop/interim-update` だけに含まれます。

- アトリビュートは、`airlink start` レコードが到着すると 0 に設定されます。
- アトリビュートは、`airlink active stop` が到着すると現在の時間に設定されます。
- アトリビュートは、`acct-stop` レコードが送信されると 0 に設定されます。

G17 アトリビュートは、次の場合に便利です。

- `cdma pdsn accounting send start-stop` コマンドが設定されていない場合。
  - セッションは休止します。G17 は現在の時間で記録されます。上記 CLI コマンドが設定されていないので、アカウントリング停止は生成されません。
  - PDSN は、このセッションの暫定アップデート アカウントリング レコードを送信し続けます。これらのメッセージには、`airlink-stop` の受信時刻を記録した値が設定された G17 が含まれます。
  - モバイルが最終的に登録を解除し、`lft = 0` で、`airlink stop` なしの A11 RRQ を受信すると、PDSN は、`airlink-stop` の受信時に記録されていた G17 アトリビュートの入ったアカウントリング停止を送信します。これで、最後のユーザ アクティビティが検出された時間の真の値が得られます。
- `cdma pdsn accounting send start-stop` コマンドが設定されてる場合。
  - PDSN は、PCF から `airlink-stop` を受信したときにアカウントリング停止を生成します。この `acct-stop` には、`airlink-stop` の受信時刻が記録された G17 が含まれます。
  - `acct-stop` が送信されると、G17 はリセットされます。最終的にセッションが終了すると、アカウントリング停止には値が 0 の G17 が含まれます。
  - AAA サーバは、G17 の前の値を使用して、最後のユーザ アクティビティを検出する必要があります。

## AAA サーバからダウンロードされたホーム エリア、最大認可集約帯域幅、およびユーザ間優先順位アトリビュート

ホーム エリア、ユーザ間優先順位、および最大認可集約帯域幅アトリビュートは PDSN によって受信され、加入者 QoS プロファイル (NVSE) 構造の一部として PCF に転送されます。これらのアトリビュートのローカル コンフィギュレーションは、Cisco PDSN リリース 3.5 ではサポートされていません。

加入者 QoS プロファイルは、PDSN からの次のメッセージで PCF に渡されます。

- セッションが新しく作成された場合は A11 セッション アップデート
- PCF 間ハンドオフ中は A11 Registration Reply

これらのアトリビュートはすべて、セッションの冗長性でスタンバイに同期されます。

### 基本動作

- ホームエリア、ユーザ間優先順位、または最大認可集約帯域幅アトリビュートが AAA サーバからダウンロードされ、解析に成功した場合、これらは PDSN で保存され、加入者 QoS プロファイル構造の一部として PCF に転送されます。
- ホーム エリア アトリビュートは、`cdma pdsn pcf PCF IP_address [ending IP_address] vendor-id NVSE vendor_ID` コマンドが設定されている場合だけ PCF に送信されます。
- 加入者 QoS プロファイルに追加されるベンダー固有アトリビュートはコンフィギュレーションに基づきます。
- 加入者 QoS プロファイルは、A11 RRP または A11 セッション アップデート メッセージのどちらかで PCF に送信されます。



- 最大認可集約帯域幅アトリビュートがダウンロードされた場合、このアトリビュートに基づくセッションの帯域幅ポリシングが PDSN で適用されます。
- ユーザセッションの作成時、これらのアトリビュートが A11 セッション アップデート メッセージを介して PCF に送信されます。
- PCF 間ハンドオフの場合、これらのアトリビュートは、A11 セッション アップデート メッセージまたは A11 RRP メッセージのどちらかで送信されます。
- 加入者 QoS プロファイルを含む A11 メッセージは、**cdma pdsn a11 session-update qos** コマンドが設定されている場合だけ、PDSN から PCF に送信されます。
- 最大認可集約帯域幅に基づく帯域幅ポリシングは、**cdma pdsn a10 police downstream** コマンドが設定されている場合だけ適用されます。
- 受信した AAA サーバアトリビュートの長さが無効の場合、Access-Accept は破棄され、PDSN でのセッションの作成は失敗します。
- PDSN で受信したアトリビュート値が指定の範囲外の場合、アトリビュートは無視されます。
- 未知のアトリビュートを受信した場合、アトリビュートは無視されます。
- 同じアトリビュートの複数のインスタンスがダウンロードされた場合、ダウンロードされたアトリビュートの最大値が採用されます。
- 加入者 QoS プロファイルのローカル コンフィギュレーションは、Cisco PDSN リリース 3.5 ではサポートされていません。
- Access-Accept で特定のアトリビュートの新規または複数の値を受信すると、PDSN 上の値は次のようにアップデートされます。
  - 最後のフローでダウンロードされたホーム エリア アトリビュートが維持されます。
  - 最大認可集約帯域幅とユーザ間優先順位アトリビュートの最大値が維持されます。
- PPP 再ネゴシエーションの場合、セッションで維持されたアトリビュートの値がリセットされ、Access-Accept で受信した値が適用されます。
- ダウンロードされた帯域幅を超えるトラフィックまたは違反するトラフィックは、セッションでは考慮されません。

## 加入者 QoS プロファイル

加入者 QoS プロファイルは、AAA サーバからダウンロードされた次のアトリビュートで構成されます。

- 最大認可集約帯域幅
- Lucent で定義されたホーム エリア
- ユーザ間優先順位

これらのアトリビュートは PDSN に保存され、加入者 QoS プロファイルの一部として PCF に転送されます。A11 レジストレーション応答または A11 セッション アップデートが加入者 QoS プロファイルを PCF に伝えます。

A11 メッセージで PCF に送られる加入者 QoS プロファイルは、アトリビュートを RADIUS VSA とした NVSE として送信されます。

## 帯域幅のポリシング

AAA サーバでのモバイルの認証中、最大認可集約帯域幅アトリビュートが、AAA サーバから Access-Accept の一部としてダウンロードされることがあります。このアトリビュートがダウンロードされると、PDSN はポリシーを内部で作成し、セッションと関連付けます。モバイルへのトラフィックは、ダウンロードされた値に基づいてポリシングされます。セッションがダウンすると、ポリシーも削除されます。

## セッションの冗長性

ダウンロードされたアトリビュートは常に、フローが作成されるたびに、またはハンドオフ中に、既存のセッション冗長性インフラストラクチャを使用してスタンバイ PDSN と同期されます。

スイッチオーバーが発生すると、パケットで新しいトークンが割り当てられるため、新しいアクティブボックスでポリシングが開始します。

## PCF に対する加入者 QoS プロファイルの設定

PDSN で、セッション アップデートを使用して PCF に加入者 QoS プロファイルを送信できるようにするには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>router(config)# cdma pdsn all session-update qos</code>	セッション アップデートを使用して加入者 QoS プロファイルを送信できます。このコマンドには、既存のタイムアウトおよび再送信 all セッション アップデート コンフィギュレーションが適用されます。

## 帯域幅ポリシングの設定

セッションのダウンストリーム データ トラフィックのポリシングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>router(config)# [no] cdma pdsn a10 police downstream</code>	セッションのダウンストリーム データ トラフィックをポリシングできます。このコマンドは、AAA サーバからダウンロードされた最大認可集約帯域幅値に基づいて設定されます。

## 加入者 QoS プロファイルでの VSA の設定

加入者 QoS プロファイルでのベンダー固有アトリビュートの送信を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	<code>router(config)# cdma pdsn pcf PCF_IP_address ending IP_address vendor-id NVSE Vendor_id</code>	<p>A11 セッション アップデートおよび A11 RRP から加入者 QoS プロファイルを送信できます。</p> <ul style="list-style-type: none"> <li>• <i>PCF_IP_address</i> : 単一または開始 PCF IP アドレス</li> <li>• <i>Ending PCF_IP_address</i> : 終了 PCF IP アドレス</li> <li>• <i>NVSE Vendor_Id</i> : PCF の Radius ベンダー ID</li> </ul>



(注) このコンフィギュレーションは、3gpp または 3gpp2 アトリビュートには必要ありません。

設定例を示します。

```
cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 65535
cdma pdsn a10 ahdhc engine 0 usable-channels 8000
cdma pdsn a10 police downstream
cdma pdsn all session-update qos
cdma pdsn pcf 10.1.1.1 10.1.1.50 vendor-id 3729
cdma pdsn timeout mobile-ip-registration 10
cdma pdsn timeout all-session-update 3
cdma pdsn send-agent-adv
cdma pdsn debug show-conditions
cdma pdsn secure pcf 150.1.4.1 spi 100 key ascii cisco
cdma pdsn secure pcf 150.1.4.10 150.1.4.18 spi 100 key ascii cisco
cdma pdsn secure pcf 150.1.4.25 spi 100 key ascii cisco
cdma pdsn secure pcf 150.1.4.123 spi 100 key ascii cisco
cdma pdsn secure pcf 150.1.4.223 spi 100 key ascii cisco
cdma pdsn secure pcf 150.1.4.224 spi 100 key ascii cisco
cdma pdsn compliance is835a handoff
```

## 設定の確認

これらの各種アトリビュートが送信されたことを確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	router# <b>show cdma pdsn</b>	PDSN のステータスと現在のコンフィギュレーションを表示します。
ステップ 2	router# <b>show cdma pdsn session</b>	PDSN のセッション情報を表示します。
ステップ 3	router# <b>show cdma pdsn statistics</b>	PDSN の VPDN、PPP、RP インターフェイス、Closed-RP インターフェイスおよびエラー統計情報を表示します。

次に例を示します。

```
router# show cdma pdsn
PDSN software version 3.5, service is enabled

All registration-update timeout 1 sec, retransmissions 5
Mobile IP registration timeout 10 sec
A10 maximum lifetime allowed 65535 sec
GRE sequencing is on
Maximum PCF's limit set to 2000
Maximum sessions limit not set (default 974 maximum)
SNMP failure history table size 100
MSID Authentication is disabled
Ingress address filtering is disabled
Sending Agent Adv in case of IPCP Address Negotiation is enabled
Allow CI_ADD option during IPCP Phase is disabled
Aging of idle users disabled
Radius Disconnect Capability enabled

Number of pcfs connected 0,
Number of pcfs 3GPP2-RP 0,
```

```

Number of sessions connected 0,
Number of sessions 3GPP2-RP 0,
Number of sessions Active 0, Dormant 0,
Number of sessions using HDLCoGRE 0, using PPPoGRE 0

router# show cdma pdsn session
Mobile Station ID IMSI 123456789123457
PCF IP Address 5.1.1.46, PCF Session ID 1
A10 connection time 119:19:10, registration lifetime 1800 sec
Number of successful A11 reregistrations 357
Remaining session lifetime 650 sec
Always-On not enabled for the user
Current Access network ID 0005-0101-2E
Last airlink record received is Unknown, airlink is active
GRE protocol type is 0x8881
GRE sequence number transmit 9, receive 7
Using interface Virtual-Access2.1, status OPN
Using AHDLC engine on slot 0, channel ID 4381
Service Option Ev-DO
Police Downstream CIR(bps) 8000,
  Normal Burst(bytes) 1500, Excess Burst(bytes) 3000
  Packets Conformed 0 Exceeded 0 Dropped packets 0
This session has 1 flow
Session Airlink State Active
QoS Parameters:
  Max Aggregate Bandwidth: 8000
  Home Area           : 10
  Inter User Priority  : 15

Flow service Simple, NAI NAI gSIP1@xxx.com
Mobile Node IP address 32.1.35.203
Packets in 0, bytes in 0
Packets out 0, bytes out

router# show cdma pdsn statistics
Bandwidth policing:
  Policing installed 0 failure 0 uninstalled 0

```

## 1 秒あたりのモバイル IP コール処理の改善

以前の Cisco PDSN リリースでは、MIP CPS レートは約 40 でした。これは SIP CPS の 125 と比較すると低速です。MIP CPS が低速だった理由として、MIP のコンフィギュレーションがインターフェイス固有だった点が挙げられます。これらのコンフィギュレーションが **virtual-template** インターフェイス（PDSN ソフトウェアでは一般的）に適用されると、MIP コンフィギュレーションの存在により、**virtual-template** からの **virtual-access** のクローニングにかなりの時間を要し、これが直接 MIP サービスの CPS に影響します。**virtual-access** は、コールの設定時にクローニングされます。**virtual-access** のクローニング時間を短縮するために、Cisco PDSN リリース 2.1 は、グローバル コンフィギュレーション モードで一般的に使用される **per-interface** コンフィギュレーションをサポートし、下位互換性のために **per-interface** をサポートします。

## always-on 機能

PDSN は、ローカル ネットワークで加入者のパケット データ セッションを維持する **always-on** サービスをサポートします。**always-on** のサポートにより、PDSN は、ユーザが接続不能であると判断しない限り、PPP アイドル タイマー切れによって加入者のパケット データ セッションを解放することはありません。

always-on サービスは、ユーザの PPP 非アクティビティ タイマー値に関係なく、加入者のパケット データ セッションを維持します。同時に、限定的な PPP 非アクティビティ タイマー値を利用することで、ユーザが接続可能な場合だけセッションを維持する方法を提供できます。PDSN は、LCP エコー (RFC 1661 と IS835B に従い) を使用して、ユーザが接続可能かどうかを判断します。

always-on サービスは、F15 "Always On" アトリビュートを受信し、AAA サーバからの Access-Accept メッセージで値が 1 に設定された場合だけユーザに対してイネーブルになります。

PDSN は、Echo-Reply-Timeout タイマーおよび Echo-Request-Attempts カウンタを設定する機能をサポートします。PDSN 側で、always-on 機能そのものをイネーブルにするために必要な追加設定は必要ありませんが、Echo-Request-Attempts をゼロに設定して、機能をディセーブルにすることができます。PPP 非アクティビティ タイマーは、AAA サーバ から設定または取得されている場合、IPCP オープン状態に入ったセッションでユーザに対して起動されます。

always-on ユーザの場合：

1. 非アクティビティ タイマーが切れると、Echo-Request-Attempts カウンタが設定された値に初期化されます。
2. Echo-Request-Attempts カウンタがゼロの場合、PPP セッションは切断されます。Echo-Request-Attempts カウンタがゼロ以外の場合は、LCP Echo-Request メッセージが送信され、Echo-Request-Attempts カウンタが減らされ、Echo-Reply-Timeout タイマーが起動します。
3. 対応する LCP Echo-Reply メッセージを受信すると、Echo-Reply-Timeout タイマーが停止し、PPP 非アクティビティ タイマーが再起動されます。
4. Echo-Reply-Timeout タイマーが切れると、上記 2 と 3 を含むステップが繰り返されます。

この機能は、VPDN ユーザにはサポートされていません。また MIP ユーザにも適用されません。

always-on ユーザの場合、アカウンティング開始または停止、または暫定レコードで F15 アトリビュートに値として 1 が送信されます。always-on 以外のユーザの場合、F15 アトリビュートが設定されている場合だけアカウンティング レコードで送信されます。

#### always-on 機能の制約事項：

- always-on の実装は IS835B 標準に従います。IS835C 固有の追加は、PDSN のこのリリースでは使用できません。
- Echo-Reply は、always-on タイマーを停止する唯一のパケットです。  
基本的に、アップストリームまたはダウンストリームのデータを受信しても、設定された再試行回数および設定された間隔内で echo-reply が受信されないと、セッションが切断されることを意味します。
- always-on 機能は、モバイル IP ユーザには適用されません。
- always-on 機能は、VPDN ユーザには適用されません。
- 休止 PPP セッションのエージング機能は、always-on ユーザとは独立して動作します。休止 PPP セッションのエージング機能は、セッションの always-on プロパティを考慮しません。

## PDSN MIB の機能強化

Cisco PDSN 4.0 ソフトウェア リリースの一環として、次の新しいオブジェクトが作成されています。

#### SystemInfo : PDSN 上のグローバル レベル

- PolicingEnabled : ポリシングがイネーブルかどうかを示すブール値。
- SessionsWithAuxiliaryConnectionsTotal : 補助接続のセッション数。

- TotalBandwidth : CLI コマンドを通して設定されるボックスの合計帯域幅。
- AvailableBandwidth : 新しいセッションに使用できる残り帯域幅。
- ccpCdmaExtAllocatedBandwidth : 割り当てられた帯域幅を指定します。
- SessionMaxAuxConnectionsAllowed : PDSN がセッションごとにサポートする補助接続数。
- SessionServiceFlowsTotal : 現在 PDSN と確立している A10 サービス フロー数。
- AuxSessionTotal : 現在 PDSN と確立している補助セッションによるセッション数。
- PolicingSessionTotal : 現在 PDSN と確立している、ポリシングがイネーブルのセッション数。
- PDSNIpAddress : PDSN を識別する IPv4 アドレス。このオブジェクトには通知からのみアクセスできます。
- DSCPSession : 現在 PDSN と確立している、DSCP がイネーブルのセッション数。
- ccpCdmaExtLoadHighReachedNotifEnabled : トラップがイネーブルかどうかを示します。
- SessionAuxConnectionsEnabled : PDSN システムがセッションに補助 A10 接続をサポートするかどうかを示すブール値。

### Pcf ベースのテーブル

- SessionsWithAuxiliaryConnectionsTotal : PCF と関連付けられた補助接続によるセッションの数
  - NewAuxConnections : PDSN で各 PCF が受信した、新しい補助 A10 接続を確立する A11 レジストレーション メッセージの数
  - ccpCdmaExtPcfSoRpRegStatsBwUnavailableSess :
  - ReRegNewAuxConnections : PDSN で各 PCF が受信した、新しい補助 A10 接続を確立する A11 再レジストレーション メッセージの数
  - RemapFlows : PDSN で各 PCF が受信した、セッションの A10 接続からフロー ID へのマッピングの変更を示す A11 レジストレーションまたは再レジストレーション メッセージの数
  - CloseAuxConnections : PDSN で各 PCF が受信した、A10 接続の削除 (セッションに存在する A10 補助接続の損失) を示す A11 再レジストレーション メッセージの数
  - SessionUpdSubscriberQos : PDSN で各 PCF が受信した A11 セッションアップデート メッセージの数
  - RegReqMaxServiceFlows : セッションあたりの補助接続の最大数に達したために各 PCF で拒否された A11 の数
  - RegReqUnSupportedSO : 追加セッション NVSE がサポートされていないサービス オプションを含んでいたために各 PCF で拒否された A11 の数
  - RegReqNonExistA10 : IP フロー マッピングが存在しない A10 へのマッピングを含んでいたために各 PCF で拒否された A11 の数
  - ccpCdmaExtPDSNIpAddressType : 呼び出しによるアクセス
  - ccpCdmaExtPDSNIpAddress : 呼び出しによるアクセス
  - ccpCdmaExtNotifReason : 呼び出しによるアクセス
  - ccpCdmaExtNotifReasonCurrentValue : 呼び出しによるアクセス
- 次にこれらのオブジェクトの例を示します。

```
Due to CPU Low Reason:
=====
```

```
Received SNMPv2c Trap:
Community: public
```

```

From: 9.11.51.83
sysUpTime.0 = 20545
snmpTrapOID.0 = ciscoCdmaExtLoadLowReachedNotif
ccpCdmaExtPDSNIpAddrType.0 = ipv4(1)
ccpCdmaExtPDSNIpAddress.0 = 03 04 53 67
ccpCdmaExtNotifReason.0 = cputhreshold(2)
ccpCdmaExtNotifReasonCurrentValue.0 = 27

```

### 帯域幅ポリシー

- `ccpCdmaExtBandwidthPolicyInstallSuccesses` : セッションにインストールされた帯域幅
- `ccpCdmaExtBandwidthPolicyInstallFailures` : セッションへのインストールに失敗した帯域幅
- `ccpCdmaExtBandwidthPolicyRemoves` : セッションのクリアによるセッションからの帯域幅の削除

### RPErrors

- `BandwidthUnavailable` : 帯域幅が利用できないために拒否された A11 の数
- `RegReqMaxServiceFlows` : セッションあたりの補助接続の最大数に達したために拒否された A11 の数
- `RegReqUnsupportedSO` : 追加セッション NVSE がサポートされていないサービス オプションを含んでいたために拒否された A11 の数
- `RegReqNonExistA10` : IP フロー マッピングが存在しない A10 へのマッピングを含んでいたために拒否された A11 の数

### RPSessUpdates

- `SessionUpdSubscriberQos` : PDSN から PCF に送信された A11 セッションアップデート メッセージの数

### RSVPStats

- `TFTCreationSuccesses` : 正常に作成された TFT の数
- `TFTCreationFailure` : 作成に失敗した TFT の数
- `TFTPacketFilterAddFailure` : 要求された TFT に追加されなかったパケット フィルタの数
- `TFTPacketFilterUnavailable` : 要求された TFT で利用できなかったパケット フィルタの数
- `TFTPacketFilterReplace` : 既存の TFT 上で置き換えられるパケット フィルタの数
- `TFTPacketFilterAddBeforeCreation` : 永続 TFT に追加されるパケット フィルタの数
- `TFTUnableToParse` : PDSN 上で解析できない TFT の数
- `TFTUnauthorized` : PDSN で受信された非認可 TFT の数。
- `TFTPrecedenceContention` : パケット フィルタ評価優先順位値で競合が存在する TFT の数
- `TFTTreatmentUnsupported` : PDSN でサポートされていない MS フロー処理値を受信された TFT の数
- `TFTMaxPacketFiltersReached` : パケット フィルタの最大許容数に達した TFT の数

### QOSStats

- `QOSSuccess` : セッションに正常に適用された QoS プロファイルの数
- `QOSFailure` : セッションへの適用に失敗した QoS プロファイルの数
- `QOSDscpRemarkd` : PDSN でリマークされたパケットの数

### RpStats

- NewAuxConnections : PDSN で受信された、新しい補助 A10 接続を確立する A11 レジストレーション メッセージの数
- ReRegNewAuxConnections : PDSN で受信された、補助 A10 接続を確立する A11 再レジストレーション メッセージの数
- RemapFlows : PDSN で受信された、セッションの A10 接続からフロー ID へのマッピングの変更を示す A11 レジストレーションまたは再レジストレーション メッセージの数
- CloseAuxConnections : PDSN で受信された、A10 接続の削除（セッションに存在する A10 補助接続の損失）を示す A11 再レジストレーション メッセージの数
- SessionUpdSubscriberQos : PDSN で受信された A11 セッション アップデート メッセージの数

### CAC

コール アドミッション制御の一部として、次の NotificationObject が導入されました。

- LoadThresholdHighReached : PDSN は最大負荷に達しました。
- LoadThresholdLowReached : PDSN は最小負荷に達しました。

### Cisco PDSN リリース 3.0 の PPP カウンタ

次の既存 MIB サブグループにオブジェクトが追加されました。

- cCdmaPppSetupStats
- cCdmaPppReNegoStats
- cCdmaPppAuthStats
- cCdmaPppReleaseStats
- cCdmaPppMiscStats

表 23 に、Cisco PDSN リリース 3.0 で追加された PPP カウンタのリストを示します。

表 23 Cisco PDSN リリース 3.0 の PPP カウンタ

CDMA PPP MIB サブグループ	カウンタの説明
cCdmaPppSetupStats	
PPP stats - LCP Failure - option issue	LCP オプション ネゴシエーションの障害により失敗した PPP コールの合計数。
PPP stats - IPCP failure option-issue	IPCP オプション ネゴシエーションの障害により失敗した PPP コールの合計数。
PPP stats - Authentication aborted	認証の再試行の最大数に達したために失敗した PPP コールの合計数。
Session Disc - no remote-ip address:	MN が PDSN によって割り当てられた IP アドレスを拒否したために解放されたセッションの合計数。
PPP stats - Lower layer disconnected:	RP レイヤによって解放されたコールの合計数。
PPP stats - TermReq-From-MN-IPCP:	IPCP 中に MS から受信した LCP Term-Req。
PPP stats - TermReq-From-PDSN-IPCP:	IPCP 中に PDSN から送信された LCP Term-Req。
PPP stats - TermReq-From-PDSN-Auth:	認証中に PDSN から送信された LCP Term-Req。



表 23 Cisco PDSN リリース 3.0 の PPP カウンタ (続き)

CDMA PPP MIB サブグループ	カウンタの説明
PPP stats - TermReq-From-MN-Auth:	認証中に MS から受信した LCP Term-Req。
PPP stats - TermReq-From-PDSN-LCP:	LCP 中に PDSN から送信された LCP Term-Req。
PPP stats - TermReq-From-MN-LCP:	LCP 中に MS から受信した LCP Term-Req。
PPP stats - A10Release-PCF-preLCP:	LCP ステージの前に PCF によって解放された A10。
PPP stats - A10Release-PDSN-preLCP:	LCP ステージの前に PDSN によって解放された A10。
PPP stats - A10Release-PCF-LCP:	LCP ステージ中に LCP Term-Req なしで PCF によって解放された A10。
PPP stats - A10Release-PDSN-LCP:	LCP ステージ中に LCP Term-Req なしで PDSN によって解放された A10。
PPP stats - A10Release-PCF-Auth:	L 認証中に CP Term-Req なしで PCF によって解放された A10。
PPP stats - A10Release-PDSN-Auth	LCP Term-Req なしの認証中に PDSN によって解放された A10。
PPP stats - A10Release-PCF-IPCP:	IPCP ステージ中に LCP Term-Req なしで PCF によって解放された A10。
PPP stats - A10Release-PDSN-IPCP:	IPCP ステージ中に LCP Term-Req なしで PDSN によって解放された A10。
PPP stats - LCP - success:	LCP を正常に終了した PPP 接続。
PPP stats - auth - success:	AUTH を正常に終了した PPP 接続。
PPP stats - IPCP - success:	IPCP を正常に終了した PPP 接続。
cCdmaPppReNegoStats	
Session Reneg - Lower layer handoff:	ハンドオフ中の PANID/CANID 比較により再ネゴシエーションされたセッションの合計数。
cCdmaPppAuthStats	
Session Authen- CHAP auth timeout:	MN は CHAP 要求に応答しません。
Session Authen- PAP auth timeout:	PDSN は MN から PAP 要求を受信しません。
Session Authen- MSCHAP auth timeout:	MN は MSCHAP 要求に応答しません。
Session Authen- sessions skipped PPP Auth:	PPP 認証を省略したセッションの合計数。
cCdmaPppReleaseStats	
PPP stats - release - pcf deregister:	PCF がレジストレーション解除を送信したために解放された PPP 接続。
PPP stats - release - lifetime expiry:	ライフ タイマーの期限切れにより解放された PPP 接続。
cCdmaPppMiscStats	
Session Data Compress - CCP negotiation failures:	CCP ネゴシエーションに失敗したセッションの合計数。
LCP Echo Stats - total LCP Echo Req.sent:	LCP Echo Request の総転送数。
LCP Echo Stats - LCP Echo Req.resent:	LCP Echo Request の総再転送数。
LCP Echo Stats - LCP Echo Reply received:	LCP Echo Reply の総受信数。

表 23 Cisco PDSN リリース 3.0 の PPP カウンタ (続き)

CDMA PPP MIB サブグループ	カウンタの説明
LCP Echo Stats - LCP Echo Request timeout:	LCP Echo Request の総タイムアウト数。
Receive Errors - unknown protocol errors:	PPP スタックで受信したパケットからプロトコル値を識別できなかった総パケット数。
Receive Errors - bad pkt length:	上記理由により破棄された総バイト数。

### Cisco PDSN リリース 3.0 の RP カウンタ

次に、Cisco PDSN リリース 3.0 の新しい MIB サブグループを示します。

- cCdmaRPRegReqErrors
- cCdmaRPRegUpdAckErrors
- cCdmaRPSessUpdAckErrors
- cCdmaRPRegReplyErrors
- cCdmaRPRegUpdErrors
- cCdmaRPSessUpdErrors
- cCdmaRpSessUpdStats
- cCdmaPcfSoRpSessUpdStats

次に、オブジェクトが追加される既存の MIB サブグループを示します。

- cCdmaTrafficStats
- cCdmaPcfSoRpRegStats
- cCdmaPcfSoRpUpdStats
- cCdmaSystemInfo
- cCdmaRpRegStats

表 24 に、Cisco PDSN リリース 3.0 でサポートされる追加 RP カウンタを示します。

表 24 Cisco PDSN リリース 3.0 でサポートされる RP カウンタ

CDMA PPP MIB サブグループ	カウンタの説明
cCdmaSystemInfo	
sysInfo - PPPoGREsessions	このシステムと現在確立している PPPoGRE セッションの合計数。
sysInfo-HDLC-GREsessions	このシステムと現在確立している HDLCoGRE セッションの合計数。
sysInfo-totalSessions	システムの最後の再起動後に確立されたセッションの合計数。
sysInfo-totalReleases	システムの最後の再起動後に解放されたセッションの合計数。
sysInfo-totalMSIDFlow	MSID サービスを現在使用しているフローの合計数。
sysInfo-totalVPDNFlow	VPDN サービスを現在使用しているフローの合計数。

表 24 Cisco PDSN リリース 3.0 でサポートされる RP カウンタ (続き)

CDMA PPP MIB サブグループ	カウンタの説明
cCdmaRpRegStats	
RegStats-Reqs	システムの最後の再起動後に受信された初回の A11 Registration Request の数。
RegStats-Disc	システムの最後の再起動後にサイレント破棄された 初回の A11 Registration Request の数。
RegStats-ReregReqs	システムの最後の再起動後に受信された A11 Registration Request の数。
RegStats-ReregDisc	システムの最後の再起動後にサイレント破棄された A11 Reregistration Request の数。
RegStats-DeregReqs	システムの最後の再起動後に受信された A11 Deregistration Request の数。
RegStats-DeregDisc	システムの最後の再起動後にサイレント破棄された A11 Deregistration Request の数。
RegStats-HandoffReqs	システムの最後の再起動後に受信された A11 Handoff Registration の数。
RegStats-HandoffAccepted	システムの最後の再起動後に受け入れられた、既存のセッション向けハンドオフ A11 Registration Request の合計数。
RegStats-HandoffDenied	システムの最後の再起動後に拒否された、既存のセッション向けハンドオフ A11 Registration Request の合計数。
RegStats-HandoffDisc	システムの最後の再起動後にサイレント破棄されたハンドオフ A11 Registration Request の数。
RegStats-ReregAirlinkStart	システムの最後の再起動後の Airlink Start を含む A11 Reregistration Request の数。
RegStats-ReregAirlinkStop	システムの最後の再起動後の Airlink Stop を含む A11 Reregistration Request の数。
RegStats-DeregAirlinkStop	システムの最後の再起動後の PCF 間アクティブハンドオフの数。
RegStats-HandoffInterPCFActive	システムの最後の再起動後の Airlink Stop を含む A11 Deregistration Request の数。
RegStats-HandoffInterPCFDormant	システムの最後の再起動後の PCF 間休止ハンドオフの数。
cCdmaRpSessUpdStats	
SessUpdStats-TransReqs	システムの最後の再起動後に送信された A11 Session Update の合計数。
SessUpdStats-AcceptedReqs	システムの最後の再起動後に受信された、Status フィールドがゼロ (対応する Registration Update が受け入れられたことを示す) に設定された A11 Session Update Acknowledgement の合計数。
SessUpdStats-DeniedReqs	システムの最後の再起動後に受信された、Status フィールドがゼロ以外 (対応する Registration Update が拒否されたことを示す) に設定された A11 Session Update Acknowledgement の合計数。

表 24 Cisco PDSN リリース 3.0 でサポートされる RP カウンタ (続き)

CDMA PPP MIB サブグループ	カウンタの説明
SessUpdStats-NotAckedReqs	システムの最後の再起動後に送信され、対応する A11 Registration Acknowledgement が受信されなかった A11 Session Update の合計数。
SessUpdStats-TransReqs	システムの最後の再起動後に送信された、再送信された A11 Registration Update を除く初回の A11 Session Update の合計数。
SessUpdStats-RetransReqs	システムの最後の再起動後に再送信された A11 Session Update の合計数。
SessUpdStats-RecAcks	システムの最後の再起動後に受信された A11 Session Update Acknowledgement の合計数。
SessUpdStats-DiscAcks	システムの最後の再起動後に破棄された A11 Session Update Acknowledgement の合計数。
SessUpdStats-AlwaysON	システムの最後の再起動後に、常時接続により送信された初回の A11 Session Update の合計数。このカウントには再送信は含まれません。
SessUpdStats-RNPDIT	システムの最後の再起動後に、RNPDIT 値がダウンロードされたために送信された初回の A11 Registration Update の合計数。このカウントには再送信は含まれません。
SessUpdStats-UnSpecFail	システムの最後の再起動後に、未指定の理由により失敗したセッションアップデートレジストレーションの数。
SessUpdStats-ParamNotUpd	システムの最後の再起動後に、セッションパラメータのために失敗したセッションアップデートレジストレーションの数。
SessUpdStats-MNAuthenFail	システムの最後の再起動後に、MN 認証の失敗により失敗したセッションアップデートレジストレーションの数。
SessUpdStats-IdentMismatchFail	システムの最後の再起動後に、レジストレーション識別の不一致のために失敗したセッションアップデートレジストレーションの数。
SessUpdStats-BadReqsFail	システムの最後の再起動後に、要求の形式の不備により失敗したセッションアップデートレジストレーションの数。
cCdmaTrafficStats	
trafficStats-SDBPaks	システムの最後の再起動後に、PDSN から PCF に送信された SDB マーク付きデータパケットの合計数。
trafficStats-SDBOctets	システムの最後の再起動後に、PDSN から PCF に送信された SDB マーク付きデータオクテットの合計数。
cCdmaPcfSoRpRegStats	
PcfSoRegStats-InitRegReqs	システムの最後の再起動後に受信された初回の A11 Registration Request の数。

表 24 Cisco PDSN リリース 3.0 でサポートされる RP カウンタ (続き)

CDMA PPP MIB サブグループ	カウンタの説明
PcfSoRegStats-InitRegDisc	システムの最後の再起動後にサイレント破棄された初回の A11 Registration Request の数。
PcfSoRegStats-RegReqs	システムの最後の再起動後に受信された A11 Registration Request の数。
PcfSoRegStats-ReregDisc	システムの最後の再起動後にサイレント破棄された A11 Reregistration Request の数。
PcfSoRegStats-DeregReqs	システムの最後の再起動後に受信された A11 Deregistration Request の数。
PcfSoRegStats-DiscardedReqs	システムの最後の再起動後にサイレント破棄された A11 Deregistration Request の数。
PcfSoRegStats-RcvdReqs	システムの最後の再起動後に受信された A11 Handoff Registration の数。
PcfSoRegStats-AcptdReqs	システムの最後の再起動後に受け入れられた、既存のセッション向けハンドオフ A11 Registration Request の合計数。
PcfSoRegStats-DeniedReqs	システムの最後の再起動後に拒否された、既存のセッション向けハンドオフ A11 Registration Request の合計数。
PcfSoRegStats-Disc	システムの最後の再起動後にサイレント破棄されたハンドオフ A11 Registration Request の数。
PcfSoRegStats-ReregAirlinkStart	システムの最後の再起動後の Airlink Start を含む A11 Reregistration Request の数。
PcfSoRegStats-ReregAirlinkStop	システムの最後の再起動後の Airlink Stop を含む A11 Reregistration Request の数。
PcfSoRegStats-DeregAirlinkStop	システムの最後の再起動後の Airlink Stop を含む A11 Deregistration Request の数。
cCdmaPcfSoRpUpdStats	
PcfSoHandoffUpdStats	システムの最後の再起動後に、PCF ハンドオフの結果送信されたアップデートレジストレーションの数。
PcfSoHandoffUpdStats-NotAckedReqs	システムの最後の再起動後に、PCF 間ハンドオフの結果送信され、対応する A11 Registration Acknowledgement を受信しなかった A11 Registration Update の合計数。
PcfSoHandoffUpdStats-RecAcks	システムの最後の再起動後に、PCF 間ハンドオフの結果送信された A11 Registration Update に対して受信された A11 Registration Acknowledgement の合計数。
PcfSoHandoffUpdStats-AcceptReqs	システムの最後の再起動後に受信された、Status フィールドがゼロ (対応する Registration Update が受け入れられたことを示す) に設定された A11 Registration Acknowledgement の合計数。

表 24 Cisco PDSN リリース 3.0 でサポートされる RP カウンタ (続き)

CDMA PPP MIB サブグループ	カウンタの説明
PcfSoHandoffUpdStats-DeniedReqs	システムの最後の再起動後に受信された、Status フィールドがゼロ以外 (対応する Registration Update が拒否されたことを示す) に設定された A11 Registration Acknowledgement の合計数。
PcfSoHandoffUpdStats-DiscAcks	システムの最後の再起動後に破棄された A11 Registration Acknowledgement の合計数。
PcfSoHandoffUpdStats-TxdReqs	システムの最後の再起動後に PCF 間ハンドオフの結果として送信された、再転送された A11 Registration Update を除く初回の A11 Registration Update の合計数。
PcfSoHandoffUpdStats-RetxdReqs	システムの最後の再起動後に、初回の Registration Update (PCF 間ハンドオフの結果として送信) が ACK も拒否もされなかったために再転送された A11 Registration Update の合計数。
PcfSoHandoffUpdStats-UnknownFail	システムの最後の再起動後に、未指定の理由により失敗したアップデート レジストレーションの数。アップデートは、PCF 間ハンドオフの結果として送信されます。
PcfSoHandoffUpdStats-AdminProhibitFail	システムの最後の再起動後に、管理上の禁止により失敗したアップデート レジストレーションの数。アップデートは、PCF 間ハンドオフの結果として送信されます。
PcfSoHandoffUpdStats-MNAuthenFail	システムの最後の再起動後に、MN 認証の失敗により失敗したアップデート レジストレーションの数。アップデートは、PCF 間ハンドオフの結果として送信されます。
PcfSoHandoffUpdStats--IdMismatch	システムの最後の再起動後に、レジストレーション識別の不一致のために失敗したレジストレーションの数。アップデートは、PCF 間ハンドオフの結果として送信されます。
PcfSoHandoffUpdStats-BadReqs	システムの最後の再起動後に、要求の形式の不備により失敗したレジストレーションの数。アップデートは、PCF 間ハンドオフの結果として送信されます。
cCdmaRPRegReqErrors	
RegReqErr-PakLen	システムの最後の再起動後、解析中に無効な Registration Request パケット長が検出されました。
RegReqErr-Protocol	システムの最後の再起動後、Registration Request Session Specific Extension で無効なプロトコル値が検出されました。
RegReqErr-Flags	システムの最後の再起動後、Registration Request で無効なフラグ値が検出されました。
RegReqErr-MHAEKey	システムの最後の再起動後、Registration Request Mobile-Home Authentication Extension で無効な認証キーが検出されました。

表 24 Cisco PDSN リリース 3.0 でサポートされる RP カウンタ (続き)

CDMA PPP MIB サブグループ	カウンタの説明
RegReqErr-SPIMismatch	システムの最後の再起動後、Registration Request Mobile-Home Authentication Extension で SPI の不一致が検出されました。
RegReqErr-SPI	システムの最後の再起動後、Registration Request Mobile-Home Authentication Extension で無効な SPI が検出されました。
RegReqErr-ConnId	システムの最後の再起動後、Registration Request で無効な接続 ID が検出されました。
RegReqErr-MNID	システムの最後の再起動後、Registration Request で無効な MN ID が検出されました。
RegReqErr-MNIDType	システムの最後の再起動後、Registration Request で無効な MN ID タイプが検出されました。
RegReqErr-MSIDLlen	システムの最後の再起動後、Registration Request で無効な MSID 長が検出されました。
RegReqErr-SSE	システムの最後の再起動後、Registration Request に Session Specific Extension がありませんでした。
RegReqErr-MHAE	システムの最後の再起動後、Registration Request に Mobile-Home Authentication Extension がありませんでした。
RegReqErr-Order	システムの最後の再起動後、Registration Request のエクステンションの順序が無効です。
RegReqErr-VSE	システムの最後の再起動後、Registration Request のベンダー固有エクステンションの順序が無効です。
RegReqErr-AppType	システムの最後の再起動後、Registration Request のベンダー固有エクステンションのアプリケーションタイプが無効です。
RegReqErr-DupAppType	システムの最後の再起動後、Registration Request のベンダー固有エクステンションのアプリケーションタイプが重複しています。
RegReqErr-AppSubType	システムの最後の再起動後、Registration Request のベンダー固有エクステンションのサブアプリケーションタイプが無効です。
RegReqErr-VendorId	システムの最後の再起動後、Registration Request のベンダー固有エクステンションのベンダー ID が無効です。
RegReqErr-CVSE	システムの最後の再起動後、Registration Request の Critical Vendor Extension が重複しています。
RegReqErr-UnknownAttr	システムの最後の再起動後、Registration Request に不明な Accounting アトリビュートがあります。

表 24 Cisco PDSN リリース 3.0 でサポートされる RP カウンタ (続き)

CDMA PPP MIB サブグループ	カウンタの説明
RegReqErr-LenAttr	システムの最後の再起動後、Registration Request で無効なアカウントングアトリビュート長が検出されました。
RegReqErr-DupAttr	システムの最後の再起動後、Registration Request で重複するアカウントングアトリビュート長を受信しました。
RegReqErr-AcctRecRetrans	システムの最後の再起動後アップデートされていない Registration Request Airlink レコードに同じアカウントングシーケンス番号とレコードタイプがあります。
RegReqErr-SeqNum	システムの最後の再起動後、Airlink アカウントングレコード Registration Request 内の無効シーケンス番号がサイレント破棄されました。
RegReqErr-DupGREKey	システムの最後の再起動後、同じ PCF から異なる MSID への Registration Request で重複する GRE Key を受信しました。
RegReqErr-SameGREKey	システムの最後の再起動後、既存セッションの Registration Request で同じ GRE Key および Airlink セットアップを受信しました。
RegReqErr-GREKeyChangeNoSetup	システムの最後の再起動後、既存セッションの Registration Request で、Airlink セットアップなしで変更された GRE を受信しました。
RegReqErr-InitNoSetup	システムの最後の再起動後、初回の Registration Request で Airlink Setup レコードを受信しませんでした。
RegReqErr-StartBeforeSetup	システムの最後の再起動後、Registration Request の Airlink セットアップの前に Airlink Start レコードを受信しました。
RegReqErr-StartOnClose	システムの最後の再起動後、Deregistration Request で Airlink Start レコードを受信しました。
RegReqErr-StartOnActive	システムの最後の再起動後、すでにアクティブなセッションに対して Registration Request で Airlink Start レコードを受信しました。
RegReqErr-StopOnDormant	システムの最後の再起動後、すでに休止しているセッションに対して Registration Request で Airlink Stop レコードを受信しました。
RegReqErr-InitStop	システムの最後の再起動後、初回の Registration Request で Airlink Stop レコードを受信しました。
RegReqErr-InitSDB	システムの最後の再起動後、初回の Registration Request で Airlink SDB を受信しました。
RegReqErr-airlinkRec	システムの最後の再起動後、Registration Request で無効な Accounting Airlink レコードタイプが検出されました。



表 24 Cisco PDSN リリース 3.0 でサポートされる RP カウンタ (続き)

CDMA PPP MIB サブグループ	カウンタの説明
RegReqErr-DeregNoSession	システムの最後の再起動後、存在しないセッションのレジストレーションリクエストに対する Deregistration Request は破棄されます。
RegReqErr-ReregInDisc	システムの最後の再起動後、切断または削除状態のセッションに Reregistration Request を受信したため、この要求は破棄されます。
RegReqErr-Memfail	システムの最後の再起動後、処理中のメモリ割り当て失敗により Registration Request は破棄されました。
RegReqErr-MaxSessions	システムの最後の再起動後、セッションの最大上限または設定数に達したため、Registration Request は拒否されました。
cCdmaRPRegUpdAckErrors	
RegUpdAckErr-PakLen	システムの最後の再起動後、解析中に無効な Registration Update ACK パケット長が検出されました。
RegUpdAckErr-Protocol	システムの最後の再起動後、Registration Update ACK Session Specific Extension で無効なプロトコル値が検出されました。
RegUpdAckErr-RUAEKey	システムの最後の再起動後、Registration Update ACK Registration Update Authentication Extension で無効な認証キーが検出されました。
RegUpdAckErr-SPI	システムの最後の再起動後、Registration Update ACK Registration Update Authentication Extension で無効な SPI が検出されました。
RegUpdAckErr-ConnId	システムの最後の再起動後、Registration Update ACK で無効な接続 ID が検出されました。
RegUpdAckErr-MNID	システムの最後の再起動後、Registration Update ACK で無効な MN ID が検出されました。
RegUpdAckErr-MNIDType	システムの最後の再起動後、Registration Update ACK で無効な MN ID タイプが検出されました。
RegUpdAckErr-MSIDLen	システムの最後の再起動後、Registration Update ACK で無効な MSID 長が検出されました。
RegUpdAckErr-SSE	システムの最後の再起動後、Registration Update ACK に Session Specific Extension がありませんでした。
RegUpdAckErr-RUAE	システムの最後の再起動後、Registration Update ACK に Registration Update Authentication Extension がありませんでした。
RegUpdAckErr-Order	システムの最後の再起動後、Registration Update ACK のエクステンションの順序が無効です。
RegUpdAckErr-VSE	システムの最後の再起動後、Registration Update ACK のベンダー固有エクステンションの順序が無効です。

表 24 Cisco PDSN リリース 3.0 でサポートされる RP カウンタ (続き)

CDMA PPP MIB サブグループ	カウンタの説明
RegUpdAckErr-NoSession	システムの最後の再起動後、存在しないセッションの Registration Update ACK に対する Deregistration Update ACK が検出されました。
RegUpdAckErr-MemFail	システムの最後の再起動後、処理中のメモリ割り当て失敗により Registration Update ACK は破棄されました。
cCdmaRPSessUpdAckErrors	
SessUpdAckErr-PakLen	システムの最後の再起動後、解析中に無効な Session Update ACK パケット長が検出されました。
SessUpdAckErr-Protocol	システムの最後の再起動後、Session Update ACK Session Specific Extension で無効なプロトコル値が検出されました。
SessUpdAckErr-RUAEKey	システムの最後の再起動後、Session Update ACK Registration Update Authentication Extension で無効な認証キーが検出されました。
SessUpdAckErr-SPI	システムの最後の再起動後、Session Update ACK Session Update Authentication Extension で無効な SPI が検出されました。
SessUpdAckErr-ConnId	システムの最後の再起動後、Session Update ACK で無効な接続 ID が検出されました。
SessUpdAckErr-MSID	システムの最後の再起動後、Session Update ACK で無効な MN ID が検出されました。
SessUpdAckErr-MSIDType	システムの最後の再起動後、Session Update ACK で無効な MN ID タイプが検出されました。
SessUpdAckErr-MSIDLen	システムの最後の再起動後、Session Update ACK で無効な MSID 長が検出されました。
SessUpdAckErr-SSE	システムの最後の再起動後、Session Update ACK に Session Specific Extension がありませんでした。
SessUpdAckErr-RUAE	システムの最後の再起動後、Session Update ACK に Session Update Authentication Extension がありませんでした。
SessUpdAckErr-Order	システムの最後の再起動後、Session Update ACK のエクステンションの順序が無効です。
SessUpdAckErr-VSE	システムの最後の再起動後、Session Update ACK で無効なベンダー固有エクステンションが検出されました。
SessUpdAckErr-NoSession	システムの最後の再起動後、存在しないセッションの Session Update ACK に対する De-Session Update ACK が検出されました。
SessUpdAckErr-MemFail	システムの最後の再起動後、処理中のメモリ割り当て失敗により Session Update ACK は破棄されました。
cCdmaRPRegReplyErrors	

表 24 Cisco PDSN リリース 3.0 でサポートされる RP カウンタ (続き)

CDMA PPP MIB サブグループ	カウンタの説明
RegRplyErr-Internal	システムの最後の再起動後、処理中に内部エラーが発生したため Registration Reply は送信されませんでした。
RegRplyErr-MemFail	システムの最後の再起動後、処理中のメモリ割り当て失敗により Registration Reply は送信されませんでした。
RegRplyErr-NoSecOrParse	システムの最後の再起動後、PCF にセキュリティの関連付けが見つからないか、リクエストの解析エラーが発生したため、PCF への応答を送信できません。
cCdmaRPRegUpdErrors	
RegUpdErr-Internal	システムの最後の再起動後、処理中に内部エラーが発生したため Registration Update は送信されませんでした。
RegUpdErr-MemFail	システムの最後の再起動後、処理中のメモリ割り当て失敗により Registration Update は送信されませんでした。

Cisco PDSN リリース 2.1 には、の MIB 機能強化が含まれています。

次の既存 MIB サブグループに PPP カウンタ オブジェクトが追加されました。

- cCdmaPppSetupStats
- cCdmaPppReNegoStats
- cCdmaPppAuthStats
- cCdmaPppReleaseStats
- cCdmaPppMiscStats

#### CDMA PDSN システム情報

ccpcEnabled OBJECT-TYPE

::= { ccpcSystemInfo 1 }

ccpcSessionTotal OBJECT-TYPE

::= { ccpcSystemInfo 2 }

#### 各 PCF の CDMA PDSN Closed-RP レジストレーション統計情報

PDSN PCF テーブルでは、現在 PDSN と対話している RAN の PCF に関する参照が維持されます。

エント리는、PCF との L2TP トンネルが確立したときに作成されます。トンネルが削除されるとエントリも削除されます。

各 PCF について維持される統計情報オブジェクトは次のとおりです。

ccpcPcfIpAddressType OBJECT-TYPE

「ccpcPcfIpAddress で指定されたアドレスのタイプを表します。」

::= { ccpcPcfPerfStatsEntry 1 }

ccpcPcfIpAddress OBJECT-TYPE

「モバイル ノードにサービスを提供する PCF の IP アドレス。」

::= { ccpcPcfPerfStatsEntry 2 }

ccpcPcfRcvdIcrqs OBJECT-TYPE

「PCF との L2TP トンネルの確立後に受信された L2TP セッションを確立する Incoming-Call-Request の合計数。」

::= { ccpcPcfPerfStatsEntry 3 }

ccpcPcfAcptdIcrqs OBJECT-TYPE

「PCF との L2TP トンネルの確立後に受け付けた Incoming-Call-Request の合計数。」

::= { ccpcPcfPerfStatsEntry 4 }

ccpcPcfDroppedIcrqs OBJECT-TYPE

「PCF との L2TP トンネルの確立後に拒否された Incoming-Call-Request の合計数。」

::= { ccpcPcfPerfStatsEntry 5 }

ccpcPcfSentIcrqs OBJECT-TYPE

「PCF との L2TP トンネルの確立後に送信された Incoming-Call-Request の合計数。」

::= { ccpcPcfPerfStatsEntry 6 }

ccpcPcfRcvdIccns OBJECT-TYPE

「PCF との L2TP トンネルの確立後に受信された Incoming-Call-Request の合計数。」

::= { ccpcPcfPerfStatsEntry 7 }

ccpcPcfAcptdIccns OBJECT-TYPE

「PCF との L2TP トンネルの確立後に受け付けられた Incoming-Call-Request の合計数。」

::= { ccpcPcfPerfStatsEntry 8 }

ccpcPcfDroppedIccns OBJECT-TYPE

「PCF との L2TP トンネルの確立後に受け付けられた Incoming-Call-Request の合計数。」

::= { ccpcPcfPerfStatsEntry 9 }

ccpcPcfRcvdCdns OBJECT-TYPE

「PCF との L2TP トンネル確立後に受信された L2TP セッションを切断する Call-Disconnect-Notify メッセージの合計数。」

::= { ccpcPcfPerfStatsEntry 10 }

ccpcPcfSentCdns OBJECT-TYPE

「PCF との L2TP トンネル確立後に PCF に送信された L2TP セッションを切断する Call-Disconnect-Notify メッセージの合計数。」

::= { ccpcPcfPerfStatsEntry 11 }

ccpcPcfDroppedCdns OBJECT-TYPE

「PCF との L2TP トンネルの確立後に破棄された Call-Disconnect-Notify メッセージの合計数。」

::= { ccpcPcfPerfStatsEntry 12 }

ccpcPcfRcvdZlbs OBJECT-TYPE

「PCF との L2TP トンネルの確立後に受信された Zero-Length-Buffer メッセージの合計数。」

```
::= { ccpcPcfPerfStatsEntry 13 }
```

ccpcPcfSentZlbs OBJECT-TYPE

「PCF との L2TP トンネルの確立後に送信された Zero-Length-Buffer メッセージの合計数。」

```
::= { ccpcPcfPerfStatsEntry 14 }
```

Cisco PDSN リリース 2.0 以降では、MIB CISCO-CDMA-PDSN-MIB モジュールは、PCF とサービス オプションによる次の統計情報を提供するように変更されています。

- PCF およびサービス オプションに基づく RP レジストレーション統計情報
- PCF およびサービス オプションに基づく RP アップデート統計情報
- PCF およびサービス オプションに基づく PPP 統計情報

### PCF およびサービス オプションに基づく RP 統計情報

リリース 1.2 では、PDSN MIB は、ボックス レベルの情報を含む RP レジストレーション統計情報を提供していました。これらの統計情報は、"cCdmaRpRegStats" というグループで定義されています。リリース 2.0 以上では、ボックス レベルの情報に加えて、PCF および SO に基づく RP 統計情報も提供され、これらの統計情報に関連する MIB が次のグループで定義されています。

cCdmaPcfSoRpRegStats OBJECT IDENTIFIER

```
::= { cCdmaPerformanceStats 10 }
```

### PCF およびサービス オプションに基づく RP アップデート統計情報

リリース 1.2 MIB は、ボックス レベルの RP アップデート統計情報を提供し、これらの統計情報に関連する MIB オブジェクトは、cCdmaRpUpdStats というグループで定義されています。これらの統計情報に加えて、リリース 2.0 の MIB は、PCF および SO に基づく RP アップデート統計情報を提供します。これらの新しい MIB オブジェクトは、次のグループで定義されています。

cCdmaPcfSoRpUpdStats OBJECT IDENTIFIER

```
::= { cCdmaPerformanceStats 11 }
```

### PCF およびサービス オプションに基づく PPP 統計情報

リリース 1.2 では、グループ "cCdmaPppStats" で定義された MIB オブジェクトは、PDSN と MN 間の PPP ネゴシエーションに関するボックス レベルの情報を提供します。リリース 2.0 では、MIB は、PCF および SO に基づく次の PPP 統計情報を提供します。

```
cCdmaPcfSoPppCurrentConns
```

```
cCdmaPcfSoPppConnInitiateReqs
```

```
cCdmaPcfSoPppConnSuccesses
```

```
cCdmaPcfSoPppConnFails
```

```
cCdmaPcfSoPppConnAborts
```

これらのオブジェクトは、次の MIB グループでグループ化されています。

cCdmaPcfSoPppSetupStats OBJECT IDENTIFIER

```
::= { cCdmaPerformanceStats 12 }
```

旧リリースと同様、SNMP を使用した CiscoWorks 2000 ネットワーク管理システムで PDSN を管理できます。標準 6500 MIBS に加えて、Cisco CDMA PDSN MIB (CISCO\_CDMA\_PDSN\_MIB.my) が PDSN ソリューションに含まれています。PDSN MIB は、引き続き次の機能をサポートします。

- 統計情報のグループ
  - ハンドオフ統計情報：PCF 間の成功と失敗、PDSN 間のハンドオフ

- サービス オプションに基づく成功および失敗の統計情報
- フロー タイプに基づく失敗の統計情報
- MSID 認証の統計情報
- アドレッシング スキームの統計情報：スタティックまたはダイナミック MIP または SIP
- 異なる重大度をサポートする TRAP しきい値グループ。エージェントは、影響を受けるサービスの重大度が設定された重大度より高い場合だけ通知を生成します。重大度は次の方法で設定できます。
  - **cdma pdsn mib trap level 1-4** を使用した CLI コマンド。または
  - SNMP を使用して、オブジェクト **cCdmaNotifSeverityLevel** を設定。

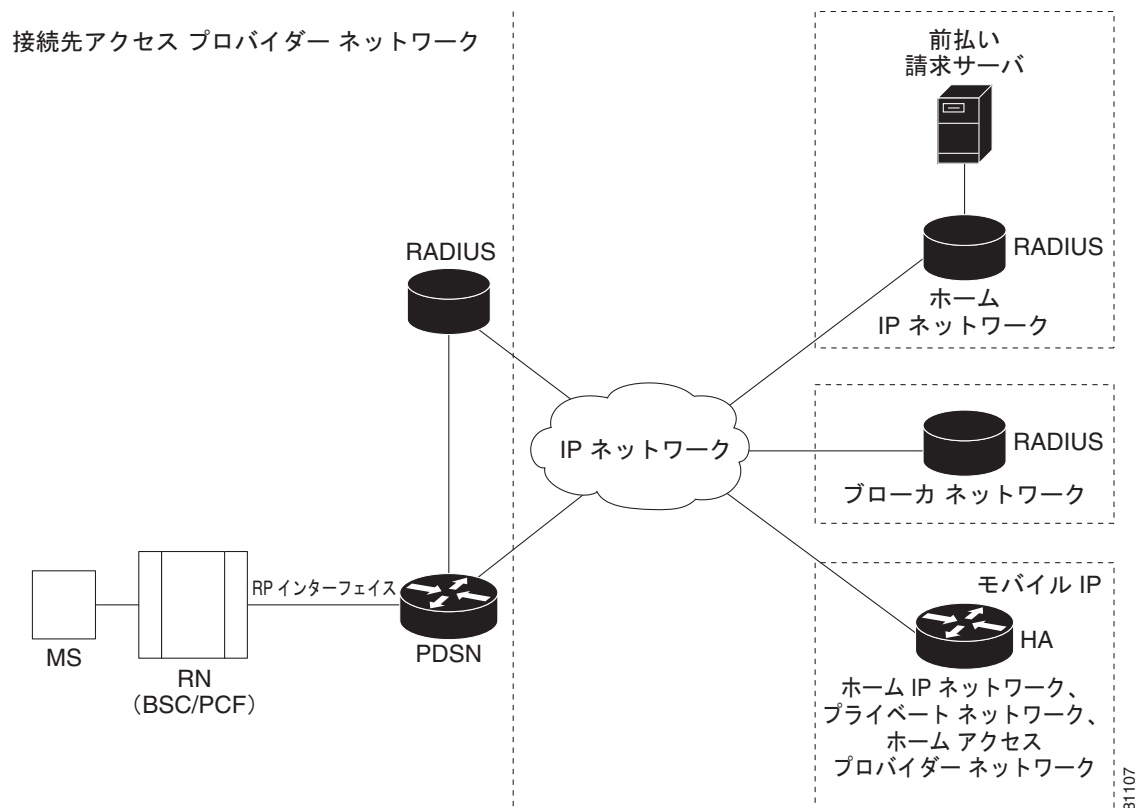
## シスコ独自の前払い請求

Cisco PDSN リリース 2.1 は、次のサービスを提供するシスコ独自の前払い請求機能をサポートします。

- リアルタイムの SIP に基づくサービスの測定。詳細については、[97 ページの「Prepaid Simple IP Call Flow」](#)を参照してください。
- リアルタイムの非差別化 MIP サービス。1 ユーザに複数の MIP フローをサポート。詳細については、[98 ページの「Prepaid Mobile IP Call Flow」](#)を参照してください。
- フロー単位のデータ ボリュームに基づくレーティング、オクテットまたはパケット カウント、およびコールの長さ。

図 6 は、前払いサービスのネットワーク参照アーキテクチャを示します。PBS は、モバイル ステーションのホーム ネットワークに置かれ、ホーム RADIUS サーバがアクセスします。前払い機能付き Cisco Access Registrar (AR) は、前払いユーザと前払い以外のユーザにサービスを提供するホーム RADIUS サーバとして使用できます。

図 6 PDSN 前払い請求アーキテクチャ



ローミング ユーザの場合、アクセス先のネットワークのローカル RADIUS サーバは、必要に応じてブローカ RADIUS サーバを使用して、ホーム RADIUS サーバに AAA サーバ要求を転送します。ローミング前払いユーザの場合、ローカルおよびブローカの AAA サーバは新しいベンダー固有の前払いアカウントリングアトリビュートをトランスペアレントにホーム RADIUS サーバに転送する必要があります。

ホーム RADIUS サーバが PBS とのインターフェイスをサポートしない既存ネットワークでは、ホーム RADIUS サーバの前に AR を配置して、プロキシのように動作させることができます。この場合、AR は、ホーム RADIUS サーバとの間のすべての認可メッセージとアカウントリングメッセージを転送し、PBS と通信します。このシナリオは、すでに RADIUS サーバが存在する場合に重要です。

このアーキテクチャでは、RADIUS サーバで追加要件が発生しますが、PDSN とのインターフェイスに変更はありません。

既存の WIN または IN ベースの前払い請求サーバを使用する場合があります。この場合、PBS は、外部前払い請求サーバとのインターフェイスになります。

### アカウントリングレコード

PDSN は、前払い以外のユーザに対する場合と同じように、フロー単位のアカウンティングレコードを生成し続けます。ただし、フローに対する最後のアカウントリング停止要求には、最終的な使用状況を報告する新しい前払いベンダー固有アトリビュート (VSA) が含まれます。

## PDSN での前払いの動作

前払いモバイルユーザがデータ サービス コールを行うと、MS は PDSN と PPP (Point-to-Point Protocol) リンクを確立します。PDSN は、AAA サーバと通信してモバイルステーションを認証します。AAA サーバは、ユーザが有効な前払い加入者であることを確認し、ユーザが利用できるサービスを特定し、請求のために使用状況を追跡します。

IP アドレスと接続のタイプを割り当てるための方法は、5 ページの「How PDSN Works」で説明する方法と似ています。

次からのセクションでは、各トピックの前払い環境における IP アドレッシングと通信レベルについて説明します。

- [前払いのシンプル IP コール フロー](#)
- [前払いのモバイル IP コール フロー](#)

## 前払いのシンプル IP コール フロー

次の例では、前払いユーザは十分な信用があり、SIP データ コールを行います。ユーザはコールの終了時に切断します。

- 
- ステップ 1** MS は、開始メッセージを送信して、コールを開始します。トラフィック チャンネルが割り当てられ、MS は CHAP を使用して認証されます。
  - ステップ 2** PDSN は、SIP フローが要求されていることを確認し、RADIUS サーバに Access-Request を送信します。
  - ステップ 3** RADIUS サーバはユーザのプロファイルを調べ、ユーザが前払いサービスを使用していることを確認します。サーバは請求サーバに初期認証要求を送信します。
  - ステップ 4** 請求サーバはユーザがコールを行う十分な割り当てを有しているかどうかをチェックし、結果を返します。
  - ステップ 5** RADIUS サーバは、PDSN に前払いユーザであることを示す Access-Accept メッセージを送信します。
  - ステップ 6** PDSN は PPP 接続を完了し、IP アドレスが MS に割り当てられます。
  - ステップ 7** PDSN は、通常どおり Accounting Request (Start) を送信し、AR に初期割り当ての認可を求める Access-Request を送信します。要求には、コールが SIP であることを示す Service ID VSA が含まれません。
  - ステップ 8** ユーザが前払いユーザであることを認識している RADIUS サーバは、請求サーバに初期割り当て認可要求を送信します。請求サーバから RADIUS サーバに割り当て情報が返されます。RADIUS サーバは Access-Accept メッセージに割り当て情報を入れて、PDSN に送ります。
  - ステップ 9** PDSN は受信した割り当て情報を保存し、この情報に基づいてユーザデータを監視します。割り当てを使い切ると、PDSN は使用状況と "Quota Depleted." (割り当てが使い切られた) という理由を示す Access-Request を AR に送信します。
  - ステップ 10** RADIUS サーバは PBS に再認可要求を送信し、PBS はユーザのアカウントをアップデートし、追加割り当てを指定し、新しい割り当て情報を RADIUS サーバに返します。
  - ステップ 11** RADIUS サーバは Access-Accept メッセージに新しい割り当て情報を入れて、PDSN に送ります。PDSN はテーブルで新しい割り当て情報をアップデートし、Access-Request が送信されてから使用された割り当てを考慮するように使用状況を調整します。PDSN は、引き続きユーザデータの監視を監視します。ユーザに十分な割り当てがある限り、ステップ 9 ~ 11 が繰り返されます。
  - ステップ 12** ユーザが切断すると、MS はコールの解放を開始し、トラフィック チャンネルが解放されます。PDSN はセッションをクリアし、Accounting Request Stop レコードを送信します。レコードには、最終的な使用状況を報告する前払い VSA が含まれます。



- ステップ 13** RADIUS サーバはそのレコードをアップデートし、最終的な使用状況レポートを PBS に送信します。PBS はユーザのアカウントをアップデートし、AR に応答します。AR は PDSN に Accounting Response を送信します。

## 前払いのモバイル IP コール フロー

次のシナリオでは、前払いユーザは MIP データ コールを行います。MIP データ セッション中ユーザの割り当てがなくなり、PDSN はコールを切断します。コール フローは単一の MIP フローを示していますが、追加フローが確立され、MS が追加 MIP Registration Request を送信するときと同様の方法で処理されます。

- ステップ 1** MS は、開始メッセージを送信して、コールを開始します。トラフィック チャンネルが割り当てられますが、MS は CHAP を省略します。
- ステップ 2** PDSN は PPP 接続を完了します。IPCP 中に MS が IP アドレスの割り当てを省略したため、PDSN は MIP を想定します。
- ステップ 3** PDSN は FA-CHAP チャレンジでエージェント アドバタイズメントを送信し、MS は FA-CHAP 応答で MIP レジストレーション要求を開始します。
- ステップ 4** PDSN は FA-CHAP とともに Access-Request を AR に送信します。AR はユーザのプロファイルを調べ、ユーザが前払いサービスを使用しているかどうかを確認します。サーバは請求サーバに認証要求を送信します。
- ステップ 5** 請求サーバはユーザがコールを行う十分な割り当てを有しているかどうかをチェックし、ok を返します。RADIUS サーバは、PDSN に前払いユーザであることを示す Access-Accept メッセージを送信します。
- ステップ 6** PDSN は MIP レジストレーション要求を HA に転送し、レジストレーション応答を受信します。PDSN は応答を MS に転送します。
- ステップ 7** PDSN は初期割り当て認可の Access-Request を送信します。要求には、このコールが MIP コールであることを示す サービス ID VSA が含まれます。ユーザが前払いユーザであることを認識する AR は、初期割り当て認可要求を PBS に送信します。請求サーバは、割り当て情報を AR に返します。AR は割り当て情報を Access-Accept メッセージに含めて、PDSN に送信します。
- ステップ 8** PDSN は受信した割り当て情報を保存し、この情報に基づいてユーザ データを監視します。割り当てを使い切ると、PDSN は使用状況と "Quota Depleted." (割り当てが使い切られた) という理由を示す Access-Request を AR に送信します。
- ステップ 9** AR は PBS に再認可要求を送信し、PBS はユーザのアカウントをアップデートし、追加割り当てを指定し、新しい割り当て情報を AR サーバに返します。
- ステップ 10** AR は Access-Accept メッセージに新しい割り当て情報を入れて、PDSN に送ります。PDSN はテーブルで新しい割り当て情報をアップデートし、Access-Request が送信されてから使用された割り当てを考慮するように使用状況を調整します。PDSN は、引き続きユーザ データの監視を監視します。ユーザに十分な資金がある限り、ステップ 8 ~ 10 が繰り返されます。
- ステップ 11** PDSN は追加割り当てを要求しますが、ユーザの割り当ては不足しているので、PBS は "Exceeded Balance" (残高超過) を理由に要求を拒否し、AR は Access-Reject を PDSN に送信します。
- ステップ 12** PDSN は MIP フローを削除し、これが最後のフローであると判断し、PCF に A11-Registration Update を送信して A10 接続の解放を要求します。PCF は ACK メッセージを送信し、トラフィック チャンネルの解放を開始します。
- ステップ 13** PDSN はセッションをクリアし、Accounting Request Stop レコードを送信します。レコードには、最終的な使用状況を報告する前払い VSA が含まれます。

**ステップ 14** AR はレコードをアップデートし、最終的な使用状況レポートを PBS に送信します。PBS はユーザのアカウントをアップデートして AR に応答します。

**ステップ 15** AR は最後に PDSN にアカウントリング応答を送信します。



(注) この機能は、Cisco PDSN リリース 2.1 の変種です。Cisco PDSN リリース 2.0 のイメージで使用できる機能については、[PDSN 機能マトリクス](#)を参照してください。

## 3DES 暗号化

PDSN には、PDSN 上で IP セキュリティをサポートする 3DES 暗号化が含まれます。MWAM 上の IP セキュリティでは、Cisco VPN Acceleration Module を使用する必要があります。

この機能では、VPDN トラフィックと MIP トラフィック (PDSN HA 間) を暗号化できます。このリリースの PDSN では、PDSN と HA 間に MIP データ トラフィック トンネルを確立する前に、各 HA のパラメータを設定する必要があります。



(注) この機能の使用は、ハードウェアのサポートに限定されます。



(注) この機能は、PDSN ソフトウェアの変種です。PDSN の特定のイメージで使用できる機能については、[PDSN 機能マトリクス](#)を参照してください。

## モバイル IP の IPSec

Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) は、加入ピア間にデータ機密保持、データ整合性、およびデータ認証を提供する IP Security (IPSec) と呼ばれるオープン標準フレームワークを開発しました。IPSec は、IP レイヤでこれらのセキュリティ サービスを提供し、Internet Key Exchange (IKE; インターネット キー エクスチェンジ) を使用して、ローカル ポリシーに基づいてプロトコルとアルゴリズムのネゴシエーションを処理し、IPSec で使用する暗号化および認証キーを生成します。IPSec を使用することにより、ホスト ペア間、セキュリティ ゲートウェイ ペア間、またはセキュリティ ゲートウェイ とホスト間の 1 つ以上のデータ フローを保護できます。

IS-835-B は、IPSec セキュリティの提供において、3 つのメカニズムを指定しています。

- 証明書
- ダイナミックに分散された事前共有秘密
- スタティックに設定された事前共有秘密



(注) IS-835-B のスタティックに設定された事前共有秘密は Cisco PDSN リリース 1.2 ではサポートされていません。CLI でスタティックに設定された IKE の事前共有秘密だけが実装およびサポートされます。

## IPSec Acceleration Module、Static IPSec を使用したハードウェアの IPSec アクセラレーション



(注) Cisco 6500 および 7600 プラットフォーム上の Cisco PDSN リリース 3.0 では、Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータで動作するブレード、Cisco IPSec Services Module (VPNSM) のサポートが必要です。VPNSM には、物理的な WAN または LAN インターフェイスはありません。VPN ポリシー用の VLAN セレクタが使用されます。Catalyst 6500 のセキュリティ モジュールについては、<http://www.in.cisco.com/issg/isbu/products/6000/6500security.shtml> を参照してください。Cisco 7600 シリーズ ルータの詳細については、<http://www.in.cisco.com/rtg/routers/products/7600/techtools/index.shtml> を参照してください。

IPSec ベースのセキュリティは、ホーム AAA サーバから受信するパラメータに応じて、PDSN と HA 間のトンネルに適用できます。各 PDSN/HA ペア間に、1 つのトンネルを確立できます。PDSN-HA ペア間の 1 つのトンネルで、コントロール メッセージ、IP-in-IP カプセル化データ、および GRE-in-IP カプセル化データの 3 種類のトラフィック ストリームを使用できます。トンネルを通過するすべてのトラフィックに、IPSec による同レベルの保護が適用されます。

IS-835-B には、RFC 2002 に基づくモバイル MIP サービスが定義されています。PDSN は、PMIP サービスおよび PMIP サービスを提供します。

プロキシ モバイル サービスでは、Mobile-Node (MN; モバイル ノード) は SIP によって PDSN/FA に接続し、PDSN/FA が HA への MN の MIP プロキシとして動作します。

Security Association (SA; セキュリティ アソシエーションまたはトンネル) は、一度確立されると、トンネルにトラフィックが存在しなくなるか、SA のライフタイムが期限切れになるまで、アクティブとして存続します。



(注) この機能は、PDSN ソフトウェアの変種です。PDSN の特定のイメージで使用できる機能については、[PDSN 機能マトリクス](#)を参照してください。

## 条件付きデバッグの機能拡張

Cisco PDSN リリース 4.1 では、アトリビュートを解析し、アカウントリング要求で送信する間、デバッグが表示されます。

- debug aaa authentication
- debug aaa authorization
- debug radius
- debug aaa per-user
- debug ppp negotiation

### Access-Accept からのデバッグ

```
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: Service-Type          [6] 6 Framed
[2]
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: Framed-IP-Pool          [88] 11 "test-pool"
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: Vendor, 3GPP2          [26] 20
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: cdma-dns-server-ip-[117] 14
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: 01 06 01 02 03 04 02 06 05 06 07 08
[????????????]
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: Vendor, Cisco          [26] 27
```

```
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: Cisco AVpair [1] 21
"ip:vrf-id=test-pdsn"
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: Vendor, Cisco [26] 34
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: Cisco AVpair [1] 28
"ip:ip-unnumbered=Loopback0"
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: Vendor, CNCTC [26] 17
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: cnctc-served-mdn [100] 11
SAMI 5/3: Aug 4 10:16:07.859: RADIUS: 74 65 73 74 2D 70 64 73 6E
[test-pdsn]
```

### IPCP のデバッグ

```
SAMI 5/3: Aug 4 10:16:07.863: Vi2.1 IPCP: O CONFNAK [REQsent] id 1 len 22
SAMI 5/3: Aug 4 10:16:07.863: Vi2.1 IPCP: Address 2.1.1.1 (0x030602010101)
SAMI 5/3: Aug 4 10:16:07.863: Vi2.1 IPCP: PrimaryDNS 1.2.3.4 (0x810601020304)
SAMI 5/3: Aug 4 10:16:07.863: Vi2.1 IPCP: SecondaryDNS 5.6.7.8 (0x830605060708)
SAMI 5/3: Aug 4 10:16:07.863: Vi2.1 IPCP: I CONFACK [REQsent] id 1 len 10
SAMI 5/3: Aug 4 10:16:07.863: Vi2.1 IPCP: Address 51.1.1.10 (0x03063301010A)
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 IPCP: I CONFREQ [ACKrcvd] id 2 len 22
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 IPCP: Address 2.1.1.1 (0x030602010101)
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 IPCP: PrimaryDNS 1.2.3.4 (0x810601020304)
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 IPCP: SecondaryDNS 5.6.7.8 (0x830605060708)
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 AAA/AUTHOR/IPCP: primary dns server 1.2.3.4
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 AAA/AUTHOR/IPCP: seconday dns server 5.6.7.8
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 IPCP: O CONFACK [ACKrcvd] id 2 len 22
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 IPCP: Address 2.1.1.1 (0x030602010101)
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 IPCP: PrimaryDNS 1.2.3.4 (0x810601020304)
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 IPCP: SecondaryDNS 5.6.7.8 (0x830605060708)
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 IPCP: State is Open
SAMI 5/3: Aug 4 10:16:07.867: AAA/AUTHOR: Processing PerUser AV vrf-id
SAMI 5/3: Aug 4 10:16:07.867: AAA/AUTHOR: Processing PerUser AV ip-unnumbered
SAMI 5/3: Aug 4 10:16:07.867: AAA/BIND(000000DE): Bind i/f
SAMI 5/3: Aug 4 10:16:07.867: Vi2.1 IPCP: Install route to 2.1.1.1
SAMI 5/3: Aug 4 10:16:07.867: RADIUS/ENCODE(000000DE):Orig. component type = PDSN
```

### アカウントिंग要求のデバッグ

```
SAMI 5/3: Aug 4 10:16:07.867: RADIUS: Framed-IP-Address [8] 6 2.1.1.1
SAMI 5/3: Aug 4 10:16:07.867: RADIUS: Vendor, CNCTC [26] 17
SAMI 5/3: Aug 4 10:16:07.867: RADIUS: cnctc-served-mdn [100] 11
SAMI 5/3: Aug 4 10:16:07.867: RADIUS: 74 65 73 74 2D 70 64 73 6E [test-pdsn]
```

### Cisco PDSN リリース 3.0 のトレース機能

条件付きデバッグは、表示されるデバッグを特定のユーザに制限するのに便利なツールですが、複数のユーザを同時にトレースする場合はわかりにくくなる場合があります。そこで、Cisco PDSN リリース 3.0 には、次の機能が追加されています。

- PDSN は、現在、CDMA デバッグから出力されるすべての行での MNID またはユーザ名の表示をサポートしています。同様のメカニズムが、MIP、PPP、AAA などの他のサブシステムにも追加されています。トレース機能で強化されたよく使用されるデバッグは次のとおりです。
  - debug ppp negotiation
  - debug aaa id
  - debug aaa accounting
  - debug aaa authentication
  - debug aaa authorization
  - debug ip mobile
  - debug cdma pdsn all events

- debug cdma pdsn accounting
  - debug cdma pdsn service-selection
  - debug cdma pdsn session events
  - cdma pdsn redundancy debugs
- デバッグの条件が一致する場合、デバッグメッセージのすべての行の先頭に、設定された条件に従ってユーザ名または IMSI（どちらか）が表示されます。



(注) a11 クラスタ デバッグでは、行頭でのユーザ名または IMSI の表示はサポートされていません。



(注) cdma pdsn redundancy デバッグでは、行頭でのユーザ名または IMSI の表示はサポートされていません。



(注) GRE デバッグでは、最初の数行の行頭には IMSI が表示されません。



(注) 一致する条件には、debug cdma pdsn a11 errors は印刷されません。



(注) debug aaa accounting ではユーザ名は行頭に表示されません。

- 上記動作は、cdma pdsn debug show-condition および ip mobile debug include username コマンドで制御されます。条件付きデバッグが、これらの CLI コマンドを使用せずにイネーブルになっている場合、デバッグにはユーザ名も IMSI も表示されません。一方、条件付きデバッグを設定せずに、上記 CLI が設定されている場合、デバッグにはユーザ名または IMSI が表示されます。

## Cisco PDSN 3.0 以前のリリースの機能強化

Cisco PDSN リリース 2.1 は、MIP コンポーネント用に追加の条件付きデバッグをサポートしています。MIP 条件付きデバッグは、NAI および MN のホーム アドレスに基づいてサポートされます。

現在、複数の条件付きデバッグをイネーブルにすると、デバッグ出力では個々の条件は表示されず、すべての CDMA 関連デバッグに対してデバッグが出力されます。

### チェック条件

条件は、debug condition username コマンドを使用して設定します。

### 削除条件

デバッグ条件は次のコマンドを使用して削除できます。

- no debug condition username : username に基づいてすべての条件を削除します。
- no debug condition username username : 指定された username の条件を削除します。

上記 CLI コマンドを使用して条件を削除すると、条件と TRUE 条件のリストを維持する IOS 条件付きデバッグ サブシステムはフラグをリセットします。すべての条件を削除すると、デバッグ情報は、フィルタを適用せずに表示されます。

また、PDSN は、CLI コマンドの既存の IOS デバッグ条件を使用して、CDMA サブシステムにモバイル加入者 ID (MSID) に基づく条件付きデバッグを利用しています。CLI コマンドのコーリング オプションは、MSID の指定に使用されます (00000000011124 にコールするデバッグ条件など)。

NAI に基づく条件付きデバッグには次のデバッグコマンドがサポートされています。NAI は foo@bar.com などの名前です。

- **debug ip mobile**
- **debug ip mobile host**
- **debug ip mobile proxy**

次のデバッグ コマンドは、NAI ベースの条件付きデバッグの影響を受けません。

- **debug ip mobile local-area**
- **debug ip mobile router**

このリリースは、次の PDSN CLI コマンドに条件付きデバッグ サポートを提供します。

- **debug cdma pdsn accounting**
- **debug cdma pdsn accounting flow**
- **debug cdma pdsn session [errors | events]**
- **debug ip mobile**
- **debug condition username**

a11 デバッグは、次の個々の CLI コマンドを使用して、さらに msid ベースのデバッグをサポートします。

- **debug cdma pdsn a11 events mnid**
- **debug cdma pdsn a11 errors mnid**
- **debug cdma pdsn a11 packet mnid**

条件付きデバッグは IOS 機能です。次の CLI コマンドは、すべてのイメージで使用できます。

```
router# debug condition ?
  application  Application
  called       called number
  calling      calling
  glbp        interface group
  interface    interface
  ip          IP address
  mac-address  MAC address
  match-list   apply the match-list
  standby     interface group
  username     username
  vcid        VC ID
```

オプションの **calling**、**username**、**ip** は CDMA または MIP サブシステムで使用されます。

```
PDSN#debug condition username ?
  WORD Username for debug filtering
```

```
PDSN#debu condition calling ?
  WORD Calling number
```

```
PDSN#debu condition ip ?
  A.B.C.D IP address
```

Cisco PDSN リリース 2.1 の条件付きデバッグの詳細については、『*Command Reference for the Cisco PDSN 2.1 Release for Cisco IOS Release 12.3(11)YF*』のデバッグ コマンドを参照してください。

## 請求の電子シリアル番号

Electronic Serial Number (ESN; 電子シリアル番号) は、モバイル デバイスなど、1 つの装置に対する一意の識別子で、認証プロセス中に使用されます。ESN は R-P Session Setup Airlink レコードのパラメータ a2、PDSN Usage Data Record (UDR) のパラメータ A2 です。どちらのパラメータもこのリリースで導入されました。

PDSN はパラメータ a2 を受け入れ、User Data Record に A2 として入れます。

この機能は Cisco Access Registrar でサポートされています。

## Mobile Equipment Identifier のサポート

Mobile Equipment Identifier (MEID; 移動体識別番号) は、IS-835D で導入された新しいアトリビュートで、最終的に ESN AVP に置き換わると考えられます。暫定的に、両方のアトリビュートが PDSN でサポートされます。

Access-Request、FA-CHAP、または MIP RRQ に MEID を含めるには、**cdma pdsn attribute send a3** コマンドを使用します。

## 1xEV-DO のサポート

PDSN は、Evolution-Data Optimized (1xEV-DO) 電気通信規格をサポートします。1xEV-DO は、高性能、高速、大容量のワイヤレス インターネット接続を提供し、パケット データ サービス向けに最適化されています。2.4 Mbps のフォワード ピーク レートでパケット データ トラフィックを転送できます。これは、現在の 1xRTT のピーク レート 144 kbps より高速です。

PDSN の 1xEV-DO テクノロジーのサポートには、次の機能強化が含まれます。

- PDSN は、Active Start Airlink Record で 1xEV-DO 向けの新しいサービス オプション値 59 (10 進数) を認識します。
- PDSN CLI コマンドは、パケット サービス オプション (1xRTT、1xEV-DO、または未定義) が表示されるように **show cdma pdsn session** でセッションを表示するように機能強化されています。

## 組み込み外部エージェント

モバイル ステーションは、FA を使用してステーションのホーム ネットワークが提供するサービスにリモート アクセスできるので、FA はモビリティにとって必須コンポーネントです。PDSN は組み込み FA を提供します。FA は、シスコの IOS ベースの HA を含む任意の標準 HA と通信します。

## AAA サーバのサポート

PDSN は、Cisco Access Registrar を含む標準 AAA サーバと通信する認証クライアントを提供し、モバイル ステーションを認証します。PDSN は、モバイル ステーションの名前 (NAI) を使用して、ローカル AAA サーバでユーザを認証します。

- PDSN は、SIP に対して次の AAA サービスをサポートします。
  - パスワード認証プロトコル (PAP) と CHAP 認証
  - アカウンティング情報

- モバイル ユーザの IP アドレス割り当て



(注) PDSN は IP アドレスの割り当てと特殊コンフィギュレーションのユーザ向けに MSID から NAI へのマッピングをサポートします。通常、これには、PPP 確立中は認証プロセスを省略し、SIP ルーティング サービスを好む MSID ベースでアクセスするユーザが含まれます。

- PDSN は、VPDN に対して次の AAA サービスをサポートします。
  - PAP および CHAP 認証
  - アカウンティング情報
- PDSN は、PMIP に対して次の AAA サービスをサポートします。
  - PAP および CHAP 認証
  - アカウンティング情報
  - IPCP フェーズ中の IP アドレスの割り当て (Registration Reply メッセージで HA から受信)
- PDSN は、MIP に対して次の AAA サービスをサポートします。
  - オプションで、モバイル ステーションからの REJ 受信時に PPP 中の認証を省略します。
  - MIP レジストレーションにより TIA/EIA/IS-835-B で定義された FA チャレンジまたは応答。
  - 「PDSN モバイル IP」セクションで説明された FA-HA および FA モバイル ステーション。
  - 最近のアドバタイズメントに対応する MIP レジストレーション要求の FA チャレンジ応答の検証。

PDSN は、AAA サーバとユーザ サービス プロファイルを使用したサービスのプロビジョニングもサポートしています。このプロファイルは、ユーザのホーム ネットワークで定義されます。これは、NAI によって参照されます。通常、ユーザのホーム ネットワークにユーザ認証情報とともに保存され、認証応答の一部として取得されます。

Cisco PDSN リリース 4.0 では、次の AAA サーバアトリビュート (表 25 を参照) が追加されています。



(注) 表 25 では、次の条件が適用されます。

- 不可：このアトリビュートがパケットに必要です。
- 可：パケットにこのアトリビュートを含めないか、インスタンスを 1 つ含めることができます。

表 25 Cisco PDSN リリース 4.0 の AAA アトリビュート

アトリビュート	タイプ	Access-Request	Access-Accept	アカウンティング メッセージ		暫定
				Accounting Start	Accounting Stop	
Differentiated Services Class Option	26/05	不可	あり	不可	不可	不可
Allowed Differentiated Services Marking	26/73	不可	あり	不可	不可	不可
Maximum Authorized Aggregate Bandwidth for Best-Effort Traffic	26/130	不可	あり	不可	不可	不可



表 25 Cisco PDSN リリース 4.0 の AAA アトリビュート

Authorized Flow Profile IDs for the User	26/131	不可	あり	不可	不可	不可
Granted QoS Parameters	26/132	不可	不可	あり	あり	あり
Maximum Per Flow Priority for the User	26/133	不可	あり	不可	不可	不可
FLOW_ID Parameter	26/144	不可	不可	不可	あり	不可
Flow Status	26/145	不可	不可	不可	あり	不可
RSVP Inbound Octet Count	26/162	不可	不可	不可	あり	あり
RSVP Outbound Octet Count	26/163	不可	不可	不可	あり	あり
RSVP Inbound Packet Count	26/164	不可	不可	不可	あり	あり
RSVP Outbound Packet Count	26/165	不可	不可	不可	あり	あり

## VPDN のパケット トランスポート

PDSN は、VPDN パケットのトランスポートをサポートしています。VPDN サービスを提供する場合、モバイル ステーションは、公衆インターネットまたは専用リンクを介して、プライベート リソースに安全にアクセスできます。VPDN トンネルは PDSN/FA からホーム IP ネットワークに接続されます。ホーム IP ネットワークは NAI と関連付けられた IP ネットワークです。

## プロキシ モバイル IP

PMIP を PPP リンク開始の一部として使用することで、モバイル ステーションの代わりに PDSN が HA に登録します。PDSN は HA からアドレスを取得し、PPP 初期化中に IPCP の一部としてそのアドレスをモバイル ステーションに転送します。

## 複数のモバイル IP フロー

PDSN では、各 IP フローが個別に登録している限り（各 IP フローには一意の NAI が必要です）、同じモバイル ステーションから複数の IP アクセス ポイントを使用できます。これで、複数の IP ホストが同じモバイル アクセス デバイス経由で通信し、ネットワークとの 1 つの PPP 接続を共有できます。アカウントिंगのために、PDSN は AAA サーバに対して各フローに個別の使用状況データ レコード (UDR) を生成することが重要です。

## 冗長性とロード バランシング

ここでは、コントローラとメンバー クラスタ モデルでのインテリジェント PDSN 選択およびロード バランシングについて説明します。

## PDSN クラスタ コントローラとメンバー アーキテクチャ

PDSN コントローラ メンバー アーキテクチャは、冗長なアクティブまたはスタンバイ コントローラを備えた 8 つのメンバーをサポートするように設計されていました。このコントローラ メンバー モードは、特定のノードを PDSN 選択の実行、およびグローバル セッション テーブル維持を担当するコント

ローラとして指定します。各メンバー ノードは、そのノードで終了するセッションの情報だけを維持します。コントローラは、すべてのセッション情報をそれぞれの間で同期させて冗長化を図ることができます。これらは、すべてのノードの状態を監視し、メンバーまたは他のコントローラの障害を検出します。

PDSN クラスタがコントローラ メンバー モードで動作している場合、コントローラは PDSN 選択機能専用となり、ベアラ セッションは終了しません。

Cisco PDSN リリース 2.1 は、次の機能強化をサポートします。

- セッション情報のバルクアップデートにより 48 メンバーをサポートするクラスタ スケーラビリティ
- クラスタ処理機能に基づく MSID 向けの条件付きデバッグのサポート
- Controller Show コマンドの機能強化
- クラスタ処理機能に基づく Clear コマンドによるクラスタ処理統計情報のクリア

PCF からアクティブ コントローラに Registration Request (RRQ) が届くと、コントローラは MSID をセッション テーブル検索のインデックスとして使用します。セッション レコード エントリが存在する場合、コントローラは、その MSID のセッションのホストとなっている PDSN に RRQ を転送します。セッション エントリが、コントローラのセッション テーブルに存在しない場合、コントローラは設定された選択アルゴリズムに基づいてメンバーを選択し、メッセージにメンバーの IP アドレスを提案する RRP を PCF に返します。

セッションがアップすると、メンバーはそのセッションのメンバー (MSID) からコントローラに Session-Up メッセージを送信します。メンバーからこのメッセージを受信したコントローラは、コントローラ内でその MSID のセッション レコードを作成し、コントローラで MSID とメンバーの関連付けを確立します。コントローラは、メンバーから Session-Down メッセージを受信すると、コントローラからセッション レコードを消去します。

コントローラは、RRQ をリダイレクトする場合、MSID のセッション レコードを作成しません。セッションが発生したメンバーから Session-Up メッセージを受信した場合だけ作成します。

コントローラ 1 台で大量のメンバー (28 ~ 48) をサポートする場合、メンバーが設定済みの定期的なアップデート間隔ごとに、複数の Session-Up/Session-Down のペアからなる 1 つのバルクアップデート パケットをコントローラに送信すると処理オーバーヘッドが低減されます。パケットでは、1 つの Session-Up/Session-Down フラグで複数の MSID が連結されるため、パケットのバイト数を減らすことができます。コントローラは、これらのバルクアップデート パケットを処理し、バルクアップデート ACK パケットをメンバーに送信します。

#### クラスタ処理機能に基づく条件付きデバッグのサポート

Cisco PDSN リリース 2.0 のクラスタ処理機能では、コントローラとメンバーの両方で次のクラスタ処理デバッグ コマンドを使用した条件付きデバッグのサポートが追加されています。

- `debug cdma pdsn cluster controller message {event | error | packet}`



(注)

コントローラ メンバー モードおよびピアツーピア モードの PDSN を同じクラスタで共存させることはできません。これらは相互に排他的です。

## PDSN コントローラ メンバー クラスタ処理

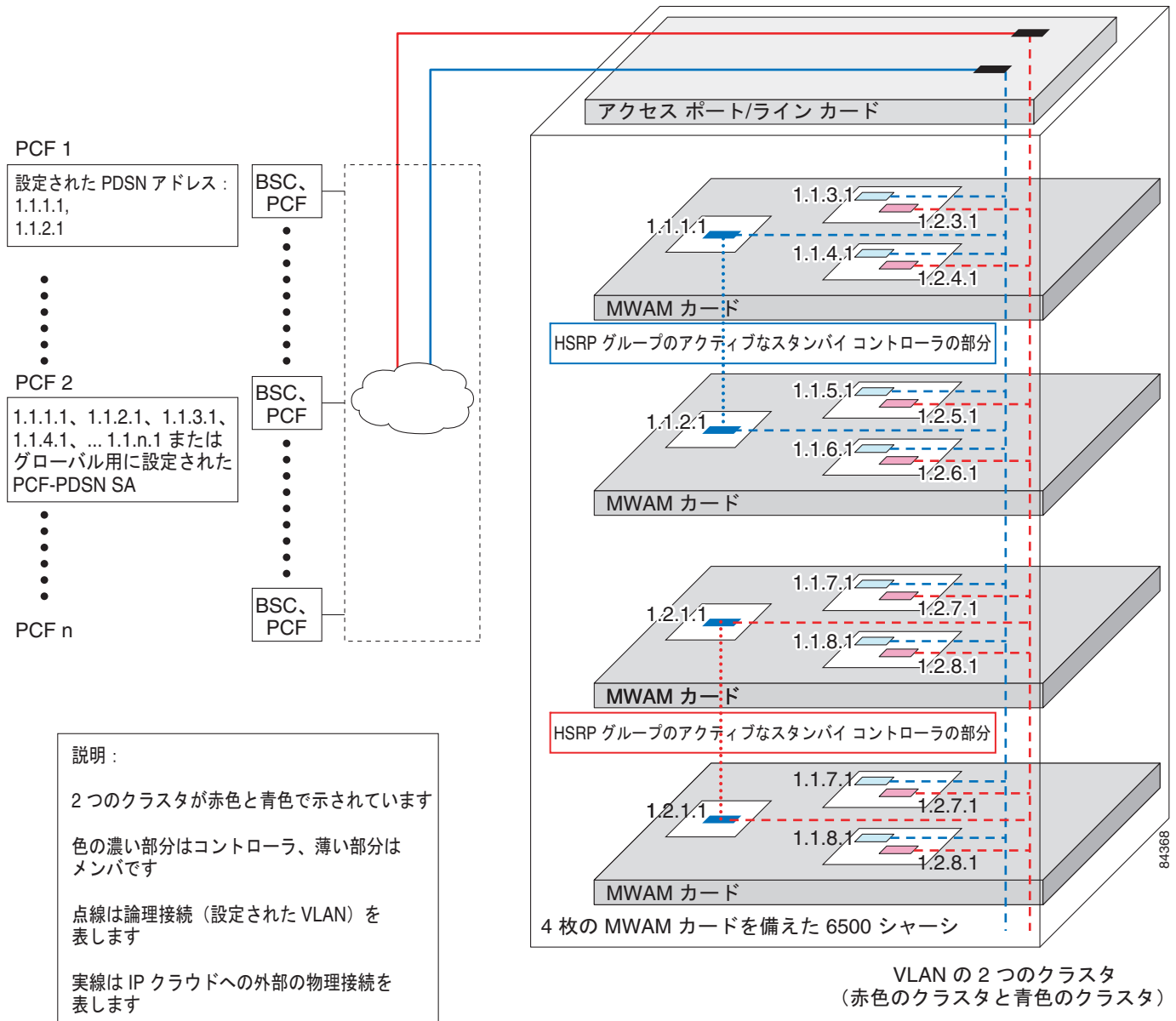
コントローラ メンバー クラスタ処理では、コントローラはクラスタ内の各メンバーの負荷およびセッション (A10 接続など) 情報を維持し、ロードバランシングまたは PDSN 間のハンドオフを回避するようにメンバーを選択します。コントローラは、各メンバーの動作状態を識別し、メンバーまたは他のコントローラの障害を検出します。メンバーは、コントローラに負荷およびセッション情報を通知しません。



(注) 新しい PDSN コントローラ メンバー クラスタ処理機能を使用できるのは、**-c6is-mz** および **-c6ik9s-mz** イメージだけです。

図 7 は、6500 または 7600 ベースの MWAM プラットフォームでのコントローラ メンバー アーキテクチャです。この図は、2つのプライマリ コントローラと2つのバックアップ コントローラを持つ2つの PDSN クラスタ、および対応するメンバーを示しています。

図 7 Catalyst 6500 上の MWAM の PDSN コントローラ メンバー アーキテクチャ



コントローラとして指定された PDSN は、メンバー PDSN の選択とロード バランシングを行います。次に、コントローラの主な機能を説明します。

- コントローラは、すべてのメンバーの負荷情報を維持します。負荷情報は、クラスタ メンバーを探して取得します。メンバーが、セッション開始または終了メッセージ内に設定可能な間隔で負荷値を送信する方法もあります。コントローラは、必要に応じて情報を交換して同期します。
- コントローラが情報を交換するリンクは、HSRP ベースの状態情報交換 (HA 冗長性はこのタイプの実装に基づきます) です。
- アクティブ コントローラおよびメンバーが情報を交換するリンクは、アクティブ コントローラのユニキャスト HSRP アドレスですが、メンバー上で設定する必要があります。
- 実際の PDSN 選択およびロードバランシング手順は、リリース 1.1 の実装と似ていますが、異なるレコード テーブルが使用されます。
- クラスタに追加された新しい PDSN コントローラの自動コンフィギュレーション：新しいコントローラが自動的に設定されるようにし、ルータの HSRP グループのメンバーとして設定する必要があります。この結果、新しいコントローラ (スタンバイ) は、アクティブ コントローラからメンバーおよびセッション レコードを自動的にダウンロードします。アクティブ コントローラは、スタンバイを必要に応じてアップデートして、レコードを同期化します。
- 新しいメンバーがクラスタに追加された場合のコントローラの自動コンフィギュレーション：新しいメンバーはアクティブ コントローラに登録され、アクティブ コントローラがスタンバイ コントローラをアップデートします。
- 冗長性：クラスタのすべてのコントローラは、すべてのメンバーのセッションおよび負荷情報を維持します。こうすることで可用性の冗長性が得られ、コントローラで障害が発生しても、セッションおよびロードバランシング情報は失われません。

## 冗長性

クラスタの冗長性は、1 度に 1 台の PDSN だけで障害が発生することを前提としています。2 つのコントローラが HSRP グループとして設定されています。1 つはアクティブ、もう 1 つはスタンバイです。コントローラには冗長性があり、メンバーはロード シェアリングを行います。

## ロード シェアリング

クラスタ メンバーのロード シェアリングは N+1 スキームです。メンバーで障害が発生すると、確立されたセッションは失われますが、全体的なグループ キャパシティにより、セッションを他のグループ メンバーと再確立できます。さらに、クラスタ メンバーはネットワーク ネイバーである必要はなくなるので、冗長性も向上します。

コントローラはイーサネット リンクを介して情報を交換します。コントローラとメンバーは、ユニキャスト インターフェイス リンクを介して情報を交換します。メンバーはメッセージをコントローラの HSRP グループ アドレスに送信します。PDSN クラスタのメンバーは、ネットワーク ネイバーである必要はありません。IP ネットワークの任意の場所で接続できます。

クラスタへのコントローラの追加は、クラスタでのコントローラの自動コンフィギュレーションにより簡略化されます。これは、HSRP に対して追加コントローラを設定することで可能になります。新しく追加されたコントローラは、自動同期化機能をイネーブルにして、アクティブ コントローラと自動的に同期化されます。同様に、新しいメンバーがクラスタに追加されると、すべてのクラスタ コントローラでメンバーの自動コンフィギュレーションが発生します。

## PDSN クラスタ メンバーの選択

コントローラによるクラスタ メンバーの選択は、*負荷要因*に基づきます。負荷要因は、メンバーに対するセッションの負荷と CPU の負荷によって計算される値です。コントローラは、セッションを最も負荷要因の小さいメンバーに割り当てて、可能な限りデータ接続がクラスタのメンバーに均等に分散するようにします。

ハンドオフを示す A11 Registration Request を受信した場合、セッションにすでにサービスを提供しているメンバーが選択されます。

## ロード バランシング

コントローラは、クラスタのすべてのメンバーの負荷情報を維持して、PDSN クラスタ メンバーを選択します。この負荷情報は、次の条件でメンバーからコントローラに転送されます。

- 定期的に。
- メンバーでセッションが確立または削除されたとき。この場合、定期タイマーは再起動されます。
- コントローラによりメンバーから要求されたとき。

セッションおよびメンバー レコードは、必要に応じてアクティブ コントローラとスタンバイ コントローラの間で同期化されます。アクティブ コントローラとスタンバイ コントローラの両方で、そのクラスタのすべてのメンバーのセッションおよび負荷情報が維持されるので、コントローラで障害が発生しても、それらの情報は失われません。

## Cisco PDSN リリース 1.2 からリリース 2.0 以上へのメンバー PDSN ソフトウェアのアップグレード

メンバー PDSN を Cisco PDSN リリース 2.0 以降にアップグレードするには、次の作業を行います。

- 
- ステップ 1** メンバー PDSN 上で次のコマンドを設定して、メンバー PDSN をクラスタから分離します。
- ```
config# cdma pdsn cluster member prohibit administratively
```
- メンバーのステータスは、メンバーがコントローラに送信する後続の定期的なキープアライブ応答メッセージでコントローラに対してアップデートされます。コントローラは、このメッセージを受信すると、新しい着信コールにこのメンバーを選択しません。
- ステップ 2** 次のコマンドを発行して、管理上禁止されているメンバー PDSN を表示します。
- ```
# show cluster controller member prohibited administratively
```
- すでにメンバーに接続されているコールは、MN がコールを切断するまで接続されたままになります。次のコマンドを使用して、禁止されたメンバーで強制的にコールを切断することもできます。
- ```
# clear cdma pdsn session all
```
- ステップ 3** すべてのコールが切断されたときに、ソフトウェアを Cisco PDSN リリース 2.0 以上にアップグレードするか、PDSN クラスタの動作を中断せずに、このメンバーをシャットダウンします。メンバーがオンラインになったときに、次のコマンドを発行して、クラスタに再び参加させるように設定できます。
- ```
config# no cdma pdsn cluster member prohibit administratively
```
- コントローラでステータスがアップデートされると、新しいメンバー PDSN が新しい着信コールに選択されるようになります。
- ステップ 4** コントローラとメンバー PDSN 間でセッション情報のスケーラブルなバルク同期化メカニズムを使用するには、次のコマンドを設定します。

```
config# cdma pdsn cluster member periodic-update 300
```

## スケーラビリティ

このリリースでは、PDSN は、最大 175,000 のセッションをサポートできる **virtual-access** サブインターフェイス上で PPP セッションを実行できる新しいスケーラビリティ機能を使用します。



(注) **virtual-access** サブインターフェイスを使用する場合、圧縮セッションは最大 20 % (または最大 4000) にする必要があります。



(注) AAA サーバで PDSN を使用している場合は、ユーザ プロファイルにアトリビュート "compression=none" が存在しないことを確認してください。このアトリビュートが存在すると、PDSN は、**virtual-access** サブインターフェイスではなく、完全な **virtual-access** インターフェイスを使用します。



(注) コール セットアップのパフォーマンスを改善するには、**no virtual-template snmp** グローバル設定コマンドを使用します。この設定は、**virtual-access** サブインターフェイスがルータの SNMP 機能に登録されるのを防ぎ、メモリ使用量を低減します。

## ハイ アベイラビリティ

### 概要

ハイ アベイラビリティにより、アクティブ スーパーバイザ エンジンで障害が発生した場合のスタンバイ スーパーバイザ エンジンへのスイッチオーバー時間を最小限に抑えることができます。

この機能以前は、高速スイッチオーバーにより、スタンバイ スーパーバイザ エンジンへの迅速なスイッチオーバーが可能でした。しかし、高速スイッチオーバーでは、スイッチオーバー前のスイッチ機能の状態が不明なため、スタンバイ スーパーバイザ エンジンがアクティブになったときに、すべてのスイッチ機能を再初期化および再起動する必要があります。

ハイ アベイラビリティではこの制約が取り除かれ、アクティブ スーパーバイザ エンジンはスタンバイ スーパーバイザ エンジンと通信し、機能プロトコルの状態を常に同期化できます。スーパーバイザ エンジン間の同期化により、スタンバイ スーパーバイザ エンジンは障害発生時にアクティブの役割を引き継ぐことができます。

さらに、ハイ アベイラビリティには、アクティブおよびスタンバイのスーパーバイザ エンジンで異なるソフトウェア イメージを実行できるバージョンニング オプションがあります。

ハイ アベイラビリティのために、システム データベースはアクティブ スーパーバイザ エンジンで維持され、システム データベースでデータが変更されると、アップデートがスタンバイ スーパーバイザ エンジンに送信されます。アクティブ スーパーバイザ エンジンは、状態が変化するとスタンバイ スーパーバイザ エンジンと通信してアップデートし、スタンバイ スーパーバイザ エンジンがサポートされている機能について現在のプロトコルの状態を認識できるようにします。スタンバイ スーパーバイザ エンジンは、すべてのモジュール、ポート、および VLAN について現在のプロトコルの状態を把握します。プロトコルをこの状態情報で初期化し、即座に実行できます。

アクティブ スーパーバイザ エンジンはシステム バス（バックプレーン）を制御し、ネットワークとの間でパケットを送受信し、すべてのモジュールを制御します。プロトコルが動作するのは、アクティブ スーパーバイザ エンジンだけです。

スタンバイ スーパーバイザ エンジンはシステム バスから分離され、パケットを交換しません。ただし、スイッチング バスからパケットを受信して、レイヤ 2 で切り替えられるフロー用のレイヤ 2 転送テーブルを学習し、テーブルに挿入します。また、スタンバイ スーパーバイザ エンジンは、スイッチング バスからパケットを受信して、レイヤ 3 で切り替えられるフロー用のマルチレイヤ スwitching (MLS) テーブルを学習し、テーブルに挿入します。スタンバイ スーパーバイザ エンジンは、パケットの転送には関与せず、どのモジュールとも通信しません。

スタンバイ スーパーバイザ エンジンの実行中にハイ アベイラビリティをイネーブルにすると、イメージバージョンの互換性がチェックされ、互換性が確認されると、データベースの同期化が開始されます。ハイ アベイラビリティの互換機能は、スイッチオーバー後、スタンバイ スーパーバイザ エンジンの保存済みの状態から継続されます。

ハイ アベイラビリティをディセーブルにすると、データベースの同期化は実行されず、スイッチオーバー後にスタンバイ スーパーバイザ エンジンですべての機能を再起動する必要があります。

ハイ アベイラビリティをイネーブルからディセーブルの状態に変更すると、アクティブ スーパーバイザ エンジンからの同期化が停止し、スタンバイ スーパーバイザ エンジンは現在の同期化データをすべて破棄します。

ハイ アベイラビリティをディセーブルからイネーブルの状態に変更すると、アクティブからスタンバイ スーパーバイザ エンジンへの同期化が開始されます（スタンバイ スーパーバイザ エンジンが存在し、イメージバージョンの互換性がある場合）。

NVRAM 同期化は、ハイ アベイラビリティがイネーブルかどうかに関係なく発生します（2 つのスーパーバイザ エンジンに互換性のある NVRAM バージョンがある場合）。

システムの起動中にスタンバイ スーパーバイザ エンジンをインストールしなかった場合、アクティブ スーパーバイザ エンジンはこれを検出し、同期化のためのデータベース アップデートはキューに入れられません。同様に、スタンバイ スーパーバイザ エンジンをリセットまたは削除すると、同期のアップデートはキューに入れられず、同期キューの保留中のアップデートは破棄されます。スタンバイ スーパーバイザ エンジンとなる 2 番目のスーパーバイザ エンジンを挿入または再起動すると、アクティブ スーパーバイザ エンジンはシステム データベース全体をスタンバイ スーパーバイザ エンジンにダウンロードします。このグローバルな同期化が完了した場合だけ、アクティブ スーパーバイザ エンジンは、スタンバイ スーパーバイザ エンジンへの個々のアップデートをキューに入れ、同期化します。



(注)

2 番目のスーパーバイザ エンジンをホット インサートまたは再起動する場合、グローバルな同期化が完了するまで数分かかることがあります。

設定の詳細を含むハイ アベイラビリティの詳細および電源管理の詳細については、「PDSN コントローラ メンバー クラスタ処理」のセクションと次の URL にあるマニュアルを参照してください。

- 『Catalyst 6500 Series Software Configuration Guide』(6.1.1a)。特に次の冗長性の設定に関する章を参照してください。
  - [http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft\\_6\\_1/configgd/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sft_6_1/configgd/index.htm)
- 『Catalyst 6000 Family IOS Software Configuration Guide, Release 12.2(9)YO』
  - <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122yo/swcg/supcfg.htm>
  - [http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122yo/swcg/pwr\\_envr.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122yo/swcg/pwr_envr.htm)

## 関連機能およびテクノロジー

- MIP
- Point-to-Point Protocol (PPP; ポイントツーポイント プロトコル)
- Authentication, Authorization and Accounting (AAA; 認証、認可、アカウントリング)
- L2TP を使用した Virtual Private Data Network (VPDN; バーチャル プライベート ダイアルアップ ネットワーク)
- Remote Authentication Dial-In User Service (RADIUS)

## 関連マニュアル

Cisco PDSN リリース 2.1 ソフトウェアの詳細については、*Cisco IOS リリース 12.3 (11) YF の Cisco PDSN 2.1 の機能に関するリリース ノート*を参照してください。

その他の参考資料は次のとおりです。

- MWAM ハードウェアおよびソフトウェアの情報については、『*Cisco Multi-processor WAN Application Module Installation and Configuration Note*』
- このマニュアルに含まれている IP セキュリティ設定コマンドについては、『*Cisco IOS Security Configuration Guide*』の IPSec と暗号化のセクション
- このマニュアルに含まれている AAA サーバの設定コマンドについては、Cisco IOS リリース 12.3 マニュアル モジュール『*Cisco IOS Security Command Reference*』と『*Cisco IOS Security Configuration Guide*』
- このマニュアルに含まれている PPP および RADIUS 設定コマンドについては、Cisco IOS リリース 12.3 マニュアル モジュール『*Cisco IOS Dial Services Command Reference*』
- MIP については、Cisco リリース 12.3 マニュアル モジュール『*Cisco IOS IP Command Reference*』および『*Cisco IOS IP Configuration Guide*』
- バーチャル プライベート ネットワークについては、Cisco リリース 12.3 マニュアル モジュール『*Cisco IOS Dial Services Configuration Guide, Network Services*』および『*Cisco IOS Dial Services Command Reference*』

## サポート対象プラットフォーム

Cisco PDSN 4.0 リリースは、Cisco 6500 Catalyst スイッチと 7600 シリーズ ルータ、および Cisco NPE-G1 ルータ上の SAMI カード用 Cisco IOS 12.4 で開発された特別リリースです。

Cisco PDSN リリース 4.0 には、2 GB メモリ付き SAMI カードを推奨します。サポート対象のプラットフォームの詳細については、*Cisco IOS リリース 12.4 (15) xx の Cisco PDSN 4.0 Feature リリース ノート*を参照してください。

## サポート対象の規格、MIB、および RFC

### 規格

- TIA/EIA/IS-835-B。ワイヤレス IP ネットワーク規格



- TIA/EIA/IS-2001-B。CDMA 2000 アクセス ネットワーク インターフェイスの相互運用性仕様 (IOS) (3GPP2 TSG-A、TR45.4 と呼ばれる)
- TIA/EIA/TSB-115。IETF プロトコルに基づくワイヤレス IP ネットワーク アーキテクチャ

## MIB

- CISCO\_CDMA\_PDSN\_MIB.my
- CISCO\_PROCESS\_MIB.my
- CISCO\_MOBILE\_IP\_MIB.my
- CISCO\_AHDLC\_MIB.my
- CISCO\_AAA\_CLIENT\_MIB.my
- CISCO\_AAA\_SERVER\_MIB.my
- CISCO\_VPDN\_MGMT\_MIB.my
- CISCO\_VPDN\_MGMT\_EXT\_MIB.my

サポートされる MIB および MIB の使用方法については、CCO の Cisco MIB Web サイト <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml> を参照してください。

## RFC

- *Internet Protocol* (インターネット プロトコル)、RFC 791
- *Compressing TCP/IP Headers for Low-speed Serial Links* (低速シリアル リンク用 TCP/IP ヘッダーの圧縮)、RFC 1144
- *The PPP Internet Protocol Control Protocol (IPCP)* (PPP インターネット プロトコル制御プロトコル (IPCF))、RFC 1332
- *PPP Authentication Protocols* (PPP 認証プロトコル)、RFC 1334
- *The Point-to-Point Protocol (PPP)* (ポイントツーポイント プロトコル (PPP))、RFC 1661
- *PPP in HDLC-like Framing* (HDLC 式フレーム構成での PPP)、RFC 1662
- *The PPP Internet Protocol Control Protocol (CCP)* (PPP インターネット プロトコル制御プロトコル (CCP))、RFC 1962
- *PPP Stac LZS Compression Protocol* (PPP Stac LZS 圧縮プロトコル)、RFC 1974
- *PPP Challenge Handshake Authentication Protocol (CHAP)* (PPP チャレンジ ハンドシェイク 認証プロトコル (CHAP))、RFC 1994
- *IP Mobility Support* (IP モビリティ サポート)、RFC 2002
- *IP Encapsulation within IP* (IP 内 IP カプセル化)、RFC 2003
- *Applicability Statement for IP Mobility Support* (IP モバイル サポートの適用可能文)、RFC 2005
- *The Definitions of Managed Objects for IP Mobility Support Using SMIPv2* (SMIPv2 を使用する IP モバイル サポートの管理対象オブジェクト定義)、RFC 2006
- *Microsoft Point-To-Point Compression (MPPC) Protocol* (Microsoft ポイントツーポイント圧縮 (MPPC) プロトコル)、RFC 2118
- *Reverse Tunneling for Mobile IP* (モバイル IP のリバース トンネリング)、RFC 2344
- *Security Architecture for the Internet Protocol* (インターネット プロトコルのセキュリティ アーキテクチャ)、RFC 2401
- *IP Authentication Header* (PPP 認証ヘッダー)、RFC 2402

- *IP Encapsulating Security Payload (ESP)* (*IP カプセル化セキュリティ ペイロード (ESP)*)、RFC 2406
- *Mobile IPv4 Challenge/Response Extensions* (*Mobile IPv4 チャレンジ/ レスポンス機能拡張*)、RFC 3012

## 設定作業

ここでは、MWAM プラットフォームで Cisco PDSN ソフトウェアを設定する手順について説明します。MWAM アプリケーションカードで PDSN のインスタンスを設定する前に、ベースとなる Catalyst 6500 または 7600 の設定を作成する必要があります。詳細については、『Cisco *Multi-processor WAN Application Module Installation and Configuration Note*』を参照してください。

## システム要件

ここでは、Cisco IOS リリース 12.4(15)XR1 のシステム要件について説明します。

- 「メモリ要件」 (P.258)
- 「サポートされるハードウェア」 (P.258)
- 「ソフトウェアの互換性」 (P.259)
- 「ソフトウェア バージョンの判断」 (P.259)
- 「PDSN イメージの設定」 (P.260)
- 「PDSN セッション冗長性インフラストラクチャの設定」 (P.264)

## メモリ要件

表 26 に、Cisco 7600 シリーズ ルータで SAMI カードをサポートする PDSN ソフトウェア機能セットのメモリ要件を示します。表では、IP 標準機能セット (PDSN 用) のメモリ要件も示します。

表 26 Cisco 7600 シリーズ ルータ上の SAMI ブレードのメモリ要件

プラットフォーム	ソフトウェア機能セット	イメージ名	必要なフラッシュメモリ	必要な DRAM メモリ	実行元
Cisco 7600 シリーズ ルータ	PDSN ソフトウェア機能セット	12.4(15)XR-c7svcsami-c6ik9s-mz.124-15.XR (これはバンドル イメージです)	128 MB	2048 MB	RAM

## サポートされるハードウェア

Cisco IOS リリース 12.4(15)XR1 は、Cisco 7600 シリーズ ルータ上の SAMI カード用に最適化されています。

CCO アカウントを持つユーザは、Cisco.com でハードウェアとソフトウェアの互換性マトリクスを使用できます。このマトリクスに Cisco プラットフォームと IOS リリースを入力して、サポートされているハードウェア コンポーネントを検索できます。ハードウェアとソフトウェアの互換性マトリクス ツールは次の URL からアクセスできます。

<http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswwmatrix.cgi>

Cisco PDSN 4.0 リリースは、Cisco 7600 シリーズ ルータおよび Cisco NPE-G1 ルータ上の SAMI カード用 Cisco IOS 12.4 で開発された特別リリースです。

Cisco PDSN リリース 4.0 には、2 GB メモリ付き SAMI カードを推奨します。

ユーザの移行用に、SAMI 上のプロセッサの 1 つは、PDDSN アプリケーションのホストとなるアクティブ MWAM プロセッサのスタンバイとして機能する必要があります。システムの同期化を行って、スタンバイ SAMI プロセッサがアクティブ MWAM プロセッサからすべてのセッションおよびフロー情報を取得するようにしてください。ユーザの移行用に、MWAM ブレードの 6 番目のプロセッサは同期化に使用されないため、プロセッサから見ると相関は 5 対 5 となります。同期の完了後、スイッチ オーバーを実行し、アクティブ MWAM をオフラインにします。SAMI がアクティブとなり、データが失われることなく、ユーザ セッションが保持されます。

SAMI と HSRP を MWAM のスタンバイとなるように設定する手順は、MWAM の冗長性に関連する手順と似ています。

ハードウェアとソフトウェアの互換性マトリクスは、CCO ログイン アカウントを持つユーザが CCO 上で使用できます。このマトリクスに Cisco プラットフォームと IOS リリースを入力して、サポートされているハードウェア コンポーネントを検索できます。ハードウェアとソフトウェアの互換性マトリクス ツールは次の URL から入手できます。

<http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswwmatrix.cgi>

## ソフトウェアの互換性

Cisco IOS リリース 12.4(15)XR1 は、Cisco IOS リリース 12.4 で開発された特別なリリースです。

Cisco IOS リリース 12.4(15)XR1 では Cisco IOS リリース 12.4 と同じ機能がサポートされ、PDSN 機能が付属しています。

## ソフトウェア バージョンの判断

ルータで実行する Cisco IOS ソフトウェアのバージョンを判断するには、ルータにログインし、次のように **show version EXEC** コマンドを入力します。

```
Router# show version
Cisco IOS Software, MWAM Software (MWAM-C6IS-M), Version 12.4(15)XN , RELEASE SOFTWARE
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 11-Dec-07 15:44 by jsomiram
```

```
ROM: System Bootstrap, Version 12.2(11)YS2 RELEASE SOFTWARE
```

```
PDSN-S2000-BAL uptime is 4 minutes
System returned to ROM by bus error at PC 0x2033D804, address 0x283 at 06:56:44 PDT Mon
Dec 3 2007
System restarted at 03:29:24 PDT Tue Dec 11 2007
System image file is "svcmwam-c6is-mz.xn"
```

```
Cisco MWAM (MWAM) processor with 997376K/32768K bytes of memory.
SB-1 CPU at 700MHz, Implementation 1025, Rev 0.2
```

```
Last reset from power-on
```

```
1 Gigabit Ethernet interface
511K bytes of non-volatile configuration memory.

Configuration register is 0x4

Router#
```

## 新しいソフトウェア リリースへのアップグレード

新しいソフトウェア リリースへのアップグレードの詳細については、次の URL にある製品速報『Cisco IOS Software Upgrade Ordering Instructions』を参照してください。

[http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957\\_pp.htm](http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm)

## PDSN イメージの設定

PDSN では、4つのクラスのユーザ サービス（SIP、VPDN を使用した SIP、MIP、および PMIP）を提供できます。ここでは、PDSN を実装するための設定作業について説明します。作業の各カテゴリでは、その作業がオプションであるのか、必須かどうかを示します。

### R-P インターフェイスの設定作業（すべてのクラスのユーザ サービスで必要）

次の作業では R-P インターフェイス（A10/A11 インターフェイスとも呼ばれる）を設定します。

R-P インターフェイスを設定するには、次の作業を実行します。

- 「PDSN サービスのイネーブル化」
- 「CDMA Ix インターフェイスの作成」
- 「ループバック インターフェイスの作成」
- 「バーチャル テンプレート インターフェイスの作成と PDSN アプリケーションへのアソシエート」
- 「R-P インターフェイス シグナリングのイネーブル化」

### ユーザ セッションの設定作業（オプション）

ユーザ セッションを設定するには、次の作業を実行します。

- 「ユーザ セッション パラメータの設定」

### セッションの冗長性設定作業

PDSN でセッションの冗長性を設定するには、次の作業を実行します。

- 「HSRP の設定」
- 「HSRP の有効化と HSRP マスター グループの設定」
- 「follow グループの設定」
- 「デバイス間冗長性の有効化」
- 「デバイス間通信トランスポートの設定」
- 「PDSN-AAA サーバ インターフェイスのループバック インターフェイスの使用」

### AAA および RADIUS の設定作業（すべてのシナリオで必須）

PDSN 環境で AAA サーバと RADIUS を設定するには、次の作業を実行します。

- 「PDSN 環境での AAA サーバの設定」

- 「PDSN 環境での RADIUS の設定」

#### 前払いの設定作業

- 「PDSN 環境での前払いの設定」

#### VPDN の設定作業（VPDN で 簡易 IP を使用するシナリオの場合に必須）

PDSN 環境で VPDN を設定するには、次の作業を実行します。

- 「PDSN 環境での VPDN の有効化」

#### モバイル IP の設定作業（モバイル IP には必須）

PDSN 上に MIP を設定するには、次の作業を実行します。

- 「モバイル IP FA の設定」
- 「モバイル IP SA の設定」
- 「ネットワーク管理のイネーブル化」

#### PDSN 選択の設定作業（オプション）

PDSN の選択を設定するには、次の作業を実行します。

- 「PDSN のクラスタ コントローラの設定」
- 「PDSN のクラスタ メンバーの設定」

#### ネットワーク管理の設定作業（すべてのシナリオのネットワーク管理で必須）

ネットワーク管理を設定するには、次の作業を実行します。

- 「ネットワーク管理のイネーブル化」

#### その他の設定作業

PDSN では次の作業はオプションです。

- 「常時接続サービスの設定」
- 「A11 セッションのアップデートの設定」
- 「SDB インジケータ マーキングの設定」
- 「PPP コントロール パケットの SDB インジケータ マーキングの設定」
- 「PDSN での PoD の設定」
- 「PDSN でのモバイル IP リソース失効の設定」
- 「(注) 実行する作業には、VPDN の設定作業、Layer 2 Tunneling Protocol (L2TP; レイヤ 2 トンネリングプロトコル) のトンネル設定作業、およびロード バランシングの設定作業もあります。特定の情報の詳細については、適切なマニュアルを参照してください。」
- 「ショート データ バースト フラグの設定」
- 「PDSN アカウンティング イベントの設定」
- 「CDMA RADIUS アトリビュートの設定」

#### チューニング、検証、およびモニタリング作業（オプション）

PDSN 要素のチューニング、検証、およびモニタリングを行うには、次の作業を実行します。

- 「PDSN のモニタリングとメンテナンス」

## PDSN サービスのイネーブル化

PDSN サービスをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>service cdma pdsn</b>	PDSN サービスをイネーブルにします。

## CDMA Ix インターフェイスの作成

CDMA Ix インターフェイスを作成するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>interface cdma-Ix1</b>	R-P インターフェイスに CDMA 仮想インターフェイスを定義します。
Router(config-if)# <b>ip address ip-address mask</b>	CDMA-Ix 仮想インターフェイスに IP アドレスとマスクを割り当てます。この IP アドレスは RAN が PDSN と通信する場合に使用されます。

## ループバック インターフェイスの作成

仮想テンプレートに直接 IP アドレスを設定するのではなく、ループバック インターフェイスを作成してから、そのループバック インターフェイスの IP アドレスを仮想テンプレートに関連付けることをお勧めします。

ループバック インターフェイスを作成するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>interface loopback number</b>	ループバック インターフェイスを作成します。ループバック インターフェイスは、常にアップしている仮想インターフェイスです。
Router(config-if)# <b>ip address ip-address mask</b>	IP アドレスをループバック インターフェイスに割り当てます。

## バーチャル テンプレート インターフェイスの作成と PDSN アプリケーションへのアソシエート

バーチャル テンプレート インターフェイスを作成すると、インターフェイスを設定して、その設定を動的に適用できます。

動的に作成して適用できるバーチャル テンプレート インターフェイスを作成するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>interface virtual-template number</b>	バーチャル テンプレート インターフェイスを作成します。
Router(config-if)# <b>ip unnumbered loopback number</b>	前に定義したループバック IP アドレスをバーチャル テンプレート インターフェイスに割り当てます。
Router(config-if)# <b>ppp authentication chap pap optional</b>	PPP 認証をイネーブルにします。

コマンド	目的
Router(config-if)# <b>ppp accounting none</b>	PPP アカウンティングをディセーブルにして 3GPP2 アカウンティングをイネーブルにします。
Router(config-if)# <b>ppp accm 0</b>	ACCM テーブルの値の送信を指定します。値には 0 を指定する必要があります。
Router(config-if)# <b>ppp timeout idle value</b>	PPP アイドル タイムアウトを指定します。
Router(config-if)# <b>exit</b>	インターフェイス コンフィギュレーション モードを終了します。
Router(config)# <b>cdma pdsn virtual-template virtual-template-num</b>	バーチャル テンプレートと PDSN アプリケーションをアソシエートします。

## R-P インターフェイス シグナリングのイネーブル化

R-P インターフェイス シグナリングをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>cdma pdsn secure pcf lower_addr [upper_addr] spi {spi_val   [inbound in_spi_val outbound out_spi_val]} key {ascii   hex} string</b>	PDSN に PCF セキュリティ アソシエーションを定義します。
Router(config)# <b>cdma pdsn a10 max-lifetime seconds</b>	PCF からの A11 レジストレーション要求で PDSN が受け入れる最大ライフタイムを指定します。
Router(config)# <b>cdma pdsn a10 gre sequencing</b>	A10 インターフェイスの発信パケットで、セッションごとの Generic Routing Encapsulation (GRE) のシーケンス番号の組み込みをイネーブルにします (これはデフォルト設定です)。
Router(config)# <b>cdma pdsn retransmit all-update number</b>	A11 レジストレーションのアップデートメッセージを再送信する最大回数を指定します。
Router(config)# <b>cdma pdsn timeout all-update seconds</b>	A11 レジストレーションのアップデートメッセージのタイムアウト値を指定します。
Router(config)# <b>cdma pdsn maximum pcf number</b>	PDSN に一度に接続できる Packet Control Function (PCF ; パケット制御機能) の最大数を指定します。

## ユーザ セッション パラメータの設定

ユーザ セッション パラメータを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>cdma pdsn maximum sessions maxsessions</b>	PDSN で使用できるモバイルセッションの最大数を指定します。
Router(config)# <b>cdma pdsn ingress-address-filtering</b>	入力アドレス フィルタリングをイネーブルにします。
Router(config)# <b>cdma pdsn msid-authentication [imsi number] [min number] [irm number] [profile-password password]</b>	MSID に基づいた認証を使用して、SIP サービスのプロビジョニングをイネーブルにします。
Router(config)# <b>cdma pdsn timeout mobile-ip-registration timeout</b>	PPP 認証を省略するユーザに対して MIP レジストレーションを実行するまでの秒数を指定します。

## PDSN セッション冗長性インフラストラクチャの設定

PDSN-SR 機能は、Cisco IOS Check-point Facility (CF) を使用して、ステートフル データを Stream Control Transmission Protocol (SCTP) を通じて冗長 PDSN へ送信します。さらに、Cisco IOS HSRP と共に、PDSN は Cisco IOS Redundancy Facility (RF) を使用してアクティブ PDSN とスタンバイ PDSN のトランシジョンを監視、報告します。

PDSN-SR を設定する前に、デバイス間冗長性インフラストラクチャを設定する必要があります。

### HSRP の設定

HSRP で、IP トラフィックを単一ルータの可用性に依存せず、ネットワーク上のホストからルーティングするため、高いネットワーク可用性を実現できます。HSRP は、アクティブなルータやスタンバイのルータを選択する際に、ルータのグループで使用されます。インターフェイスのいずれかがダウンした場合にデバイス全体がダウンしたと見なされ、スタンバイのデバイスがアクティブになってアクティブなデバイスの役割を引き継げるよう、HSRP は内部と外部両方のインターフェイスを監視します。

HSRP の設定の際は、次の推奨事項と制約事項が適用されることに注意してください。

- 少なくとも、HSRP を有効にし、1 つの PDSN インスタンスに対し 1 つのインターフェイスで定義された HSRP 「master」 グループである必要があります。「follow」グループは、すべての他の PDSN インターフェイスで、**follow** キーワード オプションを指定した **standby** インターフェイス設定コマンドを使用して設定できます。follow グループを使用することにより、次の利点があります。
  - follow グループ機能は、master グループの HSRP パラメータを共有するよう設定されているすべてのインターフェイスで有効です。
  - 同じグループを共有しているインターフェイスは、マスター インターフェイスの状態に従い、マスター インターフェイスと同じプライオリティを使用します。これにより、すべてのインターフェイスが必ず同じ HSRP 状態になります。それ以外の場合、マスター HSRP インターフェイスではなく別のロールと見なされるインターフェイスが 1 つまたは複数ある可能性があります。
  - これにより、大規模な設定の場合に、HSRP グループの数を最適化し、設定と管理のオーバーヘッドを最小限に抑えます。
  - 設定されている場合、不必要なネットワーク トラフィックを、HSRP Hello メッセージを follow グループから削除することで、インターフェイス全体から除外します。



(注)

スタンバイ PDSN で、**standby preempt** インターフェイス設定コマンドを使用してプリエンプト遅延を設定しないでください。

- 最適化のため、ブリッジやゲートウェイの仮想 MAC アドレスの学習を許可する目的で **standby use-bia** コマンドを使用しない場合、メイン インターフェイス (gig0/0) で **standby mac-refresh** コマンドにデフォルトより大きな値 (hello メッセージは 10 秒ごとに送信されます) を設定します。この値は、hello メッセージの送信間隔に使用されます。



(注)

**standby use-bia** が設定されている場合、follow グループのインターフェイス以外で hello メッセージが送信されることはありません。明らかに設定する必要がない場合以外は、**standby use-bia** を使用することをお勧めします。



- ARP マルチキャスト パケットは、アクティブに変わった HSRP 状態がある場合に送信されます。follow グループの仮想 IP アドレス に対する ARP 要求には、HSRP 状態がアクティブの場合に応答します。また、ARP マルチキャストは、スレーブ仮想 IP アドレスの設定時で、master グループがアクティブの場合に follow グループの VLAN で送信されます。

各 PDSN follow グループと同じグループ番号を、プライマリ グループで定義した番号のまま使用してください。プライマリ グループと follow グループで同じグループ番号を使用すると、多数の PDSN インターフェイスと HSRP グループがある環境で、HSRP グループを簡単に設定やメンテナンスできます。

HSRP 設定と HSRP グループの詳細情報については、次の URL を参照してください：

[http://www.cisco.com/en/US/partner/tech/tk648/tk362/tk321/tsd\\_technology\\_support\\_sub-protocol\\_home.html](http://www.cisco.com/en/US/partner/tech/tk648/tk362/tk321/tsd_technology_support_sub-protocol_home.html)

および

[http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies\\_configuration\\_example09186a0080094e90.shtml](http://www.cisco.com/en/US/partner/tech/tk648/tk362/technologies_configuration_example09186a0080094e90.shtml)

## HSRP の有効化と HSRP マスター グループの設定

インターフェイスで HSRP を有効にし、プライマリ グループを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config-if)# <b>standby</b> [group-number] ip [ip-address [secondary]]	インターフェイスで HSRP を有効にします。
Router(config-if)# <b>standby</b> [group-number] priority priority	アクティブ ルータの選択に使用するホットスタンバイ プライオリティを設定します。プライオリティ値の範囲は 1 ~ 255 です。1 はプライオリティが最低、255 は最高を表します。ローカルなルータのプライオリティが、現在のアクティブなルータよりも高い場合、ローカルなルータがアクティブなルータの代わりになるよう指定してください。
Router(config-if)# <b>standby</b> [group-number] name name	スタンバイ グループの名前を指定します。
Router(config-if)# <b>standby use-bia</b> [scope interface]	(オプション) HSRP を、割り当て済みの MAC アドレスの代わりに仮想 MAC アドレスとしてインターフェイスのバーンドイン アドレスを使用するよう設定します。

## follow グループの設定

HSRP follow グループを、follow キーワード オプションが指定された standby インターフェイス設定コマンドを使用してインターフェイスの follow グループを定義することにより、プライマリ グループの HSRP パラメータを共有するよう設定します。グループ トラッキング状態を共有し、同じプライオリティを持つインターフェイスです。

インターフェイスがプライマリ グループに従うように設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config-if)# <b>standby</b> group-number <b>follow</b> group-name	follow グループの番号と、 <b>follow</b> および共有ステータスに対するプライマリ グループの名前を指定します。 <b>(注)</b> 指定されたグループ番号をプライマリ グループ番号と同じにすることをお勧めします。
Router(config-if)# <b>standby</b> group-number ip virtual-ip-address	follow グループのグループ番号と仮想 IP アドレスを指定します。 <b>(注)</b> 上記で指定されたグループ番号は、マスターグループ番号と同じである必要があります。

### デバイス間冗長性のイネーブル化

デバイス間冗長性をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>redundancy inter-device</b>	冗長性が設定され、デバイス間設定モードになります。すべてのデバイス間設定を削除するには、このコマンドの <b>no</b> フォームを使用します。
Router(config-red-interdevice)# <b>scheme standby</b> standby-group-name	使用する冗長性スキームを定義します。現在、サポートされるスキームは <b>standby</b> のみです。 <i>standby-group-name</i> は <b>standby name</b> インターフェイス設定コマンドで指定されたスタンバイ名と一致する必要があります（「HSRP の設定」の項を参照してください）。また、スタンバイ名は両方の PDSN で同じでなければなりません。
Router(config-red-interdevice)# <b>exit</b>	グローバル コンフィギュレーション モードに戻ります。

### デバイス間通信トランスポートの設定

デバイス間の冗長性には、冗長 PDSN 間の通信を行うトランスポートが必要です。このトランスポートは、Interprocess Communication (IPC) コマンドを使用して設定します。

デバイス間通信トランスポートを、2つの PDSN 間で設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>ipc zone default</b>	Inter-device Communication Protocol (IPC) を設定し、IPC ゾーン コンフィギュレーション モードにします。 アクティブなデバイスとスタンバイのデバイス間の通信リンクを開始するには、このコマンドを使用します。
Router(config-ipczone)# <b>association 1</b>	2つのデバイスのアソシエーションを設定し、IPC アソシエーション コンフィギュレーション モードにします。 IPC アソシエーション コンフィギュレーション モードで、トランスポート プロトコル、ローカル ポート、ローカル IP アドレス、リモート ポートとリモート IP アドレスなどのアソシエーションの詳細を設定します。 有効なアソシエーション ID の範囲は 1 ~ 255 です。デフォルト値はありません。
Router(config-ipczone)# <b>no shutdown</b>	無効なアソシエーションと関連するトランスポート プロトコルを再起動します。 <b>(注)</b> トランスポート プロトコル パラメータを変更した場合はアソシエーションのシャットダウンが必要です。
Router(config-ipczone-assoc)# <b>protocol sctp</b>	Stream Control Transmission Protocol (SCTP) をこのアソシエーションのトランスポート プロトコルとして設定し、SCTP プロトコル設定モードを有効にします。
Router(config-ipc-protocol-sctp)# <b>local-port local_port_num</b>	冗長ピアとの通信に使用するローカル SCTP ポート番号を定義し、IPC トランスポート-SCTP ローカル設定モードを有効にします。 有効なポート番号の範囲は 1 ~ 65535 です。デフォルト値はありません。 <b>(注)</b> ローカル ポート番号は、ピア ルータのリモート ポート番号と一致する必要があります。
Router(config-ipc-protocol-sctp)# <b>unit1-port port_num</b>	自動同期機能が有効である場合は、SCTP ポートを設定します。
Router(config-ipc-local-sctp)# <b>local ip ip_addr</b>	冗長ピアと通信するローカル IP アドレスを定義します。ローカル IP アドレスは、ピア ルータのリモート IP アドレスと一致する必要があります。
Router(config-ipc-unit1-sctp)# <b>unit1-ip ip_addr</b>	自動同期機能が有効である場合に、冗長ピアと通信する IP アドレスを表します。

コマンド	目的
Router(config-ipc-local-sctp)# <b>keepalive</b> [period [retries]]	<p>キープアライブ パケットを有効にし、インターフェイスまたは特定のインターフェイスのトンネル プロトコルが停止する前に Cisco IOS ソフトウェアがキープアライブ パケットを応答つきで送信を試みる回数を指定します。</p> <p>この回数の有効値は 0 より大きい整数で、秒単位です。デフォルトは 10 です。リトライの有効値は 1 より大きく 355 より小さい整数です。デフォルトは、事前に使用した値です。事前に値を指定していない場合は、5 になります。</p>
Router(config-ipc-local-sctp)# <b>retransmit-timeout interval</b>	<p>メッセージ再送信時間を設定します。</p> <p>有効範囲は 300 ~ 60000 ミリ秒です。最小値のデフォルトは 1000 です。最大値のデフォルトは 60000 です。</p>
Router(config-ipc-local-sctp)# <b>path-retransmit number</b>	<p>対応する宛先アドレスが非アクティブになる前のキープアライブ リトライの最大回数を設定します。</p> <p>有効範囲は 2 ~ 10 です。デフォルトは 5 です。</p>
Router(config-ipc-local-sctp)# <b>assoc-retransmit number</b>	<p>アソシエーションが失敗を宣言する前の、宛先アドレスすべてへの再送信の最大回数を定義します。</p> <p>有効範囲は 2 ~ 20 です。デフォルトは 10 です。</p>
Router(config-ipc-local-sctp)# <b>exit</b>	<p>IPC トランスポート - SCTP ローカル設定モードを終了します。</p>
Router(config-ipc-protocol-sctp)# <b>remote-port port_num</b>	<p>冗長ピアと通信するリモート SCTP ポート番号を定義し、IPC トランスポート -SCTP リモート コンフィギュレーションモードを有効にします。</p> <p>有効なポート番号の範囲は 1 ~ 65535 です。デフォルトはありません。</p> <p>(注) リモート ポート番号は、ピア デバイスのローカル ポート番号と一致する必要があります。</p>
config-ipc-protocol-sctp)# <b>unit2-port port_num</b>	<p>自動同期機能が有効である場合に、unit2 の SCTP ポート定義します。</p>
Router(config-ipc-remote-sctp)# <b>remote-ip ip_addr</b>	<p>ローカル デバイスと通信する冗長ピアのリモート IP アドレスを定義します。すべてのリモート IP アドレスは、同じデバイスを参照する必要があります。</p> <p>すべてのアソシエーション設定を削除するには、このコマンドの <b>no</b> フォームを使用します。</p>
Router(config-ipc-unit2-sctp)# <b>unit2-ip ip_addr</b>	<p>unit1 デバイスとの通信に使用する冗長ピアの unit2 IP アドレスを定義します。</p>

## PDSN-AAA サーバ インターフェイスのループバック インターフェイスの使用

AAA サーバでアクティブなユニットとスタンバイのユニットを単一の NAS として表示するには、同じ NAS IP アドレスを両方のユニットに使用する必要があります。現在、NAS IP アドレスは **ip radius source-interface** コマンドを使用して、PDSN に設定できます。設定すると、このインターフェイスの IP アドレスが NAS IP アドレスとして使用されます。

ただし、CLI コマンドはバーチャル IP アドレス (HSRP) をサポートしていません。結果、両方のユニットが単一 NAS として表示されるようにするには、ループバック インターフェイスを設定し、このインターフェイスを発信元インターフェイスとして使用するのが唯一の方法です。この場合に使用するコマンドは **ip radius source-interface Loopback1** です。

## アクティブ-アクティブな状況进行处理するアプリケーション トラッキングの設定

コマンド	目的
Router(config)# <b>track object-id application pdsn</b>	PDSN アプリケーションのトラッキング オブジェクトを定義します。
Router(config-if)# <b>standby track object-id [decrement priority]</b>	PDSN に定義したトラッキング オブジェクトを、HSRP コンフィグに関連付けます。HSRP が、このオブジェクトの状態のトラッキングを開始します。設定されたデクリメント プライオリティは、トラッキング オブジェクトの状態に基づいて、HSRP のプライオリティを変更するために使用されます。トラッキング オブジェクトが「アップ」の場合、HSRP は設定済みのプライオリティを使用します。トラッキング オブジェクトが「ダウン」の場合、 <b>standby track</b> コマンドに指定された <b>decrement priority</b> によって、HSRP がプライオリティを下げます。

## PDSN 環境での AAA サーバの設定

アクセス コントロールは、ネットワーク サーバへのアクセスを許可するユーザと、そのユーザに使用を許可するサービスを管理する手段です。AAA ネットワーク セキュリティ サービスは、ルータまたはアクセス サーバ上でアクセス コントロールを設定するための基本的なフレームワークを提供します。AAA サーバの設定オプションの詳細については、『Cisco IOS Security Configuration Guide』の「Configuring Authentication」および「Configuring Accounting」の章を参照してください。

PDSN 環境で AAA サーバを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>aaa new-model</b>	AAA サーバのアクセス コントロールをイネーブルにします。
Router(config)# <b>aaa authentication ppp default group radius</b>	RADIUS による PPP ユーザの認証をイネーブルにします。
Router(config)# <b>aaa authorization configuration default group radius</b>	CHAP がない場合に、Network Access Identifier (NAI; ネットワーク アクセス識別子) の構築をイネーブルにします。
Router(config)# <b>aaa authorization config-commands</b>	<b>aaa authorization</b> コマンドの <i>level method1</i> コマンドが発行されたときに作成されたデフォルト値を再設定します。
Router(config)# <b>aaa authorization network if-authenticated default group radius</b>	ユーザのネットワーク アクセスを制限します。ネットワークに関連するあらゆるサービス要求に認可を実行します。デフォルトの認可方式として、group RADIUS 認可方式を使用します。

コマンド	目的
Router(config)# <b>aaa accounting update periodic minutes</b>	定期的にアカウントリング サーバに送信される中間アカウントリングレコードをイネーブルにします。推奨される期間は 60 分です。
Router(config)# <b>aaa accounting network pdsn start-stop group radius</b>	ビリング用または RADIUS 使用時のセキュリティのために要求されたサービスの AAA サーバアカウントリングをイネーブルにします。

## PDSN 環境での RADIUS の設定

RADIUS は、ネットワークでの AAA サーバ情報の交換を定義する 1 つの方法です。シスコの実装では、RADIUS クライアントはシスコのルータ上で動作し、あらゆるユーザ認証およびネットワークサーバアクセス情報が登録されている RADIUS サーバに、認証要求を送信します。RADIUS 設定オプションの詳細については、『Cisco IOS Security Configuration Guide』の「Configuring RADIUS」を参照してください。

PDSN 環境で RADIUS を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>radius-server host ip-addr key sharedsecret</b>	RADIUS サーバホストの IP アドレスを指定し、ルータと RADIUS サーバ間で使用する共有秘密文字列を指定します。
Router(config)# <b>radius-server vsa send accounting 3gpp2</b>	ベンダー固有属性 (VSA) を RADIUS IETF アトリビュート 26 で定義したとおりに使用できます。認識されたベンダー固有属性のセットを accounting アトリビュートのみに制限します。
Router(config)# <b>radius-server vsa send authentication 3gpp2</b>	ベンダー固有属性 (VSA) を RADIUS IETF アトリビュート 26 で定義したとおりに使用できます。認識されたベンダー固有属性のセットを authentication アトリビュートのみに制限します。
Router(config)# <b>radius-server attribute 55 include-in-acct-req</b>	PDSN からの G4 (イベント時刻) Accounting-Start の送信をイネーブルにします。

## PDSN 環境での前払いの設定

Cisco PDSN ソフトウェアのリリース 1.2 で前払いを設定するには、ユーザ プロファイルに `crb-entity-type=1` が含まれていることを確認します。

Cisco PDSN リリース 2.0 以降で IS835C の前払いを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
router (config)# <b>cdma pdsn accounting prepaid ? duration threshold volume</b>	期間に基づいた前払いサービスです。  割り当てごとにしきい値のパーセンテージを設定します。  ボリュームに基づいた前払いサービスです。

## PDSN 環境での VPDN の有効化

VPDN 環境で VPDN を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>vpdn enable</b>	VPDN をイネーブルにします。
Router(config)# <b>vpdn authen-before-forward</b>	トンネリングの前にローカルでユーザを認証するように指定します。

VPDN の詳細については、Cisco IOS リリース 12.3 のマニュアル『Cisco IOS Dial Services Configuration Guide: Network Services』および『Cisco IOS Dial Services Command Reference』を参照してください。

## モバイル IP FA の設定

TR-45.6 で指定されている MIP 操作には、PDSN (FA として動作) とモバイルステーションの間にチャレンジ/レスポンス メカニズムを使用してモバイルステーションを認証する機能が必要です。

MIP FA を設定するには、グローバル コンフィギュレーション モードとインターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>router mobile</b>	MIP をイネーブルにします。 このコマンドとその他の MIP コマンドは、R-P のシグナリングをイネーブルにするためにここで使用されます。SIP または MIP のどちらを実装するかにかかわらず、これらのコマンドが必要です。
Router(config)# <b>cdma pdsn send-agent-adv</b>	IPCP アドレス オプションをネゴシエートする未知のユーザ クラスを使用して新しく作成された PPP セッションで送信されるエージェント アドバタイズをイネーブルにします。
Router(config) <b>interface virtual-template number</b>	バーチャル テンプレート インターフェイスを作成します。
Router(config-if)# <b>cdma pdsn mobile-advertisement-burst</b> {[number value]   [interval msec]}	送信する FA アドバタイズの数と、新しい PPP セッションが作成される場合の間隔を設定します。
Router(config-if)# <b>ip mobile foreign-service challenge</b> {[timeout value]   [window num]}	チャレンジのタイムアウト値と、最近送信された有効なチャレンジの値の数を設定します。
Router(config-if)# <b>ip mobile foreign-service challenge forward-mfce</b>	FA のレジストレーション要求で Mobile-Foreign Challenge Extension (MFCE) および MN-AAA Authentication Extension (MNAE) を HA に送信できるようにします。
Router(config-if)# <b>ip mobile registration-lifetime seconds</b>	MIP レジストレーションの最大ライフタイムを設定します。
Router(config-if)# <b>ip mobile foreign-service</b> [reverse-tunnel [mandatory]]	このインターフェイスで MIP FA サービスをイネーブルにします。
Router(config-if)# <b>ip mobile foreign-service registration</b>	エージェント アドバタイズに R ビットを設定します。

シスコ ルータのスタンドアロンの PDSN で、CPS 比率を増やすために仮想アクセスのクローニング時間を減らすには、インターフェイスの設定ごとにグローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
<pre>Router(config)# ip mobile foreign-service     ip mobile prefix-length ip mobile registration-lifetime</pre>	<p>気付アドレスが設定されている場合に、インターフェイスで外部エージェント サービスをイネーブルにします。</p> <p>アドバタイズメントにプレフィクスの長さの拡張子を追加します。</p> <p>アドバタイズされるレジストレーションのライフタイムの値を設定します。</p>
<pre>Router(config)# ip mobile foreign-service challenge     home-access allowed     limit     registration-required     reverse-tunnel</pre>	<p>(オプション) 外部エージェントのチャレンジパラメータを設定します。</p> <p>(オプション) モバイル ノードが登録に使用できる HA アドレスを管理します。アクセス リストには、文字列または 1 ~ 99 の数字を使用できます。</p> <p>(オプション) インターフェイスで許可されたビジター数です。Busy (B) ビットは、登録されたビジター数がこの制限値に達した場合にアドバタイズされます。</p> <p>(オプション) 並置された気付アドレスを使用している場合、MN イベントからのレジストレーションを要請します。レジストレーション要求 (R) ビットがアドバタイズされます。</p> <p>(オプション) 外部エージェントでリバース トンネリングをイネーブルにします。12.3T よりも前のリリースでは、サブインターフェイスで外部エージェント サービスをイネーブルにする場合にこのキーワードを使用できません。</p>

シスコ ルータのスタンドアロン PDSN の CPS では、現在の 40 という数値から 100 CPS に改善する必要があります。

## ローカルなプロキシ モバイル IP アトリビュートの設定

一部のモバイル デバイスではサポートされていませんが、実際の MIP の代用として Cisco PDSN を設定すると、PMIP を使用することによって MIP の多くの利点を得ることができます。PMIP のアトリビュートは、すべて AAA サーバから取得できます。ローカルで PMIP アトリビュートを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
<pre>Router(config)# ip mobile proxy-host nai username@realm [flags rrq-flags] [ha homeagent] [homeaddr address] [lifetime value] [local-timezone]</pre>	<p>PDSN のローカルで PMIP アトリビュートを指定します。</p>



## モバイル IP SA の設定

モバイル ホスト、Foreign Agent (FA; 外部エージェント)、および HA の SA を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>ip mobile secure</b> {aaa-download   visitor   home-agent   proxy-host} {lower-address [upper-address]   nai string} {inbound-spi spi-in outbound-spi spi-out   spi spi} <b>key</b> {hex   ascii} string [replay timestamp [number] algorithm md5 mode prefix-suffix]	IP モバイル ユーザの SA を指定します。
Router(config)# <b>ip mobile secure proxy-host nai</b> string spi spi <b>key</b> {ascii   hex} string	PMIP ユーザの SA を指定します。

## PDSN のクラスタ コントローラの設定

ローカルで PDSN のクラスタ コントローラ アトリビュートを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。



(注) これらのコマンドは、ルータが優先設定からの PDSN メンバー機能をサポートしている場合は影響がありません。

コマンド	目的
Router(config)# <b>cdma pdsn secure cluster default spi</b> spi number [ <b>key</b> ascii   hex value ]	クラスタ 内のすべての PDSN に対してコモン セキュリティ アソシエーションを 1 つ設定します。
Router# <b>cdma pdsn cluster controller interface</b> interface name	PDSN のコントローラ/メンバー クラスタ処理のためのコントローラ機能をイネーブルにし、メッセージを送受信するインターフェイスを指定します。
Router# <b>cdma pdsn cluster controller standby</b> cluster-name	PDSN をスタンバイのクラスタ コントローラとして動作するように設定します。

## PDSN のクラスタ メンバーの設定

ローカルで PDSN のクラスタ メンバー アトリビュートを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。



(注) これらのコマンドは、ルータが優先設定からの PDSN メンバー機能をサポートしている場合は影響がありません。

コマンド	目的
Router(config)# <b>cdma pdsn secure cluster default spi</b> spi_index [ <b>key</b> ascii   hex value]	クラスタ 内のすべての PDSN に対してコモン セキュリティ アソシエーションを 1 つ設定します。
Router(config)# <b>cdma pdsn cluster member controller</b> ipaddr	PDSN をクラスタ メンバーとして動作するように設定します。
Router(config)# <b>cdma pdsn cluster member interface</b> interface name	PDSN をクラスタ メンバーとして動作するように設定します。

## ネットワーク管理のイネーブル化

PDSN で SNMP のネットワーク管理をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>snmp-server community string [ro   rw]</b>	SNMP プロトコルへのアクセスを許可するコミュニティ アクセス スtring を指定します。
Router(config)# <b>snmp-server enable traps cdma</b>	CDMA 用のネットワーク管理トラップをイネーブルにします。
Router(config)# <b>snmp-server host host-addr traps version {1   2   3 [auth   noauth   priv]}</b>	SNMP 通知操作の受信者を指定します。
Router(config)# <b>cdma pdsn failure-history entries</b>	SNMP セッションのエラー テーブルで保持できる最大エントリ数を指定します。
Router(config)# <b>no virtual-template snmp</b>	仮想アクセスのサブインターフェイスがルータの SNMP 機能によって登録されないようにします。また、使用されるメモリ量を削減し、それによってコール設定のパフォーマンスを向上させます。

## 常時接続サービスの設定

常時接続サービスは、ローカル ネットワークで加入者のパケット データ セッションを維持します。そのユーザが到達不可能であると PDSN が判断した場合を除き、PPP のアイドル時間のタイマーがタイムアウトしても、PDSN は加入者のパケット データ セッションの解放を開始しません。常時接続機能は、デフォルトで有効に設定されています。この機能に関連するデフォルトのパラメータを変更するには、次のコマンドを使用します。

コマンド	目的
Router(config)# <b>cdma pdsn a10 always-on keepalive {interval 1-65535 [attempts 0-255]   attempts 0-255}</b>	<p>PDSN の常時接続サービスのパラメータを設定します。</p> <p><b>keepalive interval</b> は、PDSN が次の LCP エコーを送信する前に、ピアからの LCP エコーの応答を待機する期間を秒数で表します。デフォルト値は 3 秒です。デフォルトの設定に戻すには、このコマンドの <b>no</b> フォームを使用します。</p> <p><b>attempts</b> は、アイドル時間のタイマーがタイムアウトした後にセッションを切断する際に、常時接続のユーザに到達不可能であると宣言する前に、LCP エコーを送信しなければならない回数です。デフォルト値は 3 です。この変数を 0 に設定すると、そのユーザの常時接続プロパティを無視することになります。</p>

## A11 セッションのアップデートの設定

A11 セッションアップデートメッセージは、A10 接続のセッションパラメータを追加、変更、またはアップデートするために、PDSN から PCF に送信されます。A11 セッションアップデート機能をイネーブルにするには、以下のタスクを実行します。

コマンド	目的
Router(config)# <b>cdma pdsn all session-update</b> {[always-on] 1-10 [rn-pdit] 0-9}	PDSN で A11 セッションアップデート機能をイネーブルにし、認証フェーズで AAA サーバからダウンロードされる常時接続アトリビュートまたは RNPDIIT アトリビュートの一方またはその両方の A11 セッションアップデートを送信します。  デフォルトのタイムアウト値は 3 秒です。デフォルトの再送信回数は 3 回です。
Router# <b>cdma pdsn retransmit all-update</b> number	A11 レジストレーションのアップデートメッセージを再送信する最大回数を指定します。使用可能な値は 0 ~ 9 です。デフォルトの再送信回数は 5 回です。

## SDB インジケータ マーキングの設定

この機能は、PTT アプリケーションの SIP シグナリングなどのショートデータバーストアプリケーションをサポートし、PDSN との対話を計画します。SIP は PTT アプリケーションで使用され、PTT コールを伝えます。メッセージは短く、エンドユーザに配信する必要があります。RAN でショートデータバーストサポートを使用して、これらをエンドユーザ、特にモバイルで終了する必要があるメッセージの場合に送信できます。これは特に、ユーザが実際に休止している場合に重要です。SDB インジケータマーキングを設定するには、次のコマンドを使用します。

コマンド	目的
Router(config)# <b>cdma pdsn all dormant sdb-indication gre-flags</b> group-number	<i>group-number</i> は、分類された一致基準を表します。特定の <i>group-number</i> に設定されたすべてのパケットは、PCF と PDSN 間での SDB 使用のフラグが付きます。  B ビット (SDB インジケータ) は <i>sdb-indication group-number</i> に一致するパケットに対し設定されます。

## PPP コントロールパケットの SDB インジケータマーキングの設定

前のセクションで説明したように、SDB を使用してデータパケットをモバイルに対して送信できる一方で、SDB を PPP コントロールパケットの配信にも使用できます。これは特に、セッションが休止している常時接続セッションで有効です。基本的に、常時接続が設定されていると、PDSN はセッションを有効にしておくために LCP エコー要求を送信（および LCP エコー応答を待機）します。反対に、このようなセッションが休止している場合、これらの LCP エコー要求を MN に送信するためのデータチャンネルを設定する必要があります。その他のオプションは、SDB を使用して LCP エコー要求をデータチャンネルを設定せずに送信するためのものです。

この機能をイネーブルにするには、前述の CLI コマンドと一緒に次の CLI コマンドを使用します。

コマンド	目的
Router(config)# <b>cdma pdsn all dormant sdb-indication match-qos-group group-number ppp-ctrl-pkts</b>	<i>group-number</i> は、分類された一致基準を表します。

## PDSN での PoD の設定

PDSN で Packet of Disconnect (POD; パケット オブ ディスコネクト) または RADIUS 切断機能をイネーブルにするには、次の手順を実行します。

コマンド	目的
Router(config)# <b>cdma pdsn radius disconnect</b>	PDSN で RADIUS 切断機能をイネーブルにします。
Router(config)# <b>aaa pod server [clients ipaddr1 [ipaddr2] [ipaddr3] [ipaddr4]] [port port-number] [auth-type {any   all   session-key}] server-key [encryption-type] string</b>	AAA サーバで POD パケットの受信をイネーブルにします。
Router(config)# <b>aaa server radius dynamic-author</b> Router(config-locsvr-radius)#? RADIUS Application commands: <b>auth-type</b> Specify the server authorization type <b>client</b> Specify a RADIUS client <b>default</b> Set a command to its defaults <b>exit</b> Exit from RADIUS application configuration mode <b>ignore</b> Override behavior to ignore certain parameters <b>no</b> Negate a command or set its defaults <b>port</b> Specify port on which local RADIUS server listens <b>server-key</b> Encryption key shared with the RADIUS clients	RADIUS アプリケーション コンフィギュレーション モードを開始し、ユーザに複数の設定オプションを提示します。

## PDSN でのモバイル IP リソース失効の設定

PDSN でのリソース失効のサポートをイネーブルにするには、次の手順を実行します。

コマンド	目的
Router(config)# <b>ip mobile foreign-service revocation [timeout value] [retransmit value] [timestamp]</b>	<p><b>timeout value</b> は、リソース失効メッセージを再送信する時間間隔 (秒) を表します。待機時間は 0 ~ 100 で、デフォルト値は 3 です。</p> <p><b>retransmit value</b> は、MIPv4 失効メッセージの再送信の最大回数を表します。</p> <p>トランザクションのリトライ回数は 0 ~ 100 です。デフォルト値は 3 です。</p> <p>(注) すべての <b>foreign-service</b> の設定はグローバルにする必要があり、バーチャル テンプレート インターフェイスの下では設定しません。</p> <p><b>timestamp</b> には、失効のタイムスタンプ フィールドの単位を指定します。失効のタイムスタンプ値の単位はミリ秒です。</p>



(注)

実行する作業には、VPDN の設定作業、Layer 2 Tunneling Protocol (L2TP; レイヤ 2 トンネリング プロトコル) のトンネル設定作業、およびロード バランシングの設定作業もあります。特定の情報の詳細については、適切なマニュアルを参照してください。

VPDN の設定の詳細については、次の URL を参照してください。

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products\\_command\\_reference\\_chapter09186a00801a7e8f.html#wp1167095](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a7e8f.html#wp1167095)

L2TP のトンネル設定の詳細については、次の URL を参照してください。

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products\\_command\\_reference\\_chapter09186a00801a7e90.html](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a7e90.html)

IOS サーバ ロード バランシングの詳細については、次の URL を参照してください。

[http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5012/products\\_feature\\_guide09186a008020b9f3.html#wp3601032](http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5012/products_feature_guide09186a008020b9f3.html#wp3601032)

## ショート データ バースト フラグの設定

この機能によって PTT アプリケーションの SIP シグナリングなどのショート データ バースト アプリケーションのサポートが追加され、PDSN との対話が計画されます。SIP は PTT アプリケーションで使用され、PTT コールを伝えます。メッセージは短く、エンドユーザに配信する必要があります。RAN でショート データ バースト サポートを使用して、これらをエンドユーザ、特にモバイルで終了する必要があるメッセージの場合に送信できます。

特定の group-number に設定されたすべてのパケットが PCF と PDSN 間での SDB の使用時にフラグが付けられるように、PDSN で SDB を設定するには、グローバル コンフィギュレーションで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>cdma pdsn all dormant sdb-indication gre-flags group-number</b>	特定の group-number に設定されたすべてのパケットが PCF と PDSN 間での SDB 使用時にフラグが付くように、SDB を設定します。

## PDSN アカウンティング イベントの設定

PDSN アカウンティング イベントの属性を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>clock timezone zone hours-offset [minutes-offset]</b>	表示のためのタイムゾーンを設定します。
Router(config)# <b>cdma pdsn accounting local-timezone</b>	PDSN アカウンティング イベントのローカルのタイムスタンプを設定します。

コマンド	目的
Router(config)# <b>cdma pdsn accounting time-of-day</b>	1 日のさまざまな時間帯のアカウント情報のトリガを設定します。
Router(config)# <b>cdma pdsn accounting send start-stop</b>	PDSN が次の内容を送信できるようにします。 <ul style="list-style-type: none"> <li>アクティブな Airlink 停止レコードを受信する場合のアカウント停止レコード (休止状態)</li> <li>アクティブな Airlink 開始レコードを受信する場合のアカウント開始レコード (アクティブな状態)</li> </ul>

## CDMA RADIUS アトリビュートの設定

PDSN で認証およびアカウント要求を設定するには、次の作業を実行します。

コマンド	目的
Router(config)# <b>cdma pdsn attribute send</b> {a1 {fa-chap   mip-rrq}   a2 {auth-req   fa-chap   mip-rrq}   a3 {auth-req   fa-chap   mip-rrq}   {c5 {acct-reqs}   f15 {acct-reqs}   f16 {acct-reqs}   f5 {fa-chap}   g1 {acct-start}   g2 {acct-start}   g17   esn-optional   meid-optional   is835a}	PDSN で認証とアカウント要求の両方をイネーブルにします。

## PDSN のモニタリングとメンテナンス

PDSN のモニタリングとメンテナンスを行うには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# <b>clear cdma pdsn cluster controller session records</b> <i>age days</i>	指定された経過時間のセッションレコードをクリアします。
Router# <b>clear cdma pdsn cluster controller session record all</b>	PDSN のクラスタコントローラのすべてのセッションレコードをクリアします。
Router# <b>clear cdma pdsn cluster controller statistics</b>	PDSN のクラスタコントローラの統計情報をクリアします。
Router# <b>clear cdma pdsn cluster member statistics</b>	PDSN のクラスタメンバーの統計情報をクリアします。
Router# <b>clear cdma pdsn session</b> {all   pcf <i>ip-addr</i>   msid <i>octet-stream</i> } {send {all-update   termreq}}	セッションをクリアします。
Router# <b>clear cdma pdsn statistics</b>	RAN-to-PDSN インターフェイス (RP) または PDSN の PPP 統計情報をクリアします。
Router# <b>clear ip mobile binding</b> {all [ <i>load standby-group-name</i> ]   <i>ip-address</i>   nai string <i>ip_address</i> }	モビリティバインディングを削除します。
Router# <b>clear ip mobile visitor</b> [ <i>ip-address</i>   nai string <i>ip_address</i> ]	ビジター情報をクリアします。

コマンド	目的
Router# <b>clear vpdn tunnel l2tp ?</b> all All L2TP tunnels hostname Based on the hostnames id Based on the tunnel ID ip Based on IP address	Closed-PR 機能のための VPDN の L2TP トンネル情報をクリアします。
Router# <b>show cdma pdsn</b>	PDSN ゲートウェイのステータスと現在の設定を表示します。
Router# <b>show cdma pdsn accounting</b>	すべてのセッションと対応するフローのアカウントリング情報を表示します。
Router# <b>show cdma pdsn accounting detail</b>	すべてのセッションと対応するフローの詳細なアカウントリング情報を表示します。
Router# <b>show cdma pdsn accounting session msid</b>	MSID で識別されるセッションのアカウントリング情報を表示します。
Router# <b>show cdma pdsn accounting session msid detail</b>	MSID で識別されるセッションのアカウントリング情報 (カウンタ名) を表示します。
Router# <b>show cdma pdsn accounting session msid flow {mn-ip-address IP_address}</b>	MSID で識別されるセッションに関連する特定のフローのアカウントリング情報を表示します。
Router# <b>show cdma pdsn accounting session msid flow user username</b>	MSID で識別されるセッションに関連する、username を持つフローのアカウントリング情報を表示します。
Router# <b>show cdma pdsn ahdlc slot_number channel [channel_id]</b>	AHDLC のエンジン情報を表示します。
Router# <b>show cdma pdsn cluster controller [configuration   statistics]</b>	PDSN クラスタ コントローラの設定と統計情報を表示します。
Router# <b>show cdma pdsn cluster controller config</b>	特定のコントローラで登録されたメンバーの IP アドレスを表示します。
Router# <b>show cdma pdsn cluster controller member [load   time   ipaddr]</b>	すべての PDSN クラスタ メンバーがレポートした負荷またはメンバーのシーク時刻までの時間 (シーク時刻から経過した時間) のいずれか、あるいは指定された IP アドレスのメンバーに関する詳細情報を表示します。
Router# <b>show cdma pdsn cluster controller queueing</b>	コントローラのキュー機能に関連する統計情報を表示します。
Router# <b>show cdma pdsn cluster member queueing</b>	メンバーのキュー機能に関連する統計情報を表示します。
Router# <b>show cdma pdsn cluster controller session [count [age days]   oldest [more 1-20 records]   imsi BCDs [more 1-20 records]</b>	セッション カウント、経過時間ごとのカウント、1 件または 2 ~ 3 件の最も古いセッション レコード、入力された IMSI に対応するセッション レコードを表示します。
Router# <b>show cdma pdsn cluster controller statistics</b>	特定のコントローラで登録されたメンバーの IP アドレスを表示します。
Router# <b>show cdma pdsn cluster member [configuration   statistics]</b>	PDSN クラスタ メンバーの設定と統計情報を表示します。
Router# <b>show cdma pdsn flow {mn-ip-address ip_address   msid string   service-type   user string}</b>	アクティブなセッションのフロー ベースの要約、および各セッションで携帯電話番号に割り当てられたフローと IP アドレスを表示します。

コマンド	目的
Router# <code>show cdma pdsn pcf [brief   ip-addr]</code>	この PDSN への R-P トンネルを持つ PCF の PCF 情報を表示します。
Router# <code>show cdma pdsn pcf secure</code>	この PDSN に設定されたすべての PCF のセキュリティ アソシエーションを表示します。
Router# <code>show cdma pdsn resource [slot_number [ahdlic-channel [channel_id]]]</code>	AHDLC のリソース情報を表示します。
Router# <code>show cdma pdsn session [brief   dormant   mn-ip-address address   msid msid   user nai]</code>	PDSN のセッション情報を表示します。
Router# <code>show cdma pdsn statistics [ ahdlic   rp [pcf ip_address]   closed-rp [pcf ip_address]   error] [ppp [pcf ip_address ]]</code>	PDSN の VPDN、PPP、RP インターフェイス、Closed-RP インターフェイス、前払い、RADIUS、およびエラー統計情報を表示します。
Router# <code>show compress detail-ccp</code>	すべてのユーザの圧縮情報を表示します。
Router# <code>show diag [slot]</code>	シスコ ルータの指定されたスロットに関連するコントローラ、インターフェイス、プロセッサ、およびポート アダプタの診断情報を表示します。
Router# <code>show interfaces virtual-access number</code>	vaccess インターフェイスの設定の説明を表示します。
Router# <code>show ip mobile cdma ipsec profile</code>	設定済みの IPSec プロファイルを表示します。
Router# <code>show ip mobile cdma ipsec security-level</code>	FA とそのセキュリティ レベルのリストを表示します。
Router# <code>show ip mobile globals</code>	MIP サブシステムでの MIPv4 レジストレーション失効のサポート状況を表示します。
Router# <code>show ip mobile proxy [host [nai string]   registration   traffic]</code>	PMIP ホストの情報を表示します。
Router# <code>show ip mobile secure</code>	MIP のモビリティ セキュリティ アソシエーションを表示します。
Router# <code>show ip mobile traffic</code>	統計情報に関連する MIPv4 レジストレーション失効メッセージを表示します。
Router# <code>show ip mobile visitor</code>	ビジターのリストを表示します。
Router# <code>show ip mobile violation</code>	セキュリティ違反に関する情報を表示します。
Router# <code>show mwam module slot_num port_num</code>	MWAM カードの個々のプロセッサに関する接続情報を表示します。
Router# <code>show tech-support cdma pdsn</code>	シスコ カスタマー エンジニアが問題を診断する場合に役立つ PDSN の情報を表示します。
Router# <code>show vpdn</code> Router# <code>show vpdn session</code> Router# <code>show vpdn tunnel</code>	Closed-RP インターフェイスに関する VPDN 情報を表示します。

## 設定例

ここでは、次の設定例について説明します。

- 「Cisco PDSN のスタンドアロン設定」
- 「Cisco PDSN のセッションの冗長性設定」
- 「Cisco PDSN のクラスタ設定」



- 「簡易 IP 用の Cisco PDSN の設定」
- 「VPDN を使用した簡易 IP 用の Cisco PDSN の設定」
- 「モバイル IP 用の Cisco PDSN の設定」
- 「Cisco PDSN の設定の組み合わせ」
- 「IPv6 の簡単な設定例」

## Cisco PDSN のスタンドアロン設定

ここでは、Cisco PDSN のスタンドアロン設定の例を示します。

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service internal
service cdma pdsn
boot-start-marker
boot-end-marker
!
!
hostname PDSN-standalone
!
logging message-counter syslog
logging buffered 2000000
!
!
!
aaa new-model
!
!
aaa group server radius auth_server_group_1
server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa group server radius acct_server_group_1
server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa authentication login default local none
aaa authentication ppp default group auth_server_group_1
aaa authorization network default group auth_server_group_1
aaa authorization configuration default group auth_server_group_1
aaa accounting update periodic 300
aaa accounting network pdsn
action-type start-stop
group acct_server_group_1
!
aaa accounting system default
action-type start-stop
broadcast
group acct_server_group_1
!
!
!
aaa session-id common
aaa memory threshold authentication reject 15
aaa memory threshold accounting disable 10

memory-size iomem 256

/* default pool cache size is 10 , recommended cache size is 50 */

```

```
sami pool-cache 50
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip source-route
ip cef
!
!
no ip domain lookup
no ipv6 cef
vpdn enable
vpdn authen-before-forward
!

!
multilink bundle-name authenticated
!
!
memory lite
archive
  log config
  hidekeys
!
!
!
!
!

!
!
!
interface Loopback0
  ip address 40.1.33.103 255.255.0.0
!
interface Loopback1
  ip address 171.1.33.103 255.255.0.0
!
interface Loopback2
  ip address 51.1.33.103 255.255.0.0
!
interface CDMA-Ix1
  ip address 30.1.33.103 255.255.0.0
  tunnel source 30.1.33.103
  tunnel key 46
  tunnel sequence-datagrams
!
interface GigabitEthernet0/0
  mtu 1600
  no ip address
  load-interval 30
  no keepalive
!
!
!
interface GigabitEthernet0/0.20
  description RP-interface
  encapsulation dot1Q 20
  ip address 20.1.33.103 255.255.0.0
!
interface GigabitEthernet0/0.50
  description PDSN-HA Connectivity
  encapsulation dot1Q 50
```

```

ip address 50.1.33.103 255.255.0.0
ip mtu 1500
!
interface GigabitEthernet0/0.60
description ReverseDirection Connectivity
encapsulation dot1Q 60
ip address 60.1.33.103 255.255.0.0
ip mtu 1500
!
interface GigabitEthernet0/0.170
description LAAA Connectivity
encapsulation dot1Q 170
ip address 170.1.33.103 255.255.0.0
ip mtu 1500
!
interface Virtual-Templat1
ip unnumbered Loopback0
peer default ip address pool sip-addr-33-pool1
no keepalive
ppp accm 0
ppp authentication pap chap optional
ppp accounting none
ppp direction callin
ppp timeout ncp 30
ppp timeout authentication 60
ppp timeout idle 7200
!
router mobile
!
ip local pool sip-addr-33-pool1 100.33.1.1 100.33.254.254 recycle delay 30
ip local pool sip-addr-33-pool1 100.34.1.1 100.34.254.254
ip local pool sip-addr-33-pool1 100.35.1.1 100.35.254.254
ip local pool msid-sip-addr-33-pool1 140.33.1.1 140.33.254.254 recycle delay 30
ip local pool msid-sip-addr-33-pool1 140.34.1.1 140.34.254.254
ip local pool msid-sip-addr-33-pool1 140.35.1.1 140.35.254.254

ip forward-protocol nd

ip route 11.1.0.0 255.255.0.0 20.1.2.100
ip route 12.1.0.0 255.255.0.0 60.1.2.100
ip route 21.1.0.0 255.255.0.0 20.1.2.100
ip route 70.1.0.0 255.255.0.0 50.1.112.102
!
!
no ip http server
no ip http secure-server
ip mobile debug include username
ip mobile foreign-agent care-of GigabitEthernet0/0.50
ip mobile foreign-agent reverse-tunnel private-address
ip mobile foreign-agent skip-aaa-reauthentication
ip mobile secure-home-agent 50.1.112.102 spi FFFFFFFF key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile foreign-service revocation
ip mobile foreign-service challenge forward-mfce
ip mobile foreign-service registration-required reverse-tunnel mandatory
ip mobile proxy-host nai @cisco.com flags 42
ip mobile proxy-registration lifetime 1800
!
ip radius source-interface Loopback1
logging main-cpu 4000 emergencies

snmp-server community public RW
snmp-server enable traps cdma
!

```

```

!
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 50 tries 5
radius-server host 170.1.4.201 auth-port 1645 acct-port 1646 key 7 045802150C2E
radius-server retransmit 5
radius-server timeout 10
radius-server deadtime 1
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
cdma pdsn radius disconnect nai
cdma pdsn accounting send start-stop
cdma pdsn tft reject include error extension

cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 1800
cdma pdsn all session-update always-on rn-pdit qos
cdma pdsn timeout mobile-ip-registration 100
cdma pdsn timeout all-update 5
cdma pdsn timeout all-session-update 5
cdma pdsn msid-authentication
cdma pdsn send-agent-adv
cdma pdsn debug show-conditions
cdma pdsn secure pcf default spi 100 key ascii testtesttesttest local-timezone replay 255
cdma pdsn secure pcf 20.1.32.1 20.1.32.7 spi 100 key ascii cisco

cdma pdsn compliance is835c account ipmobile control-packets
!
line con 0
  exec-timeout 0 0
line aux 0
  exec-timeout 0 0
line vty 0 4
  exec-timeout 0 0
  password 7 151E0A0E
!
exception data-corruption buffer truncate
ntp server 127.0.0.51 burst iburst
end

```

## Cisco PDSN のセッションの冗長性の設定

ここでは、アクティブな PDSN に Cisco PDSN のセッションの冗長性を設定する例を示します。

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service internal
service cdma pdsn
!
hostname PDSN-B
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device

```

```

    scheme standby PDSN-redundancy
    !
    !
    !
    redundancy
    no keepalive-enable
    logging message-counter syslog
    !
    !
    ipc zone default
    association 1
    no shutdown
    protocol sctp
    local-port 5000
    local-ip 20.1.23.203
    remote-port 5000
    remote-ip 20.1.33.103
    !
    aaa new-model
    !
    !
    aaa group server radius auth_server_group_1
    server 170.1.4.201 auth-port 1645 acct-port 1646
    !
    aaa group server radius acct_server_group_1
    server 170.1.4.201 auth-port 1645 acct-port 1646
    !
    aaa authentication login default local none
    aaa authentication ppp default group auth_server_group_1
    aaa authorization network default group auth_server_group_1
    aaa authorization configuration default group auth_server_group_1
    aaa accounting update periodic 300
    aaa accounting network pdsn
    action-type start-stop
    group acct_server_group_1
    !
    aaa accounting system default
    action-type start-stop
    broadcast
    group acct_server_group_1
    !
    !
    !
    aaa session-id common
    aaa memory threshold authentication reject 15
    aaa memory threshold accounting disable 10
    memory-size iomem 256
    sami pool-cache 50
    !
    mmi polling-interval 60
    no mmi auto-configure
    no mmi pvc
    mmi snmp-timeout 180
    ip source-route
    ip cef
    !
    !
    no ip domain lookup
    subscriber redundancy rate 250 1
    no ipv6 cef
    vpdn enable
    vpdn authen-before-forward
    !
    multilink bundle-name authenticated

```

```
!  
!  
archive  
  log config  
    hidekeys  
!  
!  
!  
!  
!  
!  
!  
interface Loopback0  
  ip address 40.1.33.103 255.255.0.0  
!  
interface Loopback1  
  ip address 171.1.33.103 255.255.0.0  
!  
interface Loopback2  
  ip address 51.1.33.103 255.255.0.0  
!  
interface CDMA-Ix1  
  ip address 30.1.33.103 255.255.0.0  
  tunnel source 30.1.33.103  
  tunnel key 46  
  tunnel sequence-datagrams  
!  
interface GigabitEthernet0/0  
  mtu 1600  
  no ip address  
  load-interval 30  
  no keepalive  
!  
interface GigabitEthernet0/0.20  
  description RP-interface  
  encapsulation dot1Q 20  
  ip address 20.1.23.203 255.255.0.0  
  standby delay minimum 30 reload 30  
  standby version 2  
  standby 20 ip 20.1.33.254  
  standby 20 priority 110  
  standby 20 name PDSN-redundancy  
!  
interface GigabitEthernet0/0.50  
  description PDSN-HA Connectivity  
  encapsulation dot1Q 50  
  ip address 50.1.23.203 255.255.0.0  
  ip mtu 1500  
  standby version 2  
  standby 50 ip 50.1.33.254  
  standby 50 follow PDSN-redundancy  
!  
interface GigabitEthernet0/0.60  
  description ReverseDirection Connectivity  
  encapsulation dot1Q 60  
  ip address 60.1.23.203 255.255.0.0  
  ip mtu 1500  
  standby version 2  
  standby 60 ip 60.1.33.254  
  standby 60 follow PDSN-redundancy  
!  
interface GigabitEthernet0/0.170  
  description LAAA Connectivity
```

```

encapsulation dot1Q 170
ip address 170.1.23.203 255.255.0.0
ip mtu 1500
standby version 2
standby 170 ip 170.1.33.254
standby 170 follow PDSN-redundancy
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool sip-addr-33-pool1
 no keepalive
 ppp accm 0
 ppp authentication pap chap optional
 ppp accounting none
 ppp direction callin
 ppp timeout ncp 30
 ppp timeout authentication 60
 ppp timeout idle 7200
!
router mobile
!
ip local pool sip-addr-33-pool1 100.33.1.1 100.33.254.254 recycle delay 30
ip local pool sip-addr-33-pool1 100.34.1.1 100.34.254.254
ip local pool sip-addr-33-pool1 100.35.1.1 100.35.254.254
ip local pool msid-sip-addr-33-pool1 140.33.1.1 140.33.254.254 recycle delay 30
ip local pool msid-sip-addr-33-pool1 140.34.1.1 140.34.254.254
ip local pool msid-sip-addr-33-pool1 140.35.1.1 140.35.254.254
ip forward-protocol nd
ip route 11.1.0.0 255.255.0.0 20.1.2.100
ip route 12.1.0.0 255.255.0.0 60.1.2.100
ip route 21.1.0.0 255.255.0.0 20.1.2.100
ip route 70.1.0.0 255.255.0.0 50.1.112.102
!
!
no ip http server
no ip http secure-server
ip mobile debug include username
ip mobile foreign-agent care-of GigabitEthernet0/0.50
ip mobile foreign-agent reverse-tunnel private-address
ip mobile foreign-agent skip-aaa-reauthentication
ip mobile secure home-agent 50.1.112.102 spi FFFFFFFF key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile foreign-service revocation
ip mobile foreign-service challenge forward-mfce
ip mobile foreign-service registration-required reverse-tunnel mandatory
ip mobile proxy-host nai @cisco.com flags 42
ip mobile proxy-registration lifetime 1800
!
ip radius source-interface Loopback1
logging main-cpu 4000 emergencies
snmp-server community public RW
snmp-server enable traps cdma
!
!
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 50 tries 5
radius-server host 170.1.4.201 auth-port 1645 acct-port 1646 key 7 045802150C2E
radius-server retransmit 5
radius-server timeout 10
radius-server deadtime 1
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2

```

```

!
control-plane
!
cdma pdsn radius disconnect nai
cdma pdsn accounting send start-stop
cdma pdsn tft reject include error extension
cdma pdsn virtual-template 1
cdma pdsn all session-update always-on rn-pdit qos
cdma pdsn timeout mobile-ip-registration 100
cdma pdsn timeout all-update 5
cdma pdsn timeout all-session-update 5
cdma pdsn msid-authentication
cdma pdsn send-agent-adv
cdma pdsn debug show-conditions
cdma pdsn secure pcf default spi 100 key ascii testtesttesttest local-timezone replay 255
cdma pdsn secure pcf 20.1.32.1 20.1.32.7 spi 100 key ascii cisco
cdma pdsn compliance is835c account ipmobile control-packets
cdma pdsn redundancy
!
line con 0
  exec-timeout 0 0
line aux 0
  exec-timeout 0 0
line vty 0 4
  exec-timeout 0 0
  password 7 151E0A0E
!
exception data-corruption buffer truncate
ntp server 127.0.0.51 burst iburst
end

```

スタンバイの PDSN に Cisco PDSN のセッションの冗長性を設定する例を示します。

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service internal
service cdma pdsn
!
hostname PDSN-A
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
  scheme standby PDSN-redundancy
!
!
!
redundancy
  no keepalive-enable
logging message-counter syslog
!
!
ipc zone default
  association 1
  no shutdown
  protocol sctp
  local-port 5000
  local-ip 20.1.33.103
  remote-port 5000
  remote-ip 20.1.23.203

```



```

!
aaa new-model
!
!
aaa group server radius auth_server_group_1
  server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa group server radius acct_server_group_1
  server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa authentication login default local none
aaa authentication ppp default group auth_server_group_1
aaa authorization network default group auth_server_group_1
aaa authorization configuration default group auth_server_group_1
aaa accounting update periodic 300
aaa accounting network pdsn
  action-type start-stop
  group acct_server_group_1
!
aaa accounting system default
  action-type start-stop
  broadcast
  group acct_server_group_1
!
!
!
aaa session-id common
aaa memory threshold authentication reject 15
aaa memory threshold accounting disable 10
memory-size iomem 256
sami pool-cache 50
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip source-route
ip cef
!
!
no ip domain lookup
subscriber redundancy rate 250 1
no ipv6 cef
vpdn enable
vpdn authen-before-forward
!
multilink bundle-name authenticated
!
!
archive
  log config
  hidekeys
!
!
!
!
!
!
!
interface Loopback0
  ip address 40.1.33.103 255.255.0.0
!
interface Loopback1

```

```
ip address 171.1.33.103 255.255.0.0
!
interface Loopback2
ip address 51.1.33.103 255.255.0.0
!
interface CDMA-Ix1
ip address 30.1.33.103 255.255.0.0
tunnel source 30.1.33.103
tunnel key 46
tunnel sequence-datagrams
!
interface GigabitEthernet0/0
mtu 1600
no ip address
load-interval 30
no keepalive
!
interface GigabitEthernet0/0.20
description RP-interface
encapsulation dot1Q 20
ip address 20.1.33.103 255.255.0.0
standby delay minimum 30 reload 30
standby version 2
standby 20 ip 20.1.33.254
standby 20 name PDSN-redundancy
!
interface GigabitEthernet0/0.50
description PDSN-HA Connectivity
encapsulation dot1Q 50
ip address 50.1.33.103 255.255.0.0
ip mtu 1500
standby version 2
standby 50 ip 50.1.33.254
standby 50 follow PDSN-redundancy
!
interface GigabitEthernet0/0.60
description ReverseDirection Connectivity
encapsulation dot1Q 60
ip address 60.1.33.103 255.255.0.0
ip mtu 1500
standby version 2
standby 60 ip 60.1.33.254
standby 60 follow PDSN-redundancy
!
interface GigabitEthernet0/0.170
description LAAA Connectivity
encapsulation dot1Q 170
ip address 170.1.33.103 255.255.0.0
ip mtu 1500
standby version 2
standby 170 ip 170.1.33.254
standby 170 follow PDSN-redundancy
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool sip-addr-33-pool1
no keepalive
ppp accm 0
ppp authentication pap chap optional
ppp accounting none
ppp direction callin
ppp timeout ncp 30
ppp timeout authentication 60
ppp timeout idle 7200
```

```

!
router mobile
!
ip local pool sip-addr-33-pool1 100.33.1.1 100.33.254.254 recycle delay 30
ip local pool sip-addr-33-pool1 100.34.1.1 100.34.254.254
ip local pool sip-addr-33-pool1 100.35.1.1 100.35.254.254
ip local pool msid-sip-addr-33-pool1 140.33.1.1 140.33.254.254 recycle delay 30
ip local pool msid-sip-addr-33-pool1 140.34.1.1 140.34.254.254
ip local pool msid-sip-addr-33-pool1 140.35.1.1 140.35.254.254
ip forward-protocol nd
ip route 11.1.0.0 255.255.0.0 20.1.2.100
ip route 12.1.0.0 255.255.0.0 60.1.2.100
ip route 21.1.0.0 255.255.0.0 20.1.2.100
ip route 70.1.0.0 255.255.0.0 50.1.112.102
!
!
no ip http server
no ip http secure-server
ip mobile debug include username
ip mobile foreign-agent care-of GigabitEthernet0/0.50
ip mobile foreign-agent reverse-tunnel private-address
ip mobile foreign-agent skip-aaa-reauthentication
ip mobile secure home-agent 50.1.112.102 spi FFFFFFFF key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile foreign-service revocation
ip mobile foreign-service challenge forward-mfce
ip mobile foreign-service registration-required reverse-tunnel mandatory
ip mobile proxy-host nai @cisco.com flags 42
ip mobile proxy-registration lifetime 1800
!
ip radius source-interface Loopback1
logging main-cpu 4000 emergencies
snmp-server community public RW
snmp-server enable traps cdma
!
!
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 50 tries 5
radius-server host 170.1.4.201 auth-port 1645 acct-port 1646 key 7 045802150C2E
radius-server retransmit 5
radius-server timeout 10
radius-server deadtime 1
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
cdma pdsn radius disconnect nai
cdma pdsn accounting send start-stop
cdma pdsn tft reject include error extension
cdma pdsn virtual-template 1
cdma pdsn all session-update always-on rn-pdit qos
cdma pdsn timeout mobile-ip-registration 100
cdma pdsn timeout all-update 5
cdma pdsn timeout all-session-update 5
cdma pdsn msid-authentication
cdma pdsn send-agent-adv
cdma pdsn debug show-conditions
cdma pdsn secure pcf default spi 100 key ascii testtesttesttest local-timezone replay 255
cdma pdsn secure pcf 20.1.32.1 20.1.32.7 spi 100 key ascii cisco
cdma pdsn compliance is835c account ipmobile control-packets
cdma pdsn redundancy

```

```

!
line con 0
  exec-timeout 0 0
line aux 0
  exec-timeout 0 0
line vty 0 4
  exec-timeout 0 0
  password 7 151E0A0E
!
exception data-corruption buffer truncate
ntp server 127.0.0.51 burst iburst
end

```

Cisco PDSN のセッションの冗長性を設定した場合の表示コマンドの出力を次に示します。

```

PDSN-B# show redundancy states
  my state = 13 -ACTIVE
  peer state = 8 -STANDBY HOT
    Mode = Duplex
    Unit ID = 0

Maintenance Mode = Disabled
  Manual Swact = Enabled
  Communications = Up

  client count = 12
  client_notification_TMR = 30000 milliseconds
  RF debug mask = 0x0
PDSN-B#

PDSN-A# show redundancy states
  my state = 8 -STANDBY HOT
  peer state = 13 -ACTIVE
    Mode = Duplex
    Unit ID = 0

Maintenance Mode = Disabled
  Manual Swact = Enabled
  Communications = Up

  client count = 12
  client_notification_TMR = 30000 milliseconds
  RF debug mask = 0x0
PDSN-A#

```

## Cisco PDSN の冗長性の設定（自動同期対応）

自動同期がイネーブルの場合に、Cisco PDSN のセッションの冗長性を設定する例を示します。

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service internal
service cdma pdsn
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
  scheme standby PDSN-redundancy

```

```

!
!
redundancy unit1 slot 8 unit2 slot 9
!
redundancy unit1 hostname PDSN-A unit2 hostname PDSN-B
!
redundancy
  no keepalive-enable
logging message-counter syslog
!
auto-sync all
!
ipc zone default
  association 1
    no shutdown
    protocol sctp
      unit2-port 5000
      unit2-ip 20.1.23.203
      unit1-port 5000
      unit1-ip 20.1.33.103
!
aaa new-model
!
!
aaa group server radius auth_server_group_1
  server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa group server radius acct_server_group_1
  server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa authentication login default local none
aaa authentication ppp default group auth_server_group_1
aaa authorization network default group auth_server_group_1
aaa authorization configuration default group auth_server_group_1
aaa accounting update periodic 300
aaa accounting network pdsn
  action-type start-stop
  group acct_server_group_1
!
aaa accounting system default
  action-type start-stop
  broadcast
  group acct_server_group_1
!
!
!
aaa session-id common
aaa memory threshold authentication reject 15
aaa memory threshold accounting disable 10
memory-size iomem 256
sami pool-cache 50
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip source-route
ip cef
!
!
no ip domain lookup
subscriber redundancy rate 250 1
no ipv6 cef
vpdn enable

```

```
vpdn authen-before-forward
!
multilink bundle-name authenticated
!
!
archive
 log config
  hidekeys
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 40.1.33.103 255.255.0.0
!
interface Loopback1
 ip address 171.1.33.103 255.255.0.0
!
interface Loopback2
 ip address 51.1.33.103 255.255.0.0
!
interface CDMA-Ix1
 ip address 30.1.33.103 255.255.0.0
 tunnel source 30.1.33.103
 tunnel key 46
 tunnel sequence-datagrams
!
interface GigabitEthernet0/0
 mtu 1600
 no ip address
 load-interval 30
 no keepalive
!
interface GigabitEthernet0/0.20
 description RP-interface
 encapsulation dot1Q 20
 redundancy ip address unit1 20.1.33.103 255.255.0.0 unit2 20.1.23.203 255.255.0.0
 standby delay minimum 30 reload 30
 standby version 2
 standby 20 ip 20.1.33.254
 standby 20 name PDSN-redundancy
!
interface GigabitEthernet0/0.50
 description PDSN-HA Connectivity
 encapsulation dot1Q 50
 redundancy ip address unit1 50.1.33.103 255.255.0.0 unit2 50.1.23.203 255.255.0.0
 ip mtu 1500
 standby version 2
 standby 50 ip 50.1.33.254
 standby 50 follow PDSN-redundancy
!
interface GigabitEthernet0/0.60
 description ReverseDirection Connectivity
 encapsulation dot1Q 60
 redundancy ip address unit1 60.1.33.103 255.255.0.0 unit2 60.1.23.203 255.255.0.0
 ip mtu 1500
 standby version 2
 standby 60 ip 60.1.33.254
 standby 60 follow PDSN-redundancy
!
```

```

interface GigabitEthernet0/0.170
description LAAA Connectivity
encapsulation dot1Q 170
redundancy ip address unit1 170.1.33.103 255.255.0.0 unit2 170.1.23.203 255.255.0.0
ip mtu 1500
standby version 2
standby 170 ip 170.1.33.254
standby 170 follow PDSN-redundancy
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool sip-addr-33-pool1
no keepalive
ppp accm 0
ppp authentication pap chap optional
ppp accounting none
ppp direction callin
ppp timeout ncp 30
ppp timeout authentication 60
ppp timeout idle 7200
!
router mobile
!
ip local pool sip-addr-33-pool1 100.33.1.1 100.33.254.254 recycle delay 30
ip local pool sip-addr-33-pool1 100.34.1.1 100.34.254.254
ip local pool sip-addr-33-pool1 100.35.1.1 100.35.254.254
ip local pool msid-sip-addr-33-pool1 140.33.1.1 140.33.254.254 recycle delay 30
ip local pool msid-sip-addr-33-pool1 140.34.1.1 140.34.254.254
ip local pool msid-sip-addr-33-pool1 140.35.1.1 140.35.254.254
ip forward-protocol nd
ip route 11.1.0.0 255.255.0.0 20.1.2.100
ip route 12.1.0.0 255.255.0.0 60.1.2.100
ip route 21.1.0.0 255.255.0.0 20.1.2.100
ip route 70.1.0.0 255.255.0.0 50.1.112.102
!
!
no ip http server
no ip http secure-server
ip mobile debug include username
ip mobile foreign-agent care-of GigabitEthernet0/0.50
ip mobile foreign-agent reverse-tunnel private-address
ip mobile foreign-agent skip-aaa-reauthentication
ip mobile secure home-agent 50.1.112.102 spi FFFFFFFF key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile foreign-service revocation
ip mobile foreign-service challenge forward-mfce
ip mobile foreign-service registration-required reverse-tunnel mandatory
ip mobile proxy-host nai @cisco.com flags 42
ip mobile proxy-registration lifetime 1800
!
ip radius source-interface Loopback1
logging main-cpu 4000 emergencies
snmp-server community public RW
snmp-server enable traps cdma
!
!
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 50 tries 5
radius-server host 170.1.4.201 auth-port 1645 acct-port 1646 key 7 045802150C2E
radius-server retransmit 5
radius-server timeout 10
radius-server deadtime 1
radius-server vsa send accounting
radius-server vsa send authentication

```

```

radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
cdma pdsn radius disconnect nai
cdma pdsn accounting send start-stop
cdma pdsn tft reject include error extension
cdma pdsn virtual-template 1
cdma pdsn all session-update always-on rn-pdit qos
cdma pdsn timeout mobile-ip-registration 100
cdma pdsn timeout all-update 5
cdma pdsn timeout all-session-update 5
cdma pdsn msid-authentication
cdma pdsn send-agent-adv
cdma pdsn debug show-conditions
cdma pdsn secure pcf default spi 100 key ascii testtesttesttest local-timezone replay 255
cdma pdsn secure pcf 20.1.32.1 20.1.32.7 spi 100 key ascii cisco
cdma pdsn compliance is835c account ipmobile control-packets
cdma pdsn redundancy
!
line con 0
  exec-timeout 0 0
line aux 0
  exec-timeout 0 0
line vty 0 4
  exec-timeout 0 0
  password 7 151E0A0E
!
exception data-corruption buffer truncate
ntp server 127.0.0.51 burst iburst
end

```

Cisco PDSN の冗長性を設定した場合（自動同期対応）の表示コマンドの出力を次に示します。

```

PDSN-B# show redundancy states
  my state = 13 -ACTIVE
  peer state = 8 -STANDBY HOT
  Mode = Duplex
  Unit ID = 0

Maintenance Mode = Disabled
Manual Swact = Enabled
Communications = Up

  client count = 12
  client_notification_TMR = 30000 milliseconds
  RF debug mask = 0x0

PDSN-B#

PDSN-A# show redundancy states
  my state = 8 -STANDBY HOT
  peer state = 13 -ACTIVE
  Mode = Duplex
  Unit ID = 0

Maintenance Mode = Disabled
Manual Swact = Enabled
Communications = Up

  client count = 12

```



```
client_notification_TMR = 30000 milliseconds
RF debug mask = 0x0
```

```
PDSN-A#
```

## Cisco PDSN のクラスタ設定

ここでは、CiscoPDSN のクラスタ設定の例を示します。

## Cisco PDSN のメンバー設定

Cisco PDSN リリース 5.1 のメンバーは、Cisco PDSN リリース 5.0、4.0、および 3.0 のコントローラと連携可能で、コントローラ設定を変更する必要はありません。



(注)

Cisco PDSN リリース 5.1 のメンバーは、重量の観点から負荷をレポートします。最大重量は、セッションカウントではなく 100 を基準とします。

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service internal
service cdma pdsn
boot-start-marker
boot-end-marker
!
!
hostname PDSN-Cluster-Mem
!
logging message-counter syslog
logging buffered 2000000
!
!
!
aaa new-model
!
!
aaa group server radius auth_server_group_1
server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa group server radius acct_server_group_1
server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa authentication login default local none
aaa authentication ppp default group auth_server_group_1
aaa authorization network default group auth_server_group_1
aaa authorization configuration default group auth_server_group_1
aaa accounting update periodic 300
aaa accounting network pdsn
action-type start-stop
group acct_server_group_1
!
aaa accounting system default
action-type start-stop
broadcast
group acct_server_group_1
!
!
```

```
!  
aaa session-id common  
aaa memory threshold authentication reject 15  
aaa memory threshold accounting disable 10  
!  
memory-size iomem 256  
  
/* default pool cache size is 10 , recommended cache size is 50 */  
sami pool-cache 50  
!  
mmi polling-interval 60  
no mmi auto-configure  
no mmi pvc  
mmi snmp-timeout 180  
ip source-route  
ip cef  
!  
!  
no ip domain lookup  
no ipv6 cef  
vpdn enable  
vpdn authen-before-forward  
!  
  
!  
multilink bundle-name authenticated  
!  
!  
memory lite  
archive  
  log config  
  hidekeys  
!  
!  
!  
!  
!  
  
!  
!  
!  
interface Loopback0  
  ip address 40.1.33.103 255.255.0.0  
!  
interface Loopback1  
  ip address 171.1.33.103 255.255.0.0  
!  
interface Loopback2  
  ip address 51.1.33.103 255.255.0.0  
!  
interface CDMA-Ix1  
  ip address 30.1.33.103 255.255.0.0  
  tunnel source 30.1.33.103  
  tunnel key 46  
  tunnel sequence-datagrams  
!  
interface GigabitEthernet0/0  
  mtu 1600  
  no ip address  
  load-interval 30  
  no keepalive  
!  
!  
!
```

```

interface GigabitEthernet0/0.20
description RP-interface
encapsulation dot1Q 20
ip address 20.1.33.103 255.255.0.0
!
interface GigabitEthernet0/0.50
description PDSN-HA Connectivity
encapsulation dot1Q 50
ip address 50.1.33.103 255.255.0.0
ip mtu 1500
!
interface GigabitEthernet0/0.60
description ReverseDirection Connectivity
encapsulation dot1Q 60
ip address 60.1.33.103 255.255.0.0
ip mtu 1500
!

interface GigabitEthernet0/0.170
description LAAA Connectivity
encapsulation dot1Q 170
ip address 170.1.33.103 255.255.0.0
ip mtu 1500
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool sip-addr-33-pool1
no keepalive
ppp accm 0
ppp authentication pap chap optional
ppp accounting none
ppp direction callin
ppp timeout ncp 30
ppp timeout authentication 60
ppp timeout idle 7200
!
router mobile
!
ip local pool sip-addr-33-pool1 100.33.1.1 100.33.254.254 recycle delay 30
ip local pool sip-addr-33-pool1 100.34.1.1 100.34.254.254
ip local pool sip-addr-33-pool1 100.35.1.1 100.35.254.254
ip local pool msid-sip-addr-33-pool1 140.33.1.1 140.33.254.254 recycle delay 30
ip local pool msid-sip-addr-33-pool1 140.34.1.1 140.34.254.254
ip local pool msid-sip-addr-33-pool1 140.35.1.1 140.35.254.254

ip forward-protocol nd

ip route 11.1.0.0 255.255.0.0 20.1.2.100
ip route 12.1.0.0 255.255.0.0 60.1.2.100
ip route 21.1.0.0 255.255.0.0 20.1.2.100
ip route 70.1.0.0 255.255.0.0 50.1.112.102
!
!
no ip http server
no ip http secure-server
ip mobile debug include username
ip mobile foreign-agent care-of GigabitEthernet0/0.50
ip mobile foreign-agent reverse-tunnel private-address
ip mobile foreign-agent skip-aaa-reauthentication
ip mobile secure home-agent 50.1.112.102 spi FFFFFFFF key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile foreign-service revocation
ip mobile foreign-service challenge forward-mfce
ip mobile foreign-service registration-required reverse-tunnel mandatory

```

```

ip mobile proxy-host nai @cisco.com flags 42
ip mobile proxy-registration lifetime 1800
!
ip radius source-interface Loopback1
logging main-cpu 4000 emergencies

snmp-server community public RW
snmp-server enable traps cdma
!
!
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 50 tries 5
radius-server host 170.1.4.201 auth-port 1645 acct-port 1646 key 7 045802150C2E
radius-server retransmit 5
radius-server timeout 10
radius-server deadtime 1
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
cdma pdsn radius disconnect nai
cdma pdsn accounting send start-stop
cdma pdsn tft reject include error extension

cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 1800
cdma pdsn all session-update always-on rn-pdit qos
cdma pdsn timeout mobile-ip-registration 100
cdma pdsn timeout all-update 5
cdma pdsn timeout all-session-update 5
cdma pdsn msid-authentication
cdma pdsn send-agent-adv
cdma pdsn debug show-conditions
cdma pdsn secure pcf default spi 100 key ascii testtesttesttest local-timezone replay 255
cdma pdsn secure pcf 20.1.32.1 20.1.32.7 spi 100 key ascii cisco
cdma pdsn secure cluster default spi 101 key ascii Cisco
cdma pdsn compliance is835c account ipmobile control-packets
cdma pdsn cluster member controller 20.1.33.103
cdma pdsn cluster member interface GigabitEthernet0/0.20
cdma pdsn cluster member timeout 120
!
line con 0
  exec-timeout 0 0
line aux 0
  exec-timeout 0 0
line vty 0 4
  exec-timeout 0 0
  password 7 151E0A0E
!
exception data-corruption buffer truncate
ntp server 127.0.0.51 burst iburst
end

```

Cisco PDSN のクラスタ設定の表示コマンドの出力を次に示します。

```

PDSN-Cluster-Mem# show cdma pdsn cluster controller configuration
cluster interface GigabitEthernet0/0.20 (collocated)
no R-P signaling proxy
timeout to seek member = 120 seconds

```

```

window to seek member is 2 timeouts in a row if no reply (afterwards the member is
declared offline)
default: spi 101, Timestamp +/- 0, key ascii cisco
this PDSN cluster controller is configured

Controller maximum number of load units = 100
PDSN-Cluster-Mem#

```

## Cisco PDSN のコントローラ設定

This section provides an example of Cisco PDSN controller configuration.

Cisco PDSN リリース 5.1 のクラスタ コントローラは、Cisco PDSN リリース 5.0、4.0、および 3.0 のメンバーと連携可能で、メンバーの設定を変更する必要はありません。

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service internal
service cdma pdsn
boot-start-marker
boot-end-marker
!
!
hostname PDSN-Cluster-Cntrl
!
logging message-counter syslog
logging buffered 2000000
!
!
!
aaa new-model
!
!
aaa group server radius auth_server_group_1
server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa group server radius acct_server_group_1
server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa authentication login default local none
aaa authentication ppp default group auth_server_group_1
aaa authorization network default group auth_server_group_1
aaa authorization configuration default group auth_server_group_1
aaa accounting update periodic 300
aaa accounting network pdsn
action-type start-stop
group acct_server_group_1
!
aaa accounting system default
action-type start-stop
broadcast
group acct_server_group_1
!
!
!
aaa session-id common
aaa memory threshold authentication reject 15
aaa memory threshold accounting disable 10

memory-size iomem 256

```

```
/* default pool cache size is 10 , recommended cache size is 50 */
sami pool-cache 50
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip source-route
ip cef
!
!
no ip domain lookup
no ipv6 cef
vpdn enable
vpdn authen-before-forward
!

!
multilink bundle-name authenticated
!
!
memory lite
archive
  log config
  hidekeys
!
!
!
!
!

!
!
!
interface Loopback0
  ip address 40.1.33.103 255.255.0.0
!
interface Loopback1
  ip address 171.1.33.103 255.255.0.0
!
interface Loopback2
  ip address 51.1.33.103 255.255.0.0
!
interface CDMA-Ix1
  ip address 30.1.33.103 255.255.0.0
  tunnel source 30.1.33.103
  tunnel key 46
  tunnel sequence-datagrams
!
interface GigabitEthernet0/0
  mtu 1600
  no ip address
  load-interval 30
  no keepalive
!
!
!
interface GigabitEthernet0/0.20
  description RP-interface
  encapsulation dot1Q 20
  ip address 20.1.33.103 255.255.0.0
!
interface GigabitEthernet0/0.50
```

```

description PDSN-HA Connectivity
encapsulation dot1Q 50
ip address 50.1.33.103 255.255.0.0
ip mtu 1500
!
interface GigabitEthernet0/0.60
description ReverseDirection Connectivity
encapsulation dot1Q 60
ip address 60.1.33.103 255.255.0.0
ip mtu 1500
!
interface GigabitEthernet0/0.170
description LAAA Connectivity
encapsulation dot1Q 170
ip address 170.1.33.103 255.255.0.0
ip mtu 1500
!
interface Virtual-Templat1
ip unnumbered Loopback0
no peer default ip address
no keepalive
ppp accm 0
ppp authentication pap chap optional
ppp accounting none
ppp direction callin
ppp timeout ncp 30
ppp timeout authentication 60
ppp timeout idle 7200
!
router mobile
!
ip forward-protocol nd

ip route 11.1.0.0 255.255.0.0 20.1.2.100
ip route 12.1.0.0 255.255.0.0 60.1.2.100
ip route 21.1.0.0 255.255.0.0 20.1.2.100
ip route 70.1.0.0 255.255.0.0 50.1.112.102
!
!
no ip http server
no ip http secure-server
ip mobile debug include username
ip mobile foreign-agent care-of GigabitEthernet0/0.50
ip mobile foreign-agent reverse-tunnel private-address
ip mobile foreign-agent skip-aaa-reauthentication
ip mobile secure home-agent 50.1.112.102 spi FFFFFFFF key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile foreign-service revocation
ip mobile foreign-service challenge forward-mfce
ip mobile foreign-service registration-required reverse-tunnel mandatory
ip mobile proxy-host nai @cisco.com flags 42
ip mobile proxy-registration lifetime 1800
!
ip radius source-interface Loopback1
logging main-cpu 4000 emergencies

snmp-server community public RW
snmp-server enable traps cdma
!
!
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 50 tries 5
radius-server host 170.1.4.201 auth-port 1645 acct-port 1646 key 7 045802150C2E
radius-server retransmit 5

```

```

radius-server timeout 10
radius-server deadtime 1
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
cdma pdsn radius disconnect nai
cdma pdsn accounting send start-stop
cdma pdsn tft reject include error extension

cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 1800
cdma pdsn all session-update always-on rn-pdit qos
cdma pdsn timeout mobile-ip-registration 100
cdma pdsn timeout all-update 5
cdma pdsn timeout all-session-update 5
cdma pdsn msid-authentication
cdma pdsn imsi-min-equivalence
cdma pdsn send-agent-adv
cdma pdsn debug show-conditions
cdma pdsn secure pcf default spi 100 key ascii testtesttesttest local-timezone replay 255
cdma pdsn secure pcf 20.1.32.1 20.1.32.7 spi 100 key ascii cisco
cdma pdsn secure cluster default spi 101 key ascii Cisco
cdma pdsn compliance is835c account ipmobile control-packets
cdma pdsn cluster controller interface GigabitEthernet0/0.20
cdma pdsn cluster controller timeout 120
!
line con 0
  exec-timeout 0 0
line aux 0
  exec-timeout 0 0
line vty 0 4
  exec-timeout 0 0
  password 7 151E0A0E
!
exception data-corruption buffer truncate
ntp server 127.0.0.51 burst iburst
end

```

Cisco PDSN のコントローラ設定の表示コマンドの出力を次に示します。

```

PDSN-Cluster-Cntrl# show cdma pdsn cluster controller configuration
cluster interface GigabitEthernet0/0.20
no R-P signaling proxy
timeout to seek member = 120 seconds
window to seek member is 2 timeouts in a row if no reply (afterwards the member is
declared offline)
default: spi 101, Timestamp +/- 0, key ascii cisco
this PDSN cluster controller is configured

Controller maximum number of load units = 100
PDSN-Cluster-Cntrl#

```

## Cisco PDSN コントローラの冗長性を持つコロケーション メンバー

ここでは、Cisco PDSN コントローラの冗長性を持つコロケーション メンバーを設定する例を示します。



## アクティブ モード

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service internal
service cdma pdsn
!
hostname PDSN-B
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
  scheme standby PDSN-redundancy
!
!
!
redundancy
  no keepalive-enable
logging message-counter syslog
!
!
ipc zone default
  association 1
    no shutdown
    protocol sctp
    local-port 5000
    local-ip 20.1.23.203
    remote-port 5000
    remote-ip 20.1.33.103
!
aaa new-model
!
!
aaa group server radius auth_server_group_1
  server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa group server radius acct_server_group_1
  server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa authentication login default local none
aaa authentication ppp default group auth_server_group_1
aaa authorization network default group auth_server_group_1
aaa authorization configuration default group auth_server_group_1
aaa accounting update periodic 300
aaa accounting network pdsn
  action-type start-stop
  group acct_server_group_1
!
aaa accounting system default
  action-type start-stop
  broadcast
  group acct_server_group_1
!
!
!
aaa session-id common
aaa memory threshold authentication reject 15
aaa memory threshold accounting disable 10
memory-size iomem 256

```

```

sami pool-cache 50
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip source-route
ip cef
!
!
no ip domain lookup
subscriber redundancy rate 250 1
no ipv6 cef
vpdn enable
vpdn authen-before-forward
!
multilink bundle-name authenticated
!
!
archive
  log config
  hidekeys
!
!
!
!
!
!
!
!
interface Loopback0
  ip address 40.1.33.103 255.255.0.0
!
interface Loopback1
  ip address 171.1.33.103 255.255.0.0
!
interface Loopback2
  ip address 51.1.33.103 255.255.0.0
!
interface CDMA-Ix1
  ip address 30.1.33.103 255.255.0.0
  tunnel source 30.1.33.103
  tunnel key 46
  tunnel sequence-datagrams
!
interface GigabitEthernet0/0
  mtu 1600
  no ip address
  load-interval 30
  no keepalive
!
interface GigabitEthernet0/0.20
  description RP-interface
  encapsulation dot1Q 20
  ip address 20.1.23.203 255.255.0.0
  standby delay minimum 30 reload 30
  standby version 2
  standby 20 ip 20.1.33.254
  standby 20 priority 110
  standby 20 name PDSN-redundancy
!
interface GigabitEthernet0/0.50
  description PDSN-HA Connectivity
  encapsulation dot1Q 50

```

```

ip address 50.1.23.203 255.255.0.0
ip mtu 1500
standby version 2
standby 50 ip 50.1.33.254
standby 50 follow PDSN-redundancy
!
interface GigabitEthernet0/0.60
description ReverseDirection Connectivity
encapsulation dot1Q 60
ip address 60.1.23.203 255.255.0.0
ip mtu 1500
standby version 2
standby 60 ip 60.1.33.254
standby 60 follow PDSN-redundancy
!
interface GigabitEthernet0/0.170
description LAAA Connectivity
encapsulation dot1Q 170
ip address 170.1.23.203 255.255.0.0
ip mtu 1500
standby version 2
standby 170 ip 170.1.33.254
standby 170 follow PDSN-redundancy
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool sip-addr-33-pool1
no keepalive
ppp accm 0
ppp authentication pap chap optional
ppp accounting none
ppp direction callin
ppp timeout ncp 30
ppp timeout authentication 60
ppp timeout idle 7200
!
router mobile
!
ip local pool sip-addr-33-pool1 100.33.1.1 100.33.254.254 recycle delay 30
ip local pool sip-addr-33-pool1 100.34.1.1 100.34.254.254
ip local pool sip-addr-33-pool1 100.35.1.1 100.35.254.254
ip local pool msid-sip-addr-33-pool1 140.33.1.1 140.33.254.254 recycle delay 30
ip local pool msid-sip-addr-33-pool1 140.34.1.1 140.34.254.254
ip local pool msid-sip-addr-33-pool1 140.35.1.1 140.35.254.254
ip forward-protocol nd
ip route 11.1.0.0 255.255.0.0 20.1.2.100
ip route 12.1.0.0 255.255.0.0 60.1.2.100
ip route 21.1.0.0 255.255.0.0 20.1.2.100
ip route 70.1.0.0 255.255.0.0 50.1.112.102
!
!
no ip http server
no ip http secure-server
ip mobile debug include username
ip mobile foreign-agent care-of GigabitEthernet0/0.50
ip mobile foreign-agent reverse-tunnel private-address
ip mobile foreign-agent skip-aaa-reauthentication
ip mobile secure home-agent 50.1.112.102 spi FFFFFFFF key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile foreign-service revocation
ip mobile foreign-service challenge forward-mfce
ip mobile foreign-service registration-required reverse-tunnel mandatory
ip mobile proxy-host nai @cisco.com flags 42
ip mobile proxy-registration lifetime 1800

```

```

!
ip radius source-interface Loopback1
logging main-cpu 4000 emergencies
snmp-server community public RW
snmp-server enable traps cdma
!
!
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 50 tries 5
radius-server host 170.1.4.201 auth-port 1645 acct-port 1646 key 7 045802150C2E
radius-server retransmit 5
radius-server timeout 10
radius-server deadtime 1
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
cdma pdsn radius disconnect nai
cdma pdsn accounting send start-stop
cdma pdsn tft reject include error extension
cdma pdsn virtual-template 1
cdma pdsn all session-update always-on rn-pdit qos
cdma pdsn timeout mobile-ip-registration 100
cdma pdsn timeout all-update 5
cdma pdsn timeout all-session-update 5
cdma pdsn msid-authentication
cdma pdsn send-agent-adv
cdma pdsn debug show-conditions
cdma pdsn secure pcf default spi 100 key ascii testtesttest local-timezone replay 255
cdma pdsn secure pcf 20.1.32.1 20.1.32.7 spi 100 key ascii cisco
cdma pdsn secure cluster default spi 101 key ascii Cisco
cdma pdsn compliance is835c account ipmobile control-packets
cdma pdsn cluster controller interface GigabitEthernet0/0.20
cdma pdsn cluster controller standby PDSN-redundancy
cdma pdsn cluster controller timeout 120
cdma pdsn cluster member controller 20.1.33.254
cdma pdsn cluster member interface GigabitEthernet0/0.20
cdma pdsn cluster member timeout 120
cdma pdsn redundancy
!
line con 0
  exec-timeout 0 0
line aux 0
  exec-timeout 0 0
line vty 0 4
  exec-timeout 0 0
  password 7 151E0A0E
!
exception data-corruption buffer truncate
ntp server 127.0.0.51 burst iburst

```

## スタンバイ モード

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service internal
service cdma pdsn

```

```

!
hostname PDSN-A
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
  scheme standby PDSN-redundancy
!
!
!
redundancy
  no keepalive-enable
logging message-counter syslog
!
!
ipc zone default
  association 1
  no shutdown
  protocol sctp
  local-port 5000
  local-ip 20.1.33.103
  remote-port 5000
  remote-ip 20.1.23.203
!
aaa new-model
!
!
aaa group server radius auth_server_group_1
  server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa group server radius acct_server_group_1
  server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa authentication login default local none
aaa authentication ppp default group auth_server_group_1
aaa authorization network default group auth_server_group_1
aaa authorization configuration default group auth_server_group_1
aaa accounting update periodic 300
aaa accounting network pdsn
  action-type start-stop
  group acct_server_group_1
!
aaa accounting system default
  action-type start-stop
  broadcast
  group acct_server_group_1
!
!
!
aaa session-id common
aaa memory threshold authentication reject 15
aaa memory threshold accounting disable 10
memory-size iomem 256
sami pool-cache 50
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip source-route
ip cef
!

```

```
!  
no ip domain lookup  
subscriber redundancy rate 250 1  
no ipv6 cef  
vpdn enable  
vpdn authen-before-forward  
!  
multilink bundle-name authenticated  
!  
!  
archive  
  log config  
  hidekeys  
!  
!  
!  
!  
!  
!  
!  
interface Loopback0  
  ip address 40.1.33.103 255.255.0.0  
!  
interface Loopback1  
  ip address 171.1.33.103 255.255.0.0  
!  
interface Loopback2  
  ip address 51.1.33.103 255.255.0.0  
!  
interface CDMA-Ix1  
  ip address 30.1.33.103 255.255.0.0  
  tunnel source 30.1.33.103  
  tunnel key 46  
  tunnel sequence-datagrams  
!  
interface GigabitEthernet0/0  
  mtu 1600  
  no ip address  
  load-interval 30  
  no keepalive  
!  
interface GigabitEthernet0/0.20  
  description RP-interface  
  encapsulation dot1Q 20  
  ip address 20.1.33.103 255.255.0.0  
  standby delay minimum 30 reload 30  
  standby version 2  
  standby 20 ip 20.1.33.254  
  standby 20 name PDSN-redundancy  
!  
interface GigabitEthernet0/0.50  
  description PDSN-HA Connectivity  
  encapsulation dot1Q 50  
  ip address 50.1.33.103 255.255.0.0  
  ip mtu 1500  
  standby version 2  
  standby 50 ip 50.1.33.254  
  standby 50 follow PDSN-redundancy  
!  
interface GigabitEthernet0/0.60  
  description ReverseDirection Connectivity  
  encapsulation dot1Q 60  
  ip address 60.1.33.103 255.255.0.0
```

```

ip mtu 1500
standby version 2
standby 60 ip 60.1.33.254
standby 60 follow PDSN-redundancy
!
interface GigabitEthernet0/0.170
description LAAA Connectivity
encapsulation dot1Q 170
ip address 170.1.33.103 255.255.0.0
ip mtu 1500
standby version 2
standby 170 ip 170.1.33.254
standby 170 follow PDSN-redundancy
!
interface Virtual-Templatel
ip unnumbered Loopback0
peer default ip address pool sip-addr-33-pool1
no keepalive
ppp accm 0
ppp authentication pap chap optional
ppp accounting none
ppp direction callin
ppp timeout ncp 30
ppp timeout authentication 60
ppp timeout idle 7200
!
router mobile
!
ip local pool sip-addr-33-pool1 100.33.1.1 100.33.254.254 recycle delay 30
ip local pool sip-addr-33-pool1 100.34.1.1 100.34.254.254
ip local pool sip-addr-33-pool1 100.35.1.1 100.35.254.254
ip local pool msid-sip-addr-33-pool1 140.33.1.1 140.33.254.254 recycle delay 30
ip local pool msid-sip-addr-33-pool1 140.34.1.1 140.34.254.254
ip local pool msid-sip-addr-33-pool1 140.35.1.1 140.35.254.254
ip forward-protocol nd
ip route 11.1.0.0 255.255.0.0 20.1.2.100
ip route 12.1.0.0 255.255.0.0 60.1.2.100
ip route 21.1.0.0 255.255.0.0 20.1.2.100
ip route 70.1.0.0 255.255.0.0 50.1.112.102
!
!
no ip http server
no ip http secure-server
ip mobile debug include username
ip mobile foreign-agent care-of GigabitEthernet0/0.50
ip mobile foreign-agent reverse-tunnel private-address
ip mobile foreign-agent skip-aaa-reauthentication
ip mobile secure home-agent 50.1.112.102 spi FFFFFFFF key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile foreign-service revocation
ip mobile foreign-service challenge forward-mfce
ip mobile foreign-service registration-required reverse-tunnel mandatory
ip mobile proxy-host nai @cisco.com flags 42
ip mobile proxy-registration lifetime 1800
!
ip radius source-interface Loopback1
logging main-cpu 4000 emergencies
snmp-server community public RW
snmp-server enable traps cdma
!
!
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 50 tries 5
radius-server host 170.1.4.201 auth-port 1645 acct-port 1646 key 7 045802150C2E

```

```

radius-server retransmit 5
radius-server timeout 10
radius-server deadtime 1
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
cdma pdsn radius disconnect nai
cdma pdsn accounting send start-stop
cdma pdsn tft reject include error extension
cdma pdsn virtual-template 1
cdma pdsn all session-update always-on rn-pdit qos
cdma pdsn timeout mobile-ip-registration 100
cdma pdsn timeout all-update 5
cdma pdsn timeout all-session-update 5
cdma pdsn msid-authentication
cdma pdsn send-agent-adv
cdma pdsn debug show-conditions
cdma pdsn secure pcf default spi 100 key ascii testtesttesttest local-timezone replay 255
cdma pdsn secure pcf 20.1.32.1 20.1.32.7 spi 100 key ascii cisco
cdma pdsn secure cluster default spi 101 key ascii Cisco
cdma pdsn compliance is835c account ipmobile control-packets
cdma pdsn cluster controller interface GigabitEthernet0/0.20
cdma pdsn cluster controller standby PDSN-redundancy
cdma pdsn cluster controller timeout 120
cdma pdsn cluster member controller 20.1.33.254
cdma pdsn cluster member interface GigabitEthernet0/0.20
cdma pdsn cluster member timeout 120
cdma pdsn redundancy
!
line con 0
  exec-timeout 0 0
line aux 0
  exec-timeout 0 0
line vty 0 4
  exec-timeout 0 0
  password 7 151E0A0E
!
exception data-corruption buffer truncate
ntp server 127.0.0.51 burst iburst
end

```

Cisco PDSN クラスタ コントローラとメンバーの設定の表示コマンドの出力を次に示します。

```

PDSN-B# show cdma pdsn cluster controller configuration
cluster interface GigabitEthernet0/0.20 (collocated)
no R-P signaling proxy
timeout to seek member = 120 seconds
window to seek member is 2 timeouts in a row if no reply (afterwards the member is
declared offline)
default: spi 101, Timestamp +/- 0, key ascii Cisco
this PDSN cluster controller is configured

controller redundancy:
  database in-sync or no need to sync
  group: PDSN-redundancy
Controller maximum number of load units = 100
PDSN-B#

PDSN-B# show cdma pdsn cluster member configuration
cluster interface GigabitEthernet0/0.20
IP address of controller is 20.1.33.254 (collocated)

```



```

no prohibit administratively
timeout to resend status or seek controller = 120 sec or less, randomized
resend a msg for 2 timeouts sequentially if no reply, then inform operator
default: spi 101, Timestamp +/- 0, key ascii Cisco
this PDSN cluster member is configured
PDSN-B#

PDSN-A# show cdma pdsn cluster controller configuration
cluster interface GigabitEthernet0/0.20 (collocated)
no R-P signaling proxy
timeout to seek member = 120 seconds
window to seek member is 2 timeouts in a row if no reply (afterwards the member is
declared offline)
default: spi 101, Timestamp +/- 0, key ascii Cisco
this PDSN cluster controller is configured

controller redundancy:
  database in-sync or no need to sync
  group: PDSN-redundancy
Controller maximum number of load units = 100
PDSN-A#

PDSN-A# show cdma pdsn cluster member configuration
cluster interface GigabitEthernet0/0.20
IP address of controller is 20.1.33.254 (collocated)
no prohibit administratively
timeout to resend status or seek controller = 120 sec or less, randomized
resend a msg for 2 timeouts sequentially if no reply, then inform operator
default: spi 101, Timestamp +/- 0, key ascii Cisco
this PDSN cluster member is configured
PDSN-A#

```

## Cisco PDSN コントローラのコロケーションメンバー（冗長性と自動同期対応）

ここでは、Cisco PDSN コントローラのコロケーションメンバー（冗長性と自動同期対応）を設定する例を示します。

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service internal
service cdma pdsn
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
  scheme standby PDSN-redundancy
!
!
redundancy unit1 slot 8 unit2 slot 9
!
redundancy unit1 hostname PDSN-Cntrl-A unit2 hostname PDSN-Cntrl-B
!
redundancy
  no keepalive-enable
logging message-counter syslog
!
auto-sync all
!
ipc zone default

```

```
association 1
  no shutdown
  protocol sctp
  unit2-port 5000
  unit2-ip 20.1.23.203
  unit1-port 5000
  unit1-ip 20.1.33.103
!
aaa new-model
!
!
aaa group server radius auth_server_group_1
  server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa group server radius acct_server_group_1
  server 170.1.4.201 auth-port 1645 acct-port 1646
!
aaa authentication login default local none
aaa authentication ppp default group auth_server_group_1
aaa authorization network default group auth_server_group_1
aaa authorization configuration default group auth_server_group_1
aaa accounting update periodic 300
aaa accounting network pdsn
  action-type start-stop
  group acct_server_group_1
!
aaa accounting system default
  action-type start-stop
  broadcast
  group acct_server_group_1
!
!
!
aaa session-id common
aaa memory threshold authentication reject 15
aaa memory threshold accounting disable 10
memory-size iomem 256
sami pool-cache 50
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip source-route
ip cef
!
!
no ip domain lookup
subscriber redundancy rate 250 1
no ipv6 cef
vpdn enable
vpdn authen-before-forward
!
multilink bundle-name authenticated
!
!
archive
  log config
  hidekeys
!
!
!
!
!
```

```

!
!
!
interface Loopback0
 ip address 40.1.33.103 255.255.0.0
!
interface Loopback1
 ip address 171.1.33.103 255.255.0.0
!
interface Loopback2
 ip address 51.1.33.103 255.255.0.0
!
interface CDMA-Ix1
 ip address 30.1.33.103 255.255.0.0
 tunnel source 30.1.33.103
 tunnel key 46
 tunnel sequence-datagrams
!
interface GigabitEthernet0/0
 mtu 1600
 no ip address
 load-interval 30
 no keepalive
!
interface GigabitEthernet0/0.20
 description RP-interface
 encapsulation dot1Q 20
 redundancy ip address unit1 20.1.33.103 255.255.0.0 unit2 20.1.23.203 255.255.0.0
 standby delay minimum 30 reload 30
 standby version 2
 standby 20 ip 20.1.33.254
 standby 20 name PDSN-redundancy
!
interface GigabitEthernet0/0.50
 description PDSN-HA Connectivity
 encapsulation dot1Q 50
 redundancy ip address unit1 50.1.33.103 255.255.0.0 unit2 50.1.23.203 255.255.0.0
 ip mtu 1500
 standby version 2
 standby 50 ip 50.1.33.254
 standby 50 follow PDSN-redundancy
!
interface GigabitEthernet0/0.60
 description ReverseDirection Connectivity
 encapsulation dot1Q 60
 redundancy ip address unit1 60.1.33.103 255.255.0.0 unit2 60.1.23.203 255.255.0.0
 ip mtu 1500
 standby version 2
 standby 60 ip 60.1.33.254
 standby 60 follow PDSN-redundancy
!
interface GigabitEthernet0/0.170
 description LAAA Connectivity
 encapsulation dot1Q 170
 redundancy ip address unit1 170.1.33.103 255.255.0.0 unit2 170.1.23.203 255.255.0.0
 ip mtu 1500
 standby version 2
 standby 170 ip 170.1.33.254
 standby 170 follow PDSN-redundancy
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool sip-addr-33-pool1
 no keepalive

```

```
ppp accm 0
ppp authentication pap chap optional
ppp accounting none
ppp direction callin
ppp timeout ncp 30
ppp timeout authentication 60
ppp timeout idle 7200
!
router mobile
!
ip local pool sip-addr-33-pool1 100.33.1.1 100.33.254.254 recycle delay 30
ip local pool sip-addr-33-pool1 100.34.1.1 100.34.254.254
ip local pool sip-addr-33-pool1 100.35.1.1 100.35.254.254
ip local pool msid-sip-addr-33-pool1 140.33.1.1 140.33.254.254 recycle delay 30
ip local pool msid-sip-addr-33-pool1 140.34.1.1 140.34.254.254
ip local pool msid-sip-addr-33-pool1 140.35.1.1 140.35.254.254
ip forward-protocol nd
ip route 11.1.0.0 255.255.0.0 20.1.2.100
ip route 12.1.0.0 255.255.0.0 60.1.2.100
ip route 21.1.0.0 255.255.0.0 20.1.2.100
ip route 70.1.0.0 255.255.0.0 50.1.112.102
!
!
no ip http server
no ip http secure-server
ip mobile debug include username
ip mobile foreign-agent care-of GigabitEthernet0/0.50
ip mobile foreign-agent reverse-tunnel private-address
ip mobile foreign-agent skip-aaa-reauthentication
ip mobile secure home-agent 50.1.112.102 spi FFFFFFFF key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile foreign-service revocation
ip mobile foreign-service challenge forward-mfce
ip mobile foreign-service registration-required reverse-tunnel mandatory
ip mobile proxy-host nai @cisco.com flags 42
ip mobile proxy-registration lifetime 1800
!
ip radius source-interface Loopback1
logging main-cpu 4000 emergencies
snmp-server community public RW
snmp-server enable traps cdma
!
!
radius-server attribute 8 include-in-access-req
radius-server dead-criteria time 50 tries 5
radius-server host 170.1.4.201 auth-port 1645 acct-port 1646 key 7 045802150C2E
radius-server retransmit 5
radius-server timeout 10
radius-server deadtime 1
radius-server vsa send accounting
radius-server vsa send authentication
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
cdma pdsn radius disconnect nai
cdma pdsn accounting send start-stop
cdma pdsn tft reject include error extension
cdma pdsn virtual-template 1
cdma pdsn all session-update always-on rn-pdit qos
cdma pdsn timeout mobile-ip-registration 100
cdma pdsn timeout all-update 5
cdma pdsn timeout all-session-update 5
```

```

cdma pdsn msid-authentication
cdma pdsn send-agent-adv
cdma pdsn debug show-conditions
cdma pdsn secure pcf default spi 100 key ascii testtesttesttest local-timezone replay 255
cdma pdsn secure pcf 20.1.32.1 20.1.32.7 spi 100 key ascii cisco
cdma pdsn secure cluster default spi 101 key ascii Cisco
cdma pdsn compliance is835c account ipmobile control-packets
cdma pdsn cluster controller interface GigabitEthernet0/0.20
cdma pdsn cluster controller standby PDSN-redundancy
cdma pdsn cluster controller timeout 120
cdma pdsn cluster member controller 20.1.33.254
cdma pdsn cluster member interface GigabitEthernet0/0.20
cdma pdsn cluster member timeout 120
cdma pdsn redundancy
!
line con 0
  exec-timeout 0 0
line aux 0
  exec-timeout 0 0
line vty 0 4
  exec-timeout 0 0
  password 7 151E0A0E
!
exception data-corruption buffer truncate
ntp server 127.0.0.51 burst iburst
end

```

Cisco PDSN コントローラのコロケーション メンバー（冗長性と自動同期対応）の表示コマンドの出力を次に示します。

```

PDSN-Cntrl-B# show cdma pdsn cluster controller configuration
cluster interface GigabitEthernet0/0.20 (collocated)
no R-P signaling proxy
timeout to seek member = 120 seconds
window to seek member is 2 timeouts in a row if no reply (afterwards the member is
declared offline)
default: spi 101, Timestamp +/- 0, key ascii Cisco
this PDSN cluster controller is configured

controller redundancy:
  database in-sync or no need to sync
  group: PDSN-redundancy
Controller maximum number of load units = 100
PDSN-Cntrl-B#

```

```

PDSN-Cntrl-B# show cdma pdsn cluster member configuration
cluster interface GigabitEthernet0/0.20
IP address of controller is 20.1.33.254 (collocated)
no prohibit administratively
timeout to resend status or seek controller = 120 sec or less, randomized
resend a msg for 2 timeouts sequentially if no reply, then inform operator
default: spi 101, Timestamp +/- 0, key ascii Cisco
this PDSN cluster member is configured

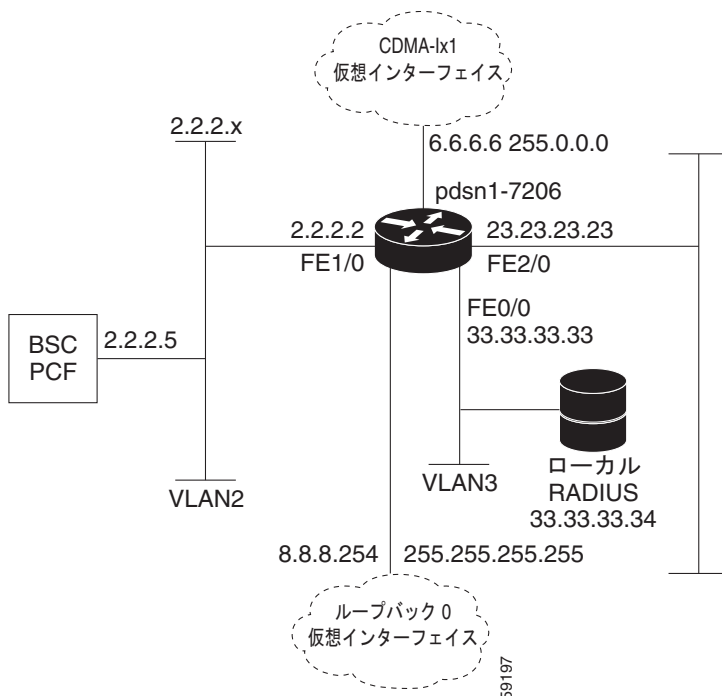
PDSN-Cntrl-B#

```

## 簡易 IP 用の Cisco PDSN の設定

図 8 とそれに続く情報に、SIP 用の PDSN アーキテクチャとそれに付随する設定の例を示します。

図 8 簡易 IP 用の PDSN : ネットワーク マップ



```

service cdma pdsn
!
hostname PDSN1-7206
!
aaa new-model
aaa authentication ppp default group radius
aaa authorization config-commands

aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting update periodic 60
aaa accounting network pdsn start-stop group radius
!
no ip gratuitous-arps
!
interface Loopback0
ip address 8.8.8.254 255.255.255.255
!
interface CDMA-Ix1
ip address 6.6.6.6 255.0.0.0
!
interface FastEthernet0/0
! Interface for communication with RADIUS server and NMS
ip address 33.33.33.33 255.255.255.0
!
!
!
interface FastEthernet1/0
! Interface to PCF - R-P

```

```

ip address 2.2.2.2 255.255.255.0
half-duplex
no cdp enable
!
interface FastEthernet2/0
! Interface to external network - Pi
ip address 23.23.23.23 255.255.0.0
!
!
!
interface Virtual-Template1
ip unnumbered Loopback0
peer default ip address pool pdsn-pool
ppp accm 0
ppp authentication chap pap optional
ppp accounting none
ppp timeout idle 2000
!
ip local pool pdsn-pool 8.8.8.1 8.8.8.253
ip classles
!
!
radius-server host 33.33.33.34 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 3
radius-server vsa send authentication 3gpp2
radius-server vsa send accounting 3gpp2
cdma pdsn virtual-template 1
cdma pdsn maximum sessions 16000
cdma pdsn a10 max-lifetime 36000
cdma pdsn msid-authentication
cdma pdsn secure pcf 2.2.2.5 spi 100 key ascii cisco
!
!
!
end

```

## VPDN を使用した簡易 IP 用の Cisco PDSN の設定

VPDN を使用した SIP の設定は、SIP の設定と同じ内容に次の 2 行を追加したものです。

```

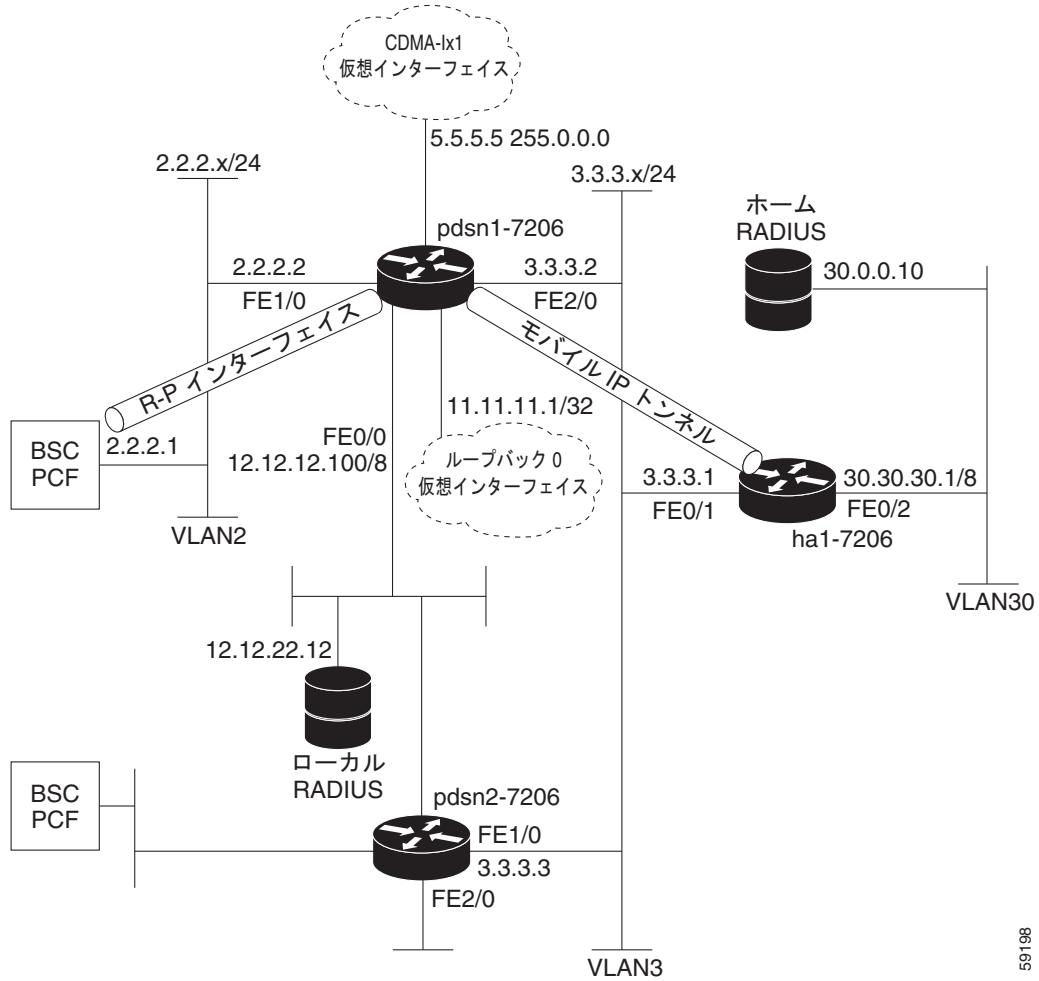
vpdn enable
vpdn authen-before-forward

```

## モバイル IP 用の Cisco PDSN の設定

図 9 とそれに続く情報に、MIP サービス用の PDSN アーキテクチャとそれに付随する設定の例を示します。次の例は、PDSN1 の設定を示しています。

図 9 モバイル IP 用の PDSN : ネットワーク マップ



```

service cdma pdsn
!
hostname PDSN1-7206
!
aaa new-model
aaa authentication login default group radius
aaa authentication login CONSOLE none
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default group radius
!
interface Loopback0
ip address 11.11.11.1 255.255.255.255
!
interface CDMA-Ix1
ip address 5.5.5.5 255.0.0.0
!

```

59198



```

interface FastEthernet0/0
description AAA NMS interface
ip address 12.12.12.100 255.0.0.0
!
interface FastEthernet1/0
description R-P interface
ip address 2.2.2.2 255.255.255.0
full-duplex
!
!
interface FastEthernet2/0
description Pi interface
ip address 3.3.3.2 255.255.255.0
full-duplex
!
interface Virtual-Template1
ip unnumbered loopback0
no ip route-cache
no keepalive
ppp authentication chap pap optional
ppp timeout idle 2000
!
router mobile
!
ip classless
no ip http server
ip mobile foreign-agent care-of FastEthernet2/0
ip mobile foreign-service challenge forward-mfce timeout 10 window 10
ip mobile foreign-service reverse-tunnel
radius-server host 12.12.22.12 auth-port 1645 acct-port 1646 key ascii cisco
!
radius-server host 12.12.22.12 auth-port 1645 acct-port 1646 key ascii cisco
radius-server retransmit 3
radius-server vsa send authentication 3gpp2
radius-server vsa send accounting 3gpp2
cdma pdsn secure pcf 2.2.2.1 spi 100 key ascii cisco
cdma pdsn virtual-template 1
cdma pdsn msid-authentication
!
!
end

```

## Cisco PDSN の設定の組み合わせ

次に、SIP、VPDN を使用した SIP、MIP、および PMIP のすべてのシナリオ用に設定された PDSN を示します。

```

service cdma pdsn
!
hostname PDSN1
!
aaa new-model
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting update periodic 60
aaa accounting network pdsn start-stop group radius
!
vpdn enable
vpdn authen-before-forward
virtual-profile aaa

```

```
username HA password 0 rosebud
username LNS password 0 cisco
username PDSN password 0 cisco
no ip gratuitous-arps
!
interface Loopback0
ip address 8.8.8.254 255.255.255.255
!
interface CDMA-Ix1
ip address 6.6.6.6 255.0.0.0
!
interface FastEthernet0/0
! Interface for communication with RADIUS server and NMS
ip address 33.33.33.33 255.255.255.0
!
!
!
interface FastEthernet1/0
! Interface to PCF - R-P
ip address 2.2.2.2 255.255.255.0
!
interface FastEthernet2/0
! Interface to external network - Pi
ip address 23.23.23.23 255.255.0.0
!
!
!
interface Virtual-Template1
ip unnumbered Loopback0
no keepalive
peer default ip address pool pdsn-pool
ppp accm 0
ppp authentication chap pap optional
ppp accounting none
ppp timeout idle 2000
!
router mobile
!
ip local pool pdsn-pool 8.8.8.1 8.8.8.253
ip classless
ip mobile foreign-agent care-of FastEthernet2/0
ip mobile foreign-service challenge forward-mfce timeout 10 window 10
ip mobile foreign-service reverse-tunnel
radius-server host 12.12.22.12 auth-port 1645 acct-port 1646 key ascii cisco
!
!
radius-server host 33.33.33.34 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 3
radius-server vsa send authentication 3gpp2
radius-server vsa send accounting 3gpp2
cdma pdsn virtual-template 1
cdma pdsn maximum sessions 16000
cdma pdsn a10 max-lifetime 36000
cdma pdsn msid-authentication
cdma pdsn secure pcf 2.2.2.5 spi 100 key ascii cisco
cdma pdsn secure cluster default spi 100 key ascii cisco
!
!
!
end
```

## IPv6 の簡単な設定例

```
PDSN:
pdsn2#sh run
Building configuration...

Current configuration : 4595 bytes
!
version 12.4
no service pad
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service cdma pdsn
!
hostname mwtcc21-pdsn2
!
boot-start-marker
boot-end-marker
!
!
redundancy inter-device
  scheme standby pdsn-sr0
!
!
redundancy
no logging queue-limit
enable password lab
!
aaa new-model
!
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa authorization configuration default group radius
aaa accounting update periodic 1
aaa accounting network pdsn start-stop group radius
!
!
aaa session-id common
!
resource manager
!
!
ipc zone default
  association 1
  no shutdown
  protocol sctp
  local-port 5000
  local-ip 4.0.0.103
  remote-port 5000
  remote-ip 4.0.0.101
!
ip subnet-zero
!
!
ip cef
ip cef accounting per-prefix non-recursive
ip domain name cisco.com
no ip dhcp use vrf connected
ip dhcp ping packets 0
!
```

```
!  
ipv6 unicast-routing  
ipv6 cef  
!  
no virtual-template snmp  
!  
!  
username pdsn2 password 0 cisco  
!  
!  
interface Loopback0  
 ip address 6.0.0.1 255.0.0.0  
!  
interface Loopback2  
 ip address 77.0.0.1 255.0.0.0  
!  
interface Loopback3  
 ip address 3.0.0.1 255.0.0.0  
!  
interface CDMA-Ix1  
 ip address 5.0.0.1 255.0.0.0  
 tunnel source 5.0.0.1  
 tunnel key 1  
 tunnel sequence-datagrams  
!  
interface FastEthernet0/0  
 ip address 10.77.154.236 255.255.255.192  
 duplex auto  
 speed auto  
!  
interface FastEthernet0/1  
 ip address 86.0.0.2 255.0.0.0  
 duplex auto  
 speed auto  
!  
interface FastEthernet1/0  
 ip address 22.22.22.3 255.0.0.0  
 duplex full  
 no cdp enable  
!  
interface FastEthernet2/0  
 ip address 88.0.0.4 255.0.0.0  
 duplex half  
 standby delay minimum 30 reload 60  
 standby 12 ip 88.0.0.251  
 standby 12 name pdsn-sr2  
!  
interface FastEthernet3/0  
 ip address 4.0.0.103 255.0.0.0  
 duplex auto  
 speed auto  
 standby delay minimum 30 reload 60  
 standby 10 ip 4.0.0.254  
 standby 10 name pdsn-sr0  
!  
interface FastEthernet3/1  
 ip address 7.0.0.4 255.0.0.0  
 duplex auto  
 speed auto  
 standby delay minimum 30 reload 60  
 standby 11 ip 7.0.0.254  
 standby 11 name pdsn-sr1  
!  
interface Ethernet4/0
```

```

no ip address
duplex half
ipv6 enable
!
interface Ethernet4/1
ip address 66.0.0.2 255.0.0.0
duplex half
ipv6 address 2001::1/64
ipv6 enable
!
interface Ethernet4/2
no ip address
shutdown
duplex half
!
interface Ethernet4/3
no ip address
shutdown
duplex half
!
interface Virtual-Template1
ip unnumbered Loopback0
ipv6 enable
ipv6 nd ra-interval 1000
ipv6 nd ra-lifetime 5000
no ipv6 nd suppress-ra
no keepalive
compress stac
ppp authentication chap pap optional
ppp accounting none
!
router mobile
!

ip default-gateway 10.77.154.193
ip classless
ip route 9.0.0.2 255.255.255.255 86.0.0.1
ip route 15.0.0.0 255.0.0.0 7.0.0.2
ip route 19.0.0.0 255.0.0.0 7.0.0.2
ip route 17.19.21.34 255.255.255.255 88.0.0.3
ip mobile foreign-agent care-of Loopback2
ip mobile foreign-service challenge forward-mfce timeout 10
ip mobile foreign-service reverse-tunnel
ip mobile registration-lifetime 60000
!
no ip http server
no ip http secure-server
!
!
ip radius source-interface Loopback3
!
!
radius-server host 9.0.0.2 auth-port 1645 acct-port 1646 key cisco
radius-server vsa send accounting
radius-server vsa send accounting 3gpp2
cdma pdsn accounting send start-stop
cdma pdsn virtual-template 1
cdma pdsn a10 max-lifetime 65535
cdma pdsn a10 ahdhc engine 0 usable-channels 8000
cdma pdsn timeout mobile-ip-registration 300
cdma pdsn send-agent-adv
cdma pdsn secure pcf 4.0.0.1 spi 100 key ascii cisco
cdma pdsn secure pcf 4.0.0.2 spi 100 key ascii cisco
cdma pdsn ipv6

```

```

cdma pdsn redundancy
cdma pdsn redundancy accounting update-periodic
!
control-plane
!
!
gatekeeper
 shutdown
!
alias dhcp hu util ma hi
alias dhcp lu util ma lo
alias dhcp o30 origin dhcp subnet size initial /30 autogrow /30
alias dhcp o29 origin dhcp subnet size initial /29 autogrow /29
alias dhcp sp30 subnet prefix-length 30
alias dhcp sp subnet prefix-length
alias dhcp sp29 subnet prefix-length 29
alias dhcp sp28 subnet prefix-length 28
alias configure nopl no ip dhcp pool ispac-odappool
alias configure cpool ip dhc poo ispac-odappool
alias configure cpl ip dhc poo ispac-odappool
alias exec shpl sh ip dhc poo
alias exec shb sh ip dhc bin
!
line con 0
  exec-timeout 0 0
  stopbits 1
line aux 0
  stopbits 1
line vty 5 15
!
!
end

```

## PDSN アカウンティング

CDMA 2000 のパケット アカウンティング モデルは、無線ネットワーク要素ごとに収集される無線固有のパラメータと、提供する PDSN ごとに収集される IP ネットワーク固有のパラメータに分割されます。TIA/EIA/IS-835-D に指定されたパケット アカウンティング手順に適合するように、PDSN では指定されたユーザセッションの無線固有のパラメータを IP ネットワーク固有のパラメータとマージして Usage Data Record (UDR) を作成します。PDSN は、パラメータをマージすると、指定されたトリガイベントの発生時に UDR をローカルの RADIUS サーバに送信します。PDSN は、RADIUS サーバが正常に UDR を受信したことを示す RADIUS サーバからの肯定的な確認応答を受信するまで、UDR を保持します。

## フロー ベースのアカウンティング

Cisco PDSN では、モバイルステーションごとに複数ユーザのセッションをサポートしています。この各ユーザのセッションをフローと呼びます。各モバイルステーションでは、1つの SIP ベースのフローと、1つ以上の MIP ベースのフローをサポートできます。各フローは一意の IP アドレスによって識別されます。各フローのために個別の UDR を生成するアカウンティング手順を、フローベースのアカウンティングと呼びます。

Cisco PDSN では、フローベースのアカウンティングをサポートしています。TIA/EIA/IS-835-D の規格により、各フローは一意の Correlation-ID によって識別されます。各フローの Accounting Start/Stop メッセージのペアは、一意の Accounting-Session-ID と相互に関連付けられています。

フローベースのアカウンティングで UDR を作成する間、無線固有のアカウンティングパラメータはすべてのフローに共通しています。アップリンクやダウンリンクのオクテットカウントなどの IP ネットワーク固有のパラメータは各フローに対して固有のものであり、そのフローに割り当てられた一意の IP アドレスによって識別されます。PDSN は、無線固有のパラメータと IP ネットワーク固有のパラメータをマージすることによって、各フロー用の UDR を作成します。これらの UDR は accounting-request (start、stop、interim) メッセージを使用して RADIUS サーバに転送されます。

次の RADIUS アトリビュートは、PDSN によって UDR に追加されます。

表 27 Accounting Start レコード

アトリビュート名	TIA/EIA/IS-835-B	Type/Subtype
NAS-IP-Address	D2	4
NAS-Port		5
NAS-Port-Type		61
User-Name	B2	1
Calling-Station-Id	A1	31
Acct-Status-Type		40
Acct-Delay-Time		41
Acct-Authentic		45
Service-Type		6
Acct-Session-Id	C1	44
Framed-Protocol		7
Framed-IP-Address	B1	8
Event-Timestamp	G4	55
CDMA-Correlation-ID	C2	26/44
CDMA-HA-IP-Addr	D1	26/7
CDMA-PCF-IP-Addr	D3	26/9
CDMA-BS-MS-Add	D4	26/10
CDMA-HRPD Subnet	D7	26/108
CDMA-User-ID	E1	26/11
CDMA-Forward-Mux	F1	26/12
CDMA-Reverse-Mux	F2	26/13
CDMA-Forward-Rate	F3	26/14
CDMA-Reverse-Rate	F4	26/15
CDMA-Service-Option	F5	26/16
CDMA-Forward-Type	F6	26/17
CDMA-Reverse-Type	F7	26/18
CDMA-Frame-Size	F8	26/19
CDMA-Forward-RC	F9	26/20
CDMA-Reverse-RC	F10	26/21
CDMA-IP-Tech	F11	26/22
CDMA-Comp-Flag	F12	26/23
CDMA-Forward PDCH RC	F16	

表 27 Accounting Start レコード (続き)

アトリビュート名	TIA/EIA/IS-835-B	Type/Subtype
CDMA-Forward DCCH Mux Option	F17	
CDMA-Reverse DCCH Mux Option	F18	
CDMA-Forward DCCH RC	F19	
CDMA-Reverse DCCH RC	F20	
CDMA-Reverse PDCH RC	F22	
CDMA-Num-Active	G9	26/30
CDMA-IP-QoS	I1	26/36
CDMA-Airlink-QoS	I4	26/39
CDMA-Granted QoS	I5	
CDMA-RP-Session-ID	Y2	26/41
CDMA-ESN	A2	26/52
CDMA-MEID	A3	26/116

表 28 Accounting Stop レコード

アトリビュート名	TIA/EIA/IS-835-B	Type/Subtype
NAS-IP-Address	D2	4
NAS-Port		5
NAS-Port-Type		61
User-Name	B2	1
Calling-Station-Id	A1	31
Acct-Status-Type		40
Acct-Delay-Time		41
Acct-Authentic		45
Service-Type		6
Acct-Session-Id	C1	44
Framed-Protocol		7
Flow ID	C6	
CDMA-Forward PDCH RC	F16	
CDMA-Forward DCCH Mux Option	F17	
CDMA-Reverse DCCH Mux Option	F18	
CDMA-Forward DCCH RC	F19	
CDMA-Reverse DCCH RC	F20	
CDMA-Reverse PDCH RC	F22	
Flow Status	F24	
Framed-IP-Address	B1	8
Event-Timestamp	G4	55



表 28 Accounting Stop レコード (続き)

アトリビュート名	TIA/EIA/IS-835-B	Type/Subtype
Acct-Output-Octets	G1	43
Acct-Input-Octets	G2	42
Acct-Input-Packets		47
Acct-Output-Packets		48
Acct-Session-Time		46
Acct-Input-Giga-Words		52
Acct-Output-Giga-Words		53
DHHC-Frame-Format	F14	26/50
CDMA-Active-Time	G8	26/49
CDMA-Correlation-ID	C2	26/44
CDMA-HA-IP-Addr	D1	26/7
CDMA-PCF-IP-Addr	D3	26/9
CDMA-BS-MS-Add	D4	26/10
CDMA-User-ID	E1	26/11
CDMA-Forward-Mux	F1	26/12
CDMA-Reverse-Mux	F2	26/13
CDMA-Forward-Rate	F3	26/14
CDMA-Reverse-Rate	F4	26/15
CDMA-Service-Option	F5	26/16
CDMA-Forward-Type	F6	26/17
CDMA-Reverse-Type	F7	26/18
CDMA-Frame-Size	F8	26/19
CDMA-Forward-RC	F9	26/20
CDMA-Reverse-RC	F10	26/21
CDMA-IP-Tech	F11	26/22
CDMA-Comp-Flag	F12	26/23
CDMA-Num-Active	G9	26/30
CDMA-IP-QoS	I1	26/36
CDMA-Mobile-IP-Signaling-In-Bound Count	G15	26/46
CDMA-Mobile-IP-Signaling-Out-Bound-Count	G16	26/47
CDMA-Airlink-QoS	I4	26/39
CDMA-RP-Session-ID	Y2	26/41
CDMA-Bad-Frame-Count	G3	26/25
CDMA-HDLC-Layer-Bytes-In	G14	26/43
CDMA-SDB-Input-Octets	G10	26/31
CDMA-SDB-Output-Octets	G11	26/32
CDMA-NumSDB-Input	G12	26/33
CDMA-NumSDB-Output	G13	26/34

表 28 Accounting Stop レコード (続き)

アトリビュート名	TIA/EIA/IS-835-B	Type/Subtype
CDMA-last-user-activity	G17	
RSVP Signaling Octets Inbound	G22	
RSVP Signaling Octets Outbound	G23	
RSVP Signaling Packets Inbound	G24	
RSVP Signaling Packets Outbound	G25	
CDMA-Reason-Ind	F13	26/24
CDMA-Session-Continue	C3	26/48
CDMA-ESN	A2	26/52
CDMA-MEID	A3	26/116

次のリストでは、Accounting Stop レコードに含める RADIUS アトリビュートに追加できる前払い VSA を識別します。

- crb-auth-reason
- crb-duration
- crb-total-volume
- crb-uplink-volume
- crb-downlink-volume
- crb-total-packets
- crb-uplink-packets
- crb-downlink-packets
- crb-session-id

表 29 Accounting Interim レコード

アトリビュート名	TIA/EIA/IS-835-B	Type/Subtype
NAS-IP-Address	D2	4
NAS-Port		5
NAS-Port-Type		61
User-Name	B2	1
Calling-Station-Id	A1	31
Acct-Status-Type		40
Acct-Delay-Time		41
Acct-Authentic		45
Service-Type		6
Acct-Session-Id	C1	44
Framed-Protocol		7
Framed-IP-Address	B1	8
Event-Timestamp	G4	55
Acct-Output-Octets	G1	43

表 29 Accounting Interim レコード (続き)

アトリビュート名	TIA/EIA/IS-835-B	Type/Subtype
Acct-Input-Octets	G2	42
Acct-Input-Packets		47
Acct-Output-Packets		48
Acct-Input-Giga-Words		52
Acct-Output-Giga-Words		53
CDMA-Active-Time	G8	26/49
CDMA-Correlation-ID	C2	26/44
CDMA-HA-IP-Addr	D1	26/7
CDMA-PCF-IP-Addr	D3	26/9
CDMA-BS-MS-Add	D4	26/10
CDMA-User-ID	E1	26/11
CDMA-Forward-Mux	F1	26/12
CDMA-Granted QoS	I5	
CDMA-HRPD Subnet	D7	26/108
CDMA-Reverse-Mux	F2	26/13
CDMA-Forward-Rate	F3	26/14
CDMA-Reverse-Rate	F4	26/15
CDMA-Service-Option	F5	26/16
CDMA-Forward-Type	F6	26/17
CDMA-Reverse-Type	F7	26/18
CDMA-Frame-Size	F8	26/19
CDMA-Forward-RC	F9	26/20
CDMA-Reverse-RC	F10	26/21
CDMA-IP-Tech	F11	26/22
CDMA-Comp-Flag	F12	26/23
CDMA-Forward PDCH RC	F16	
CDMA-Forward DCCH Mux Option	F17	
CDMA-Reverse DCCH Mux Option	F18	
CDMA-Forward DCCH RC	F19	
CDMA-Reverse DCCH RC	F20	
CDMA-Reverse PDCH RC	F22	
CDMA-Num-Active	G9	26/30
CDMA-IP-QoS	I1	26/36
CDMA-Airlink-QoS	I4	26/39
CDMA-RP-Session-ID	Y2	26/41
CDMA-HDLC-Layer-Bytes-In	G14	26/43
CDMA-Bad-Frame-Count	G3	26/25

表 29 Accounting Interim レコード (続き)

アトリビュート名	TIA/EIA/IS-835-B	Type/Subtype
CDMA-SDB-Input-Octets	G10	26/31
CDMA-SDB-Output-Octets	G11	26/32
CDMA-NumSDB-Input	G12	26/33
CDMA-NumSDB-Output	G13	26/34
CDMA-last-user-activity	G17	
Flow ID	C6	
Flow Status	F24	
RSVP Signaling Octets Inbound	G22	
RSVP Signaling Octets Outbound	G23	
RSVP Signaling Packets Inbound	G24	
RSVP Signaling Packets Outbound	G25	

## AAA サーバの認証と認可のプロファイル

ここでは、さまざまなサービス タイプ (SIP、MIP など) のためのユーザ認証および認可を行うために、AAA サーバで設定するユーザ プロファイルについて説明します。また、プロファイルに必要な最小限の設定についても説明します。

1. クライアント ルータは、Cisco Access Registrar にアクセスする際に認可される必要があります。クライアントのプロファイルには、ルータの IP アドレスと共有鍵が含まれます。次に、クライアントのプロファイルの例を示します。

```
[ //localhost/Radius/Clients/username ]
  Name = username
  Description =
  IPAddress = 9.15.68.7
  SharedSecret = lab
  Type = NAS
  Vendor =

  IncomingScript~ =
  OutgoingScript~ =
  UseDNIS = FALSE
  DeviceName =
  DevicePassword =
```

2. ユーザは、AAA サーバで設定されたプロファイルを持っている必要があります (これは、MIP のケースでは NAI にも該当します)。

ユーザ プロファイルには、ユーザ名、パスワード、および認可の実行時に取得するアトリビュートを設定できる基本プロファイルが含まれます。

次に、ユーザ プロファイルの例を示します。

```
[ //localhost/Radius/UserLists/Default/username ]
```

```
Name = username
Description =
Password = <encrypted>
AllowAnonymousPassword = FALSE
Enabled = TRUE
Group~ =
BaseProfile~ = username-sip
AuthenticationScript~ =
AuthorizationScript~ =
UserDefined1 =
```

3. 基本プロファイルには、認可の実行時にユーザに求められるアトリビュートが含まれます。

次に、基本プロファイルの例を示します。

```
[ //localhost/Radius/Profiles/username-sip ]
Name = username-sip
Description =
Attributes/
```

4. attributes に移動します

```
[ //localhost/Radius/Profiles/username-sip/Attributes ]
CDMA-IP-Technology = x
```

## さまざまなタイプのサービス用の AAA サーバのプロファイル

次に、SIP、MIP などのさまざまなタイプのサービス用の AAA サーバのプロファイルを示します。必須およびオプションのアトリビュート、およびさまざまな機能をイネーブルにするために設定する必要があるアトリビュートを指定します。

### 簡易 IP

```
CDMA-IP-Technology = x
```

次のアトリビュートはオプションです。特定のシナリオの場合のみに必要です。

- IP アドレスの割り当ては AAA サーバを通して行われる :  
Framed-IP-Address = 8.1.0.2
- ダウンロード プール名 :  
cisco-avpair = ip:addr-pool=pdsn-pool
- 圧縮をイネーブルにする :  
cisco-avpair = "lcp:interface-config=compress stac"  
cisco-avpair = "lcp:interface-config=compress mppc"  
cisco-avpair = "cp:interface-config=compress predictor"
- その他のオプションのパラメータ  
Framed-Protocol = PPP  
Framed-Routing = None  
Service-Type = Framed

### VPDN

```
cisco-avpair = vpdn:tunnel-type=l2tp
```

cisco-avpair = vpdn:ip-addresses=5.5.5.1

cisco-avpair = vpdn:l2tp-tunnel-password=cisco

次の設定は、LNS によって接続される AAA サーバではオプションです。

cisco-avpair = ip:addr-pool=pdsn-pool

### MSID ベースの認証

- (a)簡易 IP の場合 :

cisco-avpair = cdma:cdma-realm=cisco.com

CDMA-IP-Technology = x

- (b)PMIP の場合 :

cisco-avpair = lcp:cdma-user-class=3

cisco-avpair = cdma:cdma-realm=cisco.com

cisco-avpair = "lcp:spi#0 = spi 100 key ascii cisco"

cisco-avpair = lcp:cdma-ha-ip-addr=5.5.5.1

### プロキシ モバイル IP

cisco-avpair = lcp:cdma-ha-ip-addr=5.5.5.1

cisco-avpair = "lcp:spi#0 = spi 100 key ascii cisco"

cisco-avpair = lcp:cdma-user-class=3

### モバイル IP

- cisco-avpair = lcp:cdma-user-class=2

次のアトリビュートはオプションです。特定のシナリオの場合のみに必要です。

- ダイナミック HA 割り当て :

CDMA-HA-IP-Addr = 6.0.0.2

- HA でのセキュリティ アソシエーションと固定 IP アドレスのダウンロード :

cisco-avpair = "mobileip:spi#0=spi 100 key ascii cisco"

cisco-avpair = "mobileip:static-ip-addresses=20.0.0.1 20.0.0.2 20.0.0.3 20.0.0.4"

- HA での固定 IP プール名のダウンロード :

cisco-avpair = "mobileip:spi#0=spi 100 key ascii cisco"

cisco-avpair = "mobileip:static-ip-pool=mypool"

### 前払い (オプション)

- cisco-avpair = "crb-entity-type=1"

## アトリビュート

ここでは、Cisco PDSN のさまざまな Accounting アトリビュートと Authentication アトリビュートの一部をリストに示します。

## 認証および認可の RADIUS アトリビュート

PDSN、HA、および RADIUS サーバは、アカウントサービスに関して、表 32 の RADIUS アトリビュートをサポートします。認証および認可の RADIUS アトリビュートを表 30 のリストに示します。

表 30 パケット データ サービスの認証と認証 AVP

Cisco IOS 名でサポートされる認証および認可 AVP	タイプ	ベンダー	長さ	形式	説明	アクセス要求 アクセス受諾での可否	
						あり	不可
User-Name	1	-	64	ストリング	認証および認可のユーザ名。	あり	不可
User-Password	2	-	>=18 && <=130	ストリング	認証用のパスワード。	あり	不可
CHAP-Password	3	-	19	ストリング	CHAP パスワード。	あり	不可
NAS-IP-Address	4	-	4	IP アドレス	RADIUS サーバとの通信に使用する PDSN インターフェイスの IP アドレス。	あり	不可
Service Type	6	-	4	整数	ユーザが利用するサービスのタイプ。 サポートされる値： <ul style="list-style-type: none"> <li>MSID に基づいたユーザ アクセスには Outbound</li> <li>その他のユーザ アクセスには Framed</li> </ul>	あり	あり
Framed-Protocol	7	-	4	整数	フレーミング プロトコル ユーザが使用。 サポートされる値は PPP。	あり	あり
Framed-IP-Address	8	-	4	整数	ユーザに割り当てられた IP アドレス。	あり	あり
Vendor-Specific	26	-			ベンダー固有のアトリビュート。	あり	あり
Session-Time-out	27	-	4	整数	セッションが終了するまでに、ユーザに提供されるサービスの最大秒数。 アトリビュート値は、ユーザごとの「絶対タイムアウト」になります。	不可	あり
Idle-Time-out	28	-	4	整数	セッションが終了するまでの、ユーザの最大連続アイドル接続秒数。 アトリビュート値は、ユーザごとの「アイドルタイムアウト」になります。	不可	あり
Calling-Station-ID	31	15	-	ストリング	モバイル ユーザの MSID 識別番号。	あり	不可
CHAP-Challenge (オプション)	60	-	>=7	ストリング	CHAP Challenge。	あり	不可

表 30 パケット データ サービスの認証と認証 AVP (続き)

Cisco IOS 名でサポートされる認証および認可 AVP	タイプ	ベンダー	長さ	形式	説明	アクセス要求 アクセス受諾での可否	
						不可	あり
Tunnel-Type	64	-	6	-	VPN トンネリング プロトコルを使用。 サポートされる値： • PPTP は 1 (非サポート) • L2TP は 3	不可	あり
Tunnel-Medium- Type	65	-	-	-	トンネルに使用するトランスポートメディア タイプ。	不可	あり
Tunnel-Client- Endpoint	66	-	4	ip-addr	トンネルのクライアント エンドのアドレス。	不可	あり
Tunnel-Server- Endpoint	67	-	4	ip-addr	トンネルのサーバエンドのアドレス。	不可	あり
Tunnel-Password	69	-	>=5	ストリング	リモート サーバの認証に使用するパスワード。	不可	あり
Tunnel-Assignment- ID	82	-	>=3	ストリング	トンネルの発信側に、セッションが割り当てられたトンネルの識別名を伝えます。	不可	あり
addr-pool	26/1	Cisco	>=3	ストリング	アドレス取得元のローカル プール名。service=ppp および protocol=ip と使用されます。 「addr-pool」はローカル プーリングと併用されます。ローカル プール名 (ローカルで事前に設定する必要があります) が指定されます。 ローカル プールの設定には、ip-local pool コマンドを使用してください。例： • ip address-pool local • ip local pool boo 10.0.0.1 10.0.0.10 • ip local pool moo 10.0.0.1 10.0.0.20	不可	あり
Inacl#<n>	26/1	Cisco	>=3	ストリング	現在の接続期間に使用されるインターフェイスにインストールされ適用される、入力アクセス リストの ASCII アクセス リスト識別名。 service=ppp および protocol=ip、service service=ppp および protocol=ipx で使用されます。 (注) ユーザ単位のアクセス リストは、現在 ISDN インターフェイスでは使用できません。	不可	あり



表 30 パケット データ サービスの認証と認証 AVP (続き)

Cisco IOS 名でサポートされる認証および認可 AVP	タイプ	ベンダー	長さ	形式	説明	アクセス要求 アクセス受諾での可否	
						不可	あり
Inacl	26/1	Cisco	>=3	ストリング	<p>インターフェイス 入力アクセス リストの ASCII 識別名。</p> <p>service=ppp および protocol=ip と使用されます。</p> <p>SLIP または PPP/IP の IP 出力アクセス リストが含まれます (intacl=4 など)。</p> <p>アクセスリスト自体は、ルータで事前に設定する必要があります。</p>	不可	あり
outacl#<n>	26/1	Cisco	>=3	ストリング	<p>現在の接続期間に使用されるインターフェイスにインストールされ適用される、インターフェイス出力アクセス リストの ASCII アクセス リスト識別名。</p> <p>service=ppp および protocol=ip、service service=ppp および protocol=ipx で使用されます。</p>	不可	あり
Outacl	26/1	Cisco	>=3	ストリング	<p>インターフェイス 出力アクセス リストの ASCII 識別名。</p> <p>service=ppp および protocol=ip、service service=ppp および protocol=ipx で使用されます。</p> <p>SLIP または PPP/IP の IP 出力アクセス リストが含まれます (outacl=4 など)。</p> <p>アクセスリスト自体は、ルータで事前に設定する必要があります。</p>	不可	あり
interface-config	26/1	Cisco	>=3	ストリング	<p>Virtual Profiles を持つ、ユーザ独自の AAA サーバ インターフェイス設定情報。</p> <p>等号 (=) が付いている情報は、すべての Cisco IOS インターフェイス設定コマンドとして使用できます。</p>	不可	あり

表 30 パケット データ サービスの認証と認証 AVP (続き)

Cisco IOS 名でサポートされる認証および認可 AVP	タイプ	ベンダー	長さ	形式	説明	アクセス要求	アクセス受諾での可否
SPI	26/1	Cisco	>=3	ストリング	MIP レジストレーション中にモバイル ユーザの認証に使用する、HA で必要な認証情報を伝えます。  SPI (セキュリティ パラメータ インデックス)、キー、認証アルゴリズム、認証モード、再送保護タイムスタンプ範囲を提供します。  コンフィギュレーションコマンド <b>ip mobile secure host addr</b> と同じ構文の情報です。基本的に、そのストリングの後ろに残りのコンフィギュレーション コマンドを一字一句指定します。	-	-
IP-Pool-Definition	26/217	Cisco	>=3	ストリング	X a.b.c Z という形式を使用したアドレスのプールを定義します。X はプール インデックス番号、a.b.c はプールの開始 IP アドレス、Z はプールの IP アドレスの番号です。  たとえば、3 10.0.0.1 5 はダイナミック割り当て用に 10.0.0.1 から 10.0.0.5 まで割り当てます。	不可	あり
Assign-IP-Pool	26/218	Cisco	4	整数	識別された IP プールから、IP アドレスを割り当てます。	不可	あり
Link-Compression	26/233	Cisco	4	整数	使用されるリンク圧縮プロトコル。次の値をサポートしています。  <ul style="list-style-type: none"> <li>• 0 : なし</li> <li>• 1 : Stac</li> <li>• 2 : Stac-LZS</li> <li>• 3 : MS-Stac</li> </ul>	不可	あり
Network-PMIP-NAI	26/192	3GPP2	>=9	ストリング	AGW および HA 間のネットワーク PMIP バインディングのために AGW が使用する NAI を指定します。	不可	あり
PMIP-Based-Mobility-Capability	26/193	3GPP2	6	整数	AGW が AAA サーバに対するネットワーク PMIP をサポートすることを示します。	あり	あり
PMIP-HA-Info-IPv4-Service	26/194	3GPP2	14	-	IPv4 サービスに使用されるネットワーク PMIP4 HA または PMIP6 Local Mobility Anchor (LMA) 関連の情報を指定します。	不可	あり
3GPP2-BSID	26/10	3GPP2	12	ストリング	ベースステーション ID。	あり	不可
3GPP2-PCF-IP-Addr	26/9	3GPP2	4	ip-addr	サービス側 PCF の IP アドレス。	あり	不可

表 30 パケット データ サービスの認証と認証 AVP (続き)

Cisco IOS 名でサポートされる認証および認可 AVP	タイプ	ベンダー	長さ	形式	説明	アクセス要求 アクセス受諾での可否	
						あり	不可
NAS-Port	5	-	4	整数	RADIUS サーバとの通信に使用される Cisco PDSN 上のポート番号。	あり	不可
3GPP2-User-Zone-ID	26/11	3GPP2	4	整数	Tiered Services ユーザゾーン。	あり	不可
Framed-IP Address	8	-	4	ip-addr	ユーザに割り当てられた IP アドレス。	あり	不可

表 31 パケット データ サービスの認証と認証 AVP

Cisco IOS 名でサポートされる認証および認可 AVP	タイプ	ベンダー	長さ	形式	説明	アクセス要求 アクセス受諾での可否	
						不可	あり
mobileip-mn-lifetime	26/1	Cisco	>=3	ストリング	プロキシ MIP RRQ で使用するライフタイムを定義。	不可	あり
mobileip-mn-ipaddr	26/1	Cisco	>=3	ストリング	スタティックアドレス割り当て用の MN IP アドレス。このアトリビュートが存在する場合、このアドレスは Proxy MIP RRQ で使用されます。	不可	あり
mobileip-mn-flags	26/1	Cisco	>=3	ストリング	プロキシ MIP RRQ で使用するフラグを定義します。	不可	あり
static-ip-addresses	26/1	Cisco	>=3	ストリング	同じ NAI でマルチフローのスタティックアドレスに対応する IP アドレスリスト。 • HA で使用	不可	あり
static-ip-pool	26/1	Cisco	>=3	ストリング	同じ NAI でマルチフローのスタティックアドレスに対応する IP アドレスプール名。 • HA で使用	不可	あり
ip-addresses	26/1	Cisco	>=3	ストリング	ダイナミックアドレス割り当てに使用する IP アドレスリスト。 • HA で使用	不可	あり
ip-pool	26/1	Cisco	>=3	ストリング	ダイナミックアドレス割り当てに使用する IP アドレスプール名。 • HA で使用	不可	あり

表 31 (続き) パケット データ サービスの認証と認証 AVP

CDMA-Realm	26/34	Cisco	>=3 && <=64	ストリン グ	MSID に基づいたアクセスの、 MSID@realm 形式でユーザ名を構築 するために使用する「レルム」情報。 構築されたユーザ名は、課金目的で のみ使用されます。  レルム情報のフォーマットは、次の ようになります。  • ユーザのレルムを指定する ASCII 文字列	不可	あり
CDMA-User-Class	26/35	Cisco	1	整数	ユーザが加入しているサービスのタ イプ。  次の値をサポートしています。  • SIP は 1 • MIP は 2	不可	あり
3GPP2-Reverse-Tunnel- Spec	26/4	3GPP2	4	整数	反転トンネリングの要不要を示しま す。  次の値をサポートしています。  • 反転トンネリングが不要の場合、 0。 • 反転トンネリングが必要な場合、 1。	不可	あり
3GPP2-Home-Agent- Attribute	26/7	3GPP2	4	ip address	HA のアドレス。	あり	あり
3GPP2-IP-Technology	26/22	3GPP2	4	整数	ユーザが加入しているサービスのタ イプを示します。  次の値をサポートしています。  • SIP は 1 • MIP は 2	不可	あり
3GPP2-Correlation-Id	26/44	3GPP2	8	ストリン グ	特定のユーザ フロー向けに生成され たすべてのアカウント記録レコー ドを示します。	あり	あり
3GPP2-Always-On	26/78	3GPP2	4	整数	常時接続サービスを示します。  次の値をサポートしています。  • 常時接続でないユーザには 0 • 常時接続のユーザには 1	不可	あり

## アカウントティング サービスの RADIUS アトリビュート

表 32 は、アカウントティング サービスの RADIUS アトリビュートをサポートする PDSN および RADIUS サーバのリストです。各アカウントティング メッセージのさまざまなアトリビュートに含まれるものを詳述します。メッセージのアトリビュートに含まれるものとそうでないものを設定することはできません。

表 32 パケット データ サービスのアカウントティング AVP

名前	3GPP2 タイプ	AVP Type	ベン ダー	長さ	形式	説明	参照する仕 様書	アトリビュートの存在		
								start	stop	interi m
User-Name	B2	1	-	64	ストリ ング	モバイル ユーザのネッ トワーク アクセス識別 子 (NAI)。	RFC 2865	あり	あり	あり
NAS-IP- Address	D2	4	-	4	ip-addr	PDSN/FA アドレス。	RFC 2865	あり	あり	あり
NAS-Port	-	5	-	4	整数	RADIUS サーバとの通 信に使用される PDSN 上のポート番号。	RFC 2865	あり	あり	あり
Service-Type	-	6	-	4	整数	ユーザが利用するサー ビスのタイプ。  サポートされる値：  <ul style="list-style-type: none"> <li>MSID ベースの ユーザ アクセスに は「Outbound」</li> <li>他の種類のユーザ アクセスには 「Framed」</li> </ul>	RFC 2865	あり	あり	あり
Framed- Protocol	-	7	-	4	整数	フレーミング プロトコ ル ユーザが使用。  サポートされる値：  <ul style="list-style-type: none"> <li>PPP</li> </ul>	RFC 2865	あり	あり	あり
Framed-IP- Address	B1	8	-	4	ip-addr	ユーザに割り当てられ た IP アドレス。	RFC 2865	あり	あり	あり
Calling- Station-Id	A1	31	-	15	ストリ ング	モバイル ユーザの MSID 識別番号。	RFC 2865	あり	あり	あり

表 32 パケット データ サービスのアカウントイング AVP (続き)

名前	3GPP2 タイプ	AVP Type	ベン ダー	長さ	形式	説明	参照する仕 様書	アトリビュートの存在		
								start	stop	interi m
Acct-Status- Type	-	40	-	4	整数	Accounting レコード タイプ。 サポートされる値： <ul style="list-style-type: none"> <li>• Start は 1</li> <li>• Stop は 2</li> <li>• Interim-Update は 3</li> <li>• Accounting-On は 7</li> <li>• Accounting-Off は 8</li> </ul>	RFC 2866	あり	あり	あり
Acct-Delay- Time	-	41	-	4	整数	PDSN がこのアカウン ティング レコードの送 信を試行した秒数。	RFC 2866	あり	あり	あり
Acct-Input- Octets	G2	42	-	4	整数	モバイル ユーザが送信 した IP パケットのオク テットの合計 (検証)。	RFC 2866	あり	あり	あり
Acct-Output- Octets	G1	43	-	4	整数	モバイル ユーザに対し て送信された IP パ ケットのオクテットの 合計 (検証)。	RFC 2866	あり	あり	あり
Acct-Session- Id	C1	44	-	4	ストリ ング	PDSN によって作成さ れた一意の課金 ID。 stop レコードと start レコードはログ ファイ ルと一致する必要があります。	RFC 2866	あり	あり	あり
Acct- Authentic	-	45	-	4	整数	ユーザの認証方法。 サポートされる値： <ul style="list-style-type: none"> <li>• RADIUS は 1</li> <li>• ローカルは 2</li> <li>• リモートは 3</li> </ul>	RFC 2866	あり	あり	あり
Acct-Session Time	-	46	-	4	整数	ユーザがサービス提供 を受けた秒数。	RFC 2866	あり	あり	あり
Acct-Input- Packets	-	47	-	4	整数	モバイル ユーザから送 信されたパケット数 (検証)。	RFC 2866	あり	あり	あり
Acct-Output- Packets	-	48	-	4	整数	モバイル ユーザ宛てに 送信されたパケット数 (検証)。	RFC 2866	あり	あり	あり

表 32 パケット データ サービスのアカウントリング AVP (続き)

名前	3GPP2 タイプ	AVP Type	ベン ダー	長さ	形式	説明	参照する仕 様書	アトリビュートの存在		
								start	stop	interim
EventTime stamp	G4	55	-	4	整数	RADIUS start メッセージまたは stop メッセージの一部の場合、それぞれ、課金セッションの開始または停止を示します。 RADIUS interim メッセージにも使用されます。この場合、interim メッセージがトリガされたイベントの時刻を示します。	RFC 2869	あり	あり	あり
NAS-Port-Type	-	61	-	4	整数	PDSN の物理ポートの種類。	RFC 2865	あり	あり	あり
発信元 IPv6 プレフィクス	B#	97	-	4-20	IPv6-prefix	MS の IPv6 プレフィクスを伝送します。長さには、予約されたバイト数と、プレフィクスの長さフィールドのバイト数が含まれます (RFC 3162、2.3 を参照)。	RFC 3162	あり	あり	あり
IPv6 インターフェイス ID	B4	96	-	10	ストリング	モバイル フローのインターフェイス ID。	RFC 3162	あり	あり	あり
3GPP2-ESN	A2	26/52	3GPP2	15	ストリング	ESN の ASCII 文字列。	IS-835-B	あり	あり	あり
3GPP2-MEID	A3	26/116	3GPP2	14	ストリング	MEID の ASCII 文字列。	IS-835-D	あり	あり	あり
3GPP2-HA-IP-Addr	D14	26/7	3GPP2	4	ip-addr	HA の IP アドレス。	IS-835-B	あり	あり	あり
3GPP2-PCF-IP-Addr	D3	26/9	3GPP2	4	ip-addr	サービス側 PCF の IP アドレス。	IS-835-B	あり	あり	あり
3GPP2-BSID	D4	26/10	3GPP2	12	ストリング	ベースステーション ID。	IS-835-B	あり	あり	あり
3GPP2 IS-835-D (005-D)	D7	26/108	3GPP2	37	ストリング	HRPD システムのサブネット。	IS-835-B	あり	あり	あり
3GPP2-User-Zone-ID	E1	26/11	3GPP2	4	整数	Tiered Services ユーザーゾーン。	IS-835-B	あり	あり	あり
3GPP2-Forward-Mux-Option	F1	26/12	3GPP2	4	整数	転送方向多重オプション。	IS-835-B	あり	あり	あり

表 32 パケット データ サービスのアカウントリング AVP (続き)

名前	3GPP2 タイプ	AVP Type	ベン ダー	長さ	形式	説明	参照する仕 様書	アトリビュートの存在		
								start	stop	interi m
3GPP2-Reverse-Mux-Option	F2	26/13	3GPP2	4	整数	反転方向多重オプション。	IS-835-B	あり	あり	あり
3GPP2-Service-Option	F5	26/16	3GPP2	4	整数	CDMA エア インターフェイス サービス オプション。 サポートされる値： <ul style="list-style-type: none"> <li>• 07H、</li> <li>• 0fH、</li> <li>• 1007H、</li> <li>• 016H、</li> <li>• 017H、</li> <li>• 018H、</li> <li>• 019H、 25 decimal</li> <li>• 021H、 33 decimal</li> <li>• 03BH、 59 decimal</li> </ul>	IS-835-B	あり	あり	あり
3GPP2-Forward-Traffic-Type	F6	26/17	3GPP2	4	整数	Forward Traffic Type。 サポートされる値： <ul style="list-style-type: none"> <li>• プライマリは 0</li> <li>• セカンダリは 1</li> </ul>	IS-835-B	あり	あり	あり
3GPP2-Reverse-Traffic-Type	F7	26/18	3GPP2	4	整数	Forward Traffic Type。 サポートされる値： <ul style="list-style-type: none"> <li>• プライマリは 0</li> <li>• セカンダリは 1</li> </ul>	IS-835-B	あり	あり	あり
3GPP2-Fundamental-Frame-Size	F8	26/19	3GPP2	4	整数	Fundamental Channel フレーム サイズ。 サポートされる値： <ul style="list-style-type: none"> <li>• No Fundamen- tal は 0</li> <li>• 5ms フレームは 1</li> <li>• 20ms フレームは 2</li> </ul>	IS-835-B	あり	あり	あり
3GPP2-Forward-Fundamental-RC	F9	26/20	3GPP2	4	整数	Forward Fundamental RC。 仕様書に使用に関する記述はありません。	IS-835-B	あり	あり	あり



表 32 パケット データ サービスのアカウントイング AVP (続き)

名前	3GPP2 タイプ	AVP Type	ベン ダー	長さ	形式	説明	参照する仕 様書	アトリビュートの存在		
								start	stop	interi m
3GPP2-Reverse-Fundamental-RC	F10	26/21	3GPP2	4	整数	Reverse Fundamental RC。 仕様書に使用に関する記述はありません。	IS-835-B	あり	あり	あり
3GPP2-IP-Technology	F11	26/22	3GPP2	4	整数	SIP、MIP、またはその他のテクノロジーを指定します。 サポートされる値： <ul style="list-style-type: none"> <li>• SIP は 1</li> <li>• MIP は 2</li> </ul> その他の値も設定できますが、デフォルトは次のとおりです。 <ul style="list-style-type: none"> <li>• PMIP は 2</li> <li>• VPDN は 1</li> </ul>	IS-835-B	あり	あり	あり
3GPP2-Comp-Tunnel-Flag	F12	26/23	3GPP2	4	整数	単一パケットのデータ接続中のプライベートネットワークまたはISP アクセスのための、MS に代わって確立された強制トンネルの呼び出しのインジケータ。 サポートされる値： <ul style="list-style-type: none"> <li>• トンネルなしの場合は 0</li> <li>• 非セキュア トンネルの場合は 1</li> <li>• セキュア トンネルの場合は 2</li> </ul>	IS-835-B	あり	あり	あり

表 32 パケット データ サービスのアカウントリング AVP (続き)

名前	3GPP2 タイプ	AVP Type	ベン ダー	長さ	形式	説明	参照する仕 様書	アトリビュートの存在		
								start	stop	interi m
3GPP2- Release- Indicator	F13	26/24	3GPP2	4	整数	停止レコードを送信する理由を指定します。 サポートされる値： <ul style="list-style-type: none"> <li>不明の場合は 0</li> <li>PPP/サービス タイムアウトの場合は 1</li> <li>ハンドオフの場合は 2</li> <li>PPP 終了の場合は 3</li> <li>MIP レジストレーションエラーの場合は 4</li> </ul>	IS-835-B	あり	あり	あり
3GPP2-Bad- PPP-Frame- Count	G3	26/25	3GPP2	4	整数	修正不可能なエラーが発生したために PDSN によってドロップされた、モバイル ステーションからの PPP フレームの数。	IS-835-B	あり	あり	あり
3GPP2-Num- Active- Transitions	G9	26/30	3GPP2	4	整数	ユーザによって休止からアクティブに移行された数。	IS-835-B	あり	あり	あり
3GPP2-SDB- Octet-Count- Terminating	G10	26/31	3GPP2	4	整数	ショート データ バースト経由でユーザ宛てに送信されたオクテットの合計。	IS-835-B	あり	あり	あり
3GPP2-SDB- Octet-Count- Originating	G11	26/32	3GPP2	4	整数	ショート データ バースト経由でユーザによって送信されたオクテットの合計。	IS-835-B	あり	あり	あり
3GPP2-Num- SDB- Terminating	G12	26/33	3GPP2	4	整数	ユーザ宛てに送信されたショート データ バーストのトランザクション合計。	IS-835-B	あり	あり	あり
3GPP2-Num- SDB- Originating	G13	26/34	3GPP2	4	整数	ユーザによって送信されたショート データ バーストのトランザクション合計。	IS-835-B	あり	あり	あり

表 32 パケット データ サービスのアカウントイング AVP (続き)

名前	3GPP2 タイプ	AVP Type	ベン ダー	長さ	形式	説明	参照する仕 様書	アトリビュートの存在		
								start	stop	interi m
3GPP2-IP- QOS	I1	26/36	3GPP2	4	整数	ユーザ データに関連付 けられた Differentiated Services Code Point。  仕様書に使用に関する 記述はありません。	IS-835-B	あり	あり	あり
3GPP2- Airlink-QOS	I4	26/39	3GPP2	4	整数	ユーザ データに関連付 けられたエアリンク QoS を示します。  仕様書に使用に関する 記述はありません。	IS-835-B	あり	あり	あり
3GPP2-RP- Session-ID	Y2	26/41	3GPP2	4	整数	ユーザ セッションに関 連付けられた RP Session ID。	IS-835-B	あり	あり	あり
3GPP2-Num- Bytes- Received- Total	G14	26/43	3GPP2	4	整数	PDSN の HDLC レイヤ によって反対方向で受 信した総バイト数。	IS-835-B	あり	あり	あり
3GPP2- Correlation-ID	C2	26/44	3GPP2	8	整数	PDSN でこの NAI につ いて認可されたすべての 課金セッションを示 します。	IS-835-B	あり	あり	あり
3GPP2- MobileIP- InBound- Signaling- Count	G15	26/46	3GPP2	4	整数	モバイルによって送信 されたレジストレー ション要求と請求のオ クテットの合計数。	IS-835-B	あり	あり	あり
3GPP2- MobileIP- OutBound- Signaling- Count	G16	26/47	3GPP2	4	整数	モバイル宛に送信され たレジストレーション 応答およびアダタイ ズメントのオクテット の合計数。	IS-835-B	あり	あり	あり
3GPP2- Session- Continue	C3	26/48	3GPP2	4	整数	RADIUS サーバに対す る Session Continue Indicator。  サポートされる値：  • セッション停止の 場合は 0  • セッション続行の 場合は 1	IS-835-B	あり	あり	あり

表 32 パケット データ サービスのアカウントリング AVP (続き)

名前	3GPP2 タイプ	AVP Type	ベン ダー	長さ	形式	説明	参照する仕 様書	アトリビュートの存在		
								start	stop	interi m
3GPP2-Active - Time	G8	26/49	3GPP2	4	整数	トラフィック チャンネル でのアクティブな接続 時間の合計秒。	IS-835-B	あり	あり	あり
3GPP2- DCCH- Frame-Format	F14	26/50	3GPP2	4	整数	DCCH チャンネルでのフ レーム サイズ。 サポートされる値： <ul style="list-style-type: none"> <li>• 0 (DCCH なし)</li> <li>• 1 (5 ms および 20 ms)</li> <li>• 2 (20ms)</li> <li>• 3 (5 ms)</li> </ul>	IS-835-B	あり	あり	あり
3GPP2-Always- On	F15	26/78	3GPP2	4	整数	常時接続サービスを示 します。 サポートされる値： <ul style="list-style-type: none"> <li>• イネーブルでない 場合は 0</li> <li>• イネーブルの場合 は 1</li> </ul>	IS-835-B	あり <sup>1</sup>	あり <sup>2</sup>	あり <sup>3</sup>
CDMA-Forwa rd PDCH RC	F16	26/83	3GPP2	4	整数	転送パケット データ チャンネルの無線設定 (このパラメータは、 MS が 1xEV DV の性 能を持つことを示すも のとして使用すること ができます)。	IS-835-B	あり	あり	あり
CDMA-Forwa rd DCCH Mux Option	F17	26/84	3GPP2	4	整数	転送個別制御チャンネル 多重オプション。	IS-835-B	あり	あり	あり
CDMA-Rever se DCCH Mux Option	F18	26/85	3GPP2	4	整数	反転個別制御チャンネル 多重オプション。	IS-835-B	あり	あり	あり
CDMA-Forwa rd DCCH RC	F19	26/86	3GPP2	4	整数	転送個別制御チャンネル での無線チャンネルの形 式と構成。 データ レート、変調、 拡大レートに特性を持 つ、一組の転送送信形 式 [6]。	IS-835-B	あり	あり	あり

表 32 パケット データ サービスのアカウントティング AVP (続き)

名前	3GPP2 タイプ	AVP Type	ベン ダー	長さ	形式	説明	参照する仕 様書	アトリビュートの存在		
								start	stop	interi m
CDMA-Rever se DCCH RC	F20	26/87	3GPP2	4	整数	反転個別制御チャンネル での無線チャンネルの形 式と構成。  データ レート、変調、 拡大レートに特性を持 つ、一組の反転方向送 信形式 [6]。	IS-835-B	あり	あり	あり
CDMA-Rever se PDCH RC	F22	26/114	3GPP2	4	整数	反転パケット データ チャンネルの無線設定 (このパラメータは、 MS が 1xEV DV 拡張 型反転パケット データ レートに対応している ことの指示として使用 できます)。	IS-835-B	あり	あり	あり
Flow ID	C6	26/144	3GPP2	2	ストリ ング	IP フロー ID を示しま す。	IS-835-B	あり	あり	あり
Flow Status	F24	26/145	3GPP2	4	整数	IP フロー ステータス を示します。	IS-835-B	あり	あり	あり
CDMA-Grante d QoS	I5	26/132	3GPP2	変数	ストリ ング	IP フローに許可された QoS。	IS-835-B	あり	あり	あり
RSVP Signaling Octets Inbound	G22	26/162	3GPP2	4	整数	MS によって送信され た RSVP シグナリング オクテット。	IS-835-B	あり	あり	あり
RSVP Signaling Octets Outbound	G23	26/163	3GPP2	4	整数	MS 宛てに送信された RSVP シグナリング オ クテット。	IS-835-B	あり	あり	あり
RSVP Signaling Packets Inbound	G24	26/164	3GPP2	4	整数	MS によって送信され た RSVP シグナリング パケットの数。	IS-835-B	あり	あり	あり
RSVP Signaling Packets Outbound	G25	26/165	3GPP2	4	整数	MS 宛てに送信された RSVP シグナリング パ ケットの数。	IS-835-B	あり	あり	あり

1. 常時接続サービスがユーザに対してイネーブルになっている場合にのみ、F15 が送信されます。ただし、それをすべてのユーザに送信するための設定オプションが提供されます。
2. 常時接続サービスがユーザに対してイネーブルになっている場合にのみ、F15 が送信されます。ただし、それをすべてのユーザに送信するための設定オプションが提供されます。
3. 常時接続サービスがユーザに対してイネーブルになっている場合にのみ、F15 が送信されます。ただし、それをすべてのユーザに送信するための設定オプションが提供されます。

## 前払い RADIUS アトリビュート

表 33 で、前払い固有のアトリビュートについて説明します。

表 33 前払い固有の標準アトリビュート

名前	長さ	形式	説明	アトリビュートの存在		
				アクセス要求	アクセス受諾	アクセス拒否
PPAC	>2	オクテット文字列	<ul style="list-style-type: none"> <li>PDSN 機能</li> <li>ユーザを認可するための前払いメカニズム</li> </ul>	あり (必須)	あり (必須)	-
PPAQ	>8	オクテット文字列	<ul style="list-style-type: none"> <li>ユーザを認可するための前払い割り当て</li> <li>ユーザが使用した前払い割り当て</li> </ul>	あり (必須)	あり (必須)	-
PTS	>8	オクテット文字列	<ul style="list-style-type: none"> <li>前払いタリフスイッチ機能</li> <li>タリフスイッチ後にユーザが使用した前払い割り当て</li> </ul>	あり (必須)	あり (オプション)	-

## 接続の確立/解放メッセージでの必須の AVP

表 34 に、接続の確立/解放メッセージで実行される情報エレメントを示します。

表 34 接続の確立/解放メッセージ

メッセージタイプ	説明	必須 AVP	オプション AVP	サポートされていない AVP
ICRQ	Incoming Call Request	Msg Type、Session ID、Call Serial No、Data-Message-Payload-Indicator	Calling Number1、Session Inquiry、MSC/BSID、ESN、MEID	Bearer Type、Phys Chan ID、Called Number、Sub Address
ICRP	Incoming Call	ReplyMsg Type、Session ID	-	-
ICCN	Incoming Call Connected	Msg Type、Framing Type、Tx Conn Speed2、CDMA-Service-Configuration-Record	Rx Conn Speed3、Sequencing Required	Init Rcv Cfg Msg4、Last Sent Cfg Msg、Last Rcv Cfg Msg、Proxy Auth Type、Proxy Auth Name、Proxy Auth Chal、Proxy Auth ID、Proxy Auth Resp、Private Group ID
CDN	Call Disconnect Notify	Msg Type、Result Code、Session ID	Q.931 Cause Code	-

## Call-Disconnect-Notify メッセージで使用される Q.931 原因コード

Call-Disconnect メッセージでは、未承諾のコール切断の場合に、原因コード AVP を使用して追加情報を提供します。この AVP は、原因コードと原因メッセージのフィールドで構成されます。原因コードのフィールドは、常に 0 に設定されます。L2TP セッションが切断されると、他の値が設定されます。Q.931 規格に定義されている原因コードと原因メッセージの内容は十分ではありません。Closed-RP では、コールの管理を行うために追加の値が定義されています (表 35)。

表 35 Call-Disconnect-Notify メッセージ

原因コード	原因メッセージ	説明
0	253 および 43	通常の切断。
0	254	PDSN が RP ハンドオフを完了しました。古い RP セッションが CDN で切断されました。
0	255	ICRP が Session Inquiry AVP を受信しました。要求された MSID の PPP セッションが見つかりません。
0	その他の Q.931 値	通常の切断。

## 用語集

1XRTT - 単一キャリア、無線送信テクノロジー

1xEV-DO - Evolution-Data Optimized

3GPP2 - 3rd Generation Partnership Project 2 (第 3 世代パートナーシッププロジェクト 2)

A10 - ユーザ データ用に 3GPP2 TSG-A で定義されたインターフェイス

A11 - コントロール メッセージ用に 3GPP2 TSG-A で定義されたインターフェイス

AAA - Authentication, Authorization and Accounting (認証、認可、アカウントニング)

ACCM - Asynchronous Control Character Map (非同期コントロール文字マッピング)

AGW - Access Gateway (アクセス ゲートウェイ)

AH - Authentication Header (認証ヘッダー)

AHDLC - Asynchronous High-Level Data Link Control (非同期ハイレベル データリンク コントロール)

AN - Access Network (アクセス ネットワーク)

APN - Access Point Name (アクセス ポイント ネーム)

AUX - Auxiliary (補助)

BG - Border Gateway (ボーダ ゲートウェイ)

BSC - Base Station Controller (ベース ステーション コントローラ)

BSS - Base Station Subsystem (ベース ステーション サブシステム)

BTS - Base Transceiver Station (ベース トランシーバ ステーション)

CCE - Common Classification Engine

CDMA - Code Division Multiple Access (符号分割多重接続)

CEF - Cisco Express Forwarding

CHAP - Challenge Handshake Authentication Protocol (チャレンジ ハンドシェイク 認証プロトコル)

CLID - Calling Station IDentification  
CN - Corresponding Node (対応ノード)  
CoA - Care-of-Address (気付アドレス)  
CPS - Calls Per Second (秒単位のコール)  
CRB - Cisco RADIUS Billing (Cisco RADIUS 請求) (VSA の一部)  
CVSE - Critical Vendor Specific Extension  
DES - Data Encryption Standard  
DFP - Dynamic Feedback Protocol (ダイナミック フィードバック プロトコル)  
DNS - Domain Name Server (ドメイン ネーム サーバ)  
DSCP - Differentiated Services Code Point (DiffServ コード ポイント)  
EAP - Extensible Authentication Protocol (拡張認証プロトコル)  
EIA - Electronic Industries Alliance  
ESN - Electronic Serial Number (電子シリアル番号)  
EVDO - EVolved Data Optimized  
FA - Foreign Agent (外部エージェント)  
FAC - Foreign Agent Challenge (外部エージェント チャレンジ)  
GGSN - GPRS Gateway Support Node (GPRS ゲートウェイ サポート ノード)  
GRE - Generic Routing Encapsulation (総称ルーティング カプセル化)  
HA - Home Agent (ホーム エージェント)  
HAAA - Home AAA (ホーム AAA)  
HDLC - High-Level Data Link Control (ハイレベル データリンク コントロール)  
HRPD - High Rate Packet Data  
HSRP - Hot Standby Router Protocol (ホット スタンバイ ルータ プロトコル)  
IMSI - International Mobile Subscriber Identifier  
IOMEM-I/O MEMory  
IP - Internet Protocol (インターネット プロトコル)  
IPC - Interprocessor Communication (プロセッサ間通信)  
IPCP - IP Control Protocol (IP コントロール プロトコル)  
IS-835B - CDMA 2000 Wireless Data Architecture の仕様  
ISP - Internet Service Provider (インターネット サービス プロバイダー)  
ITU - International Telecommunications Union (国際電気通信連合)  
L2TP - Layer 2 Tunneling Protocol (レイヤ 2 トンネリング プロトコル)  
LAC - L2TP Access Controller (L2TP アクセス コントローラ)  
LB - Load Balancer (ロード バランサ)  
LCP - Link Control Protocol (リンク制御プロトコル)  
LMA - Local Mobility Anchor  
LNS - L2TP Network Server (L2TP ネットワーク サーバ)  
MAC - Medium Access Control (メディア アクセス制御)



MEID - Mobile Equipment Identifier (移動体識別番号)  
MIB - Management Information Base  
MIN - Mobile Identification Number  
MIP - Mobile IP (モバイル IP)  
MN - Mobile Node (モバイル ノード)  
MQC - Modular QoS CLI  
MS - Mobile Station (モバイル ステーション) (= TE + MT)  
MSC - Mobile Switching Center  
mSEF - Mobile Severely Errored Frame  
MSID - Mobile Station Identification (モバイル ステーション ID)  
MT - Mobile Termination (モバイル ターミネーション)  
MTU - Maximum Transmission Unit (最大転送単位)  
MWAM - Multi-processor WAN Application Module (マルチプロセッサ WAN アプリケーション モジュール)  
MWTM - Mobile Wireless Transport Manager (モバイル ワイヤレス トランスポート マネージャ)  
NAI - Network Access Identifier (ネットワーク アクセス識別子)  
NAS - Network Access Server (ネットワーク アクセス サーバ)  
NMS - Network Management System (ネットワーク管理システム)  
NVRAM - Non-Volatile Random Access Memory (不揮発性ランダム アクセス メモリ)  
NVSE - Normal Vendor specific Extension (標準のベンダー固有エクステンション)  
PMIP - Proxy Mobile IP (プロキシ モバイル IP)  
PAP - Password Authentication Protocol (パスワード認証プロトコル)  
PCF - Packet Control Function (パケット制御機能)  
PCOP - Proxy Control Processor (プロキシ コントロール プロセッサ)  
PDSN - Packet Data Serving Node (パケット データ サービス ノード)  
POD - Packet Of Disconnect (パケット オブ ディスコネクト)  
PPP - Point-to-Point Protocol (ポイントツーポイント プロトコル)  
PPTP - Point-to-Point Tunneling Protocol (ポイントツーポイント トンネリング プロトコル)  
PTT - Push To Talk  
QoS - Quality of Service  
RADIUS - Remote Authentication Dial-in User Service (リモート認証ダイヤルイン ユーザ サービス)  
RAN - Radio Access Network (無線アクセス ネットワーク)  
R - Radio Frequency (無線周波数)  
RP - Radio-PDSN Interface (無線 - PDSN インターフェイス)  
RRQ - Registration Request (レジストレーション要求)  
RSVP - Resource reSerVation Protocol (リソース予約プロトコル)  
SAMI - Service and Application Module for IP  
SCCCN - Start-Control-Channel-Connected

SCCRQ - Start-Control-Connection-Reply  
 SDB - Short Data Burst (ショート データ バースト)  
 SEF - Severely Errored Frame  
 SIP - Simple IP (簡易 IP)  
 SNMP - Simple Network Management Protocol (簡易ネットワーク管理プロトコル)  
 SO - Service Option (サービス オプション)  
 SSO - Stateful SwitchOver  
 SPI Value - Security Parameter Index Value (セキュリティ パラメータ インデックス値)  
 TE - Terminal Equipment (ターミナル装置)  
 TFT - Traffic Flow Template (トラフィック フロー テンプレート)  
 TIA - Telecommunications Industry Association (米国電気通信産業協会)  
 TID - Tunnel Identifier (トンネル識別子)  
 UDR - Usage Data Record  
 UDP - User Datagram Protocol (ユーザ データグラム プロトコル)  
 VAAA - Visiting AAA  
 Vaccess - Virtual Access (仮想アクセス)  
 VPDN - Virtual Packet Data Network (仮想パケット データ ネットワーク)  
 VRF - Virtual Routing and Forwarding (VPN ルーティングおよび転送)  
 VSA - Vendor-specific Attribute (ベンダー固有アトリビュート)  
 WAP - Wireless Application Protocol (ワイヤレス アプリケーション プロトコル)

## 製品資料



(注)

印刷版および電子版の資料は、初版発行後に改訂されることがあります。改訂については Cisco.com に掲載されますので、本サイトにてご確認をお願いいたします。

表 36 に、入手可能な製品資料の一覧を示します。

表 36 製品資料

参照先	利用可能な形式
Cisco Packet Data Serving Node Release 5.1 for Cisco IOS Release 12.4(22)XR1	<ul style="list-style-type: none"> <li>PDF (マニュアル CD-ROM に収録)</li> <li>以下の Cisco.com サイトに掲載 :  <a href="http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr1/feature/guide/pdsn5_1_fcs.html">http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr1/feature/guide/pdsn5_1_fcs.html</a></li> </ul>

## 関連資料



(注)

印刷版および電子版の資料は、初版発行後に改訂されることがあります。改訂については Cisco.com に掲載されますので、本サイトにてご確認をお願いいたします。

表 37 に、入手可能な追加資料の一覧を示します。

表 37 関連資料

参照先	利用可能な形式
Command Reference for Cisco PDSN Release 5.1 in IOS Release 12.4(22)XR1	<ul style="list-style-type: none"> <li>PDF (マニュアル CD-ROM に収録)</li> <li>以下の Cisco.com サイトに掲載 :  <a href="http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr1/command/reference_xr1/pdsn_5_1cr.html">http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr1/command/reference_xr1/pdsn_5_1cr.html</a> </li> </ul>
Release Notes for Cisco PDSN Release 5.1 in IOS Release 12.4(22)XR1	<ul style="list-style-type: none"> <li>PDF (マニュアル CD-ROM に収録)</li> <li>以下の Cisco.com サイトに掲載 :  <a href="http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr1/release/notes/124_22xr1rn.html">http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_xr1/release/notes/124_22xr1rn.html</a> </li> </ul>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

© 2009 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2009–2010, シスコシステムズ合同会社.  
All rights reserved.

