Cisco GGSN リリース 9.2
コンフィギュレーション ガイド

Cisco GGSN Release 9.2 Configuration Guide

Cisco IOS リリース 12.4(22)YE2
Cisco Service and Application Module for IP
Cisco 7600 シリーズ インターネット ルータ プラットフォーム

最終更新日 2009 年 12 月 11 日

Customer Order Number: OL-19936-03-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/）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。

Cisco GGSN リリース 9.2 コンフィギュレーション ガイド

CONTENTS

このマニュアルについて

ここでは、『*Cisco GGSN リリース 9.2 コンフィギュレーション ガイド*』の対象読者、構成、および表記法について説明します。

マニュアルの変更履歴

次の表は、このマニュアルの各リリースに加えられた主な変更点を示しています。最新の変更が最初に示されています。

リビジョン	日付	変更点
OL-19936-03	12/07/2009	リリース 9.2、Cisco IOS 12.4(22)YE2。拡張クォータ サーバ インターフェイス機能に関する情報の追加。
OL-19936-02	08/04/2009	リリース 9.0、Cisco IOS 12.4(22)YE1。レイヤ 3 地理的冗長性およびパッシブ ルート抑制機能に関する情報の追加。
OL-19936-01	04/15/2009	初版。

対象読者

このマニュアルは、Cisco Gateway GPRS Support Node（GGSN）のセットアップ、インストール、設定、および運用を行うネットワーク管理者や他の担当者を対象としています。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	説明
第 1 章「GPRS および UMTS の概要」	2.5G General Packet Radio Service（GPRS; グローバル パケット ラジオ サービス）テクノロジーと 3G Universal Mobile Telecommunications System（UMTS）テクノロジー、および Cisco GGSN ソフトウェアにおけるそれらの実装について簡単に説明します。
第 2 章「ゲートウェイ GPRS サポート ノード（GGSN）の設定プランニング」	Cisco GGSN を設定する前に理解しておく必要がある情報について説明します。
第 3 章「GGSN での GTP サービスの設定」	Cisco GGSN をイネーブルにし、GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）オプションを設定する方法について説明します。
第 4 章「GGSN での IPv6 PDP サポートの設定」	Cisco GGSN で、Internet Protocol Version 6（IPv6）Packet Data Protocol（PDP; パケット データ プロトコル）コンテキストのサポートを設定する方法について説明します。
第 5 章「ゲートウェイ GPRS サポート ノード（GGSN）の GPRS トンネリング プロトコル（GTP）セッション冗長性の設定」	2 つの GGSN 間に GTP Session Redundancy（GTP-SR; GTP セッション冗長性）を設定する方法について説明します。
第 6 章「GGSN での課金の設定」	ゲートウェイ GPRS サポート ノード（GGSN）に課金機能を設定する方法について説明します。
第 7 章「拡張サービス認識課金の実装」	Cisco GGSN を拡張サービス認識 GGSN として実装する方法について説明します。拡張サービス認識 GGSN では、前払い加入者のリアルタイムのクレジット制御、および前払い加入者と後払い加入者のサービス認識課金が可能になります。
第 8 章「GGSN へのネットワーク アクセスの設定」	Cisco GGSN から Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）、Public Data Network（PDN; 公衆データ網）、および任意で Virtual Private Network（VPN; バーチャル プライベート ネットワーク）へのアクセスを設定する方法について説明します。また、GGSN にアクセス ポイントを設定する方法についても説明します。
第 9 章「GGSN での PPP サポートの設定」	GGSN でのさまざまな Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）サポート方式、およびこれらの方式の設定方法について説明します。
第 10 章「GGSN での QoS の設定」	Quality of Service（QoS）機能を設定し、Cisco GGSN でトラフィック フローを識別する方法について説明します。
第 11 章「GGSN でのセキュリティの設定」	Cisco GGSN でのセキュリティ機能の設定方法について説明します。Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）および Remote Authentication Dial-In User Service（RADIUS）についても説明します。
第 12 章「GGSN でのダイナミック アドレッシングの設定」	Cisco GGSN でダイナミック IP アドレッシングを設定する方法について説明します。
第 13 章「GGSN でのロード バランシングの設定」	Cisco IOS ソフトウェアの Server Load Balancing（SLB; サーバ ロード バランシング）機能を使用して、ロード バランシング機能をサポートするように Cisco GGSN を設定する方法について説明します。
付録 A「モニタリング通知」	GPRS または UMTS に関連する問題を管理するために、Cisco GGSN SNMP 通知をイネーブルおよびモニタリングする方法について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
`screen` フォント	システムが表示する端末セッションおよび情報は `screen` フォントで示しています。
太字の `screen` フォント	ユーザが入力しなければならない情報は、**太字の `screen` フォント**で示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、*イタリック体の screen フォント*で示しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合せは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。

（注）は、次のように表しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒントは、次のように表しています。

ヒント 「*問題解決に役立つ情報*」です。ヒントには、トラブルシューティングや操作方法ではなく、知っておくと役立つ情報が記述される場合もあります。

注意は、次のように表しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

インストールと設定に関する情報の詳細については、次の資料を参照してください。

- 『*Release Notes for Cisco GGSN Release 9.0 on the Cisco SAMI, Cisco IOS Release* 12.4(22)YE1』
- 『*Cisco Service and Application Module for IP User Guide*』
- 『*Cisco IOS Network Management Configuration Guide*』
- 『*Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers*』
- 『*Cisco 7600 Series Cisco IOS Software Configuration Guide*』
- 『*Cisco 7600 Series Cisco IOS Command Reference*』
- 『*Cisco IOS Quality of Service Solutions Configuration Guide*, Cisco IOS Release 12.4』
- Management Information Base（MIB; 管理情報ベース）の詳細については、次の URL を参照してください。

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- 『Cisco IOS Configuration Guides and Command References, Release 12.4』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

GPRS および UMTS の概要

この章では、2.5G General Packet Radio Service（GPRS; グローバル パケット ラジオ サービス）テクノロジーと 3G Universal Mobile Telecommunications System（UMTS）テクノロジー、および Cisco Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）ソフトウェアにおけるそれらの実装について簡単に説明します。

この章は、次の内容で構成されています。

概要

GPRS および UMTS は、Global System for Mobile communication（GSM; モバイル通信用グローバル システム）ネットワークが進化したものです。GSM は、世界中で使用されているデジタル セルラー テクノロジーですが、主にヨーロッパとアジアで使用されています。GSM は、デジタル ワイヤレス通信において、世界をリードする規格です。

GPRS は、2.5G のモバイル通信テクノロジーです。2.5G を利用すると、モバイル ワイヤレス サービス プロバイダーは、GSM ネットワークを介したパケットベースのデータ サービスをモバイル加入者に対して提供できます。GPRS は、インターネット アクセス、イントラネットまたは企業内アクセス、インスタント メッセージ、マルチメディア メッセージなどに一般的に適用されています。GPRS は、European Telecommunications Standards Institute（ETSI; ヨーロッパ電気通信標準化協会）によって標準化されました。現在では、GPRS の標準化作業は Third Generation Partnership Program（3GPP; 第 3 世代パートナーシップ プロジェクト）で行われています。

UMTS は 3G のモバイル通信テクノロジーであり、Wideband Code Division Multiple Access（W-CDMA; 広帯域コード分割多重アクセス）無線テクノロジーを提供します。W-CDMA テクノロジーによって、より高いスループット、リアルタイム サービス、およびエンドツーエンドの Quality of Service（QoS）を実現できます。W-CDMA テクノロジーでは、モバイル ワイヤレス加入者に対して、画像、グラフィック、ビデオ通信などのマルチメディア情報、および音声、データを提供することもできます。UMTS は、3GPP によって標準化されました。

GPRS/UMTS パケット コアは、2 つの主要なネットワーク要素によって構成されています。

- ゲートウェイ GPRS サポート ノード（GGSN）

  モバイル携帯電話ユーザに、Public Data Network（PDN; 公衆データ網）または指定されたプライベート IP ネットワークに対するアクセスを提供します。

  Cisco GGSN は、Cisco IOS ソフトウェアによって実装されています。

- Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）

  Radio Access Network（RAN; 無線アクセス ネットワーク）を GPRS/UMTS コアに接続します。SGSN では、次の処理が行われます。

  - ユーザ セッションを GGSN にトンネリングします。
  - Mobile Station（MS; モバイル ステーション）との間でデータを送受信します。
  - モバイル ステーション（MS）の位置に関する情報を保持します。
  - MS および GGSN と直接通信します。

  SGSN のサポートは、シスコのパートナー、またはその他のベンダーによって提供されます。

図 1-1 は、Cisco 7600 シリーズ ルータの Cisco Service and Application Module for IP（SAMI）で GGSN が実装された場合のネットワーク構成要素を示しています。

図 1-1　Cisco 7600 シリーズ ルータの SAMI で GGSN が実装された場合の GPRS/UMTS ネットワーク構成要素

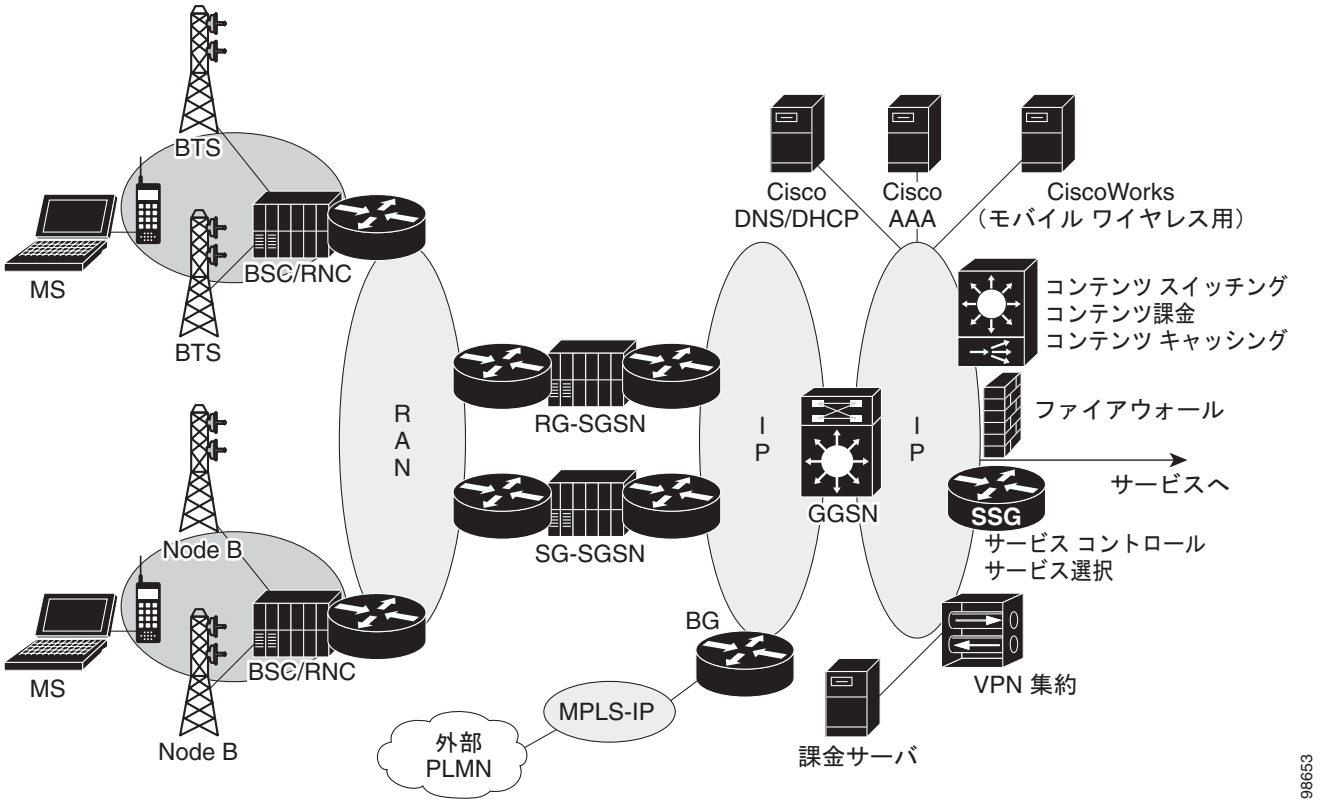


図 1-1 に示すように、RAN は、2.5G と 3G とでは異なる構成要素で構成されています。

2.5G 環境では、RAN は Base Transceiver Station（BTS; 無線基地局）に接続するモバイル ステーションで構成されています。BTS から Base Station Controller（BSC; ベース ステーション コントローラ）に接続されます。3G 環境では、RAN は Node B に接続するモバイル ステーションから構成されます。Node B から Radio Network Controller（RNC; 無線ネットワーク コントローラ）に接続されます。

RAN は、SGSN を介して GPRS/UMTS コアに接続します。SGSN は、サービス ネットワーク（インターネットやイントラネットなど）へのゲートウェイとして動作する GGSN にユーザ セッションをトンネリングします。SGSN と GGSN との間の接続は、GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）と呼ばれるトンネリング プロトコルを使用して確立されます。GTP バージョン 0（GTPv0）は 2.5G アプリケーションに対応し、GTP バージョン 1（GTPv1）は 3G アプリケーションに対応しています。GTP は、IP 上で伝送されます。

ネットワーク内の複数の SGSN および GGSN は、まとめて GPRS Support Node（GSN; GPRS サポート ノード）と呼ばれます。

（注）　事業者固有の設定に応じて、RAN、GPRS/UMTS コア、およびサービス ネットワークは、IP ネットワークまたは Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）ネットワークとなります。

GGSN では、モバイル セッションに IP アドレスを割り当てる場合、アクセス ポイントに定義された次のいずれかの方法が使用されます。

- Dynamic Host Configuration Protocol（DHCP）
- Remote Authentication Dial-In User Service（RADIUS）サーバ
- GGSN 上に設定されたローカル アドレス プール

GGSN では、RADIUS サーバを使用して、リモート ユーザを認可および認証できます。DHCP および RADIUS は、グローバル レベルで設定することも、GGSN に設定されたアクセス ポイントごとに設定することもできます。

IPSec Virtual Private Network（VPN）Acceleration Services Module では、IPSec による暗号化が実行されます。

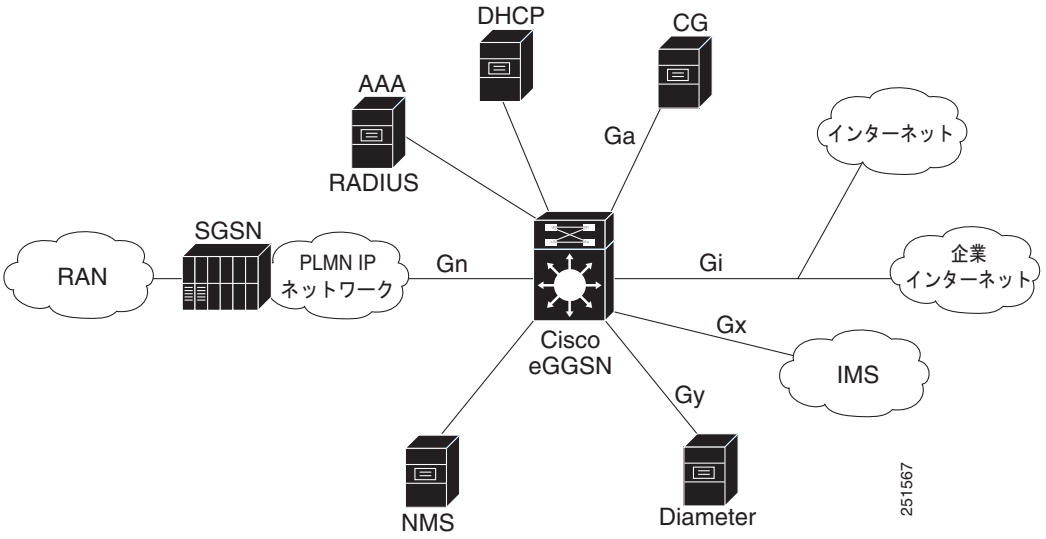
GPRS インターフェイス リファレンス モデル

2.5G GPRS 規格および 3G UMTS 規格では、異なるネットワーク要素間の通信パスを指すために*インターフェイス*という用語が使用されます。GPRS/UMTS 規格では、これらのインターフェイスを介した異なる GPRS/UMTS ネットワーク要素間の通信における要件および特性が定義されています。GPRS/UMTS ネットワークの説明では、これらのインターフェイスについて頻繁に言及されます。

図 1-2 は、Cisco GGSN 機能に実装されている主なインターフェイスを示しています。

- Gn/Gp インターフェイス：GGSN と SGSN との間のインターフェイス。Gn インターフェイスは、GPRS/UMTS ネットワークの同じ Public Land Mobile Network（PLMN; パブリック ランド モバイル ネットワーク）内の 2 つの GSN 間のインターフェイスです。Gp インターフェイスは、異なる PLMN にある 2 つの GSN 間のインターフェイスです。GTP は、Gn/Gp インターフェイスで定義されたプロトコルです。
- Gi インターフェイス：GPRS/UMTS ネットワークと、外部 Packet Data Network（PDN; パケット データ ネットワーク）との間の参照ポイント。
- Ga インターフェイス：GPRS/UMTS ネットワーク内の、GGSN と課金ゲートウェイとの間のインターフェイス。

図 1-2　GGSN インターフェイス



Cisco GGSN 機能には、次のような追加のインターフェイスが実装されています。

- Gy：拡張サービス認識課金のための、Diameter Credit Control Application（DCCA）用の Diameter サーバへのインターフェイス。
- Gx：Policy and Charging Rules Function（PCRF; ポリシー / 課金ルール機能）と Policy and Charging Enforcement Function（PCEF; ポリシー / 課金実施機能）との間の参照ポイント。Gx インターフェイスは、Policy and Charging Control（PCC; ポリシー / 課金制御）ルールのプロビジョニングおよび削除に使用されます。Gx インターフェイスでは、Diameter プロトコルが使用されます。
- AAA インターフェイス：Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバへのインターフェイス。AAA インターフェイスでは、RADIUS プロトコルが使用されます。
- DHCP：DHCP サーバ インターフェイス。
- NMS：ネットワーク管理インターフェイス。

仮想テンプレート インターフェイス

GGSN と SGSN との間、および GGSN と PDN との間の接続を設定するために、Cisco GGSN ソフトウェアでは、*仮想テンプレート* インターフェイスという内部インターフェイスが使用されます。仮想テンプレートは、論理インターフェイスです。仮想テンプレートは、特定のインターフェイスには直接結び付けられませんが、インターフェイスにダイナミックに関連付けることができます。

仮想テンプレート インターフェイスには、ルータ上の物理インターフェイスと同様に IP アドレスを割り当てることができます。また、仮想テンプレート インターフェイスに IP ルーティング特性を設定することもできます。仮想テンプレート インターフェイスでは、特定の GPRS/UMTS 固有の要素を設定する必要があります。たとえば、GTP カプセル化を設定したり（SGSN との通信に必要です）、ネットワーク上のどの PDN がアクセス可能かを判断するために GGSN によって使用されるアクセス リストを設定したりする必要があります。

アクセス ポイント設定

GPRS/UMTS 規格では、Access Point Name（APN; アクセス ポイント ネーム）と呼ばれるネットワーク ID が定義されています。APN によって、ユーザが GPRS/UMTS ネットワーク内の GGSN から接続可能なサービスまたはネットワークが識別されます。

APN を設定するために、Cisco IOS GGSN ソフトウェアでは次の設定要素を使用します。

- アクセス ポイント：APN およびそれに関連付けられたアクセス特性を定義します。アクセス特性には、セキュリティやダイナミック アドレッシング方式などがあります。
- アクセス ポイント リスト：GGSN の仮想テンプレートに関連付けられる論理インターフェイス。アクセス ポイント リストには、1 つ以上のアクセス ポイントが含まれています。
- アクセス グループ：PDN との間のアクセスを制御するためにアクセス ポイントに追加で設定されるセキュリティ。従来の IP アクセス リストの定義に従って MS から GGSN へのアクセスを許可する場合、IP アクセス グループには（アクセス ポイントで）PDN へのアクセスを許可するかどうかも定義します。IP アクセス グループ設定では、PDN から MS へのアクセスを許可するかどうかも定義できます。

アクセス ポイント設定の詳細については、「GGSN でのアクセス ポイントの設定」（P.8-7）を参照してください。

利点

2.5G GPRS テクノロジーには、次のような利点があります。

- 既存の回線交換 GSM ネットワーク上でパケットベースの無線インターフェイスを利用できます。これにより、無線帯域幅はパケットの送受信時にだけ使用されるため、無線スペクトラムの効率性が大幅に向上します。
- 現在広く導入されている GSM 上に GPRS サービスを追加することを希望するネットワーク サービス プロバイダーに対しては、既存の GSM ネットワーク インフラストラクチャに対するアップグレードがサポートされています。
- 従来の回線交換 GSM データ サービスよりも高速なデータ レートがサポートされています。
- Short Message Service（SMS; ショート メッセージ サービス）よりも長いメッセージがサポートされています。
- データ ネットワークおよびサービスに対する幅広いアクセス方法がサポートされています。アクセス方法には、VPN や Internet Service Provider（ISP; インターネット サービス プロバイダー）を経由した企業サイト アクセスや、Wireless Application Protocol（WAP; ワイヤレス アプリケーション プロトコル）などがあります。

上記の利点に加えて、3G UMTS テクノロジーには次の利点があります。

- 約 256 Mbps というより高速なデータ レートがサポートされています。
- 指定された QoS での、コネクション型無線アクセス ベアラがサポートされており、これによりエンドツーエンドの QoS が確保されます。

Cisco IOS リリース 12.4(22)YE2 で導入された機能

Cisco GGSN リリース 9.2、Cisco IOS リリース 12.4(22)YE2 では、Cisco GGSN と Cisco CSG2 との間の*拡張*クォータ サーバ インターフェイス上でのサービス コントロール メッセージの交換がサポートされるようになりました。

このサポートにより、Cisco GGSN において、Cisco GGSN リリース 9.2 よりも前のリリースでサポートされていたサービス認識前払いユーザおよびサービス認識後払いユーザに加えて、次のタイプのユーザに対して eG-CDR を生成できるようになりました。

- サービス認識前払い（GTP）ユーザ

  OCS アドレス選択を使用して実装されたサービス認識 GGSN では、GGSN は前払いユーザのクォータ サーバとして機能しません。OCS アドレス選択が実装されたサービス認識 GGSN では、Cisco CSG2 が、クォータを取得する OCS サーバとの直接の GTP 接続を確立します。GGSN は、拡張クォータ サーバ インターフェイス経由でサービス使用状況を取得して、eG-CDR を生成します。

- サービス認識後払いユーザ

  GGSN は、サービス認識後払いユーザのクォータ サーバとして機能しません。GGSN は、拡張クォータ サーバ インターフェイスを使用して、Cisco CSG2 から使用状況を取得し、その使用状況を eG-CDR に追加します。

- ポリシー / 課金制御（PCC）対応（Gx）ユーザ

  Gx 対応ユーザが前払い（Gy）ユーザでもある場合は、eG-CDR 生成のサポートが Cisco IOS リリース 12.4(22)YE2 以前のリリースに存在しており、クォータ サーバ メッセージで受信した使用状況に基づいてサービス コンテナが eG-CDR に追加されます。

  Gx ユーザが、CSG2 と OCS の直接インターフェイスが存在する実装での前払いユーザ、または（サービス認識または非サービス認識の）後払いユーザでもある場合、GGSN は拡張クォータ サーバ インターフェイス経由で CSG2 から使用状況を取得し、その使用状況を eG-CDR に追加します。

（注） Cisco IOS リリース 12.4(22)YE2 以降では、拡張クォータ サーバ インターフェイスが GGSN でイネーブルになっている場合、GGSN はサービス認識後払いユーザまたは Gx 後払いユーザのクォータ サーバとして機能しないため、これらのユーザは Cisco CSG2 で後払いとして設定する必要があります。Cisco CSG2 の設定の詳細については、『*Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide*』を参照してください。

拡張クォータ サーバ インターフェイスの設定、およびサービス コントロール メッセージ交換のサポートのイネーブルについては、「GGSN でのクォータ サーバ インターフェイスの設定」（P.7-6）を参照してください。

Cisco IOS リリース 12.4(22)YE1 で導入された機能

Cisco GGSN リリース 9.0、Cisco IOS リリース 12.4(22)YE1 では、次の機能のサポートが導入されました。

- レイヤ 3 地理的冗長性
- パッシブ ルート抑制

レイヤ 3 地理的冗長性

Cisco GGSN リリース 9.0、Cisco IOS リリース 12.4(22)YE1 では、レイヤ 3 地理的 GTP セッション冗長性のサポートが導入されました。

Cisco GGSN ソフトウェアでは、Cisco IOS Hot Standby Routing Protocol（HSRP; ホットスタンバイ ルーティング プロトコル）、Cisco IOS Check-point Facility（CF）と Redundancy Framework（RF）、および Stream Control Transmission Protocol（SCTP）を使用して、Layer 2（L2; レイヤ 2）のローカル GTP-SR および Layer 3（L3; レイヤ 3）の地理的 GTP-SR（リモート冗長性）の実装をサポートしています。

HSRP は、IP ネットワークにネットワーク冗長性を提供し、ネットワーク エッジ デバイスまたはアクセス回線における第 1 ホップの障害からユーザ トラフィックが即時かつ透過的に回復されることを保証します。

L3 HSRP を使用した地理的冗長性の実装では、アクティブ Cisco GGSN およびスタンバイ Cisco GGSN は、WAN を介して接続された Cisco SAMI 上に設定されます。Cisco GGSN ソフトウェアの以前のリリースでは、アクティブ GGSN とスタンバイ GGSN との間の接続は、LAN だけに制限されていました（L2 HSRP）。

ローカル冗長性または地理的冗長性を実装できますが、これらの実装は相互に排他的です（1 つの GGSN に、両方のタイプの冗長性を同時に設定することはできません）。

地理的冗長性設定の実装については、第 5 章「ゲートウェイ GPRS サポート ノード（GGSN）の GPRS トンネリング プロトコル（GTP）セッション冗長性の設定」を参照してください。

パッシブ ルート抑制

地理的冗長性の実装では、ルーティング アップデートを送信する必要があるのはアクティブ GGSN だけです。したがって、地理的冗長性を実装する場合、GGSN がスタンバイ モードのときは、GGSN インターフェイスからルーティング アップデートが送信されないように設定する必要があります。

パッシブ ルート抑制をイネーブルにする方法の詳細については、第 5 章「ゲートウェイ GPRS サポート ノード（GGSN）の GPRS トンネリング プロトコル（GTP）セッション冗長性の設定」を参照してください。

Cisco IOS リリース 12.4(22)YE で導入された機能

Cisco GGSN リリース 9.0、Cisco IOS リリース 12.4(22)YE では、次の機能のサポートが導入されました。

次の既存の機能の拡張も導入されました。

- 「デバッグ」（P.1-11）
- 「DFP 重み」（P.1-12）
- 「HSPA QoS 拡張機能」（P.1-12）
- 「管理情報ベース（MIB）」（P.1-13）
- 「モバイル ステーション背後の複数のサブネット」（P.1-13）
- 「統計情報」（P.1-13）

粒状課金およびストレージ

Cisco GGSN では、グローバル レベルおよびアクセス ポイント レベル（粒状課金）の 2 つのレベルにおける課金設定がサポートされています。

粒状課金では、GGSN ごとに最大 30 個の*課金グループ*を設定できます。各グループでは、一意のプライマリ、セカンダリ、およびターシャリの課金ゲートウェイと、iSCSI ターゲットを定義できます。また、課金グループは、APN と関連付けることができます。

課金グループを使用すると、課金レコードを所属先の APN ごとに異なる宛先に送信できます。

APN に関連付けられている課金グループがない場合は、デフォルトの課金グループが使用されます。デフォルトの課金グループとは、グローバル レベルで設定された課金ゲートウェイ、iSCSI ターゲット、スイッチオーバー優先度などを指します。

課金グループ 0 が、グローバル レベルで定義されるデフォルト課金グループです。これ以外に、課金グループ 1 ～ 29 を設定して、APN と関連付けることができます。

粒状課金およびストレージについては、「粒状課金およびストレージの設定」（P.6-25）を参照してください。

GRX トラフィック分離

Cisco GGSN は、Gn および Gp インターフェイスで SGSN からのトラフィックを受信します。Gn トラフィックは、同じ PLMN 内の SGSN から受信します。Gp トラフィックは、異なる PLMN 内の SGSN から受信します。これらのトラフィックは、GPRS Roaming Exchange（GRX）経由で GGSN に着信します。

プライバシーやセキュリティを確保するために、Cisco GGSN では、Gn インターフェイスにおいて VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）がサポートされています。Gn インターフェイスで VRF がサポートされているため、GRX トラフィックを分離して、異なるルーティング テーブルに属するものとすることができます。

Gn インターフェイスで GRX トラフィックを分離するための VRF の設定については、「GGSN Gn インターフェイスでの GRX トラフィックの分離」（P.11-31）を参照してください。

Gx インターフェイス

Cisco GGSN リリース 9.0 以降、APN をポリシー / 課金制御（PCC）対応にすることができます。

PCC 対応 APN（Gx インターフェイス）は、PCRF と PCEF との間の参照ポイントです。PCC ファイルを PCRF から PCEF にプロビジョニングおよび削除するために使用されます。

Cisco GGSN における PCC 対応 APN については、「APN での PCC のイネーブル」（P.7-30）を参照してください。

Gy インターフェイス

Cisco Content Services Gateway - 2nd Generation（CSG2）アプリケーションと連携するように設定された場合、Cisco GGSN ではオンライン課金がサポートされます。Cisco GGSN では、Diameter Credit Control Application（DCCA）インターフェイスにおいて Cisco IOS Diameter プロトコルを使用したオンライン課金がサポートされています。DCCA インターフェイスは、Gy インターフェイスとも呼ばれます。

以前のリリースでは、Cisco GGSN は汎用 DCCA（RFC 4006『*Diameter Credit-Control Application*』に定義されています）、および一部の 3GPP アトリビュート（3GPP 技術仕様書 32.299『*Telecommunication Management; Charging management; Diameter Charging Applications*』に定義されています）をサポートしていました。

Cisco GGSN リリース 9.0 以降では、Gy インターフェイスは、次の追加の 3GPP 機能をサポートするように拡張されました。

- 前払い Packet Data Protocol（PDP; パケット データ プロトコル）の次のトリガー タイプでのトリガー タイプ AVP のサポート。
  - CHANGE_IN_SGSN_IP_ADDDRESS
  - CHANGE_IN_QOS
  - CHANGE_IN_LOCATION
  - CHANGE_IN_RAT

  3GPP トリガー タイプ AVP は、Multiple-Service-Credit-Control（MSCC; 複数サービス信用管理）AVP に含まれています。MSCC AVP は、DCCA サーバから Cisco GGSN 機能に送信される Credit Control Answer（CCA; クレジット制御応答）内にあります。Cisco GGSN は、DCCA クライアントとして動作します。

  CCA は、複数の MSCC AVP を含むことができます。サポートされているカテゴリのいずれかを GGSN が受信すると、関連する各カテゴリに対してトリガーがイネーブルになります。これらのカテゴリは、Cisco GGSN コマンドを使用してイネーブルにすることもできます。詳細については、『*Cisco GGSN Configuration Guide*』の「Configuring Enhanced Service-Aware Billing」を参照してください。

  MSCC AVP で与えられたクォータは、カテゴリ（つまりサービス）と関連付けられています。各 MSCC AVP は、3GPP トリガー タイプ AVP を含むことができます。これらの 3GPP トリガー タイプ AVP では、関連付けられたクォータを DCCA クライアントが再認可する原因となるイベントが指定されます。

（注） サポートされていない 3GPP トリガー タイプが指定された MSCC を受信した場合、GGSN はこれらの MSCC を無視します。サポートされていないトリガー タイプを受信した場合は、以前にインストールされたトリガーが適用されます。

- 次の再認可しきい値のサポート。
  - Time-Quota-Threshold
  - Volume-Quota-Threshold
  - Time-Quota-Mechanism

  任意で、DCCA サーバは、上記の 3GPP AVP を含む MSCC AVP が設定された CCA を送信できます。これらの AVP は、GGSN に対して、クォータのしきい値に達した場合に再認可を要求するように指示します。

（注）　Time-Quota-Mechanism は、Cisco GGSN リリース 9.0 では完全にはサポートされていません。

詳細については、「DCCA メッセージのベンダー固有 AVP のサポートのイネーブル」（P.7-24）を参照してください。

Cisco GGSN Gy インターフェイスに対する拡張をサポートするために、次のコマンドが変更されました。

- **content postpaid**
- **gprs charging service-record include**
- **gprs dcca**
- **trigger**

合法的傍受

合法的傍受によって、裁判所または行政機関による命令を根拠として、Law Enforcement Agency（LEA; 司法当局）が個人に対して電子監視を実施できます。合法的傍受プロセスを容易にするために、特定の法律および規制によって、Service Provider（SP; サービス プロバイダー）およびインターネット サービス プロバイダー（ISP）に対して、認可された電子監視を明示的にサポートするようにネットワークを実装することが定められています。

Cisco GGSN リリース 9.0 以降では、Cisco GGSN に合法的傍受のサポートを実装できます。Cisco GGSN における合法的傍受のサポートの詳細については、「Cisco GGSN での合法的傍受サポートの実装」（P.11-36）を参照してください。

P-CSCF ロード バランシング

Cisco GGSN では、Proxy Call Session Control Function（P-CSCF）ロード バランシングがサポートされています。

P-CSCF ロード バランシングがイネーブルになっている場合、Cisco GGSN では、ラウンドロビン アルゴリズムを使用して、PDP コンテキストの作成応答で送信する P-CSCF サーバを選択します。P-CSCF サーバは、PDP コンテキストの作成要求に Protocol Configuration Option（PCO; プロトコル設定オプション）Information Element（IE; 情報エレメント）の P-CSCF アドレス要求フィールドが含まれている場合に送信されます。

P-CSCF ロード バランシングがイネーブルになっていない場合、Cisco GGSN は事前に設定されたすべての P-CSCF サーバのリストを送信します。

P-CSCF ロード バランシングのイネーブルについては、「APN での Proxy-CSCF 検出サポートの設定」（P.8-48）を参照してください。

スタンドアローン GGSN の前払いクォータ実施

Cisco GGSN では、2 種類の前払いクォータ実施がサポートされています。

前払いクォータ実施は、eGGSN 設定（Cisco CSG2 と連携するように設定された Cisco GGSN）またはスタンドアローン モードで動作する Cisco GGSN によって行うことができます。

スタンドアローン モードの Cisco GGSN で前払いクォータ実施を行う場合、GGSN は、データ量ベース、時間ベース、またはその両方で前払い加入者のデータ パケットをモニタリングします。

スタンドアローン GGSN 前払いクォータ実施の設定については、「スタンドアローン GGSN の前払いクォータ実施の設定」（P.7-31）を参照してください。

機能拡張

Cisco GGSN リリース 9.0 では、次の機能が拡張されました。

- 「デバッグ」（P.1-11）
- 「DFP 重み」（P.1-12）
- 「Gy インターフェイス」（P.1-9）
- 「HSPA QoS 拡張機能」（P.1-12）
- 「管理情報ベース（MIB）」（P.1-13）
- 「モバイル ステーション背後の複数のサブネット」（P.1-13）
- 「統計情報」（P.1-13）

デバッグ

Cisco リリース 9.0 では、次のデバッグ アクションを実行できます。

- **debug gprs verbose** 特権 EXEC コマンドを使用した、デバッグ コマンドの詳細レベルの制御。
- **next-call** キーワード オプションを指定して **debug condition** 特権 EXEC コマンドを使用することによる、GGSN に対する next-call 条件付きデバッグの設定。

  最大 5 つの next-call 条件付きデバッグ設定、または next-call デバッグ条件が設定された PDP を任意のタイミングで設定できます。

  next-call 条件付きデバッグをモニタリングおよびメンテナンスするには、次のコマンドを使用します。

  - 既存の next-call デバッグ条件または next-call デバッグ条件が設定された PDP を表示する場合は、**show debugging condition** コマンド
  - 既存の PDP に設定されているデバッグをクリアする場合は **clear gprs gtp debug next-call** コマンド
  - next-call デバッグ条件を削除する場合は、**next-call** キーワードが指定された **no debug condition** コマンド

DFP 重み

Cisco GGSN Dynamic Feedback Protocol（DFP）サポートが拡張されました。Cisco GGSN リリース 9.0 では、CPU およびメモリの負荷が、DFP の重み計算の要素として組み込まれています。

GTP ロード バランシングでは、Cisco IOS SLB が DFP マネージャとして定義され、サーバ ファームの各 GGSN に DFP エージェントが定義されます。DFP エージェントは、GGSN の重みをレポートします。DFP エージェントは、CPU 使用率、プロセッサ メモリ、および各 GGSN に対して開始できる PDP コンテキストの最大数に基づいて各 GGSN の重みを計算します。

各 GGSN の重みは、主に、許可されている PDP コンテキストの最大数に対する GGSN 上の既存の PDP コンテキストの比率に基づいています。

デフォルトでは、CPU 使用率およびメモリ使用率は、使用率が 85% を超えてからでないと DFP の重み計算に組み込まれません。Cisco GGSN リリース 9.0 では、CPU およびメモリの負荷が重み付け計算で考慮される基準となる利用率を設定できます。使用率をカスタマイズするには、**cpu-load** および **mem-load** キーワード オプションを指定して **gprs dfp** グローバル コンフィギュレーション コマンドを使用します。

gprs dfp コマンドは、DFP 重みの拡張機能をサポートするように変更されています。

DFP 重みの設定については、「GGSN での DFP サポートの設定」（P.13-21）を参照してください。

HSPA QoS 拡張機能

High-Speed Uplink Packet Access（HSUPA; 高速アップリンク パケット アクセス）と High-Speed Downlink Packet Access（HSDPA; 高速ダウンリンク パケット アクセス）は、あわせて High-Speed Packet Access（HSPA; 高速パケット アクセス）と呼ばれます。

HSPA は、W-CDMA におけるパケットベースのデータ サービスであり、次の機能によって既存のプロトコルのパフォーマンスを拡張および向上するものです。

- 5 MHz 帯域幅において、最大 8 ～ 256 Mbps のデータ転送をサポートします。
- モバイル デバイスが、ビデオ クリップなどの大容量のデータを PDN との間で送受信することを可能にします。
- ビデオ会議などの、大量のデータをやり取りするサービスをサポートします。

Cisco GGSN は、MS によってネットワークに送信されるサービス リクエスト内の QoS 情報を受信します。QoS 情報によって、MS が要求するサービスのタイプが決定されます。GGSN は、現在の動作状態に基づいて、ネゴシエーションされた QoS を返します。ネゴシエーションされた QoS によって、ユーザが実際に経験するサービスの品質が決定されます。

（注）　HSPA は、GTPv1 PDP コンテキストでだけサポートされています。

CAC 最大 QoS ポリシーの設定については、「CAC 最大 QoS ポリシーの設定」（P.10-13）を参照してください。

次の Cisco GGSN CAC 最大 QoS ポリシー コンフィギュレーション コマンドが変更されて、HSPA 用の大きな値がサポートされるようになりました。

- **gbr traffic-class**
- **mbr traffic-class**

管理情報ベース（MIB）

Cisco GGSN リリース 9.0 以降では、CISCO-ISCSI MIB がサポートされています。

モバイル ステーション背後の複数のサブネット

Cisco GGSN ソフトウェアの以前のリリースでは、モバイル ステーション背後へのルーティング機能においては、MS 背後に 1 つのサブネットだけを設定できました。Framed-Route（アトリビュート 22）に複数のルートが含まれている場合、GGSN では最初のルートが使用され、後続のすべてのルートは無視されていました。

Cisco GGSN リリース 9.0 以降、Cisco GGSN では、MS あたり最大 16 のサブネットを設定できます。

MS 背後での複数のサブネットの設定については、「APN でのモバイル ステーション背後へのルーティングの設定」（P.8-45）を参照してください。

統計情報

Cisco GGSN リリース 9.0 では、次の統計情報拡張のサポートが導入されました。

- **GPRS スループット**

  gprs throughput intervals グローバル コンフィギュレーション コマンドを使用して設定された 2 つの間隔の間に収集されたスループット統計情報で保持する履歴項目数を設定するには、グローバル コンフィギュレーション モードで **gprs throughput history** コマンドを使用します。

  最新のスループット統計情報を表示するには、**show gprs throughput history** 特権 EXEC コマンドを使用します。スループット統計情報の履歴を表示するには、**show gprs throughput history** 特権 EXEC コマンドを使用します。

- **コール セットアップ レート**

  APN のコール レート統計情報が収集される間隔を設定するには、グローバル コンフィギュレーション モードで **gprs callrate interval** コマンドを使用します。設定された間隔の間に収集されたコール レート統計情報で保持する履歴項目数を設定するには、グローバル コンフィギュレーション モードで **gprs callrate history** コマンドを使用します。

  最新のコール レート統計情報を表示するには、**show gprs callrate** 特権 EXEC コマンドを使用します。コール レート統計情報の履歴を表示するには、**show gprs callrate history** コマンドを使用します。

以前のリリースで導入された機能

Cisco GGSN では、以前のリリースで導入された次の機能もサポートしています。

- Release 99（R99）、Release 98（R98）、および Release 97（R97）のサポートと準拠
- GTPv0 および GTPv1 メッセージング
- IP PDP および PPP PDP タイプ
- GTPv0 と GTPv1 の両方、および IP PDP タイプと PPP PDP タイプに対する Cisco Express Forwarding（CEF）スイッチング
- GTPv1 PDP では、最大 11 のセカンダリ PDP コンテキストのサポート
- 仮想 APN

- APN ごとの VPN ルーティングおよび転送（VRF）
- VRF インスタンスあたり複数の APN
- VPN サポート
  - Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネリング
  - PPP PDP タイプの Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）拡張機能
  - IP PDP タイプの PPP 再生成
  - 802.1Q Virtual LAN（VLAN; 仮想 LAN）
- セキュリティ機能
  - 重複 IP アドレス保護
  - PLMN 範囲チェック
  - 外部モバイル ステーションのブロック
  - スプーフィング防止機能
  - モバイル ステーション間のリダイレクション
- QoS
  - UMTS クラス、およびディファレンシエーテッド サービス（DiffServ）とのインターワーキング
  - 遅延 QoS
  - 標準 QoS
  - GPRS QoS（R97 および R98）から UMTS QoS（R99）、およびその逆への変換
  - Call Admission Control（CAC; コール アドミッション制御）
  - Per-PDP ポリシング
- ダイナミック アドレス割り当て
  - 外部 DHCP サーバ
  - 外部 RADIUS サーバ
  - ローカル プール
- APN ごとの統計情報
- 匿名アクセス
- RADIUS 認証およびアカウンティング
- アカウンティング
  - 待機アカウンティング
  - PDP ごとのアカウンティング
  - APN にマッピングされた RADIUS サーバ グループを使用した認証およびアカウンティング
  - IP PDP タイプの 3GPP Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）
  - 透過モード アカウンティング
  - クラス アトリビュート
  - 中間更新

  - セッション アイドル タイマー
  - Packet of Disconnect（PoD; パケット オブ ディスコネクト）
- ダイナミック エコー タイマー
- 2.5G および 3G SGSN 間での GGSN インターワーキング、および次の方向での Registration Authority（RA; 登録局）更新
  - 2.5G SGSN から 2.5G SGSN
  - 2.5G SGSN から 3G SGSN
  - 3G SGSN から 3G SGSN
  - 3G SGSN から 2.5G SGSN
- 課金
  - 時間トリガー
  - 課金プロファイル
  - ターシャリ課金ゲートウェイ
  - プライマリ課金ゲートウェイへのスイッチバック
- メンテナンス モード
- 複数の信頼できる PLMN ID
- GGSN-IOS SLB メッセージング
- セッション タイムアウト
- HSDPA および（必要に応じて）関連する 3GPP R5
- 拡張仮想 APN
- SGSN から送信される新しい IE（ユーザ位置、Radio Access Technology（RAT; 無線アクセス テクノロジー）、MS Time Zone（MSTZ; MS タイム ゾーン）、Customized Application for Mobile Enhanced Logic （CAMEL）課金情報、およびユーザ位置情報の各種 IE）
- GTP SLB スティッキ性
- GGSN が開始する PDP コンテキストの更新要求
- P-CSCF 検出
- 次の用途の拡張 MIB
  - Cisco Content Services Gateway（CSG）
  - DCCA
  - APN レベルの定期アカウンティング タイマー
  - PPP 再生成のスケーラビリティ
  - 直接トンネル
  - Change of Authorization（CoA; 認可の変更）
  - GGSN が開始する PDP コンテキストの更新
- RADIUS 認可の変更メッセージ

  RADIUS 認可の変更（CoA）メッセージには、セッションの認可をダイナミックに変更するための情報が含まれています。CoA メッセージは、ポート 1700 で受信されます。

Cisco GGSN では、RFC 3576 に定義されている RADIUS CoA メッセージをサポートするために、基本の Cisco IOS AAA が使用されます。また、Cisco GGSN では、更新された QoS を示す追加の 3GPP QoS アトリビュート、および PDP コンテキストを識別する Acct-Session-ID が使用されます。

QoS VSA は、各バイトが QoS アトリビュートでエンコードされたストリングです（3GPP TS 24.008 に定義されています）。Accounting-session-id は、標準アトリビュート タイプ 44 を使用するストリングです。

AAA および RADIUS の詳細については、『*Cisco* IOS Security Configuration Guide, Release 12.4』を参照してください。

CoA 手順の一環として中間アカウンティング レコードが生成されるようにするには、次の条件が満たされていることを確認してください。

- **aaa accounting update newinfo** グローバル コンフィギュレーション コマンドがグローバルに設定されていること
- APN で、**interim update** キーワード オプションを指定して **aaa-accounting** アクセス ポイント コンフィギュレーション コマンドが設定されていること

- ダウンロード可能な QoS プロファイル

  Cisco GGSN では、AAA サーバからの QoS プロファイルのダウンロードがサポートされています。

  APN が非透過モードで設定されている場合、ユーザは PDP コンテキストが作成される前に認証されます。GGSN は、ユーザが指定した PCO オプションにパラメータを含めて access-request を AAA サーバに送信します。または、APN で匿名ユーザがイネーブルになっている場合は、匿名認証を使用して access-request を AAA サーバに送信します。

  RADIUS からの access-accept では、セッション タイムアウト値やアイドル タイムアウト値などのユーザ固有アトリビュートをダウンロードして、PDP コンテキストに適用できます。さらに、QoS プロファイルは QoS VSA 経由でもダウンロードできます（3GPP TS 24.0008 に定義されています）。3GPP QoS プロファイル アトリビュートが AAA サーバからの access-accept で受信された場合、GGSN はアトリビュートを取得して、PDP コンテキストに適用します。アトリビュートが有効でない場合、またはアトリビュートにフォーマット エラーがある場合、このアトリビュートは無視されて、SGSN によって要求された QoS プロファイルが QoS ネゴシエーションに使用されます。

  3GPP QoS アトリビュートには、vendor-id として 10415 が、code として 5 が設定されています。

- PPP 再生成のスケーラビリティ：Cisco GGSN では、ソフトウェア Interface Description Block（IDB; インターフェイス デスクリプション ブロック）上で動作する PPP セッションに PDP を再生成できます。PPP セッションがソフトウェア IDB 上で動作することを許可すると、サポートされる最大セッション数が増加します。

- PPP 再生成の匿名ユーザ アクセス

  PPP が再生成された PDP で匿名ユーザ アクセスをサポートすると、ユーザ名およびパスワードを送信できないユーザに対して PDP を作成できます。たとえば、WAP ユーザはユーザ名およびパスワードを送信できません。

  PPP 再生成が設定された APN で **anonymous user** アクセス ポイント ユーザ コンフィギュレーション コマンドが設定されている場合、PPP が再生成された PDP でユーザ名およびパスワードが PCO IE に含まれていない PDP コンテキストの作成要求を受信すると、その APN の匿名ユーザ設定が LNS に認証用として送信されます。PCO IE にユーザ名およびパスワードが含まれている場合は、APN に匿名ユーザが設定されていても、指定されたユーザ名とパスワードを使用して LNS へのトンネルが作成されます。

PDP コンテキストの作成要求内のユーザ名とパスワードは、匿名ユーザ設定よりも優先されます。

APN における匿名ユーザ アクセスの設定については、「追加の実アクセス ポイント オプションの設定」（P.8-20）を参照してください。

- ダウンロード可能なプール名のサポート

  APN で **ip-address-pool radius-client** アクセス ポイント コンフィギュレーション コマンドが設定されている場合、ユーザの認証中に Access-Accept メッセージの一部としてアドレス プール名が受信されたときは、そのアドレス プールがモバイル ステーションへの IP アドレスの割り当てに使用されます。Access-Accept メッセージに IP アドレスも含まれている場合は、アドレス プール名よりも IP アドレスが優先されます。つまり、プールからアドレスが割り当てられるのではなく、Access-Accept メッセージの IP アドレスが使用されます。

  ダウンロード可能なプール名を設定する場合は、APN で **radius-client** キーワード オプションを指定して **ip-address pool** アクセス ポイント コンフィギュレーション コマンドが設定されていることを確認してください。

```
gprs access-point-list gprs
  access-point 3
   access-point-name qos1.com
   ip-address-pool radius-client
...

ip local pool pool1500 ipaddress ipaddress
```

  ip-address-pool アクセス ポイント コンフィギュレーション コマンドの詳細については、「追加の実アクセス ポイント オプションの設定」（P.8-20）を参照してください。RADIUS の設定の詳細については、『Cisco IOS Security Configuration Guide』を参照してください。

- 直接トンネルのサポート

  直接トンネル機能によって、SGSN は、RNC と GGSN との間に直接のユーザ プレーン トンネルを確立できます。

  SGSN は、RNC とコア ネットワークとの間のゲートウェイとして動作します。直接トンネル機能では、シグナリング トラフィック（モバイル デバイスの位置を追跡するためのトラフィック）、およびモバイル デバイスとインターネットとの間で交換される実際のデータ パケットの両方が処理されます。

  Cisco GGSN リリース 8.0 よりも前のリリースでは、トンネルは GGSN と SGSN との間、および SGSN と RNC との間にだけ存在できました。このようなトンネル設定では、すべてのデータ パケットが SGSN を通過する必要があります。SGSN は、一方のトンネルの終端となり、パケットを抽出して、他方のトンネルに送出する必要があります。この処理には時間と処理パワーが必要となります。

  直接トンネルのサポートにより、SGSN は RNC と GGSN との間で直接トンネルを開始でき、SGSN でデータ パケットを処理する必要がなくなります。SGSN では、他の RNC によってカバーされているエリアにモバイル デバイスが移動した場合でも、トンネルを変更することによって、引き続き場所の移動に関する問題への対応が行われます。

  具体的には、直接トンネル処理は次のように実行されます。

  a. SGSN は、次の要素を含む PDP コンテキストの更新要求とともに、直接トンネルを開始します。

  - DTI ビットが 1 に設定された直接トンネル フラグ IE。

  - RNC ユーザ トラフィック アドレス。

  - データ TEID。

  - GGSN によって、RNC ユーザ トラフィック アドレスおよび Data TEID が更新されます。MS への G-PDU を送信する場合、GGSN は更新された情報を使用します。

b. RNC ユーザ トラフィック アドレスからエラー通知メッセージを受信すると、GGSN は PDP コンテキストの更新要求を開始します。この PDP コンテキストの更新要求には、エラー通知ビットが設定された直接トンネル フラグ IE が含まれています。

c. SGSN から PDP コンテキストの更新応答を受信するまでの間、GGSN では MS アドレスに対する後続のパケットが廃棄されます。

d. SGSN から PDP コンテキストの更新応答を受信します。原因が「Request Accepted」である場合、PDP は維持されます。原因が「Not Request Accepted」である場合、PDP はローカルで削除されます。

（注） 直接トンネルのサポートは、国際的なローミングには適用されません。また、直接トンネルのサポートは、SGSN が前払いシステムによってトラフィック フローのカウントを依頼された場合には適用されません。

CHAPTER 2

ゲートウェイ GPRS サポート ノード（GGSN）の設定プランニング

この章では、Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）を設定する前に理解しておく必要がある情報について説明します。

この章は、次の内容で構成されています。

前提条件

GGSN を実装するプラットフォームに応じて前提条件は異なります。ここでは、GGSN をネットワーク内に設定する前に、従う必要がある一般的なガイドラインを示します。

はじめに

Cisco GGSN リリース 9.0 は、Cisco 7600 シリーズ ルータ プラットフォームの Cisco Service and Application Module for IP（SAMI）でサポートされています。

GGSN の設定を開始する前に、モバイル ユーザが GGSN を使用してアクセスできるようにするネットワークがわかっている必要があります。ネットワークを識別したあと、ネットワークに設定するインターフェイスを計画し、これらのネットワークへの関連アクセス ポイントを計画して、GGSN でそれらを設定します。

たとえば、Public Data Network（PDN; 公衆データ網）経由のインターネット アクセスに加えて、2 つのプライベート企業イントラネットへのアクセスをユーザに提供するとします。この場合、ユーザが PDN にアクセスできるようにするために 1 つ、2 つのプライベート イントラネットのそれぞれに 1 つずつ、合計 3 つのアクセス ポイントを設定する必要があります。

プラットフォームの前提条件

Cisco 7600 シリーズ ルータ プラットフォームに GGSN を設定する場合、次の項に示す要件が満たされていることを確認します。

必要なハードウェアおよびソフトウェア

Cisco 7600 シリーズ インターネット ルータ プラットフォームに Cisco GGSN リリース 9.2 を実装するには、次のハードウェアおよびソフトウェアが必要です。

- ネットワークに接続するためのポートを持つ任意のモジュール
- Cisco 7600 シリーズ ルータおよび Cisco IOS リリース 12.2(33)SRC 以降が稼動している次のスーパーバイザ エンジンのいずれか
  - マルチレイヤ スイッチ フィーチャ カード 3 を搭載した Cisco 7600 シリーズ Supervisor Engine 720（WS-SUP720）
  - マルチレイヤ スイッチ フィーチャ カード 3 およびポリシー フィーチャ カード 3B を搭載した Cisco 7600 シリーズ Supervisor Engine 720（WS-SUP720-3B）
  - マルチレイヤ スイッチ フィーチャ カード 3 およびポリシー フィーチャ カード 3BXL を搭載した Cisco 7600 シリーズ Supervisor Engine 720（WS-SUP720-3BXL）
  - Cisco SAMI で LCP ROMMON Version 12.2(121) 以降が稼動している、マルチレイヤ スイッチ フィーチャ カードを搭載した Cisco 7600 シリーズ Supervisor Engine 32（WS-SUP32-GE-3B）
  - Cisco SAMI で LCP ROMMON Version 12.2(121) 以降が稼動している、マルチレイヤ スイッチ フィーチャ カードおよび 10 ギガビット イーサネット アップリンクを搭載した Cisco 7600 シリーズ Supervisor Engine 32（WS-SUP32-10GE-3B）

  または、Cisco IOS リリース 12.2(33)SRE 以降が稼動している次の Cisco 7600 シリーズ ルート スイッチ プロセッサのいずれか
  - Distributed Forwarding Card 3C を搭載した Cisco 7600 シリーズ Route Switch Processor 720（RSP720-3C-GE）
  - Distributed Forwarding Card 3CXL を搭載した Cisco 7600 シリーズ Route Switch Processor 720（RSP720-3CXL-GE）

  スーパーバイザ エンジンで稼動している Cisco IOS リリースのアップグレードの詳細については、『Release Notes for Cisco IOS Release 12.2SR』の「Upgrading to a New Software Release」の項を参照してください。Cisco SAMI 上の LCP ROMMON イメージの確認およびアップグレードについては、『*Cisco Service and Application Module for IP User Guide*』を参照してください。

（注） スーパーバイザ エンジンで必要な Cisco IOS ソフトウェアは、使用するスーパーバイザ エンジンおよび Cisco SAMI プロセッサで稼動している Cisco モバイル ワイヤレス アプリケーションに依存します。

GPRS トンネリング プロトコル（GTP）セッション冗長性

上記の必要なハードウェアおよびソフトウェアに加えて、GPRS Tunneling Protocol Session Redundancy（GTP-SR; GPRS トンネリング プロトコル セッション冗長性）の実装には少なくとも次のものが必要です。

- 1 ルータ実装では、Cisco 7600 シリーズ ルータに 2 つの Cisco SAMI
- 2 ルータ実装では、Cisco 7600 シリーズ ルータのそれぞれに 1 つの Cisco SAMI

拡張サービス認識課金

必要なハードウェアおよびソフトウェアに加えて、拡張サービス認識課金の実装には、さらに Cisco Content Services Gateway - 2nd Generation ソフトウェアが稼動している Cisco SAMI が各 Cisco 7600 シリーズ ルータに必要です。

必要な基本設定

スイッチからネットワーク内のさまざまな要素への接続を確立したあと、Cisco SAMI 上で GGSN を実装およびカスタマイズする前に次の基本設定を完了しておく必要があります。

スーパーバイザ エンジン設定

スーパーバイザ エンジンで、次の点を確認します。

1. 各 GGSN インターフェイスにレイヤ 3 ルーテッド VLAN が作成されているようにします。たとえば、次のインターフェイスに VLAN を作成します。
   - Gn VLAN：Gn インターフェイスを相互接続します。
   - Ga VLAN：Ga インターフェイスを相互接続します。
   - AAA/OAM/DHCP VLAN：Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）、Operation, Administration, and Maintenance（OAM; 運用管理および保守）、および Dynamic Host Configuration Protocol（DHCP）の機能に使用される GGSN インターフェイスを相互接続します。
   - Access Point Name（APN; アクセス ポイント ネーム）Gi インターフェイスごとに 1 つの VLAN

   VLAN は VLAN データベース モードまたはグローバル コンフィギュレーション モードから設定できます。拡張範囲 VLAN は VLAN データベース モードでは設定できません。拡張範囲 VLAN を設定できるのはグローバル コンフィギュレーション モードだけです。

（注） Route Processor Redundancy Plus（RPR+）冗長性は、VLAN データベース モードで入力された設定をサポートしません。RPR（+）を使用した冗長スーパーバイザ モジュールで高可用性を設定している場合は、VLAN データベース モードではなくグローバル コンフィギュレーション モードで VLAN を設定してください。そうしないと、VLAN 情報が冗長スーパーバイザ モジュールと同期化されません。

グローバル コンフィギュレーションモードから VLAN を設定するには、次のコマンドを使用します。

```
Sup#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sup(config)#vlan 222
Sup(config-vlan)#end
Sup#
```

上記の例では、VLAN 222 はレイヤ 2 スイッチド VLAN です。この VLAN に関連付けられているサブネットは、スーパーバイザ エンジンのルーティング テーブルに認識されていません。VLAN 222 をレイヤ 3 スイッチド VLAN（またはルーテッド VLAN）として設定するには、スーパーバイザ エンジンで VLAN 222 インターフェイスを設定して、このインターフェイスに IP アドレスを割り当てます。

```
Sup# configure terminal
Sup(config)# interface vlan222
Sup(config-if)# ip address n.n.n.n mask
Sup(config-if)# no ip redirects
```

次に、スーパーバイザ エンジンで VLAN を設定する例を示します。

```
Sup# show running-config
!
. . .
vlan 103,110,160,200,300-301,310
!
!
interface Vlan103
 description Gn VLAN
 ip address 10.20.21.1 255.255.255.0
 no ip redirects
!
interface Vlan110
 description OAM/AAA/DHCP VLAN
 ip address 10.20.50.1 255.255.255.0
 no ip redirects
!
interface Vlan200
 description Ga Charging VLAN
 no ip address
 no ip redirects
!
interface Vlan310
 description VLAN for APN Internet
 ip address 10.20.51.1 255.255.255.0
```

VLAN 設定の詳細については、『*Cisco 7600 Series Cisco IOS Software Configuration Guide*』を参照してください。

2. Cisco IOS ソフトウェアの Server Load Balancing（SLB; サーバ ロード バランシング）機能がインストールされ、GTP ロード バランシング用に設定されているようにします。詳細については、「*IOS Server Load Balancing*」フィーチャ モジュールおよび第 13 章「GGSN でのロード バランシングの設定」を参照してください。

3. 複数の Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）をイネーブルにし、VLAN を VLAN グループに割り当ててから、次のコマンドを使用して VLAN グループを SAMI に割り当てることで、SAMI に対するトラフィックを許可します。

```
!
...
!
svclc multiple-vlan-interfaces
svclc module 7 vlan-group 71, 73
svclc vlan-group 71, 71
svclc vlan-group 73, 95, 100, 101
!
...
!
```

（注）　VLAN ID はスーパーバイザ エンジンおよび Cisco SAMI 設定の VLAN ID と一致している必要があります。Cisco SAMI の設定の詳細については、『*Cisco Service and Application Module for IP User Guide*』を参照してください。

4. Cisco SAMI PowerPC（PPC）に設定されている各 GGSN インスタンスにスタティック ルートが設定されているようにします。

```
...
!
ip route 10.20.30.1 255.255.255.255 10.20.21.20
ip route 10.20.30.2 255.255.255.255 10.20.21.21
ip route 10.20.30.3 255.255.255.255 10.20.21.22
ip route 10.20.30.4 255.255.255.255 10.20.21.23
ip route 10.20.30.5 255.255.255.255 10.20.21.24
!
...
```

GGSN 設定

Cisco SAMI PPC の各 GGSN インスタンスで、次の点を確認します。

1. スーパーバイザ エンジンにスタティック ルートが設定されているようにします。

```
!
...
!
ip route 0.0.0.0 0.0.0.0 10.20.21.1
...
!
```

2. 802.1Q カプセル化をイネーブルにしたサブインターフェイスが、スーパーバイザ エンジンに作成した各 VLAN に設定されているようにします。

   次に、スーパーバイザ エンジンに設定されている VLAN 103 への Gn サブインターフェイスを GGSN で設定する例を示します。

```
!
...
interface GigabitEthernet0/0.2
 description Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
...
!
```

   設定の詳細については、次の項を参照してください。

   - Ga サブインターフェイス：「課金ゲートウェイへのインターフェイスの設定」（P.6-2）
   - Gn サブインターフェイス：「SGSN へのインターフェイスの設定」（P.8-1）
   - Gi サブインターフェイス：「PDN へのインターフェイスの設定」（P.8-12）

設定例

次に、スーパーバイザ エンジンおよび Cisco SAMI PPC で稼動している GGSN インスタンスの基本設定例を示します。

スーパーバイザ エンジン

```
hostname 7600-a
!
boot system flash
boot device module 7 cf:4
!
svclc multiple-vlan-interfaces
svclc module 7 vlan-group 71, 73
svclc vlan-group 71, 71
svclc vlan-group 73, 95, 100, 101
vtp mode transparent
redundancy
 mode rpr-plus
 main-cpu
  auto-sync running-config
  auto-sync standard
!
power redundancy-mode combined
!
!
vlan 1
 vlan1 1002
 vlan2 1003
!
vlan 2
 name SNIFFER
!
vlan 71,95
!
vlan 100
 name Internal_Gi_for_GGSN-SAMI
!
vlan 101
 name Internal_Gn/Ga
!
vlan 165
!
vlan 302
 name Gn_1
!
vlan 303
 name Ga_1
!
vlan 1002
 vlan1 1
 vlan2 1003
!
vlan 1003
 vlan1 1
 vlan2 1002
 parent 1005
 backupcrf enable
!
vlan 1004
 bridge 1
 stp type ibm
```

```
!
vlan 1005
 bridge 1
!
interface FastEthernet8/22
 description To SGSN
 no ip address
 switchport
 switchport access vlan 302
!
interface FastEthernet8/23
 description To CGF
 no ip address
 switchport
 switchport access vlan 302
!
interface FastEthernet8/26
 description To DHCP/RADIUS Servers
 no ip address
 switchport
 switchport access vlan 95
!
interface FastEthernet8/31
 description To BackBone
 no ip address
 switchport
 switchport access vlan 71
!
interface FastEthernet9/32
 description To CORPA
 no ip address
 switchport
 switchport access vlan 165
 no cdp enable
!
!interface Vlan1
 no ip address
 shutdown
!
interface Vlan71
 description VLAN to tftpserver
 ip address 1.7.46.65 255.255.0.0
!
interface Vlan95
 description VLAN for RADIUS and DHCP
 ip address 10.2.25.1 255.255.255.0
!
interface Vlan100
 description Internal VLAN SUP-to-SAMI Gi
 ip address 10.1.2.1 255.255.255.0
!
interface Vlan101
 description VLAN to GGSN for GA/GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan165
 description VLAN to CORPA
 ip address 165.1.1.1 255.255.0.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
!
interface Vlan303
 ip address 40.0.3.1 255.255.255.0
```

```
!
router ospf 300
 log-adjacency-changes
 summary-address 9.9.9.0 255.255.255.0
 redistribute static subnets route-map GGSN-routes
 network 40.0.2.0 0.0.0.255 area 300
 network 40.0.3.0 0.0.0.255 area 300
!
ip classless
ip route 9.9.9.72 255.255.255.255 10.1.1.72
ip route 9.9.9.73 255.255.255.255 10.1.1.73
ip route 9.9.9.74 255.255.255.255 10.1.1.74
ip route 9.9.9.75 255.255.255.255 10.1.1.75
ip route 9.9.9.76 255.255.255.255 10.1.1.76
ip route 110.72.0.0 255.255.0.0 10.1.1.72
ip route 110.73.0.0 255.255.0.0 10.1.1.73
ip route 110.74.0.0 255.255.0.0 10.1.1.74
ip route 110.75.0.0 255.255.0.0 10.1.1.75
ip route 110.76.0.0 255.255.0.0 10.1.1.76
!
access-list 1 permit 9.9.9.0 0.0.0.255
!
route-map GGSN-routes permit 10
 match ip address 1
!
```

Cisco SAMI プロセッサの GGSN インスタンス

```
service gprs ggsn
!
hostname 7600-7-2
!
ip cef
!
interface Loopback0
 description USED FOR DHCP gateway
 ip address 110.72.0.2 255.255.255.255
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.1
 description Gi
 encapsulation dot1Q 100
 ip address 10.1.2.72 255.255.255.0
!
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
interface GigabitEthernet0/0.71
 description TFTP or Backbone
 encapsulation dot1Q 71
 ip address 1.7.46.72 255.255.0.0
!
interface GigabitEthernet0/0.95
 description CNR and CAR
```

```
 encapsulation dot1Q 95
 ip address 10.2.25.72 255.255.255.0
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.2.1
ip route 40.1.2.1 255.255.255.255 10.1.1.1
ip route 40.1.3.10 255.255.255.255 10.1.1.1
ip route 40.2.2.1 255.255.255.255 10.1.1.1
ip route 40.2.3.10 255.255.255.255 10.1.1.1
ip route 40.3.2.3 255.255.255.255 10.1.1.1
ip route 40.4.2.3 255.255.255.255 10.1.1.1
!
gprs access-point-list gprs
  access-point 1
   access-point-name CORPA.com
   ip-address-pool dhcp-proxy-client
   aggregate auto
   dhcp-server 10.2.25.90
   dhcp-gateway-address 110.72.0.2
!
```

制約事項

Cisco GGSN の設定時には、次の点に注意してください。

- GGSN でサポートされる PDP コンテキストの最大数の実質的な上限は、使用されるメモリおよびプラットフォームと GGSN 設定によって異なります（Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）の方式が端末装置およびモバイル終端を超えてパケットを転送するように設定されているかどうか、Dynamic Feedback Protocol（DFP）が使用されているか、またはメモリ保護機能がイネーブルか、サポートされている PDP コンテキスト作成のレートなどによって異なります）。

（注）　DFP では、PPP PDP を IP PDP と比較します。1 つの PPP PDP は 8 つの IP PDP と等しくなり、1 つの IPv6 PDP は 8 つの IPv4 PDP と等しくなります。

表 2-1 は、1 GB のメモリ オプションの Cisco SAMI でサポートできる PDP コンテキストの最大数を示しています。表 2-2 は、2 GB のメモリ オプションの Cisco SAMI でサポートできる PDP コンテキストの最大数を示しています。

表 2-1　　1 GB の SAMI でサポートされる PDP 数

PDP タイプ	GGSN ごとの最大数	SAMI ごとの最大数[1]
IPv4	66,000	400,000
IPv6	8,000	48,000
PPP 再生成	16,000	96,000
PPP	8,000	48,000

1. 6 つの GGSN が設定されている SAMI ごとの最大数。

表 2-2　2 GB SAMI でサポートされる PDP の数

PDP タイプ	GGSN ごとの最大数	SAMI ごとの最大数[1]
IPv4	136,000	816,000
IPv6	16,000	96,000
PPP 再生成	32,000	192,000
PPP	16,000	96,000

1. 6 つの GGSN が設定されている SAMI ごとの最大数

- CPU 高使用率による問題を回避するために、次のような設定を推奨します。
  - 起動時の CPU 使用率を抑えるには、グローバル コンフィギュレーション モードで **no logging console** コマンドを設定して、コンソール端末へのロギングをディセーブルにします。
  - ピアの Hello パケットを処理する準備が完了するまで Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）インターフェイスが自身をアクティブとして宣言しないようにするには、HSRP グループの初期化の前に HSRP インターフェイスで **standby delay minimum 100 reload 100 interface** コンフィギュレーション コマンドを使用して遅延期間を設定します。
  - PPP PDP の処理（作成および削除）が増大する期間など、その他の理由による CPU 高使用率の問題を最小限に抑えるには、**no logging event link-status** インターフェイス コマンドを使用して、GGSN のすべての仮想テンプレート インターフェイスでインターフェイス データ リンク ステータスの変更通知をディセーブルにします。

```
!
interface Virtual-Template1
description GGSN-VT
ip unnumbered Loopback0
encapsulation gtp
no logging event link-status
gprs access-point-list gprs
end
```

サービス認識 GGSN の実装では、次のようなその他の特記事項、制限事項、および制約事項が適用されます。

- Content Services Gateway - 2nd Generation（CSG2）と GGSN の間で Remote Authentication Dial-In User Service（RADIUS）アカウンティングがイネーブルになり、PDP コンテキストのユーザ情報を含む Known User Entries Table（KUT; 認識ユーザ エントリ テーブル）エントリが読み込まれます。
- CSG2 は、すべての GGSN インターフェイスのクォータ サーバ アドレスで設定されている必要があります。
- CSG2 上のサービス ID は、Diameter Credit Control Application（DCCA）サーバ上のカテゴリ ID と一致する数値文字列として設定されます。
- RADIUS を使用しない場合、Cisco CSG2 は GGSN 上の RADIUS エンドポイントとして設定されます。
- Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）では、GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）N3 要求と T3 再送信の数に設定されている値は、使用可能なすべてのサーバ タイマー（RADIUS、DCCA、および CSG2）の合計よりも大きい必要があります。

  特に、SGSN N3*T3 は次の値よりも大きい必要があります。

2 x RADIUS タイムアウト + *N* x DCCA タイムアウト + CSG2 タイムアウト

上記の意味を次に示します。

- 2 は、認証とアカウンティングの両方を示します。
- *N* は、サーバ グループで設定されている Diameter サーバの数を示します。

（注） デフォルトより低い N3* T3 を設定すると、TCP ベースの遅い課金パスに影響を与える可能性があります。

その他の参考資料

基本接続の実装に関連するその他の情報については、次の項を参照してください。

- 「関連資料」（P.2-11）
- 「規格」（P.2-11）
- 「管理情報ベース（MIB）」（P.2-12）
- 「コメント要求（RFC）」（P.2-12）
- 「シスコのテクニカルサポート」（P.2-13）

関連資料

- 『*Release Notes for Cisco GGSN Release 9.0 on the Cisco SAMI, Cisco IOS Release 12.4(22)YE1*』
- 『*Cisco Service and Application Module for IP User Guide*』
- 『*Cisco IOS Network Management Configuration Guide*』
- 『*Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers*』
- 『*Cisco 7600 Series Cisco IOS Software Configuration Guide*』
- 『*Cisco 7600 Series Cisco IOS Command Reference*』
- 『*Cisco IOS Quality of Service Solutions Configuration Guide*, Cisco IOS Release 12.4』
- 『Cisco IOS Configuration Guides and Command References, Release 12.4』

規格

Cisco GGSN リリース 9.0 は、次の Third Generation Partnership Program（3GPP; 第 3 世代パートナーシップ プログラム）規格をサポートしており、以前の 3GPP Technical Specifications（TS; 技術仕様）と下位互換性があります。

表 2-3　Cisco GGSN リリース 9.0 でサポートされている第 3 世代パートナーシップ プログラム（3GPP）規格

3G TS 番号	タイトル	リリース	GGSN リリース 9.0
29.060	GTP across Gn and Gp（Gn および Gp 上の GTP）	7	8.1.0
29.061	Interworking with PDN（PDN とのインターワーキング）	7	7.5.0

表 2-3　Cisco GGSN リリース 9.0 でサポートされている第 3 世代パートナーシップ プログラム（3GPP）規格 （続き）

3G TS 番号	タイトル	リリース	GGSN リリース 9.0
32.015	Charging（課金）	99	3.12.0
32.215	Charging（課金）	5	5.9.0
32.251	Charging（課金）	7	7.5.1

（注）　Cisco GGSN リリース 9.0 は、上記 TS の一部のセクションに対する限定サポートを提供しています。

GGSN インターフェイスは次の Special Mobile Group（SMG）規格に準拠しています。

- Ga インターフェイス：SMG#28 R99
- Gn インターフェイス：SMG#31 R98

管理情報ベース（MIB）

- CISCO-GGSN-EXT-MIB
- CISCO-GGSN-MIB
- CISCO-GGSN-QOS-MIB
- CISCO-GGSN-SERVICE-AWARE-MIB
- CISCO-GPRS-ACC-PT-MIB
- CISCO-GPRS-CHARGING-MIB
- CISCO-GPRS-GTP-CAPABILITY-MIB
- CISCO-GTP-MIB
- CISCO-ISCSI

Management Information Base（MIB; 管理情報ベース）の詳細については、次の URL を参照してください。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

コメント要求（RFC）

- RFC 1518、*An Architecture for IP Address Allocation with CIDR*（Classless Inter-Domain Routing（CIDR）を使用した IP アドレス割り当てのアーキテクチャ）
- RFC 1519、*Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*（Classless Inter-Domain Routing（CIDR）：アドレス割り当ておよび集約方式）
- RFC 1661、*The Point-to-Point Protocol (PPP)*（ポイントツーポイント プロトコル（PPP））
- RFC 2461、*Neighbor Discovery for IP Version 6 (IPv6)*（IP Version 6（IPv6）の近隣探索）
- RFC 2462、*IPv6 Stateless Address Autoconfiguration*（IPv6 ステートレス アドレス自動設定）
- RFC 2475、*An Architecture for Differentiated Services*（ディファレンシエーテッド サービスのアーキテクチャ）
- RFC 3162、*RADIUS and IPv6*（RADIUS および IPv6）

- RFC 3588、*Diameter Base Protocol*（Diameter 基本プロトコル）
- RFC 3720、*Internet Small Computer Systems Interface (iSCSI)*（インターネット スモール コンピュータ システム インターフェイス（iSCSI））
- RFC 4006、*Diameter Credit-Control Application*（Diameter クレジットコントロール アプリケーション）

シスコのテクニカルサポート

シスコ テクニカルサポート Web サイトには、製品、テクノロジー、ソリューション、テクニカル ティップス、およびツールへのリンクなど、数千ページに及ぶ検索可能なテクニカル コンテンツが掲載されています。登録されている Cisco.com ユーザは、このページからさらに詳細なコンテンツにアクセスできます。

http://www.cisco.com/techsupport

CHAPTER 3

GGSN での GTP サービスの設定

この章では、Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）を設定し、GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）オプションを設定する方法について説明します。

この章に記載されている GGSN コマンドの詳細については、使用している GGSN リリースの『*Cisco GGSN Command Reference*』を参照してください。

この章に記載されているその他のコマンドのマニュアルを参照するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。GGSN の設定に役立つその他の Cisco IOS ソフトウェア マニュアルのリストについては、「関連資料」（P.2-11）を参照してください。

この章は、次の内容で構成されています。

GTP の概要

GTP は、General Packet Radio Service（GPRS; グローバル パケット ラジオ サービス）/Universal Mobile Telecommunication System（UMTS）ネットワークでマルチプロトコル パケットをトンネリングするために使用されるプロトコルです。Gn インターフェイス上で、GPRS/UMTS バックボーン ネットワーク内の GSN 間のプロトコルとして定義されます。

Cisco GGSN は、GTP バージョン 0（GTP v0）と GTP バージョン 1（GTP v1）の両方を同時にサポートしています。GPRS R97/R98 は GTP バージョン 0 を使用し、UMTS R99 は GTP バージョン 1 を使用します。

GGSN は、Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）の機能に応じて、使用する GTP バージョンを自動的に選択します。

GGSN サービスの設定

Cisco GGSN ソフトウェアは、*仮想テンプレート インターフェイス*という論理インターフェイスを使用して、Cisco Service and Application Module for IP（SAMI）プロセッサで実行される Cisco IOS ソフトウェアのインスタンスを GGSN として設定します。

ここでは、GGSN サービスを設定するときに完了する必要がある主要なタスクについて説明します。以降の設定作業では、Cisco SAMI プロセッサ上の Cisco IOS インスタンスが GGSN として設定された場合に、GGSN からサービング GPRS サポート ノード（SGSN）および Public Data Network（PDN; 公衆データ網）への接続を確立する方法について説明します。

GGSN の設定では、次の要件を満たす必要があります。

- グローバル コンフィギュレーション モードで **service gprs ggsn** コマンドを使用して、Cisco IOS ソフトウェアのインスタンスごとに GGSN エンティティを 1 つだけ設定します。1 つの Cisco SAMI に最大 6 つの GGSN を設定できます（プロセッサごとに 1 つの GGSN）。
- 各 GGSN で、GTP カプセル化を使用して、単一のデフォルト仮想テンプレート インターフェイスを（仮想テンプレート番号 1 として）設定します。このデフォルト仮想テンプレート インターフェイスは、**gprs service ggsn** がイネーブルであるかぎり、設定解除しないでください（GPRS Roaming Exchange（GRX; GPRS ローミング エクスチェンジ）トラフィックを分離するために、GTP カプセル化を使用するその他の仮想テンプレート インターフェイスを設定できます。GRX トラフィックの分離の詳細については、「GGSN Gn インターフェイスでの GRX トラフィックの分離」（P.11-31）を参照してください）。
- ルータおよびメモリ サイズに応じて、メモリ保護しきい値が適切に設定されていることを確認します。メモリ保護しきい値の設定の詳細については、「GGSN メモリ保護モードしきい値の設定」（P.6-6）を参照してください。

GGSN サービス設定の作業リスト

GGSN サービス用の Cisco IOS GGSN ソフトウェアのインスタンスを実行する Cisco SAMI プロセッサを設定するには、次の作業を実行します。

- 「GGSN サービスのイネーブル」（P.3-2）
- 「ループバック インターフェイスの作成」（P.3-3）
- 「GGSN のデフォルト GTP 仮想テンプレート インターフェイスの作成」（P.3-3）
- 「CEF スイッチングのイネーブル」（P.3-4）

GGSN サービスのイネーブル

グローバル コンフィギュレーション モードで **service gprs ggsn** コマンドを使用して、Cisco SAMI プロセッサごとに GGSN エンティティを 1 つだけ設定します。

GGSN 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)# service gprs ggsn`	Cisco IOS ソフトウェア インスタンスが GGSN として機能することを指定します。

ループバック インターフェイスの作成

仮想テンプレートで IP アドレスを直接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、**ip unnumbered loopback** インターフェイス コンフィギュレーション コマンドを使用して、ループバック インターフェイス IP アドレスを GTP カプセル化に使用される仮想テンプレートに関連付けることを推奨します。

（注）　**ip unnumbered loopback** コマンドを使用してループバック インターフェイスの IP アドレスを仮想テンプレート インターフェイスに割り当てない場合、パケットは Cisco Express Forwarding（CEF）スイッチドにならないため、パフォーマンスに影響を与えます。

ループバック インターフェイスは、常に稼動しているインターフェイスをエミュレートするソフトウェア専用インターフェイスであり、すべてのプラットフォームでサポートされる仮想インターフェイスです。インターフェイス数は、作成または設定するループバック インターフェイスの数です。作成できるループバック インターフェイスの数に制限はありません。GGSN は、ループバック インターフェイスを使用して複数の異なる機能の設定をサポートしています。

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
ステップ 1	`Router(config)# interface loopback number`	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、常に稼動している仮想インターフェイスです。
ステップ 2	`Router(config-if)# ip address ip-address mask`	ループバック インターフェイスに IP アドレスを割り当てます。

GGSN のデフォルト GTP 仮想テンプレート インターフェイスの作成

GGSN で GTP カプセル化を使用して、デフォルト GTP 仮想テンプレート インターフェイスを（仮想テンプレート番号 1 として）1 つだけ設定します。デフォルト GTP 仮想テンプレートは設定が必須であり、**service gprs ggsn** が設定されている場合は設定を解除しないようにする必要があります。

（注）　デフォルト GTP 仮想テンプレート（Virtual-Template 1）には、**ip address** または **ip unnumbered** コマンドを使用して有効な IP アドレスが関連付けられている必要があります。

GGSN のデフォルト GTP 仮想テンプレート 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
ステップ 1	`Router(config)# interface virtual-template 1`	仮想テンプレート インターフェイスを作成します。*number* によって、仮想テンプレート インターフェイスが識別されます。このコマンドにより、インターフェイス コンフィギュレーション モードになります。
ステップ 2	`Router(config-if)# description description`	インターフェイスの説明。

	コマンド	目的
ステップ 3	`Router(config-if)# ip unnumber loopback number`	以前に定義されたループバック IP アドレスを仮想テンプレート インターフェイスに割り当てます。
ステップ 4	`Router(config-if)# encapsulation gtp`	仮想テンプレート インターフェイスで送信されるパケットのカプセル化タイプとして GTP を指定します。
ステップ 5	`Router(config-if)# gprs access-point-list gprs`	新しいアクセス ポイント リストの名前を指定するか、既存のアクセス ポイント リストの名前を参照し、アクセス ポイント リスト コンフィギュレーション モードを開始します。

CEF スイッチングのイネーブル

CEF スイッチングは、Forwarding Information Base（FIB）テーブルおよび隣接関係テーブルを使用して、パケット スイッチングを行います。隣接関係テーブルは、レイヤ 3 ネットワーク アドレスによってインデックス化されており、パケットを転送するために対応するレイヤ 2 情報が含まれています。

CEF スイッチングによって、ルートキャッシュ テーブルの使用およびテーブル エントリのエージングアウトとテーブルへのデータの再入力に必要なオーバーヘッドはなくなります。FIB テーブルによって IP ルーティング テーブルの内容全体がミラーリングされるため、ルートキャッシュ テーブルは必要なくなります。

スイッチング パスの詳細については、『*Cisco IOS Switching Services Configuration Guide*』を参照してください。

CEF スイッチングを GGSN でグローバルにイネーブルにすると、GGSN のすべてのインターフェイスで CEF スイッチングが自動的にイネーブルになります。

（注）　CEF スイッチングが正しく機能するようにするには、**no ip cef** コマンドを使用して CEF スイッチングをディセーブルにしたあと、少し待機してからイネーブルにします。

GGSN で CEF スイッチ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)# ip cef`	GGSN で CEF をイネーブルにします。

GGSN でのエコー タイミングの設定

GGSN は、エコー タイミングを使用して SGSN または外部課金ゲートウェイがアクティブかどうかを判別します。

GTP パスをアクティブにするには、SGSN がアクティブである必要があります。SGSN がアクティブであるかどうかを判別するために、GGSN と SGSN はエコー メッセージを交換します。GGSN はさまざまな方式のエコー メッセージ タイミングをサポートしますが、GGSN が SGSN にエコー要求メッセージを送信するときに、基本エコー フローが開始されます。SGSN は対応するエコー応答メッセージを GGSN に返送します。

特定の回数のリトライ（設定可能な値）後も GGSN が応答を受信しない場合、GGSN は SGSN がアクティブではないと想定します。これは GTP パス障害を意味し、GGSN はそのパスに関連付けられた Packet Data Protocol（PDP; パケット データ プロトコル）コンテキスト要求をすべてクリアします。

ここでは、GGSN でサポートされるさまざまな方式のエコー タイミングおよびその設定方法について説明します。内容は次のとおりです。

GGSN でのエコー タイミングの概要

GGSN は、デフォルト エコー タイマーとダイナミック エコー タイマーという 2 つの異なる方式のエコー タイミングをサポートしています。GGSN で一度に使用できるタイマーは 1 つだけです。次の項では、これら 2 つのタイマーについて説明します。

（注）　完結に示すために、このマニュアルでは GGSN と SGSN 間のエコー タイミングの動作について説明します。GPRS/UMTS ネットワークで外部課金ゲートウェイが使用されている場合、GGSN は同じタイプのエコー タイマーを使用して課金ゲートウェイ パスを維持します。

デフォルト エコー タイマーの概要

デフォルト エコー タイマーは、GGSN で自動的にイネーブルになります。ただし、代わりにダイナミック エコー タイミング方式をイネーブルにすることを選択できます。

GGSN でデフォルト エコー タイマーを使用している場合、次のコマンドが適用されます。

- **gprs gtp n3-requests**：GGSN がエコー要求メッセージの送信を試行する最大回数を指定します。デフォルトは 5 回です。
- **gprs gtp path-echo-interval**：GGSN が SGSN または外部課金ゲートウェイからの応答を待機する秒数、および応答の受信後に GGSN が次のエコー要求メッセージを送信する前に待機する秒数を指定します。デフォルトは 60 秒です。
- **gprs gtp t3-response**：要求に対する応答を受信していない場合に、GGSN がシグナリング要求メッセージを再送信する前に待機する初期秒数を指定します。この時間は、リトライごとに倍になります。デフォルトは 1 秒です。

図 3-1 は、指定されたパス エコー間隔内に応答が正常に受信される場合のデフォルト エコー要求のシーケンスを示しています。GGSN は、パス エコー間隔（**gprs gtp path-echo-interval** コマンドで指定。デフォルトは 60 秒）内にエコー応答を受信した場合、別のエコー要求メッセージを 60 秒（または **gprs gtp path-echo-interval** コマンドで設定された時間）後に送信します。このメッセージ フローは、指定したパス エコー間隔で GGSN が SGSN からエコー応答メッセージを受信する間は継続されます。

図 3-1　パス正常モードのデフォルト GTP パス エコー間隔要求のシーケンス

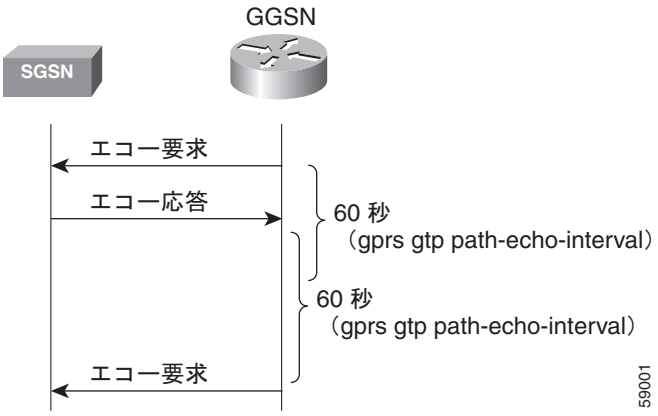
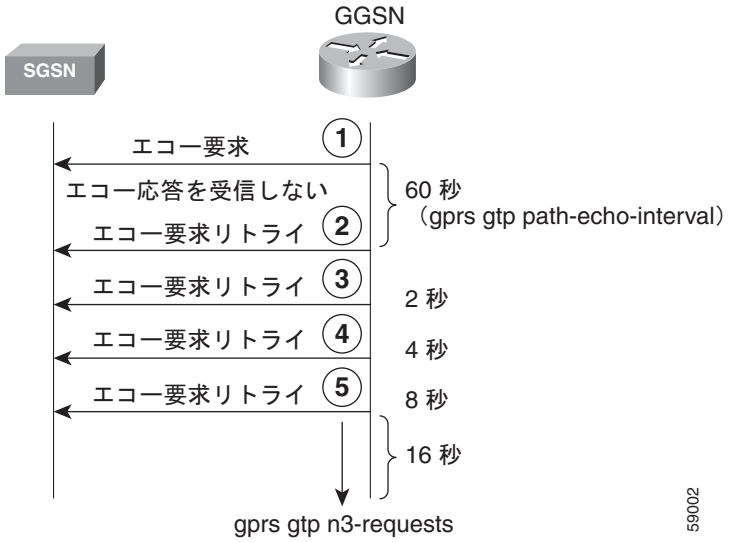


図 3-2 は、指定されたパス エコー間隔内に GGSN がエコー要求に対する応答を受信できない場合のデフォルト エコー要求のシーケンスを示しています。GGSN は、パス エコー間隔内に SGSN からエコー応答メッセージを受信できない場合、N3 要求カウンタ（**gprs gtp n3-requests** コマンドで指定。デフォルトは 5）に達するまでエコー要求メッセージを再送信します。N3 要求カウンタには初期要求メッセージが含まれるため、リトライの総数は N3 - 1 です。T3 タイマーはリトライごとに 2 倍になります（この係数の値は設定可能ではありません）。

図 3-2　パス障害モードのデフォルト エコー タイミング要求のシーケンス



たとえば、N3 がデフォルトの 5 に設定され、T3 がデフォルトの 1 秒に設定されている場合、GGSN は 4 つのエコー要求メッセージを再送信します（初期要求 + 4 リトライ = 5）。GGSN は、SGSN から 60 秒のパス エコー間隔内にエコー応答を受信しない場合、パス エコー間隔が過ぎると即座に最初のエコー要求リトライ メッセージを送信します。GGSN がエコー応答を受信しない間は、T3 時間は追加のエコー要求ごとに 2 倍の秒数になります。したがって、GGSN は別のメッセージを 2 秒、4 秒、8 秒で再送信します。5 番めのメッセージのあと、GGSN はエコー応答を最後の間隔である 16 秒間待機します。

GGSN は、N3 要求カウンタの間隔内に SGSN からエコー応答メッセージを受信できない場合、PDP コンテキストをすべて削除し、GTP パスをクリアします。この例では、最初の要求メッセージが送信されてから PDP コンテキストがクリアされるまでの経過時間の合計は、次のとおりです。

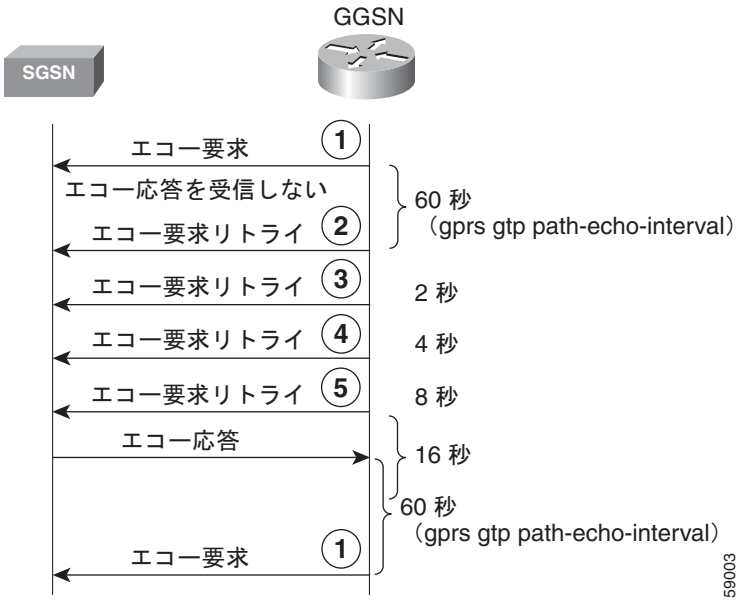
60 + 2 + 4 + 8 + 16 = 90 秒

60 はパス エコー間隔の初期値であり、残りの 4 つの間隔は後続のリトライでの T3 タイマーの増加を示しています。パスは、さらに 60 秒後に（つまり、150 秒で）クリアされます。

GGSN は、N3 x T3 の送信時間内にエコー応答を受信した場合、エコー要求のシーケンスの正常モードに戻ります。

図 3-3 は、エコー要求の N3 x T3 の再送信内にエコー応答メッセージを受信する GGSN を示しています。このシナリオでは、5 回の N3 要求というデフォルト設定に従って、GGSN は初期エコー要求に続いて 4 つのリトライを送信しました（合計で 5 つの要求）。GGSN は、5 番めの最後のリトライのあと、残りの 16 秒のうちにエコー応答を受信します。これで GGSN は正常モードに戻り、60 秒（**gprs gtp path-echo-interval** コマンドの値）待機してから、次のエコー要求メッセージを送信します。

図 3-3　エコー応答が N3 x T3 の再送信内に受信されるデフォルト エコー タイミング



ダイナミック エコー タイマーの概要

GGSN のデフォルト エコー タイマーはネットワーク輻輳に対応するように設定できないため、GTP パスが早くクリアされることがあります。ダイナミック エコー タイマー機能により、GGSN はネットワーク輻輳中に GTP パスをより適切に管理できます。GGSN がダイナミック エコー タイミングを実行できるようにするには、**gprs gtp echo-timer dynamic enable** コマンドを使用します。

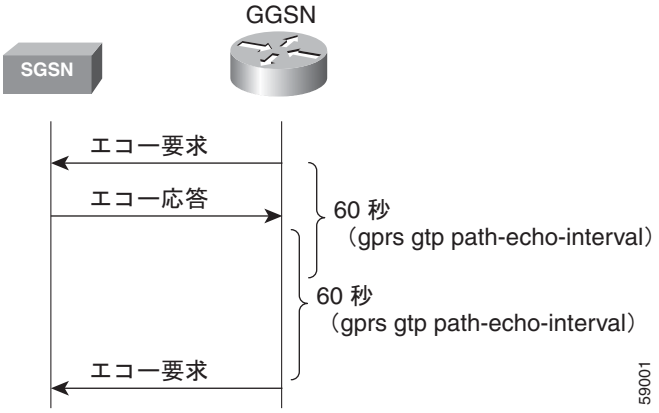
ダイナミック エコー タイマーがデフォルト エコー タイマーと異なるのは、計算された Round-Trip Time（RTT; ラウンドトリップ時間）および RTT 統計に適用される設定可能な係数または乗数を使用するためです。パスによって RTT は異なる場合があるため、ダイナミック エコー タイマーはパスによって異なる場合があります。

GGSN でダイナミック エコー タイマーを使用している場合、次のコマンドが適用されます。

- **gprs gtp echo-timer dynamic enable** : GGSN でダイナミック エコー タイマーをイネーブルにします。
- **gprs gtp echo-timer dynamic minimum** : ダイナミック エコー タイマーの最小間隔（秒単位）を指定します。スムーズ係数が掛けられた RTT がこの値よりも小さい場合、GGSN はこのコマンドで設定された値を使用します。デフォルトは 5 秒です。
- **gprs gtp echo-timer dynamic smooth-factor** : ダイナミック エコー タイマーがパス エコー間隔内に SGSN から応答を受信しなかった場合、リトライの送信を待機する時間を計算するときにダイナミック エコー タイマーが使用する乗数を指定します。デフォルトは 2 です。
- **gprs gtp n3-requests** : GGSN がエコー要求メッセージの送信を試行する最大回数を指定します。デフォルトは 5 回です。
- **gprs gtp path-echo-interval** : GGSN が、SGSN または外部課金ゲートウェイからの応答を受信したあと、次のエコー要求メッセージを送信する前に待機する秒数を指定します。デフォルトは 60 秒です。

図 3-4 は、指定されたパス エコー間隔内に応答が正常に受信される場合のダイナミック エコー要求のシーケンスを示しています。デフォルト エコー タイミング方式と同様に、GGSN は、パス エコー間隔（**gprs gtp path-echo-interval** コマンドで指定。デフォルトは 60 秒）内にエコー応答を受信した場合、別のエコー要求メッセージを 60 秒（または **gprs gtp path-echo-interval** コマンドで設定された時間）後に送信します。このメッセージ フローは、指定したパス エコー間隔で GGSN が SGSN からエコー応答メッセージを受信する間は継続されます。

図 3-4　　パス正常モードのダイナミック GTP パス エコー間隔要求のシーケンス



GGSN は、ダイナミック エコー タイマーが使用する RTT 統計を計算します。RTT は、特定のエコー要求メッセージの送信とそれに対応するエコー応答メッセージの受信との間の時間です。受信された最初のエコー応答に対して RTT が計算され（図 3-5 を参照）、GGSN でこの統計が記録されます。RTT 値は非常に小さい数字になる場合があるため、ダイナミック エコー タイマーが使用する最小時間があります。この値は、**gprs gtp echo-timer dynamic minimum** コマンドを使用して設定されます。

図 3-5　ダイナミック エコー タイミング要求のシーケンスの RTT 計算

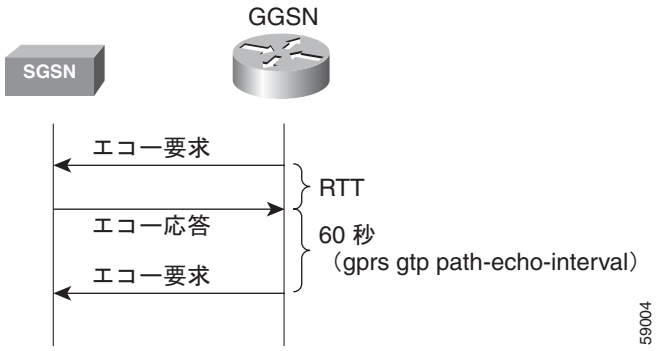
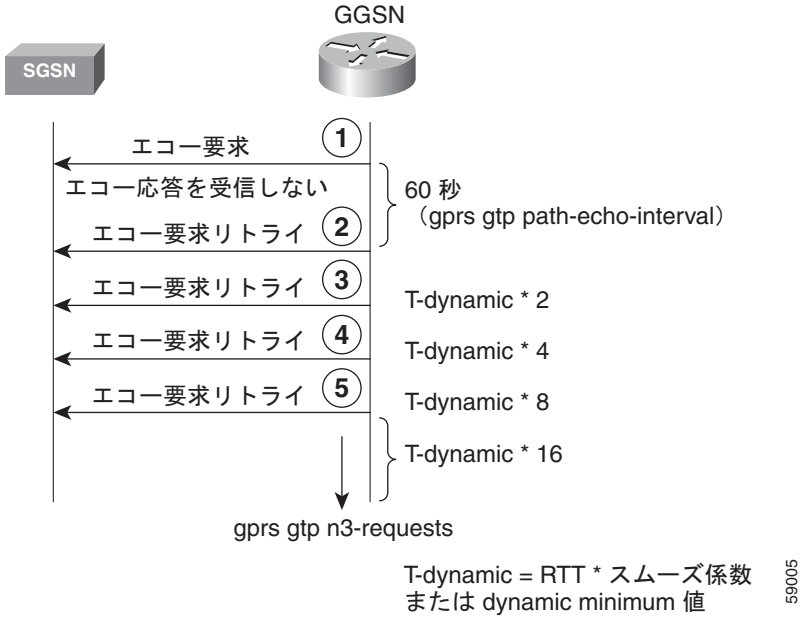


図 3-6 は、パス障害モードのダイナミック エコー タイミング要求のシーケンスを示しています。GGSN は、パス エコー間隔内に SGSN からエコー応答メッセージを受信できない場合、再送信つまりパス障害モードになります。パス障害モード中、GGSN は *T-dynamic* という値を使用します。T-dynamic は、dynamic minimum か、またはスムーズ係数が掛けられた RTT 統計のいずれか大きいほうになります。

図 3-6　パス障害モードのダイナミック エコー タイミング要求のシーケンス



T-dynamic は、基本的には、GGSN でデフォルト エコー タイマー方式で使用される **gprs gtp t3-response** コマンドの代わりに使用します。T-dynamic タイマーは、N3 要求カウンタに達するまで（N3 要求カウンタには初期要求メッセージが含まれます）、リトライごとに 2 倍になります（この係数も設定可能ではありません）。

たとえば、RTT が 6 秒、dynamic minimum が 5 秒、N3 が 5、およびスムーズ係数が 3 の場合、GGSN はパス障害モードで最大 4 つのエコー要求メッセージ（初期要求 + 4 リトライ = 5）を再送信します。GGSN は、SGSN から 60 秒のパス エコー間隔内にエコー応答を受信しない場合、パス エコー間隔が過ぎると即座に最初のエコー要求リトライ メッセージを送信します。RTT x スムーズ係数が 18 秒（6 x 3）であり、dynamic minimum の 5 秒よりも大きいため、dynamic minimum 値は使用されません。T-dynamic 値が 18（RTT x スムーズ係数）であるため、GGSN は別のリトライ エコー要求メッセージを 36 秒（18 x 2）、72 秒（18 x 4）、および 144 秒（18 x 8）で送信します。5 番めのメッセージのあと、GGSN はエコー応答を最後の間隔である 288 秒間（18 x 16）待機します。

GGSN は、この間隔内に SGSN からエコー応答メッセージを受信できない場合、GTP パスをクリアし、PDP コンテキストをすべて削除します。最初の要求メッセージが送信されてから PDP コンテキストがクリアされるまでの経過時間の合計は、次のとおりです。

60 + 36 + 72 + 144 + 288 = 600 秒

60 はパス エコー間隔の初期値であり、残りの 4 つの間隔は後続のリトライでの T-dynamic タイマーの増加を示しています。パスは、さらに 60 秒後に（つまり、660 秒で）クリアされます。

GGSN は、N3 x T-dynamic の送信時間内にエコー応答を受信した場合、エコー要求のシーケンスの正常モードに戻ります。正常モードでは、GGSN はエコー要求を開始し、図 3-4 に示されているように指定されたパス エコー間隔に従って応答を待機します。

再送信のシーケンス番号付け

GGSN は、再送信中にエコー要求メッセージのシーケンス番号を増やしません。したがって、GGSN がエコー応答を受信していない間は、N3 要求制限に達するか応答が受信されるまで、GGSN はすべてのエコー要求リトライに対して同じシーケンス番号を使用し続けます。応答が受信されると、次のエコー要求メッセージのシーケンス番号は 1 増加します。

GGSN が、シーケンス番号の大きいエコー要求メッセージを送信したにもかかわらず、現在のエコー要求メッセージよりも小さいシーケンス番号のエコー応答を受信した場合、その応答は無視されます。

エコー タイミング設定の作業リスト

ここでは、GGSN でのデフォルト エコー タイミング方式のカスタマイズ、またはダイナミック エコー タイミング方式のイネーブルおよび設定に必要な作業について説明します。デフォルトでは、GGSN はデフォルト エコー タイミング方式を有効にします。

GGSN でエコー タイミングを設定するには、次の作業を実行します。

- 「デフォルト エコー タイマーのカスタマイズ」（P.3-11）（使用する場合、推奨）
- 「ダイナミック エコー タイマーの設定」（P.3-11）（任意）
- 「エコー タイマーのディセーブル化」（P.3-12）（任意）

デフォルト エコー タイマーのカスタマイズ

デフォルト エコー タイミング方式は、GGSN で自動的にイネーブルになります。デフォルト エコー タイマーを使用する場合は、必要に応じて次のコマンドを変更してネットワークを最適化することを推奨します。

GGSN でデフォルト エコー タイミング方式をカスタマイズするには、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
ステップ 1	`Router(config)# gprs gtp n3-requests requests`	（任意）GGSN がシグナリング要求の SGSN への送信を試行する最大回数を指定します。デフォルトは 5 です。
ステップ 2	`Router(config)# gprs gtp path-echo-interval interval`	（任意）GGSN が、SGSN または外部課金ゲートウェイからの応答を受信したあと、次のエコー要求メッセージを送信する前に待機する秒数を指定します。デフォルトは 60 秒です。
ステップ 3	`Router(config)# gprs gtp t3-response response-interval`	（任意）要求に対する応答を受信していない場合に、GGSN がシグナリング要求メッセージを再送信する前に待機する初期時間を指定します。この時間は、リトライごとに倍になります。デフォルトは 1 秒です。

ダイナミック エコー タイマーの設定

GGSN でダイナミック エコー タイミング方式を有効化するには、ダイナミック エコー タイマーをイネーブルにする必要があります。ダイナミック エコー タイマーを有効化したあと、対応するオプションを変更してネットワークのタイミング パラメータを最適化できます。

GGSN でダイナミック エコー タイミング方式を設定するには、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
ステップ 1	`Router(config)# gprs gtp echo-timer dynamic enable`	GGSN でダイナミック エコー タイマーをイネーブルにします。
ステップ 2	`Router(config)# gprs gtp echo-timer dynamic minimum number`	（任意）ダイナミック エコー タイマーで使用される最小間隔を指定します。デフォルトは 5 秒です。
ステップ 3	`Router(config)# gprs gtp echo-timer dynamic smooth-factor number`	（任意）ダイナミック エコー タイマーのリトライの送信を待機する時間を計算するために GGSN が使用する乗数を指定します。デフォルトは 2 です。
ステップ 4	`Router(config)# gprs gtp n3-requests requests`	（任意）GGSN がシグナリング要求の SGSN への送信を試行する最大回数を指定します。デフォルトは 5 です。
ステップ 5	`Router(config)# gprs gtp path-echo-interval interval`	（任意）GGSN が、SGSN または外部課金ゲートウェイからの応答を受信したあと、次のエコー要求メッセージを送信する前に待機する秒数を指定します。デフォルトは 60 秒です。

エコー タイマーのディセーブル化

何らかの理由で GGSN による SGSN または外部課金ゲートウェイのエコー処理の実行をディセーブルにする必要がある場合、パス エコー間隔に 0 秒を指定できます。

エコー タイマーをディセーブルにするには、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)# gprs gtp path-echo-interval 0`	（任意）0 秒のパス間隔を指定します。これにより、GGSN によるエコー処理の実行はディセーブルになります。

エコー タイミング設定の確認

ここでは、GGSN でエコー タイミング方式を確認する方法について説明します。内容は次のとおりです。

- 「エコー タイミング パラメータの確認」（P.3-12）
- 「GTP パスごとのダイナミック エコー タイマーの確認」（P.3-13）

エコー タイミング パラメータの確認

GGSN がエコー タイミングに使用しているパラメータを確認するには、**show gprs gtp parameters** または **show running-config** 特権 EXEC コマンドを使用します。

GGSN は、ダイナミック エコー タイマーがイネーブルではない場合でも、ダイナミック エコー タイマーに適用されるパラメータに対してデフォルト値を自動的に設定します。したがって、**show gprs gtp parameters** コマンドでは、どちらのエコー タイミング方式が現在有効になっているかはわかりません。

デフォルト エコー タイミング パラメータの確認

デフォルト エコー タイマーで使用されているパラメータを確認するには、**show gprs gtp parameters** 特権 EXEC コマンドを使用し、次の太字で表示されているパラメータを確認します。

```
Router# show gprs gtp parameters
   GTP path echo interval                          = 60
    GTP signal max wait time T3_response           = 1
    GTP max retry N3_request                       = 5
    GTP dynamic echo-timer minimum                 = 5
    GTP dynamic echo-timer smooth factor           = 2
    GTP buffer size for receiving N3_buffer        = 8192
    GTP max pdp context                            = 45000
```

ダイナミック エコー タイミング パラメータの確認

ダイナミック エコー タイマーで使用されているパラメータを確認するには、**show gprs gtp parameters** 特権 EXEC コマンドを使用し、次の太字で示されているパラメータを確認します。

```
Router# show gprs gtp parameters
   GTP path echo interval                          = 60
    GTP signal max wait time T3_response            = 1
    GTP max retry N3_request                        = 5
    GTP dynamic echo-timer minimum                  = 5
    GTP dynamic echo-timer smooth factor            = 2
    GTP buffer size for receiving N3_buffer         = 8192
    GTP max pdp context                             = 45000
```

GTP パスごとのダイナミック エコー タイマーの確認

show running-config 特権 EXEC コマンドを使用すると、ダイナミック エコー タイマーがイネーブルかどうかを確認できます。

ダイナミック エコー タイマーの値は、GGSN での GTP パスごとに異なります。GGSN でダイナミック エコー タイマーがイネーブルかどうか、およびダイナミック エコー タイマー（T-dynamic）の値（秒単位）を確認するには、**show gprs gtp path** 特権 EXEC コマンドを使用します。

ダイナミック エコー タイマーが有効ではない場合、ダイナミック エコー タイマー出力フィールドの対応するパスの横に「Disabled」と表示されます。

ステップ 1　ダイナミック エコー タイマーがイネーブルであることを確認するには、**show running-config** コマンドを使用し、次の出力例の最後の方に太字で示されているように **gprs gtp dynamic echo-timer enable** コマンドが表示されることを確認します。

```
Router# show running-config

Current configuration : 6769 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service gprs ggsn
!
ip cef
!
. . .
!

interface loopback 1
 ip address 10.41.41.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
. . .
!
gprs access-point-list gprs
  access-point 1
   access-point-name gprs.cisco.com
   exit
```

```
   !
  access-point 2
   access-point-name gprt.cisco.com
   access-mode non-transparent
   aaa-group authentication test2
   aaa-group accounting test2
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.65.0.1
   dhcp-gateway-address 10.65.0.1
   exit
   !
!
gprs ms-address exclude-range 10.21.1.0 10.21.1.5
gprs gtp echo-timer dynamic enable
gprs gtp echo-timer dynamic smooth-factor 5
gprs gtp echo-timer dynamic minimum 10
gprs gtp response-message wait-accounting
!
. . .
!
end
```

ステップ 2　対応する GTP パスの T-dynamic 値を確認するには、**show gprs gtp path all** 特権 EXEC コマンドを使用します。

次の例は、GGSN でダイナミック エコー タイマーがイネーブルであり、T-dynamic 値の 5 秒および 2 秒が対応するパスに対して使用されていることを示しています。

```
Router# show gprs gtp path all
         Total number of path : 2

Local address           Remote address          GTP version    Dynamic echo timer
10.41.41.1(3386)        10.18.18.200(3386)      0              5
10.10.10.1(2123)        10.10.10.4(2123)        1              2
```

GGSN 設定のカスタマイズ

ここでは、デフォルト設定をさらにカスタマイズするために GGSN で設定できるオプションの一部について説明します。

GPRS/UMTS 課金オプションの設定の詳細については、「課金オプションのカスタマイズ」（P.6-11）を参照してください。

この項は、次の内容で構成されています。

GTP シグナリング オプションの設定

GGSN サポート用の Cisco IOS ソフトウェアのインスタンスを設定するために使用されるコマンド以外に、GGSN 機能では、GTP 設定をカスタマイズするために使用できる複数のオプション コマンドがサポートされています。

特定の GTP 処理オプションについては、デフォルト値が推奨値を表しています。その他のオプション コマンドもデフォルト値に設定されていますが、必要に応じて、またはハードウェアに応じてこれらのコマンドを変更して、ネットワークを最適化することを推奨します。ここでは、GTP シグナリングを最適化するために使用を検討する必要があるコマンドの一部について説明します。

GTP シグナリング設定を最適化するには、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)# gprs gtp n3-requests requests`	（任意）GGSN がシグナリング要求の送信を試行する最大回数を指定します。デフォルトは 5 です。
`Router(config)# gprs gtp path-echo-interval interval`	（任意）GGSN が GTP パス障害をチェックするエコー要求メッセージを送信する前に待機する秒数を指定します。デフォルトは 60 秒です。
`Router(config)# gprs gtp t3-response response_interval`	（任意）要求に対する応答を受信していない場合に、GGSN がシグナリング要求メッセージを再送信する前に待機する初期秒数を指定します。この時間は、リトライごとに倍になります。デフォルトは 1 秒です。

（注）　これらの GTP シグナリング コマンドは、GGSN でエコー タイミングをサポートするためにも使用されます。GGSN でのエコー タイミングの詳細については、「GGSN でのエコー タイミングの設定」（P.3-4）を参照してください。

その他の GTP シグナリング オプションの設定

ここでは、ネットワークのニーズに対応するために必要に応じて変更可能な、その他の GTP シグナリング オプションの一部について説明します。

その他の GTP シグナリング オプションを設定するには、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)# gprs gtp map signalling tos tos-value`	（任意）GTP シグナリング パケットの IP Type of Service（ToS; サービス タイプ）マッピングを指定します。デフォルトは 5 です。
`Router(config)# gprs gtp n3-buffer-size bytes`	（任意）GGSN が GTP シグナリング メッセージおよびトンネリング プロトコルで送信されるパケットを受信するために使用する受信バッファのサイズを指定します。デフォルトは 8192 バイトです。

コマンド	目的
`Router(config)# gprs gtp response-message pco ipcp nack`	（任意）与えられた値（ゼロ以外）が要求された値と異なる IP Control Protocol（IPCP; IP コントロール プロトコル）オプションを返すときに、GGSN が PDP コンテキストの作成応答の GTP Protocol Configuration Option（PCO; プロトコル設定オプション）Information Element（IE; 情報エレメント）で IPCP Conf-Nack（コード 03）を返すことを指定します（返されるアドレス値がゼロのオプションの場合は、IPCP Conf-Reject（コード 04））。 GGSN でサポートされる、要求されたすべての IPCP アドレス オプションについて、デフォルトでは、GGSN は PDP コンテキストの作成応答の PCO IE で IPCP Conf-Ack（コード 2）を送信します（返される値は、要求された値と同じか、異なる場合があり、またゼロの場合もあります）。
`Router(config)# gprs gtp response-message pco ipcp message-length`	IPCP オプションを返すときに PDP コンテキストの作成応答の PCO IE のヘッダーに追加される、メッセージの長さを示す追加フィールドを設定します。

GGSN での PDP コンテキストの最大数の設定

GGSN でサポートされる PDP コンテキストの最大数の実質的な上限は、使用されるメモリおよびプラットフォームと GGSN 設定によって異なります（Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）の方式が端末装置およびモバイル終端を超えてパケットを転送するように設定されているかどうか、Dynamic Feedback Protocol（DFP）が使用されているか、またはメモリ保護機能がイネーブルか、サポートされている PDP コンテキスト作成のレートなどによって異なります）。

（注）　DFP では、PPP PDP を IP PDP と比較します。1 つの PPP PDP は 8 つの IPv4 PDP と等価です。1 つの IPv6 PDP は 8 つの IPv4 PDP と等価です。

表 3-1 は、1 GB のメモリ オプションの Cisco SAMI でサポートできる PDP コンテキストの最大数を示しています。表 3-2 は、2 GB のメモリ オプションの Cisco SAMI でサポートできる最大数を示しています。

表 3-1　　1 GB の SAMI でサポートされる PDP 数

PDP タイプ	GGSN ごとの最大数	SAMI ごとの最大数[1]
IPv4	66,000	400,000
IPv6	8,000	48,000
PPP 再生成	16,000	96,000
PPP	8,000	48,000

1. 6 つの GGSN が設定されている SAMI ごとの最大数

表 3-2　2 GB の SAMI でサポートされる PDP 数

PDP タイプ	GGSN ごとの最大数	SAMI ごとの最大数[1]
IPv4	136,000	816,000
IPv6	16,000	96,000
PPP 再生成	32,000	192,000
PPP	16,000	96,000

1. 6 つの GGSN が設定されている SAMI ごとの最大数

（注）　PDP コンテキストが許可可能な最大数に達すると、GGSN はセッションが使用可能になるまで新しい PDP コンテキストを拒否します。

GGSN で PDP コンテキストの最大数を設定するには、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)# gprs maximum-pdp-context-allowed` *pdp-contexts*	GGSN で有効化できる PDP コンテキストの最大数を指定します。

DFP をロード バランシングとともに使用する場合の PDP コンテキストの最大数の設定

DFP を GPRS/UMTS ロード バランシングとともに使用する場合も、GGSN ごとの PDP コンテキストの最大数を指定する必要があります。デフォルト値である 10000 PDP コンテキストを使用しないでください。45000 が推奨値です。非常に小さい値は、GPRS/UMTS ロード バランシング環境のパフォーマンスに影響します。

（注）　GPRS/UMTS ロード バランシングの設定の詳細については、Cisco.com の次の URL で「*IOS Server Load Balancing*」12.1(9)E ドキュメントを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e9/index.htm

DFP の GGSN で PDP コンテキストの最大数を設定するには、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)# gprs maximum-pdp-context-allowed 45000`	GGSN で有効化できる PDP コンテキストの最大数として 45000 を指定します。

GGSN でのセッションの制御

GPRS/UMTS では、常時オンのサービスがモバイル ユーザに提供されます。GGSN は、一定の数の PDP コンテキストだけをサポートできます。サポートされる PDP コンテキスト数は、設定およびプラットフォームのメモリ リソースによって異なります。

ネットワーク接続を提供する GGSN とのセッションは、そのセッションでアクティビティが発生しなくても確立できます。GGSN で PDP コンテキストが確立されたあとは、セッションにアクティビティがあるかどうかに関係なく、リソースは GGSN で使用されています。したがって、GGSN でセッションを確立しておく時間を制御するセッション タイマーを設定し、そのあとは PDP コンテキストがクリアされるようにする場合があります。

また、特定のメンテナンス機能（Access Point Name（APN; アクセス ポイント ネーム）設定の変更など）を実行する場合は、PDP コンテキストを手動で削除できます。

この項は、次の内容で構成されています。

セッション タイマーの設定

ここでは、GGSN でセッション アイドル時間および絶対セッション時間を設定し、GGSN がセッションをいつ削除するかを制御する方法について説明します。この項は、次の内容で構成されています。

GGSN でのセッション アイドル タイマーおよび絶対セッション タイマーの概要

GGSN では、セッション アイドル タイマー（RADIUS アトリビュート 28）および絶対セッション タイマー（RADIUS アトリビュート 27）の時間を設定することによって、PDP コンテキストのクリアを制御できます。セッション アイドル タイマーおよび絶対セッション タイマーによって、GGSN がモバイル セッションをパージするまでに待機する時間が指定されます。

セッション アイドル時間に対して指定される時間は、セッションに属するすべての PDP コンテキストで同じですが（GTPv1 モバイル セッションには複数の PDP コンテキストがある場合があります）、そのセッションの PDP コンテキストごとに個別のタイマーが開始されます。したがって、セッション アイドル タイマーは PDP ごとですが、タイマー時間はセッションごとです。絶対セッション タイマーはセッションに基づいており、セッション（アクティブまたは非アクティブ）の絶対時間が制御されます。絶対セッション タイマーを超過すると、GGSN はセッションの PDP コンテキスト（同じ International Mobile Subscriber Identity（IMSI）または Mobile Station（MS; モバイル ステーション）アドレスを持つコンテキスト）をすべて削除します。

（注）　セッション アイドル タイムアウト（RADIUS アトリビュート 28）サポートは、IP PDP、GGSN で終端する PPP PDP、および PPP 再生成 PDP（PPP Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）PDP ではありません）に適用されます。絶対セッション タイムアウト（アトリビュート 27）サポートは、IP PDP および GGSN で終端する PPP PDP（PPP 再生成または PPP L2TP PDP ではありません）に適用されます。設定されると、セッション アイドル タイマーは PDP コンテキストごとに開始され、絶対セッション タイマーはセッションに基づいて開始されます。

すべてのアクセス ポイントで発生するセッションに対して GGSN でタイマーをグローバルに設定できます。また、特定のアクセス ポイントに対してタイマーを設定できます。GGSN で設定できるセッション アイドル タイマーおよび絶対セッション タイマー以外に、RADIUS サーバはセッション タイムアウト アトリビュートも指定できます。

次のリストは、GGSN がタイマーを実装する順序を示しています。

1. RADIUS サーバ：非透過的アクセス モードに対してアクセス ポイントが設定されており、RADIUS サーバによってタイムアウト アトリビュートが返される場合、GGSN は RADIUS サーバから送信されるアトリビュートに基づいてタイムアウト値を設定します。RADIUS サーバのタイムアウト アトリビュートは、秒単位で指定されます。RADIUS サーバによって返される値が 30 秒未満の場合、GGSN はタイムアウト値を 30 秒に設定します。値が 30 秒を超える場合、GGSN はタイムアウト値を RADIUS サーバによって返される値と同じ値に設定します。
2. アクセス ポイント：透過的アクセス モードに対してアクセス ポイントが設定されているか、またはアクセス ポイントが非透過的アクセス モードであり、RADIUS サーバによってタイムアウト値が返されない場合、GGSN は **gtp pdp-context timeout session** コマンドまたは **gtp pdp-context timeout idle** コマンドに対して指定された値を使用します。
3. グローバル タイマー：GGSN は、RADIUS サーバまたはアクセス ポイントからタイムアウト値を受信しない場合、**gprs gtp pdp-context timeout session** コマンドまたは **gprs gtp pdp-context timeout idle** コマンドに対して指定された値を使用します。

要約すると、RADIUS サーバからのタイムアウト値が GGSN でのタイマー設定よりも優先され、特定のアクセス ポイントのタイマーがグローバルに設定されたタイマーよりも優先されます。

pdp-context timeout session コマンドおよび **gtp pdp-context timeout idle** コマンドの値は、**gprs gtp pdp-context timeout session** コマンドまたは **gprs gtp pdp-context timeout idle** コマンドの値を上書きします。

（注）　セッション タイマー（アイドルまたは絶対）をイネーブルにすると、タイマーが期限切れになったために PDP コンテキストの終端に対してトリガーされた GGSN CDR（G-CDR）は、「managementIntervention」という原因値を持ちます。

セッション アイドル タイマーの設定

GGSN は、RADIUS Idle-Timeout（アトリビュート 28）フィールドをサポートします。GGSN は、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）サーバによって送信されたアクセス要求パケット内にアトリビュート 28 値がある場合、それを格納します。PDP コンテキストがこのコマンドで指定された時間よりも長い時間アイドルであった場合、GGSN はコンテキストを終了します。

タイマーに対して指定された時間はセッションのすべての PDP コンテキストに適用されますが、タイマーは PDP コンテキストごとに開始されます。

セッション アイドル タイマーは、グローバルに設定することも、APN で設定することもできます。APN レベルで設定された値によって、グローバルに設定された値が上書きされます。

（注）　PDP コンテキストに対して開始されたセッション アイドル タイマーは、Transport Protocol Data Unit（TPDU; 転送プロトコル データ ユニット）トラフィックおよびその PDP コンテキストの GTP シグナリング メッセージによってリセットされます。たとえば、PDP コンテキストの更新要求が受信された場合、セッション アイドル タイマーはその PDP コンテキストに対してリセットされます。

GGSN でのセッション アイドル タイマーのグローバルな設定

GGSN が PDP コンテキストをパージする前に、任意のアクセス ポイントでコンテキストがアイドルであることを許可する時間を設定するには、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)# gprs gtp pdp-context timeout idle` *seconds* [**uplink**]	GGSN が PDP コンテキストをパージする前に、任意のアクセス ポイントでコンテキストがアイドルであることを許可する時間（秒単位）を指定します。有効な範囲は、30 ～ 429467 です。デフォルトは 259200 秒（72 時間）です。 任意で、**uplink** キーワード オプションを指定して、アップリンク方向だけでセッション アイドル タイマーをイネーブルにします。**uplink** キーワード オプションを指定しない場合、セッション アイドル タイマーは両方向（アップリンクおよびダウンリンク）でイネーブルになります。

（注）　代わりに、グローバル コンフィギュレーション モードで **gprs idle-pdp-context purge-timer** *hours* コマンドを使用して、セッション アイドル タイマーをグローバルに設定できます。ただし、2 つの方式を同時に設定することはできません。

GGSN のアクセス ポイントでのセッション アイドル タイマーの設定

GGSN が PDP コンテキストをパージする前に、特定のアクセス ポイントでコンテキストがアイドルであることを許可する時間を設定するには、アクセス ポイント 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-access-point)# gtp pdp-context timeout idle` *seconds* [**uplink**]	GGSN が PDP コンテキストをパージする前に、特定のアクセス ポイントでコンテキストがアイドルであることを許可する時間（秒単位）を指定します。有効な範囲は、30 ～ 429467 です。デフォルトは 259200 秒（72 時間）です。 任意で、**uplink** キーワード オプションを指定して、アップリンク方向だけでセッション アイドル タイマーをイネーブルにします。**uplink** キーワード オプションを指定しない場合、セッション アイドル タイマーは両方向（アップリンクおよびダウンリンク）でイネーブルになります。

（注）　代わりに、**session idle-time** *hours* アクセス ポイント コンフィギュレーション コマンドを使用して、アクセス ポイントでセッション アイドル タイマーを設定できます。ただし、2 つの方式を同時に設定することはできません。

GGSN でのセッション アイドル タイマーのディセーブル化

デフォルトでは、すべてのアクセス ポイントについて、GGSN はセッションのアイドルな PDP コンテキストを 72 時間後にパージします。PDP コンテキストがアイドルであることを無期限に許可する場合は、RADIUS サーバ上のユーザ プロファイルでセッション アイドル時間として 0 を設定して、特定のユーザのタイマーをディセーブルにすることができます。ユーザが RADIUS によって認証されていない場合は、セッション アイドル タイマーをディセーブルにすることはできません。

絶対セッション タイマーの設定

GGSN は、RADIUS Session-Timeout（アトリビュート 27）フィールドをサポートします。絶対セッション タイマーをイネーブルにすると、GGSN は、AAA サーバによって送信されたアクセス要求パケット内にアトリビュート 27 値がある場合、それを格納します。セッションの時間がこのコマンドで指定された値を超過すると、GGSN はセッションに属する PDP コンテキスト（同じ IMSI または MS アドレスを持つコンテキスト）をすべて終了します。

絶対セッション タイマーは、グローバルに、および APN で設定できます。APN レベルで設定された値によって、グローバルに設定された値が上書きされます。

デフォルトでは、絶対セッション タイマーはディセーブルです。

（注）　GGSN 絶対セッション タイマーでは、GGSN をイネーブルにし、グローバル コンフィギュレーション モードで **gprs radius attribute session-timeout** コマンドを使用して、Session-Timeout（アトリビュート 27）を RADIUS 要求に含めておく必要があります。

GGSN での絶対セッション タイマーのグローバルな設定

GGSN がセッションを終了し、そのセッションに属する PDP コンテキストをすべてパージする前に、任意のアクセス ポイントでセッションが存在することを許可する時間を設定するには、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)# gprs gtp pdp-context timeout session` *seconds*	GGSN がセッションを終了し、同じ IMSI または MS アドレスを持つ PDP コンテキストをすべてパージする前に、任意のアクセス ポイントでセッションが存在することを許可する時間（秒単位）を指定します。有効な範囲は、30 ～ 4294967 秒です。

GGSN のアクセス ポイントでの絶対セッション タイマーの設定

GGSN がセッションを終了し、そのセッションに属する PDP コンテキストをすべてパージする前に、特定のアクセス ポイントでセッションが存在することを許可する時間を設定するには、アクセス ポイント 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-access-point)# gtp pdp-context timeout session` *seconds*	GGSN がセッションを終了し、同じ IMSI または MS アドレスを持つ PDP コンテキストをすべてパージする前に、特定のアクセス ポイントでセッションが存在することを許可する時間（秒単位）を指定します。有効な範囲は、30 ～ 4294967 秒です。

GGSN での絶対セッション タイマーのディセーブル化

デフォルトでは、GGSN で絶対セッション タイマーはディセーブルです。絶対セッション タイマーをイネーブルにしたあとでデフォルト設定に戻すには、グローバル コンフィギュレーション コマンドまたはアクセス ポイント コンフィギュレーション コマンドの **no** フォーム（**no gprs gtp pdp-context timeout session** または **no gtp pdp-context timeout session**）を使用します。

タイマー設定の確認

特定の PDP コンテキストのタイマー情報を表示するには、**show gprs gtp pdp-context** コマンドおよび **tid** キーワードまたは **imsi** キーワードを使用します。次の例は、セッション アイドル タイマーが 200 時間（720000 秒）、絶対セッション タイマーが 24 時間（86400 秒）に設定された PDP コンテキストに対する **show gprs gtp pdp-context tid** コマンドの出力例を示しています。タイマーの値は、**session timeout** フィールドおよび **idle timeout** フィールドに太字で表示されています。

```
Router#show gprs gtp pdp-context tid 1111111111111111
TID              MS Addr         Source  SGSN Addr       APN
1111111111111111 10.1.1.1        Radius  10.8.8.1        dns.com

    current time :Mar 18 2002 11:24:36
    user_name (IMSI):1111111111111111   MS address:10.1.1.1
    MS International PSTN/ISDN Number (MSISDN):ABC
    sgsn_addr_signal:10.8.8.1           sgsn_addr_data:10.8.0.1
    control teid local: 0x63493E0C
    control teid remove: 0x00000121
    data teid local:  0x63483E10
    data teid remote:  0x00000121
    primary pdp: Y      nsapi: 0
    signal_sequence: 0                  seq_tpdu_up:     0
    seq_tpdu_down:   0
    upstream_signal_flow:  1            upstream_data_flow:  2
    downstream_signal_flow:14           downstream_data_flow:12
    RAupdate_flow:         0
    pdp_create_time:  Mar 18 2002 09:58:39
    last_access_time: Mar 18 2002 09:58:39
    mnrgflag:         0                 tos mask map:00
   session timeout: 86400
    idle timeout: 720000
    gprs qos_req:091101               canonical Qos class(req.):01
    gprs qos_neg:25131F               canonical Qos class(neg.):01
    effective bandwidth:0.0
    rcv_pkt_count:     0              rcv_byte_count:  0
    send_pkt_count:    0              send_byte_count: 0
    cef_up_pkt:        0              cef_up_byte:    0
    cef_down_pkt:      0              cef_down_byte:  0
    cef_drop:           0             out-sequence pkt: 0
```

```
Src addr violation:            2 paks,     1024 bytes
Dest addr violation:           2 paks,     1024 bytes
Redirected mobile-to-mobile traffic:  2 paks,     1024 bytes
charging_id:        29160231
visitor: No        roamer: No
charging characteristics: 0
charging characteristics received: 0
pdp reference count:2
primary dns:        2.2.2.2
secondary dns:      4.4.4.4
primary nbns:       3.3.3.3
secondary nbns:     5.5.5.5
ntwk_init_pdp:      0
Framed_route 5.5.5.0 mask 255.255.255.0

** Network Init Information **
MNRG Flag: 0               PDU Discard Flag: 0
SGSN Addr: 172.16.44.1     NIP State:        NIP_STATE_WAIT_PDP_ACTIVATION
Buf.Bytes: 500
```

GGSN でのセッションの削除

必要に応じて、**clear gprs gtp pdp-context** 特権 EXEC コマンドを使用して、PDP コンテキストを手動で削除できます。

PDP コンテキストは、Terminal Identifier（TID; 端末 ID）、IMSI 値、またはアクセス ポイント（IP バージョン別またはそのアクセス ポイントでアクティブなすべての PDP）別に削除できます。

Third Generation Partnership Program（3GPP）規格で定義されているように、デフォルトでは、GGSN は PDP コンテキストの削除要求を SGSN に送信し、SGSN からの応答を待機してから PDP コンテキストを削除します。また、複数の PDP コンテキストを削除する場合、一度に削除できるのは特定の数の PDP コンテキストだけです。

SGSN が GGSN の PDP コンテキストの削除要求に応答しない場合、タスクの完了が大きく遅延する場合があります。Fast PDP Delete 機能（**no-wait-sgsn** および **local-delete** アクセス ポイント キーワード オプション）を使用して、この遅延をなくすことができます。Fast PDP Delete 機能を使用すると、GGSN で SGSN からの応答を待機しないで APN 内の PDP コンテキストを削除するか、または GGSN で PDP コンテキストの削除要求を SGSN に送信しないで PDP コンテキストをローカルで削除できます。

Fast PDP Delete 機能を使用する場合は、次の点に注意してください。

- Fast PDP Delete 機能は、APN または GGSN がメンテナンス モードの場合にだけ使用できます。したがって、**no-wait-sgsn** および **local-delete** キーワード オプションは、APN または GGSN がメンテナンス モードの場合にだけ使用できます。
- **no-wait-sgsn** および **local-delete** キーワード オプションを指定してこのコマンドを入力すると、GGSN で次の注意が表示されます。

  ```
  Deleting all PDPs without successful acknowledgements from the SGSN will result in the
  SGSN and GGSN going out of sync. Do you want to proceed ? [n]:
  ```

  デフォルトは **no** です。削除を取り消すには、**n** を入力して Enter キーを押します。削除を続行するには、**y** を入力して Enter キーを押します。
- サービス認識 PDP を処理する場合、Fast PDP Delete 機能が使用されていて GGSN が SGSN からの応答を待機していないときは、GGSN は Cisco Content Services Gateway（CSG）および Diameter サーバからの応答を待機する必要があります。したがって、Fast PDP Delete 機能はサービス認識 PDP に対してはそれほど有効ではありません。

- PDP コンテキストの削除要求が失われた場合、SGSN は PDP コンテキストを削除できなくなります。この状態により、GGSN と SGSN で生成される Call Detail Record（CDR; 呼詳細レコード）に不整合が発生する場合があります。
- **no-wait-sgsn** キーワード オプションが指定された場合、GGSN は SGSN への PDP コンテキストの削除要求を調整しないため、GGSN が SGSN を PDP コンテキストの削除要求でフラッドさせる場合があります。
- Fast PDP Delete 機能は、**clear gprs gtp-context** 特権 EXEC コマンドで開始された PDP 削除だけに適用されます。障害状態中の PDP 削除など、その他の状況による PDP 削除には影響しません。

PDP コンテキストを手動で削除するには、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(config-access-point)# clear gprs gtp pdp-context {tid tunnel-id | imsi imsi_value | path ip-address [remote_port_num] | access-point access-point-index [no-wait-sgsn | local-delete] | pdp-type {ipv6 | ipv4} | all}`	1 つ以上のパケット データ プロトコル（PDP）コンテキスト（モバイル セッション）を TID、IMSI 値、パス、またはアクセス ポイント（IP バージョン別またはアクティブなすべての PDP）別にクリアします。 （注）　**no-wait-sgsn** および **local-delete** キーワード オプションは、APN がメンテナンス モードの場合にだけ使用できます（**service-mode maintenance** コマンドを使用）。

APN をメンテナンス モードにする方法の詳細については、「APN メンテナンス モードの設定」（P.3-28）を参照してください。

GTP エラー メッセージのフロー制御の設定

GTP エラー通知メッセージは、SGSN が送信した PDP コンテキストのデータを GGSN が見つけられないときに、GGSN から SGSN に送信されます。このエラー通知メッセージは、PDP コンテキストが見つからないため、SGSN 側で PDP コンテキストを消去できることを SGSN に通知します。

デフォルトでは、GGSN は GTP エラー メッセージのフロー制御をディセーブルにします。

グローバル コンフィギュレーション モードで **gprs gtp error-indication-throttle** コマンドを使用して、GTP エラー メッセージの送信のフロー制御をイネーブルにすることができます。このコマンドによって、エラー通知メッセージが送信されるたびに減少するカウンタの初期値が設定されます。カウンタがゼロに達すると、GGSN はエラー通知メッセージの送信を停止します。1 秒後に、GGSN はこのカウンタを設定されたスロットル値にリセットします。

GTP エラー メッセージのフロー制御を設定するには、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)# gprs gtp error-indication-throttle window-size size`	GGSN が 1 秒間に送信するエラー通知メッセージの最大数を指定します。size は 0 ～ 256 の整数です。デフォルト値はありません。

GGSN での削除済み SGSN パスの履歴維持の設定

削除済み SGSN パスについて収集された統計情報を格納するように Cisco GGSN を設定できます。

GGSN で統計情報の履歴を格納する削除済み SGSN パス エントリの最大数を設定するには、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)# **gprs gtp path history** *number*	GGSN で統計情報の履歴を格納する削除済み SGSN パス エントリの最大数を設定します。有効な値は、1 ～ 1000 です。デフォルトは 100 です。

（注）　エントリ数を小さい値に変更すると、古い値は削除されます。

SGSN ごとのエコー要求の抑制

オペレータは、グローバル コンフィギュレーション モードで **gprs gtp path sgsn** コマンドを使用して、他の SGSN のエコー要求をそのまま維持しながら、GGSN からのエコー要求に応答できない GSN のエコー要求を選択的にディセーブルにすることができます。また、GSN の特定のポートについてエコー要求をディセーブルにすることもできます。

新しいパスが作成されると、**gprs gtp path** コマンドを使用してエコー要求を抑制する場合、GGSN はパス パラメータ（つまり宛先アドレスおよびポート）が設定済みの条件のいずれかに一致するかどうかをチェックします。パラメータが一致した場合、GGSN はそのパスのパス エコー間隔を 0 に設定します。一致しない場合、グローバルなパス エコー間隔設定がエコー要求の送信に使用されます。

IP アドレスの範囲または単一の IP アドレスに対して、任意でポート番号を指定して、エコー要求をディセーブルにすることができます。

エコー要求を抑制するには、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)# **gprs gtp path sgsn** *start-ip-address* [*end-ip-address*] [*UDP port*] **echo 0**	*start-ip-address* から *end-ip-address* の範囲の設定された User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポートに対応するすべての SGSN について、作成されたパスのエコー間隔要求が 0（ディセーブル）であることを指定します。

次の例は、1 つの SGSN のエコー要求をディセーブルにします。

```
Router(config)# gprs gtp path sgsn 10.10.10.10 echo 0
```

次の例は、1 つの SGSN のポート 4000 だけのエコー要求をディセーブルにします。

```
Router(config)# gprs gtp path sgsn 10.10.10.10 4000 echo 0
```

GGSN が開始する PDP コンテキストの更新要求のサポートの設定

（注）　GGSN が開始する PDP コンテキストの更新要求は、GTPv1 PDP コンテキストに対してサポートされます。

Cisco GGSN リリース 8.0 以降、Cisco GGSN は PDP コンテキストの更新要求（3GPP TR 29.060 v7.5.1、section 7.3.3 で定義）を SGSN に送信して、PDP コンテキストの QoS をネゴシエーションできます。

Gx 環境の Cisco Content Services Gateway（CSG）などの外部エンティティは、新しい QoS プロファイルを GGSN にプッシュして、特定の PDP コンテキストで適用できます。次に、GGSN は SGSN への PDP コンテキストの更新要求で、変更を Radio Access Network（RAN; 無線アクセス ネットワーク）にプッシュします。

また、PDP コンテキストに対して直接トンネルが使用されている場合、Radio Network Controller（RNC; 無線ネットワーク コントローラ）からのエラー通知メッセージのために、GGSN は PDP コンテキストの更新要求を SGSN に送信します。

GGSN では、次の情報エレメント（IE）が PDP コンテキストの更新要求に含まれています。

- リカバリ
- Network Service Access Point Identifier（NSAPI; ネットワーク サービス アクセス ポイント ID）
- QoS プロファイル
- 直接トンネル フラグ（RNC から受信された直接トンネル エラー通知により更新要求が開始された場合）

QoS が再ネゴシエーションされると、SGSN は PDP コンテキストの更新応答を GGSN に返してプロセスを完了します。SGSN からの PDP コンテキストの更新応答の Cause 値が「Request Accepted」の場合、次のアクションのいずれかが発生します。

- PDP コンテキストの更新要求が RNC からのエラー通知メッセージによって開始された場合、PDP コンテキストは維持されます。
- PDP コンテキストの更新要求が新しい QoS を含む Change of Authorization（CoA; 認証の変更）によって開始された場合、新しい QoS を通信するために Interim-Acct-Update メッセージが送信されます（PDP コンテキストの更新要求で指定される QoS 値は、SGSN によって下方にネゴシエーションされている場合があります）。GGSN は Acct-Update メッセージで同じ内容通知します。

PDP コンテキストの更新応答の Cause 値が「Request Accepted」以外の場合、次のアクションのいずれかが発生します。

- PDP コンテキストの更新要求が RNC からのエラー通知によって開始された場合、PDP はローカルで削除されます。
- PDP コンテキストの更新要求がグローバル コンフィギュレーション モードで CoA コマンドによって開始された場合は、次のとおりです。
  - **gprs gtp update qos-fail delete** グローバル コンフィギュレーション コマンドまたは **gtp update qos-fail delete** アクセス ポイント コンフィギュレーション コマンドが設定されている場合、GGSN は PDP コンテキストを削除し、Acct-Stop メッセージで更新失敗の通知を送信します。
  - **gprs gtp update qos-fail delete** グローバル コンフィギュレーション コマンドまたは **gtp update qos-fail delete** アクセス ポイント コンフィギュレーション コマンドが設定されていない場合、GGSN は PDP コンテキストを維持し、ネゴシエーションされた QoS 値でアカウンティング中間レコードを生成します。

– すべての失敗において、失敗を示すエラー メッセージが記録されます。

（注）　直接トンネル PDP コンテキストの更新要求の失敗に対して、エラー メッセージの syslog は生成されません。

GGSN が開始する PDP コンテキストの更新要求をグローバルに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発行します。

コマンド	目的
`Router(config)# gprs gtp update qos-fail delete`	GGSN が開始する QoS 更新が失敗し、APN で **gtp update qos-fail** アクセス ポイント コンフィギュレーション コマンドを使用して、GGSN が開始する PDP コンテキストの更新要求の失敗アクションが設定されていない場合に、PDP コンテキストを削除するように GGSN を設定します。

GGSN が開始する PDP コンテキストの更新要求を APN でイネーブルにするには、アクセス ポイント コンフィギュレーション モードで次のコマンドを発行します。

コマンド	目的
`Router(config-access-point)# gtp update qos-fail delete`	GGSN が開始する QoS 更新が失敗した場合に、PDP コンテキストを削除するように GGSN を設定します。

サービス モード機能の使用

GGSN サービス モード機能を使用すると、GGSN でのすべてのアクティブなセッションに影響を与えずに、設定変更およびコールのテストを行うことができます。サービス モード状態は、グローバルに、アクセス ポイントで、および GGSN 課金機能に対して設定できます。運用およびメンテナンスという 2 つのサービス モード状態があります。デフォルトのモードは運用です。

グローバル メンテナンス モードの設定

GGSN をグローバル メンテナンス モードにすると、新しい PDP コンテキストの作成要求はすべて拒否されます。したがって、グローバル メンテナンス モードの間は、GGSN 全体で新しい PDP コンテキストは有効化されません。

次の項では、グローバル メンテナンス モードの使用方法の例を示します。

新しい GGSN の追加

1. GGSN サービスをイネーブルにし、GGSN をメンテナンス モードにします。

```
Router(config)# service ggsn
Router(config)# gprs service-mode maintenance
```

2. 使用するネットワーク用に GGSN を設定します。
3. GGSN を運用モードにします。

```
Router(config)# gprs service-mode operational
```

GGSN の変更

1. GGSN をメンテナンス モードにします。

```
Router(config)# gprs service-mode maintenance
```

すべての APN の既存の PDP が正常に解放され（平均セッション時間は約 1 時間）、バッファリングされた CDR が課金ゲートウェイに送信されるのを待機します。アクティブな課金ゲートウェイがないために CDR が課金ゲートウェイに送信されない場合は、**gprs charging service-mode** コマンドを使用して課金機能をメンテナンス モードにし、**clear gprs charging cdr all no-transfer** コマンドを発行して CDR を手動でクリアします。課金機能をメンテナンス モードにする方法の詳細については、「課金メンテナンス モードの設定」（P.3-30）を参照してください。

2. 必要に応じて GGSN 設定を変更します。
3. GGSN を運用モードに戻します。

```
Router(config)# gprs service-mode operational
```

GGSN の無効化

1. GGSN をメンテナンス モードにします。

```
Router(config)# gprs service-mode maintenance
```

すべての APN の既存の PDP が正常に解放され（平均セッション時間は約 1 時間）、バッファリングされた CDR が課金ゲートウェイに送信されるのを待機します。アクティブな課金ゲートウェイがないために CDR が課金ゲートウェイに送信されない場合は、**gprs charging service-mode** コマンドを使用して課金機能をメンテナンス モードにし、**clear gprs charging cdr all no-transfer** コマンドを発行して CDR を手動でクリアします。課金機能をメンテナンス モードにする方法の詳細については、「課金メンテナンス モードの設定」（P.3-30）を参照してください。

2. GGSN をサービスから削除します。

```
Router(config)# no service gprs ggsn
```

GGSN のグローバルなサービス モード状態を設定するには、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)# gprs service-mode [operational | maintenance]`	グローバルなサービス モード状態を設定します。デフォルトは運用モードです。

（注）　GGSN がグローバル メンテナンス モードの場合、すべての APN もメンテナンス モードになります。

APN メンテナンス モードの設定

GGSN の他の APN のセッションに影響を与えずに新しい APN の追加または既存の APN の変更を行えるように、APN のサービス モード状態を設定できます。

APN がメンテナンス モードの場合、PDP コンテキストの作成要求は受け入れられません。アクティブな PDP コンテキストが解放されると（または **clear gprs gtp pdp-context access-point** コマンドを使用して手動でクリアされると）、APN 関連のすべてのパラメータは設定または変更可能になり、APN は運用モードに設定されます。

また、APN を追加および設定すると、グローバル コンフィギュレーション モードで **gprs service-mode test imsi** コマンドを使用してテスト ユーザを（GGSN ごとに 1 つ）設定し、PDP コンテキスト作成を実行して、設定を確認できます。

（注）　**gprs service-mode test imsi** コマンドを使用してテスト ユーザから PDP コンテキスト作成をテストするには、GGSN が運用モード（**gprs service-mode operational** コマンド）である必要があります。

APN を削除するには、APN サービス モード状態をメンテナンス モードに変更し、既存のすべての PDP が解放されるのを待機してから、**no access-point-name** コマンドを使用して APN を削除します。

APN のサービス モード状態を設定するには、アクセス ポイント 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-access-point)# service-mode [operational | maintenance]`	APN のサービス モード状態を設定します。

次の項では、APN メンテナンス モードの使用方法の例を示します。

新しい APN の追加

1. 新しい APN を追加し、メンテナンス モードにします（デフォルトでは、APN は運用モードです）。

```
Router(config-access-point)# access-point-name apn-num
Router(config-access-point)# service-mode maintenance
```

2. APN を設定します。
3. APN 設定のテスト用の PDP コンテキストを作成します。

```
Router(config)# gprs service-mode test imsi imsi-value
```

4. APN を運用モードにします。

```
Router(config-access-point)# service-mode operational
```

APN の変更

1. APN をメンテナンス モードにします。

```
Router(config-access-point)# service-mode maintenance
```

PDP コンテキストが解放されるのを待機するか、**clear gprs gtp pdp-contexts access-point** コマンドを使用して手動でクリアします。

2. APN を変更します。
3. APN 設定のテスト用の PDP コンテキストを作成します。

```
Router(config)# gprs service-mode test imsi imsi-value
```

4. APN を運用モードにします。

```
Router(config-access-point)# service-mode operational
```

APN の削除

1. APN をメンテナンス モードにします。

```
Router(config-access-point)# service-mode maintenance
```

PDP コンテキストが解放されるのを待機するか、**clear gprs gtp pdp-contexts access-point** コマンドを使用して手動でクリアします。

2. APN を削除します。

```
Router(config-access-point)# no access-point-name apn-num
```

課金メンテナンス モードの設定

GGSN の課金機能は主に、呼詳細レコード（CDR）の収集と課金ゲートウェイへの CDR の送信で構成されます。GGSN 課金機能のサービス モード状態は、CDR の収集には影響しません。ただし、課金機能がメンテナンス サービス モード状態になると、CDR は課金ゲートウェイに送信されません。

課金機能がメンテナンス モードの場合、課金ゲートウェイを追加、削除、または変更できます（たとえば、課金ゲートウェイの IP アドレス、優先度、および番号を変更します）。課金機能がメンテナンス モードのときに新しいプライマリ課金ゲートウェイが設定された場合、GGSN の課金機能が運用モードに戻されると、累積されたすべての CDR は新しい課金ゲートウェイに送信されます。

メンテナンス モード中は、収集されたすべての CDR および保留キューの CDR は GGSN 上に格納されます。必要に応じて、**clear gprs charging cdr all no-transfer** コマンドを使用して、これらの格納された CDR をクリアできます。クリアされると、課金機能が運用モードに戻されたときに、課金ゲートウェイに送信されません。

次の課金機能コンフィギュレーション コマンドでは、課金機能はメンテナンス モードである必要があります。

- **gprs charging path-protocol**
- **gprs charging header short**
- **gprs charging map data tos**
- **gprs charging message transfer-request command-ie**
- **gprs charging message transfer-response number-responded**
- **gprs charging port**
- **gprs default charging-gateway**
- **gprs charging send-buffer**

デフォルトでは、課金機能は運用モードです。課金機能のサービス モード状態を設定するには、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)# **gprs charging service-mode** [**operational** | **maintenance**]	GGSN の課金機能のサービス モード状態を設定します。

次の項では、課金メンテナンス モードの使用方法の例を示します。

課金ゲートウェイの変更

1. GGSN 課金機能をメンテナンス モードにします。

   ```
   Router(config)# gprs charging service-mode maintenance
   ```

   CDR は収集されますが、送信されません。収集されバッファリングされたすべての CDR は、課金機能が運用モードに戻されるまで格納されます。運用モードになったときに、課金ゲートウェイに送信されます。

2. 課金設定（ゲートウェイ数、パス プロトコル、順序など）を変更します。
3. 必要に応じて、格納された CDR および保留中の CDR をすべてクリアして、課金機能が運用モードに戻されたときに課金ゲートウェイに送信されないようにします。

   ```
   Router(config)# clear gprs charging cdr all no-transfer
   ```

4. 課金機能を運用モードに戻します。

   ```
   Router(config)# gprs charging service-mode operational
   ```

GGSN に格納された CDR および保留キューの CDR を手動ですべてクリアするには、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)# **clear gprs charging cdr all no-transfer**	課金機能がメンテナンス モードのときに、格納された CDR および保留キューの CDR をクリアします。

（注）　CDR をクリアするには、GGSN はグローバル メンテナンス モード（**gprs service-mode maintenance** コマンドを使用）および課金メンテナンス モード（**gprs charging service-mode maintenance** コマンドを使用）である必要があります。

（注）　GGSN が課金メンテナンス モードおよびグローバル メンテナンス モードの場合、GGSN は既存の PDP に対して CDR を作成しません。

GGSN での GTP のモニタリングおよびメンテナンス

ここでは、GGSN で GTP をモニタリングするために使用できる **show** コマンドの要約を示します。

次の特権 EXEC コマンドを使用して GGSN で GTP のモニタリングおよびメンテナンスを行います。

コマンド	目的
Router# **show gprs access-point**	GGSN のアクセス ポイントに関する情報を表示します。
Router# **show gprs access-point statistics**	GGSN のアクセス ポイントのデータ量と PDP アクティベーションおよび非アクティベーション統計情報を表示します。
Router# **show gprs gtp ms** {**imsi** *imsi* | **access-point** *access-point-index* | **all**}	GGSN で現在アクティブなモバイル ステーション（MS）のリストを表示します。

コマンド	目的
Router# **show gprs gtp parameters**	GGSN での現在の GTP 設定に関する情報を表示します。
Router# **show gprs gtp path** {**remote-address** *ip-address* [*remote-port-num*] | **version** *gtp-version* | **all**}	GGSN と他の GPRS/UMTS デバイス間の 1 つ以上の GTP パスに関する情報を表示します。
Router# **show gprs gtp path statistics history** *number*	履歴に格納されている GTP パス エントリの統計情報を表示します。
Router# **show gprs gtp path statistics remote-address** *ip-address* [**remote-port** *port-num*]	特定のパスの統計情報を表示します。
Router# **show gprs gtp pdp-context** {**tid** *tunnel_id* [**service** [**all** | **id** *id_string*]] | **ms-address** *ip_address* [**access-point** *access-point-index*] | **imsi** *imsi* [**nsapi** *nsapi* [**tft**]] | **path** *ip-address* [*remote-port-num*] | **access-point** *access-point-index* | **pdp-type** {**ip** | **ppp**} | **qos-umts-class** {**background** | **conversational** | **interactive** | **streaming**} | **qos-precedence** {**low** | **normal** | **high**} | **qos-delay** {**class1** | **class2** | **class3** | **classbesteffort**} | **version** *gtp-version*} | **msisdn** [*msisdn*] | **ms-ipv6-addr** *ipv6-address* | **all**}	現在アクティブな PDP コンテキストの一覧を表示します。 （注）　**show gprs gtp pdp-context** コマンドのオプションは、GGSN でイネーブルになっている QoS 方式のタイプによって異なります。
Router# **show gprs gtp statistics**	GGSN の現在の GTP 統計情報を表示します（情報エレメント（IE）、GTP シグナリング、GTP PDU 統計情報など）。
Router# **show gprs gtp status**	GGSN での GTP の現在のステータスに関する情報を表示します。
Router# **show gprs service-mode**	GGSN の現在のサービス モードおよびサービス モードが最後に変更された時刻を表示します。

設定例

ここには次の例があります。

- 「GGSN の設定例」（P.3-32）
- 「ダイナミック エコー タイマーの設定例」（P.3-34）

GGSN の設定例

次の例は、基本的な GGSN GTP サービスを設定するために使用するコマンドのいくつかを含む GGSN 設定例の一部を示しています。

```
Router# show running-config

Current configuration : 3521 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enables GGSN services
!
service gprs ggsn
!
ip cef
```

```
!
! Configures a loopback interface
!
interface loopback 1
 ip address 10.40.40.3 255.255.255.0
!
! Defines the virtual-template interface
! with GTP encapsulation
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
. . .
!
gprs access-point-list gprs
!
  access-point 1
   access-point-name gprs.cisco.com
   exit
!
  access-point 2
   access-point-name gprt.cisco.com
   exit
   !
  access-point 3
   access-point-name gpru.cisco.com
   access-mode non-transparent
   aaa-group authentication abc
   exit
!
! Configures GTP parameters
!
gprs maximum-pdp-context-allowed 90000
gprs gtp path-echo-interval 0
gprs default charging-gateway 10.15.15.1
!
! Enables the memory protection feature to become active if the memory threshold falls
! below 50 MB
!
gprs memory threshold 512
!
. . .

. . .
!
end
```

ダイナミック エコー タイマーの設定例

次の例は、ダイナミック エコー タイマーの GGSN 設定例の一部を示しています。この例では、ダイナミック エコー タイマーはイネーブルであり、スムーズ係数はデフォルト値の 2 から 5 に変更されており、dynamic minimum 値はデフォルト値の 5 秒から 10 秒に変更されています。

```
Router# show running-config

Current configuration : 6769 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service gprs ggsn
!
ip cef
!
. . .
!
interface loopback 1
 ip address 10.41.41.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
. . .
!
gprs access-point-list gprs
  access-point 1
   access-point-name gprs.cisco.com
   exit
   !
  access-point 2
   access-point-name gprt.cisco.com
   access-mode non-transparent
   aaa-group authentication test2
   aaa-group accounting test2
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.65.0.1
   dhcp-gateway-address 10.65.0.1
   exit
!
! Enables the dynamic echo timer
!
gprs gtp echo-timer dynamic enable
!
! Configures a smooth factor of 5
!
gprs gtp echo-timer dynamic smooth-factor 5
!
! Configures the dynamic minimum as 10 seconds
!
gprs gtp echo-timer dynamic minimum 10
gprs gtp response-message wait-accounting
!
end
```

CHAPTER 4

GGSN での IPv6 PDP サポートの設定

この章では、Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）で、Internet Protocol Version 6（IPv6）Packet Data Protocol（PDP; パケット データ プロトコル）コンテキストのサポートを設定する方法について説明します。

この章に記載されている GGSN コマンドの詳細については、使用している Cisco GGSN リリースの『*Cisco GGSN Command Reference*』を参照してください。

この章に記載されているその他のコマンドのマニュアルを参照するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。GGSN の設定に役立つその他の Cisco IOS ソフトウェア マニュアルのリストについては、「関連資料」（P.2-11）を参照してください。

この章は、次の内容で構成されています。

GGSN での IPv6 PDP の概要

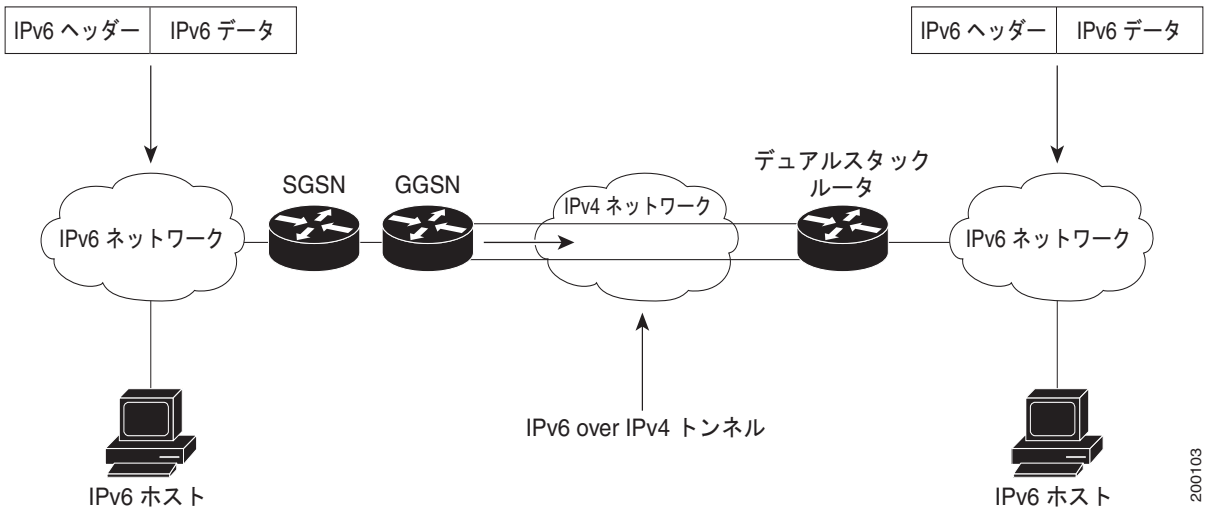
ここでは、Cisco GGSN での IPv6 PDP サポートの概要について説明します。IPv6 のアドレス形式およびアドレッシング スキームを含む、Cisco IOS ソフトウェアでの IPv6 の実装の詳細については、『*Cisco IOS IPv6 Configuration Guide*』を参照してください。

Cisco GGSN は、IPv6 プライマリ PDP コンテキスト アクティベーション、および（RFC 2461 および RFC 2462 で規定されている）IPv6 ステートレス自動設定による Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）で開始された変更および非アクティベーションの手順をサポートしています。Cisco 7600 シリーズ ルータのスーパーバイザ エンジン モジュールで設定された IPv6 over IPv4 トンネルによって、既存の IPv4 インフラストラクチャ上にある独立したリモートの IPv6 ネットワーク間の接続が確立されます。

（注） トンネルはスーパーバイザ エンジンから設定する必要があります。GGSN からのトンネリングはサポートされていません。

図 4-1 は、IPv6 over IPv4 トンネルの設定を示しています。

図 4-1　IPv6 over IPv4 トンネルの設定



IPv6 ステートレス自動設定

IPv6 ノード上のすべてのインターフェイスには、リンクローカル アドレスが必要です。リンクローカル アドレスは、通常、インターフェイスの ID およびリンクローカル プレフィクス FE80::/10 から自動的に設定されます。リンクローカル アドレスによって、ノードはリンク上の他のノードと通信できるようになります。また、リンクローカル アドレスを使用して、ノードをさらに設定できます。

ノードは、ネットワークに接続して、サイトローカルおよびグローバルの IPv6 アドレスを自動生成できます。手動での設定や、Remote Authentication Dial-In User Service（RADIUS）サーバなどのサーバによる支援は必要ありません。IPv6 では、リンク上のルータ（この例では Cisco GGSN）が、サイトローカルおよびグローバルのプレフィクスをアドバタイズし、Router Advertisement（RA; ルータ アドバタイズメント）でリンクのデフォルト ルータとして機能することをアドバタイズします。RA は定期的に送信され、システム起動時にホストによって送信される、ルータ送信要求メッセージへの応答として送信されます。

Cisco GGSN で、PDP コンテキストの作成応答によって IPv6 Mobile Station（MS; モバイル ステーション）にインターフェイス ID が割り当てられます。または、MS で、インターフェイス ID（64 ビット）を、RA に含まれるプレフィクス（64 ビット）に追加することによって、サイトローカルおよびグローバルの IPv6 アドレスを自動的に設定できます。

ノードによって設定された、結果の 128 ビット IPv6 アドレスは、リンク上での一意性を確保するために重複アドレス検出の対象となります。RA でアドバタイズされるプレフィクスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスもグローバルに一意であることが保証されます。Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）パケット ヘッダーの Type フィールドに 133 という値が指定された、ルータ送信要求メッセージは、ホストによってシステム起動時に送信されます。これにより、ホストでは次にスケジュールされた RA を待機せずに即座に自動設定を実行できます。

図 4-2 は、IPv6 ステートレス自動設定による IPv6 PDP コンテキストの作成について示しています。

図 4-2　IPv6 ステートレス自動設定を使用した Cisco GGSN での IPv6 PDP コンテキスト作成

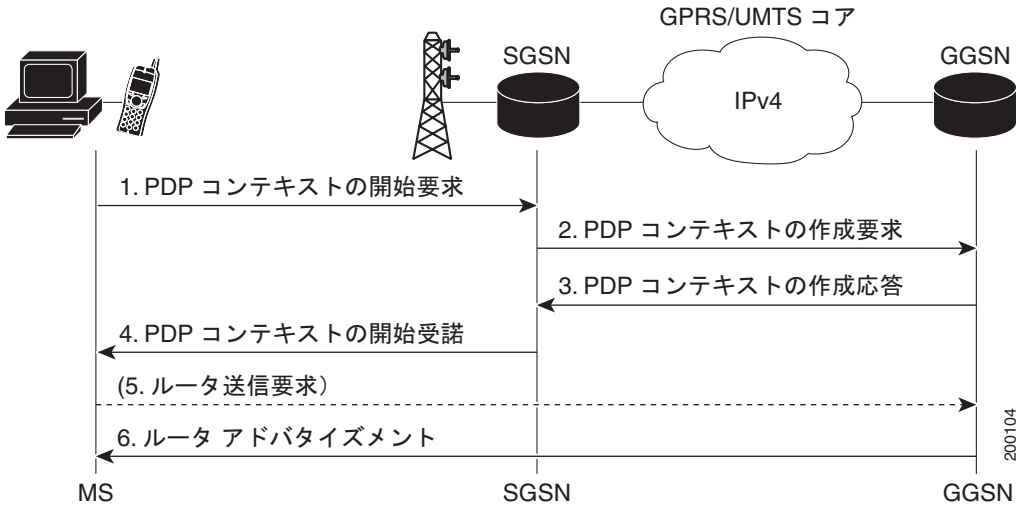


図 4-2 に示すコール フローの手順では、次のことが実行されます。

1. PDP コンテキストの開始要求：MS から SGSN に PDP コンテキストの開始要求が送信されます。
2. PDP コンテキストの作成要求：SGSN から GGSN に PDP コンテキストの作成要求が送信されます。

   SGSN から PDP コンテキストの作成要求を受信すると、GGSN では、PDP コンテキストに割り当てられたプレフィクスと GGSN によって生成されたインターフェイス ID で構成される IPv6 アドレスが生成されます。
3. PDP コンテキストの作成応答：PDP コンテキストの作成応答で GGSN から SGSN にアドレスが返されます。

   MS が GGSN へのリンク上で単独であると見なされるため、インターフェイス ID は PDP コンテキスト全体で一意である必要はありません。MS では、受信したアドレスからインターフェイス ID が抽出されて格納され、リンクローカル アドレスおよび完全な IPv6 アドレスを作成するために使用されます。
4. PDP コンテキストの開始受諾：SGSN から MS に PDP コンテキストの開始受諾が送信され、コンテキストが確立されます。
5. ルータ送信要求：MS から GGSN にルータ送信要求が送信される場合と、されない場合があります。
6. ルータ アドバタイズメント：GGSN から RA が定期的に送信されます。

   RA では、GGSN から 64 ビットのプレフィクス（ステップ 3 で提供したものと同じプレフィクス）が送信されます。MS で RA が受信されると、ステップ 3 で受信したインターフェイス ID またはローカルで生成されたインターフェイス ID と、RA で提供されたプレフィクスを連結することによって、完全な IPv6 アドレスが作成されます。RA に複数のプレフィクスが含まれる場合、MS では 1 つめのプレフィクスだけが考慮され、残りは破棄されます。

   PDP コンテキストの作成応答で GGSN によってアドバタイズされるプレフィクスはプレフィクスの範囲内で一意であるため、MS では重複アドレス検出を実行する必要がありません。このため、GGSN では、重複アドレスを検出するために MS によって送信される場合があるネイバー送信要求が破棄されることがあります。

サポートされる機能

IPv6 PDP コンテキストでは、Cisco GGSN によって次の機能がサポートされています。

- IPv6 ステートレス自動設定による IPv6 GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）v0 および GTPv1 PDP の確立。
- ローカルに設定された 64 ビットのプレフィクス プールからの IPv6 プレフィクス割り当て。
- GGSN による RA の送信、および MS からのルータ送信要求メッセージの応答。
- IPv6 G-CDR 生成。
- デュアルスタック Access Point Name（APN; アクセス ポイント ネーム）（IPv4 と IPv6 両方の PDP が同時にサポートされます）。
- IPv6 DNS アドレス割り当てに対する、APN ごとの IPv6 DNS アドレス設定（要求された場合）。
- RADIUS 認証、アカウンティング、および RADIUS サーバからの IPv6 アドレス割り当て。
- Per-APN RA タイマー。このタイマーには、RA 間隔、ライフタイム間隔、および最初の RA が送信されるまでの初期間隔が含まれます。
- IPv6 APN に対する ACL の標準サポートおよび拡張サポート。
- GPRS 固有のセキュリティ機能（アドレス検証機能およびモバイル間トラフィック リダイレクション機能）。
- QoS（マーキングおよびコール アドミッション制御）。
- IPv6 サーバに対する Proxy Call Session Control Function（Proxy-CSCF）サポート。

制約事項

GGSN で IPv6 PDP コンテキスト サポートを設定する前に、次の制限事項および制約事項に注意してください。

- IPv6 PDP コンテキストでは、次の機能はサポートされていません。
  - セカンダリ PDP コンテキスト
  - Per-PDP ポリシング
  - DHCPv6 によるステートフル アドレス自動設定
  - DHCPv6 リレーまたはプロキシ クライアント
  - ステートフル IPv6 自動設定
  - GTP Session Redundancy（GTP-SR; GTP セッション冗長性）
  - 拡張サービス認識課金
  - PPP PDP および PPP 再生成
  - VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）

    （デュアルスタック APN が設定されていて、APN で VRF がイネーブルである場合、IPv4 PDP コンテキストは VRF に移動され、IPv6 PDP コンテキストはグローバル ルーティング テーブルに留まります。）
  - ルート プローブ、モバイル背後でのルーティング、single-pdp セッション、およびプライマリとバックアップの NetBios Name Service

（注）　IPv6 PDP コンテキストに対してサポートされている APN 設定、またはサポートされていない APN 設定のリストについては、第 8 章「GGSN へのネットワーク アクセスの設定」を参照してください。

- IP CEF および IPv6 CEF をイネーブルにする必要があります（IPv6 CEF では、IP CEF がイネーブルである必要があります）。
- Public Land Mobile Network（PLMN; パブリック ランド モバイル ネットワーク）、SGSN、GGSN、および課金ゲートウェイのすべてのインフラストラクチャ ノードは、IPv4 ノードであると想定されます。
- IPv6 はスーパーバイザ エンジン モジュールで実装する必要があります。
- IPv6 over IPv4 トンネルは、スーパーバイザ エンジン モジュールから設定する必要があります。GGSN からのトンネリングはサポートされていません。
- RADIUS が PLMN のインフラストラクチャ ノードとして実装されている必要があります。
- **no virtual-template snmp** コマンドが設定されている必要があります。
- **no virtual-template subinterface** が設定されている必要があります。
- 次のコマンドは、IPv6 ベース仮想テンプレートでは設定しないでください。
  - **snmp if-index persists**
  - **ntp disable**

GGSN での IPv6 PDP サポートの実装

GGSN で IPv6 サポートを設定するには、次の項で説明する作業を実行します。

- 「GGSN での IPv6 トラフィックの転送のイネーブル」（P.4-5）（必須）
- 「IPv6 ベース仮想テンプレート インターフェイスの設定」（P.4-6）（必須）
- 「APN での IPv6 サポートのイネーブル」（P.4-8）（必須）
- 「ローカル IPv6 プレフィクス プールの設定」（P.4-10）（必須）
- 「IPv6 のモニタリングおよびメンテナンス」（P.4-13）（任意）

GGSN での IPv6 トラフィックの転送のイネーブル

GGSN で IPv6 トラフィックを転送するには、Cisco Express Forwarding（CEF）および IPv6 CEF が GGSN でグローバルにイネーブルである必要があります。また、CEF を使用して IPv6 トラフィックを転送する場合は、**ipv6 unicast-routing** コマンドを使用して、GGSN でグローバルに IPv6 ユニキャスト データグラムの転送を設定する必要もあります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **ipv6 unicast-routing**
5. **ipv6 cef**

手順の詳細

	コマンドまたは処理	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip cef** **例：** `Router# configure terminal`	IPv4 の Cisco Express Forwarding をルータ上でグローバルにイネーブルにします。
ステップ 4	**ipv6 unicast-routing** **例：** `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 5	**ipv6 cef** **例：** `Router(config)# ipv6 cef`	IPv6 の CEF をルータ上でグローバルにイネーブルにします。

IPv6 ベース仮想テンプレート インターフェイスの設定

GGSN で確立された IPv6 PDP コンテキストごとに、仮想アクセス サブインターフェイスが作成されます。RA タイマーなどの仮想アクセスの設定は、APN に割り当てられる IPv6 ベース仮想テンプレート インターフェイスからクローンされます。IPv6 ベース仮想テンプレートで設定されるコマンドでは、IPv6 プロトコルの動作が定義されます。

それぞれ設定の異なる複数のベース仮想テンプレートを設定できます。ベース仮想テンプレートは複数の APN で共有できます。ただし、（**ipv6 base-vtemplate** コマンドを使用して）APN に割り当てることができるベース仮想テンプレートは一度に 1 つだけです。

PDP コンテキストの作成要求が受信されると、APN に割り当てられたベース仮想テンプレートから仮想サブインターフェイスがクローンされ、IPv6 アドレスが IPv6 仮想アクセス サブインターフェイスの作成後に APN での設定に従って割り当てられます。仮想アクセス サブインターフェイスが作成されたあとに PDP コンテキストの作成応答が返され、認証およびアドレス割り当てが正常に完了します。

注意　重大なパフォーマンス上の問題を回避するために、IPv6 ベース仮想テンプレート インターフェイスで、**no ipv6 nd ra suppress** コマンドが*設定されていて*、**no-virtual-template subinterface** コマンドが*設定されていない*ことを確認してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number*
4. **ipv6 enable**
5. **no ipv6 nd ra suppress**
6. **ipv6 nd ra interval** {*maximum-secs* [*minimum-secs*] | *msec maximum-msecs* [*minimum-msecs*]}
7. **ipv6 nd ra lifetime** *seconds*
8. **ipv6 nd ra initial** [**exponential**] *InitialAdvertInterval InitialAdvertisements*
9. **ipv6 nd prefix default** *infinite infinite* **off-link**
10. **exit**

手順の詳細

	コマンドまたは処理	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface virtual-template** *number* **例：** `Router(config)# interface virtual-template number`	仮想テンプレート インターフェイスを作成します。number によって、仮想テンプレート インターフェイスが識別されます。
ステップ 4	**ipv6 enable** **例：** `Router(config-if)# ipv6 enable`	明示的な IPv6 アドレスで設定されていないインターフェイスでの IPv6 処理をイネーブルにします。 **（注）** このコマンドを実行すると、インターフェイスで IPv6 リンクローカル ユニキャスト アドレスが自動的に設定され、IPv6 処理のインターフェイスもイネーブルになります。
ステップ 5	**no ipv6 nd ra suppress** **例：** `Router(config-if)# no ipv6 nd ra suppress`	非 LAN インターフェイス タイプ（シリアル インターフェイスやトンネル インターフェイスなど）での IPv6 ルータ アドバタイズメント伝送の送信をイネーブルにします。
ステップ 6	**ipv6 nd ra interval** {*maximum-secs* [*minimum-secs*] | *msec maximum-msecs* [*minimum-msecs*]} **例：** `Router(config-if)# ipv6 nd ra interval 21600`	インターフェイスでの IPv6 RA 伝送の間隔を設定します。
ステップ 7	**ipv6 nd ra lifetime** *seconds* **例：** `Router(config-if)# ipv6 nd ra lifetime 21600`	インターフェイスでの IPv6 ルータ アドバタイズメントの、ルータのライフタイム値を秒単位で設定します。

	コマンドまたは処理	目的
ステップ 8	**ipv6 nd ra initial** [**exponential**] *InitialAdvertInterval InitialAdvertisements* **例：** `Router(config-if)# ipv6 nd ra initial 3 3`	IPv6 ルータ アドバタイズメント伝送間の間隔（秒）、および初期フェーズ中にインターフェイスで送信される RA の数を設定します。 任意で、指数キーワード オプションを指定して、*InitialAdvertInterval* に指定される値が初期タイマー値として使用され、後続の伝送ごとに倍増されるように設定します。
ステップ 9	**ipv6 nd prefix default infinite infinite off-link** **例：** `Router(config-if)# ipv6 nd prefix default infinite infinted off-link` **ipv6 nd prefix** {*ipv6-prefix/prefix-length* | **default**} [**no-advertise** | [*valid-lifetime preferred-lifetime* [**off-link** | **no-rtr-address** | **no-autoconfig**]] | [**at valid-date** | *preferred-date* [**off-link** | **no-rtr-address** | **no-autoconfig**]]	IPv6 ルータ アドバタイズメントに含める IPv6 プレフィクスを設定します。
ステップ 10	**exit** **例：** `Router(config-if)# exit`	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。

APN での IPv6 サポートのイネーブル

APN で設定されたコマンドでは、その APN で処理される IPv6 PDP コンテキストの動作（使用する IPv6 アドレス割り当ての方法など）が定義されます。また、GTP IPv6 要素（プライマリおよびバックアップ DNS の IPv6 アドレスなど）も定義されます。

IPv6 PDP コンテキストでサポートされている APN 設定オプションのリストについては、第 8 章「GGSN へのネットワーク アクセスの設定」を参照してください。

APN で IPv6 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。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-point** *access-point-index*
4. **access-point-name** *apn-name*
5. **ipv6 dns primary** *ipv6-address* [**secondary** *ipv6-address*]
6. **ipv6** [**enable** | **exclusive**]
7. **ipv6 ipv6-address-pool** {**local** *pool-name* | **radius-client**}
8. **ipv6 ipv6-access-group** *ACL-name* [**up** | **down**]
9. **ipv6 base-vtemplate** *number*
10. **exit**

手順の詳細

	コマンドまたは処理	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-point** *access-point-index* **例：** `Router(config)# access-point 2`	アクセス ポイント番号を指定し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 4	**access-point-name** *apn-name* **例：** `Router(config-access-point)# access-point-name ipv6_apn1.com`	定義されたアクセス ポイントでユーザが GGSN からアクセスできる PDN のネットワーク（またはドメイン）名を指定します。
ステップ 5	**ipv6** [**enable** | **exclusive**] **例：** `Router(config-access-point) ipv6 enable`	アクセス ポイントで IPv6 PDP コンテキストを許可するように設定します。 • enable：APN で IPv4 と IPv6 両方の PDP コンテキストのサポートを設定します。 • exclusive：APN で IPv6 PDP コンテキストだけのサポートを設定します。 デフォルトでは、IPv4 PDP コンテキストだけが APN でサポートされています。
ステップ 6	**ipv6 dns primary** *ipv6-address* [**secondary** *ipv6-address*] **例：** `Router(config-access-point) ipv6 dns primary 2001:999::9`	プライマリ（およびバックアップ）IPv6 DNS のアドレスが、要求された場合に IPv6 PDP コンテキストの作成応答で送信されるように指定します。
ステップ 7	**ipv6 ipv6-address-pool** {**local** pool-name | **radius-client**} **例：** `Router(config-access-point) ipv6 ipv6-address-pool local localv6`	アクセス ポイントのダイナミック IPv6 プレフィクス割り当て方法を設定します。 **（注）** Cisco GGSN の今回のリリースでは、ローカルに設定されたプールによる IPv6 プレフィクス割り当てがサポートされています。
ステップ 8	**ipv6 ipv6-access-group** *ACL-name* [**up** | **down**] **例：** `Router(config-access-point) ipv6 ipv6-access-group ipv6filter down`	Access Control List（ACL; アクセス コントロール リスト）設定をアップリンクまたはダウンリンクのペイロード パケットに適用します。

	コマンドまたは処理	目的
ステップ 9	**ipv6 base-vtemplate** *number* **例：** `Router(config-access-point) ipv6 base-vtemplate 10`	IPv6 PDP コンテキストの仮想サブインターフェイスの作成時に、APN での IPv6 RA パラメータのコピー元となるベース仮想テンプレート インターフェイスを指定します。
ステップ 10	**exit** **例：** `Router(config-access-point)# exit`	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。

ローカル IPv6 プレフィクス プールの設定

IPv6 のプレフィクス プール機能は、IPv4 のアドレス プール機能に類似しています。主な違いは、IPv6 では単一アドレスではなくプレフィクスが割り当てられることです。

IPv4 の場合、IP アドレスは、ローカルに設定されたプールから取得するか、または AAA サーバから取得できます。Cisco GGSN では、ローカル プールによるプレフィクス割り当てがサポートされています。

ローカル IPv6 プレフィクス プールの設定時に、プール間で重複するメンバシップは許可されません。プールを設定すると、設定の変更はできません。プールの設定を変更すると、プールは削除されて再作成され、以前に割り当てられたすべてプレフィクスが解放されます。

次のコマンドを使用してローカル IPv6 プレフィクス プールを設定する方法の詳細については、『*Cisco IOS IPv6 Configuration Guide*』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 local pool** *poolname prefix/prefix-length assigned-length* [**shared**] [**cache-size** *size*]
4. **exit**

手順の詳細

	コマンドまたは処理	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたは処理	目的

ステップ 3	**ipv6 local pool** *poolname prefix/prefix-length assigned-length* [**shared**] [**cache-size** *size*]
	
	例：
	`Router(config)# ipv6 local pool pool1 2001:0DB8::/48 64`
	
	`Router# show ipv6 local pool`
	
	`Pool Prefix Free In use`
	
	`pool1 2001:0DB8::/48 65516 20`
		ローカル IPv6 プレフィクス プールを設定します。
		（注） 割り当てられた長さとして値 64 を設定する必要があります。GGSN で受け入れられるプレフィクスの最小の長さは /48 です。

ステップ 4	**exit** **例：** `Router(config)# exit`	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。

IPv6 アクセス コントロール リストの設定

IPv6 アクセス コントロール リストでは、設定済みの IPv6 フィルタに基づいて IPv6 関連のトラフィックが制限されます。フィルタには、IP パケットを照合するルールが含まれています。一致したパケットを許可するか、拒否するかについても、このルールに規定されています。

ipv6 ipv6-access-group アクセス ポイント コンフィギュレーション コマンドを使用すると、IPv6 アクセス制御フィルタが APN に適用されます。

次のコマンドを使用して IPv6 アクセス コントロール リストを設定する方法の詳細については、『*Cisco IOS IPv6 Configuration Guide*』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **deny** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [**operator** [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input]** [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number]* [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**]
5. **permit** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address}* [**operator** [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | *host destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | **mh-type**]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
6. **exit**

手順の詳細

	コマンドまたは処理	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 access-list** *access-list-name* **例：** `Router(config)# ipv6 access-list ipv6filter`	IPv6 アクセス リスト名を定義し、GGSN を IPv6 アクセス リスト コンフィギュレーション モードにします。
ステップ 4	**deny** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [**operator** [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**] **例：** `Router(config-ipv6-acl)# deny ipv6 any 2001:200::/64`	IPv6 アクセス リストの拒否条件を設定します。
ステップ 5	**permit** *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address}* [**operator** [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | *host destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | **mh-type**]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] **例：** `Router(config-ipv6-acl)# permit ipv6 any any`	IPv6 アクセス リストの許可条件を設定します。
ステップ 6	**exit** **例：** `Router(config)# exit`	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。

その他の IPv6 サポート オプションの設定

ここでは、アクセス ポイントで設定できる IPv6 固有のその他のオプションについて簡単に説明します。

これらのオプションの設定方法の詳細については、このマニュアルの他の章を参照してください。これらのオプションは IPv6 PDP コンテキストにだけ適用されます。すべての APN IPv6 コンフィギュレーション オプションの要約については、第 8 章「GGSN へのネットワーク アクセスの設定」を参照してください。

GGSN アクセス ポイントの IPv6 固有のその他のオプションを設定するには、アクセス ポイント 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
ステップ 1	`Router(config-access-point)# ipv6 ipv6-access-group` *ACL-name* `[up | down]`	（任意）アクセス コントロール リスト（ACL）設定をアップリンクまたはダウンリンクのペイロード パケットに適用します。
ステップ 2	`Router(config-access-point)# ipv6 redirect [all | intermobile]` *ipv6-address*	（任意）GGSN で IPv6 トラフィックを外部 IPv6 デバイスにリダイレクトするように設定します。使用できるオプションは次のとおりです。 • **all**：すべての IPv6 トラフィックを APN の外部の IPv6 デバイスにリダイレクトします。 • **intermobile**：モバイル間 IPv6 トラフィックを外部の IPv6 デバイスにリダイレクトします。 • *ipv6-address*：IPv6 トラフィックのリダイレクト先となる IPv6 外部デバイスの IP アドレス。
ステップ 3	`Router(config-access-point)# ipv6 security verify source`	（任意）GGSN で、アップストリーム Transport Protocol Data Unit（TPDU; 転送プロトコル データ ユニット）の IPv6 送信元アドレスを、以前に MS に割り当てられたアドレスと照合して検証できるようにします。

IPv6 のモニタリングおよびメンテナンス

次の特権 EXEC **show** コマンドを使用して、GGSN での IPv6 設定および IPv6 PDP をモニタリングできます。

コマンド	目的
`Router# show gprs access-point`	GGSN のアクセス ポイントに関する情報を表示します。
`Router# show gprs access-point statistics`	GGSN のアクセス ポイントのデータ量および PDP アクティベーションと非アクティベーションの統計を表示します。
`Router# show gprs access-point status`	アクセス ポイントのアクティブな PDP の数、およびそのうちの IPv4 PDP の数と IPv6 PDP の数を表示します。
`Router# show gprs gtp pdp-context`	現在アクティブな PDP コンテキストの一覧を表示します。

コマンド	目的
Router# s**how gprs gtp status**	GGSN 上の GTP の現在のステータスに関する情報を表示します。
Router# **show gprs pcscf**	GGSN で P-CSCF 検出用に設定された P-CSCF サーバ グループの一覧を表示します。

設定例

次の例は、GGSN で設定された IPv6 サポートを示しています。IPv6 関連のコンフィギュレーション ステートメントは太字で示されています。

```
ip cef
!
ipv6 unicast-routing
ipv6 cef
!
interface Virtual-Template10
  ipv6 enable
  no ipv6 nd ra suppress
  ipv6 nd ra interval 21600
  ipv6 nd ra lifetime 21600
  ipv6 nd ra initial 3 3
  ipv6 nd prefix default infinite infinite off-link
!
access-point 2
 access-point-name ipv6_test.com
  ipv6 dns primary 2001:999::9
  ipv6 enable
  ipv6 ipv6-address-pool local localv6
  ipv6 base-vtemplate 10
!
ipv6 local pool localv6 2001:234::/48 64
!
!
```

CHAPTER 5

ゲートウェイ GPRS サポート ノード（GGSN）の GPRS トンネリング プロトコル（GTP）セッション冗長性の設定

この章では、2 つの Cisco Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）間に GPRS Tunneling Protocol Session Redundancy（GTP-SR; GPRS トンネリング プロトコル セッション冗長性）を設定する方法について説明します。

（注） Cisco GGSN では、IPv4 Packet Data Protocol（PDP; パケット データ プロトコル）コンテキストの場合にだけ GTP-SR がサポートされています。

この章に記載されている GGSN コマンドの詳細については、『*Cisco GGSN Command Reference*』を参照してください。

この章に記載されているその他のコマンドのマニュアルを参照するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。GGSN の設定時に役立つその他の Cisco IOS ソフトウェア マニュアルのリストについては、「関連資料」（P.2-11）を参照してください。

この章は、次の内容で構成されています。

GTP-SR の概要

Cisco GGSN でサポートされている GTP-SR を使用すると、別々の Cisco Service and Application Module for IP（SAMI）モジュールに設定されている 2 つの GGSN を 1 つのネットワーク エンティティとして示すことができます。冗長設定の一方の GGSN で障害が発生した場合でも、GTP-SR によって、モバイル加入者に引き続きサービスが提供されます。

GTP-SR 設定では、アクティブ GGSN が PDP セッションを確立および終了して、必要なステートフル データをスタンバイ GGSN に送信します。アクティブな PDP セッションの現在の状態を保持しておくために、スタンバイ GGSN はアクティブ GGSN によって送信されたステートフル データを受信します。スタンバイ GGSN は、アクティブ GGSN で障害が発生したことを検出するとアクティブになり、アクティブ GGSN の責務を引き継ぎます。

Cisco GGSN ソフトウェアでは、Cisco IOS Hot Standby Routing Protocol（HSRP; ホットスタンバイ ルーティング プロトコル）、Cisco IOS Check-point Facility（CF）と Redundancy Framework（RF）、および Stream Control Transmission Protocol（SCTP）を使用して、Layer 2（L2; レイヤ 2）のローカル GTP-SR および Layer 3（L3; レイヤ 3）の地理的 GTP-SR（リモート冗長性）の実装をサポートしています。

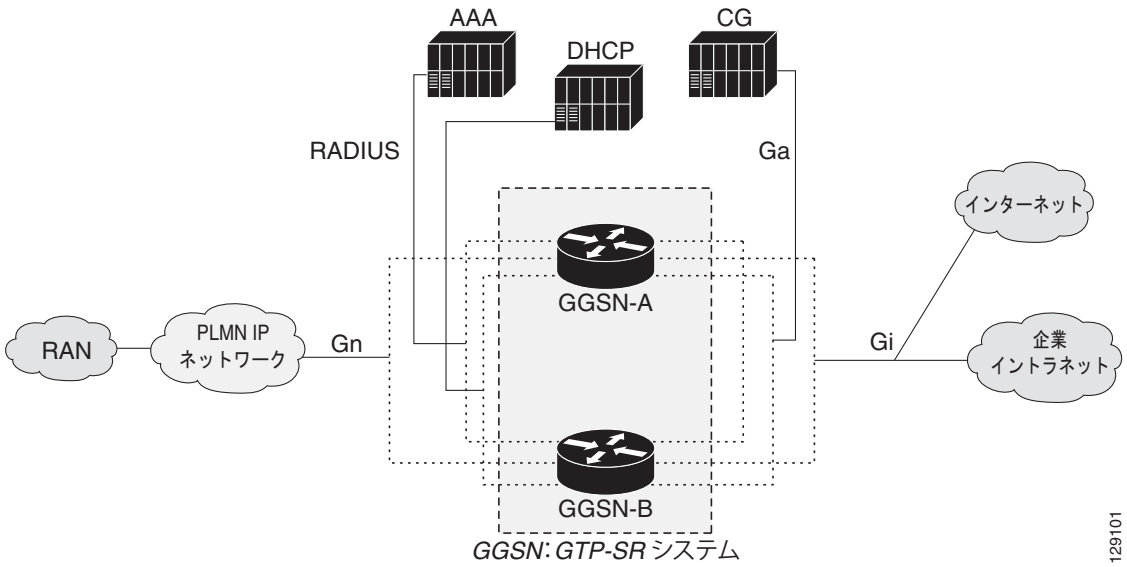
（注） 冗長 GGSN で GTP-SR をイネーブルにするには、GGSN 間に GTP-SR デバイス間インフラストラクチャを設定する必要があります。GTP-SR デバイス間インフラストラクチャの設定の詳細については、「GTP セッション冗長性デバイス間インフラストラクチャの設定」（P.5-7）を参照してください。

GTP-SR の設定例（図 5-1 および図 5-2）では、次の点に注意してください。

- GTP-SR は、アクティブ/スタンバイ動作モード、ステートフル セッション同期、およびスイッチオーバー イベント検出とリカバリで構成されています。
- アクティブ/スタンバイ動作
  - GGSN は設定に基づいてアクティブまたはスタンバイになります。
  - 地理的冗長性を実装した場合、アクティブ GGSN はルート アドバタイズメントに基づいてルーティング プロトコル経由でパケットを受信します。ローカル冗長性を実装した場合、アクティブ GGSN は MAC アドレス挿入に基づいてパケットを受信します。
  - アクティブ GGSN はコントロール メッセージを処理して加入者のデータ トラフィックをトンネリングします。
  - スタンバイ GGSN はセッション状態および転送エントリを保持して、データ損失を最小限に抑えます。
- ステートフル セッション同期
  - スイッチオーバーに対してセッション永続性が維持されます。
  - 1 対 1 のステートフル セッション同期がサポートされています。
  - アクティブ GGSN はすべてのセッションをスタンバイ GGSN にダウンロードします。
  - ネットワーク帯域幅を最大限に利用するために、変更された状態およびバンドル イベントだけがメッセージで送信されます。
  - 同期には信頼性の高いトランスポートが使用されます。

図 5-1 に、ローカル GTP-SR の実装を示します。

図 5-1　ローカル GTP-SR の実装

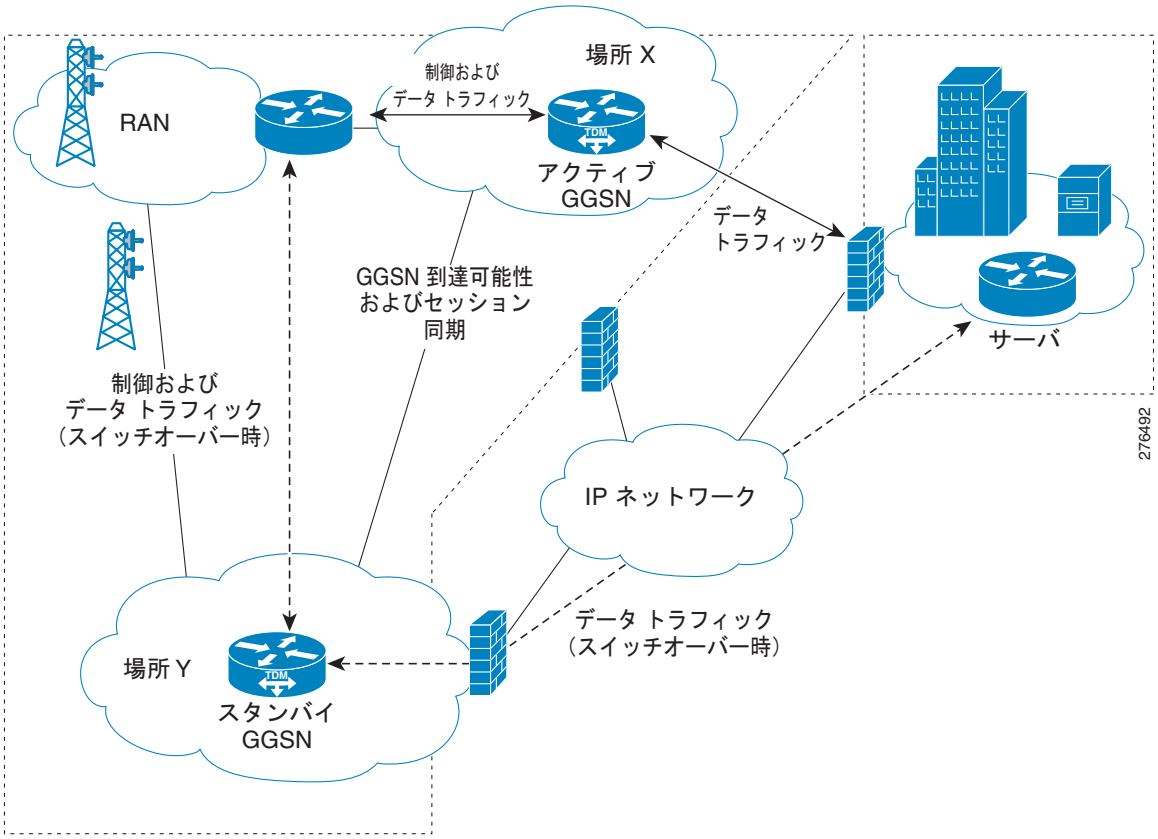


ローカル GTP-SR の注意事項

- L2 HSRP によって、ローカル GTP-SR のサポートが提供されています。
- アクティブ GGSN およびスタンバイ GGSN は同じローカル サイト（同じ LAN）に配置されています。
- アクティブ GGSN およびスタンバイ GGSN は同じローカル HSRP グループに参加するように設定されています。
- HSRP トランスポートは L2 ベースのマルチキャスティングです。

図 5-2 に、地理的 GTP-SR の実装を示します。

図 5-2　地理的 GTP-SR の実装



地理的 GTP-SR の注意事項

- L3 HSRP によって、地理的 GTP-SR のサポートが提供されています。
- アクティブ GGSN およびスタンバイ GGSN は、地理的に離れた場所に配置され、WAN で接続されています。
- アクティブ GGSN およびスタンバイ GGSN は同じ地理的 HSRP グループに参加するように設定されています。
- HSRP トランスポートは IP ユニキャスト ルーティングです。この場合、2 つの場所の間でユニキャスト IP アドレスをルーティングできる必要があります。
- L2 HSRP と L3 HSRP は相互排他的であるため、L3 HSRP がイネーブルの場合、L2 HSRP は自動的にディセーブルになります。
- Open Shortest Path First（OSPF）を Interior Gateway Protocol（IGP）として使用してルートをアドバタイズする必要があるのは、アクティブ GGSN だけです。したがって、スタンバイ GGSN として機能するときには OSPF 隣接関係を形成しないように、GGSN インターフェイスを設定する必要があります。

前提条件

Cisco GGSN の GTP-SR の要件は、次のとおりです。

- マルチレイヤ スイッチ フィーチャ カードを搭載した Cisco Supervisor Engine 720（Sup720）および Route Switch Processor（RSP）（シスコ製品 ID：SUP720-MSFC3-BXL）が搭載されている 2 台の Cisco 7600 シリーズ ルータ。

  ローカル冗長性の場合、Sup720 で Cisco IOS リリース 12.2(33)SRB1 以降が稼動している必要があります。地理的冗長性の場合、Sup720 で Cisco IOS リリース 12.2(33)SRC 以降が稼動している必要があります。

- Cisco 7600 シリーズ ルータのそれぞれに 2 つの Cisco SAMI。Cisco SAMI プロセッサで同じ Cisco GGSN リリース、つまり、ローカル冗長性の場合は Cisco IOS リリース 12.4(15)XQ 以降、地理的冗長性の場合は Cisco IOS リリース 12.4(22)YE1 が稼動している必要があります。
- HSRP バージョン 2。
- HSRP 対応インターフェイスの IP アドレスや SCTP 設定のリモート IP アドレスなど、区別が必要な特定のプロトコル関連設定を除いて、アクティブ GGSN とスタンバイ GGSN は同じ設定にする必要があります。各設定は、GTP-SR 設定の両方の GGSN に同じ順序で指定されている必要があります。
- 新しい Cisco GGSN イメージをロードまたはアップグレードする場合は、両方の GGSN を（実質的に）同時にロードする必要があります。
- Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）では、GTP N3 要求および T3 再送信の数に、スイッチオーバー タイマーの値よりも大きい値が設定されている必要があります。この設定により、スイッチオーバー時に送信された要求を廃棄せずに、新しいアクティブ GGSN でサービスできます。
- グローバル コンフィギュレーション モードで **ip radius source-interface** コマンドを使用して、指定されているインターフェイスの IP アドレスを、発信するすべての Remote Authentication Dial-In User Service（RADIUS）パケットに使用するように RADIUS が設定されている必要があります。

制限事項および制約事項

GTP-SR を設定する前に、次の制限事項および制約事項に注意してください。

- PDP コンテキスト：次のタイプの PDP コンテキストでは、冗長性はサポートされていません。スイッチオーバーと同時に、次の PDP コンテキストは、新しいアクティブ GGSN で再確立する必要があります。
  - IPv6 PDP
  - Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）タイプの PDP
  - PPP 再生成 /Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）アクセスの PDP
  - ネットワークにより開始された PDP
- タイマー：セッション タイマーを除いて、GGSN タイマーはスタンバイ GGSN と同期されません。スイッチオーバーが発生すると、新しいアクティブ GGSN のタイマーが増加的に再開されます。増加的にタイマーを再開することにより、タイマーが同時にタイムアウトしないようにします。

  PDP コンテキストがスタンバイ GGSN で再作成されると、セッション タイマーは最初のセッション タイマーの値から経過時間を引いた時間で再開されます。スタンバイ GGSN でセッションがタイムアウトになると、PDP コンテキストは削除されます。

- カウンタ：スイッチオーバーが発生すると、「cgprsAccPtSuccMsActivatedPdps」などのステータス カウンタおよび一部の統計情報カウンタはゼロ以外の値になります。この値は、スイッチオーバーが発生したときのカウンタの値です。その他のカウンタはすべてゼロにリセットされます。

  GGSN リロードが発生すると、すべてのカウンタがゼロに戻ります。
- GTP シグナリングおよびデータに関連するシーケンス番号は、アクティブ GGSN とスタンバイ GGSN の間で同期化されません。
- 課金：スタンバイ GGSN での PDP コンテキストの課金の確立に関連するすべての情報が同期化されます。ただし、PDP コンテキストのユーザ データ関連の課金情報は同期化されません。したがって、課金ゲートウェイに送信されていない以前のアクティブ GGSN の Call Detail Record（CDR; 呼詳細レコード）は、スイッチオーバーが発生するとすべて失われます。
- GTP-SR 設定が 2 つの GGSN 間で確立されると、片方の GGSN の設定変更によって、変更が保存される前に GGSN がリロードされる可能性があります。設定変更が失われないようにするには、GGSN の設定を変更する前に GTP-SR をディセーブルにします。GTP-SR をディセーブルにする方法の詳細については、「GTP セッション冗長性のディセーブル」（P.5-15）を参照してください。
- GTP セッション冗長性（GTP-SR）環境では、スタンバイ GGSN で **clear gprs gtp pdp-context** コマンドを*使用しないでください*。このコマンドをスタンバイ GGSN で発行すると、コマンドが処理される前に確認を要求するプロンプトが表示されます。GGSN の冗長ステートがアクティブかスタンバイかを判断するには、**show gprs redundancy** コマンドを使用します。
- 地理的冗長性の設定時には、次の点に注意してください。
  - L2 HSRP と L3 HSRP は相互排他的です。
  - L2 HSRP 設定から L3 HSRP 設定に移行するには、システム リロードが必要です。
  - L3 HSRP を使用している場合、Cisco GGSN がスイッチオーバーしても Cisco Content Services Gateway - 2nd Generation はスイッチオーバーしません。したがって、ユーザは過剰請求される可能性があります。
  - Cisco IOS リリース 12.2(33)SRC の 1 シャーシ当たりの制限は、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ピアが 1000 個、または OSPF ネイバーが 1000 個です。したがって、Cisco SAMI PPC の 1 GGSN 当たりの制限は 160 個の BGP ピアまたは 160 個の OSPF ネイバーになります。
  - 発信元のインターフェイス（RADIUS、課金、Diameter など）は、アクティブ GGSN とスタンバイ GGSN の両方で同じ IP アドレスを使用して設定され、OSPF ルーティング プロトコル経由で配信される必要があります。

GTP セッション冗長性のイネーブル

GTP-SR を設定するには、次の項の手順を記載されている順序で実行します。

- 「GTP セッション冗長性デバイス間インフラストラクチャの設定」（P.5-7）
- 「インターフェイスでのパッシブ ルート抑制の設定」（P.5-14）
- 「GGSN での GTP-SR のイネーブル」（P.5-15）

GTP セッション冗長性デバイス間インフラストラクチャの設定

GTP-SR 機能では、Cisco IOS CF を使用して、冗長設定した GGSN に SCTP 経由でステートフル データを送信します。また、Cisco GGSN では Cisco IOS RF を Cisco IOS HSRP とともに使用して、アクティブ GGSN とスタンバイ GGSN での移行をモニタリングおよびレポートします。

冗長 GGSN で GTP-SR をイネーブルにする前に GTP-SR デバイス間インフラストラクチャを設定するには、次の項の手順を実行します。

- 「HSRP の設定」（P.5-7）
- 「デバイス間冗長性のイネーブル」（P.5-12）
- 「デバイス間通信トランスポートの設定」（P.5-12）

HSRP の設定

HSRP は一般的に冗長性に使用されるプロトコルです。ネットワーク上のホストからの IP トラフィックをルーティングするときに単一ルータの可用性に依存しないため、HSRP では、高度なネットワーク可用性が提供されます。

HSRP は、ルータ グループ内におけるアクティブ ルータおよびスタンバイ ルータを選択するために使用されます。HSRP は、いずれかのインターフェイスがダウンしている場合に、デバイス全体がダウンしていると見なされるように、内部インターフェイスおよび外部インターフェイスの両方をモニタリングします。デバイスがダウンしていると見なされると、スタンバイ デバイスがアクティブになり、アクティブ デバイスの責務を引き継ぎます。

具体的には、HSRP により次の機能が提供されます。

- アクティブ/スタンバイのダイナミックなロール選択
- 障害検出用のハートビート
- アクティブ GGSN でだけパケットを受信する方法

レイヤ 3 の地理的冗長性をサポートするために、HSRP ではこれら 3 つの機能が次のように拡張されています。

- ロール選択は、リンクローカル マルチキャストではなく IP ユニキャスト ルーティングに基づいて行われます。
- ハートビートもリンクローカル マルチキャストではなくピア間の IP ユニキャスト メッセージであり、アクティブ GGSN をトリガしてルートをアドバタイズします。
- GGSN IP アドレスのルートおよび加入者ネットワークは、仮想 MAC アドレスをリッスンしてトラフィックをアクティブ GGSN にダイレクトするのではなく、（アクティブ GGSN によって）アドバタイズされます。

（注）　HSRP では、仮想 IP アドレスおよび MAC アドレスはパケットを受信するために使用されます。これらのアドレスは、L3 の地理的冗長性にルーティングが使用される場合には不要です。したがって、L3 の地理的冗長性を実装する場合は、HSRP グループの仮想 IP アドレスをゼロに設定します。

制約事項および推奨事項

HSRP を設定する場合は、次の推奨事項および制約事項が適用されます。

- 最低でも、HSRP をイネーブルにして、HSRP *プライマリ グループ*を GGSN インスタンスごとに 1 つのインターフェイス上で定義する必要があります。独自の個別 VLAN を使用する、GGSN 上のその他の各 HSRP インターフェイスは、*クライアント グループ*として設定できます。

クライアント グループ機能を使用すると、クライアント グループとして設定されているすべてのインターフェイスでプライマリ グループの HSRP パラメータを共有できます。これにより、多数の GGSN インターフェイスおよび HSRP グループを含む環境で、簡単に HSRP グループを設定およびメンテナンスできるようになります。プライマリ グループおよび関連付けられているクライアント グループは、同じグループ追跡状態を共有して、同じ優先度を持ちます。

通常、HSRP グループは次のインターフェイスで必要となります。1 つのグループをプライマリ グループとして設定し、残りをクライアント グループとして設定します。各インターフェイスはそれぞれ異なる VLAN に設定する必要があります。

- Gn インターフェイス：プライマリ グループ
- Ga インターフェイス：クライアント グループ
- Dynamic Host Configuration Protocol（DHCP）（Gi インターフェイスと共有可能）：クライアント グループ
- Gi Access Point Name（APN; アクセス ポイント ネーム）（VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）ごと）：クライアント グループ
- RADIUS：クライアント グループ
- Diameter：クライアント グループ
- クォータ サーバ：クライアント グループ

その他のインターフェイスを HSRP クライアント グループとして設定するには、**standby** インターフェイス コンフィギュレーション コマンドを使用し、プライマリ グループと同じグループ番号を使用して **follow** キーワード オプションを指定します。

- 各クライアント グループに対して、プライマリ グループに使用されているグループ番号と同じグループ番号を使用します。プライマリ グループとクライアント グループに同じグループ番号を使用すると、多数の GGSN インターフェイスおよび HSRP グループを含む環境で、簡単に HSRP グループを設定およびメンテナンスできるようになります。
- 同じ物理 VLAN にマップされる別のアクティブ / スタンバイ GGSN ペアでは、同じ HSRP グループを使用できません。
- HSRP をインターフェイスに設定している場合は、**standby preempt** インターフェイス コンフィギュレーション コマンドを使用してプリエンプト遅延を設定できます。ただし、GTP-SR 設定では、必要不可欠な場合を除いてプリエンプト遅延を設定しないことを推奨します。プリエンプト遅延を設定しないことで、不要なスイッチオーバーを防ぐことができます。プリエンプト遅延を設定する必要がある場合は、プリエンプトが有効になる前にバルク同期を完了できるように、十分な遅延を指定するようにします。
- ローカル冗長性を実装するとき、**standby use-bia** コマンドを使用せずにブリッジおよびゲートウェイで仮想 MAC アドレスを認識できるようにしている場合は、最適化のために **standby mac-refresh** コマンドでデフォルトより大きい値を設定します。デフォルトでは、メイン インターフェイス（gig 0/0）で 3 秒ごとに hello メッセージが送信されます。設定すると、すべての HSRP グループ（プライマリおよび follow）で、ノードがアクティブ モードの場合にだけ hello メッセージを送信します。

（注） HSRP 初期設定が設定されたあとにその他の HSRP 設定が追加されると、GGSN がリロードされます。

Cisco IOS HSRP の設定の詳細については、『*Cisco IOS IP Configuration Guide* Release 12.3』の「Configuring the Hot Standby Router Protocol」の項を参照してください。

インターフェイスでの L2 HSRP のイネーブルおよびローカル HSRP プライマリ グループの設定

L2 HSRP はデフォルトの HSRP です。L2 HSRP はローカル冗長性（同じ LAN の 2 つの Cisco GGSN 間の冗長性）をサポートしています。

インターフェイスで L2 HSRP をイネーブルにしてプライマリ 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
ステップ 1	`Router(config)# interface GigabitEthernet0/number`	1000-Mbps イーサネット インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-if)# encapsulation dot1Q vlan_id`	仮想 LAN（VLAN）の指定したサブインターフェイス上のトラフィックの IEEE 802.1Q カプセル化をイネーブルにします。
ステップ 3	`Router(config-if)# ip address ip address ip-address mask`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 4	`Router(config-if)# standby version 2`	HSRP バージョン 2 をイネーブルにします。
ステップ 5	`Router(config-if)# standby [group-number] ip [ip-address [secondary]]`	インターフェイスで HSRP をイネーブルにします。
ステップ 6	`Router(config-if)# standby [group-number] priority priority`	（任意）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。 優先度の値の範囲は、1 ～ 255 です。値 1 は優先度が最も低く、値 255 は優先度が最も高いことを示します。たとえば、ローカル ルータの優先度が現在のアクティブ ルータの優先度を上回っている場合、ローカル ルータはアクティブ ルータとして確立しようと試みます。
ステップ 7	`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 8	`Router(config-if)# standby use-bia [scope interface]`	（任意）事前に割り当てられている MAC アドレスを使用する代わりに、インターフェイスの Burned-In Address（BIA; バーンドイン アドレス）を仮想 MAC アドレスとして使用するように設定します。

次に、L2 HSRP の設定例を示します。

```
interface GigabitEthernet0/0.7
 encapsulation dot1Q 21
 ip address 172.2.2.1 255.255.0.0
 standby 1 ip 172.2.2.10
 standby 1 name local
```

インターフェイスでの L3 HSRP のイネーブルおよび地理的 HSRP プライマリ グループの設定

L3 HSRP では、地理的冗長性がサポートされています。地理的冗長性は、地理的に離れた場所に配置され、WAN で接続されている 2 つの Cisco GGSN 間の冗長性です。

地理的冗長性の実装では、ルーティング アップデートを送信する必要があるのはアクティブ デバイスだけです。したがって、L3 HSRP グループを設定する場合、GGSN がスタンバイ GGSN のときにはルーティング アップデートを送信しないようにインターフェイスを設定する必要もあります。パッシブ ルート抑制をイネーブルにする方法の詳細については、「インターフェイスでのパッシブ ルート抑制の設定」（P.5-14）を参照してください。

インターフェイスで L3 HSRP をイネーブルにしてプライマリ 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
ステップ 1	`Router(config)# interface GigabitEthernet0/number`	1000-Mbps イーサネット インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-if)# encapsulation dot1Q vlan_id`	仮想 LAN（VLAN）の指定したサブインターフェイス上のトラフィックの IEEE 802.1Q カプセル化をイネーブルにします。
ステップ 3	`Router(config-if)# ip address ip address ip-address mask`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 4	`Router(config-if)# standby version 2`	HSRP のバージョンを HSRP バージョン 2 に変更します。
ステップ 5	`Router(config-if)# standby [group-number] ip none`	インターフェイスで HSRP をイネーブルにして、HSRP メッセージからの Virtual IP（VIP; 仮想 IP）ラーニングをディセーブルにします。VIP ラーニングは L3 HSRP には使用しません。
ステップ 6	`Router(config-if)# standby [group-number] priority priority`	（任意）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。 優先度の値の範囲は、1 ～ 255 です。値 1 は優先度が最も低く、値 255 は優先度が最も高いことを示します。たとえば、ローカル ルータの優先度が現在のアクティブ ルータの優先度を上回っている場合、ローカル ルータはアクティブ ルータとして確立しようと試みます。
ステップ 7	`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 8	`Router(config-if)# standby group-number unicast destination destination-ip [source source-ip]`	IP ユニキャスト ルーティングを使用するように HSRP グループを設定し、ピア デバイスの宛先アドレスおよび送信元アドレスを設定します。 最大で 4 つの宛先を定義できます。 **standby unicast** コマンドを設定すると、仮想 IP（VIP）が 0.0.0.0 に、仮想 MAC アドレスがインターフェイスのアドレスに設定されます。 ユニキャスト トランスポートをイネーブルにすると、元々の L2 ベースのマルチキャスト トランスポートが自動的にディセーブルになります。 **source** *ip-address* キーワード オプションを指定する場合は、HSRP パケットの送信元 IP アドレスを指定します。指定しない場合、送信元 IP アドレスは対応するインターフェイスの設定から取得されます。

次に、L3 HSRP の設定例を示します。

プライマリ GGSN

```
interface GigabitEthernet0/0.7
 encapsulation dot1Q 21
 ip address 10.0.0.3 255.255.0.0
 standby 1 ip none
 standby 1 name geo
 standby 1 unicast destination 172.0.0.1
```

スタンバイ GGSN

```
interface GigabitEthernet0/0.8
 encapsulation dot1Q 21
 ip address 172.0.0.1 255.255.0.0
 standby 1 ip none
 standby 1 name geo
 standby 1 unicast destination 10.0.0.3
```

HSRP クライアント グループの設定

GGSN インターフェイスで HSRP をイネーブルにしてプライマリ グループを設定したあと、その他の GGSN インターフェイスを HSRP クライアント グループとして設定すると、プライマリ グループの HSRP パラメータを共有するようにこれらのインターフェイスを設定できます。

GGSN インターフェイスをクライアント グループとして設定するには、**standby** コマンドを使用し、プライマリ グループと同じグループ番号および名前を使用して **follow** キーワードを指定します。

これらのインターフェイスはグループ追跡状態を共有し、同じ優先度を持ちます。

（注） 優先度、名前、トラッキング、およびタイマーなどの HSRP グループ パラメータは、プライマリ グループだけで設定します。これらのパラメータはプライマリ グループから継承されるため、クライアント グループでは設定しないでください。

プライマリ グループに従うようにインターフェイスを設定するには、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
ステップ 1	`Router(config-if)# standby` *group-number* **ip** [*virtual-ip-address* | **none**]	グループ番号および次の内容を指定します。 • *virtual-ip-address*：L2 HSRP の場合、クライアント グループの仮想 IP アドレスを指定します（指定するグループ番号は、プライマリ グループ番号と同じである必要があります）。 • **none**：L3 HSRP の場合、HSRP メッセージからの仮想 IP（VIP）ラーニングをディセーブルにします。
ステップ 2	`Router(config-if)# standby` *group-number* **follow** *group-name*	クライアント グループが従い、ステータスを共有するプライマリ グループの番号および名前を指定します。 **（注）** 指定するグループ番号は、プライマリ 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

HSRP プライマリ グループは、2 つの GGSN 間のセッション冗長性をイネーブルにするために Cisco IOS RF と関連付けられます。

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
ステップ 1	`Router(config)# redundancy inter-device`	冗長性を設定し、デバイス間コンフィギュレーション モードを開始します。 すべてのデバイス間設定を削除するには、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。現在サポートされているスキームは、「standby」だけです。 • *standby-group-name*：**standby name** コマンド（「HSRP の設定」（P.5-7）を参照）で指定したスタンバイ名と一致している必要があります。また、スタンバイ名は冗長設定の両方の GGSN で同じである必要があります。
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

デバイス間冗長性には、冗長 GGSN 間の通信に使用する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; プロセス間通信）コマンドを使用して設定します。

2 つの GGSN 間のデバイス間通信トランスポ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
ステップ 1	`Router(config)# ipc zone default`	Interdevice Communication Protocol（IPC; デバイス間通信プロトコル）を設定し、IPC ゾーン コンフィギュレーション モードを開始します。 このコマンドを使用して、アクティブ GGSN とスタンバイ GGSN 間の通信リンクを開始します。
ステップ 2	`Router(config-ipczone)# association 1`	2 つの GGSN 間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 モードを開始します。 IPC アソシエーション コンフィギュレーション モードで、アソシエーションの詳細を設定します。これらの詳細には、トランスポート プロトコル、ローカル ポートとローカル IP アドレス、およびリモート ポートとリモート IP アドレスが含まれています。 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。

	コマンド	目的
ステップ 3	`Router(config-ipczone)# no shutdown`	ディセーブルにされているアソシエーションおよび関連付けられているトランスポート プロトコルを再開します。 **（注）** トランスポート プロトコルのパラメータを変更するには、アソシエーションをシャットダウンする必要があります。
ステップ 4	`Router(config-ipczone-assoc)# protocol sctp`	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 コンフィギュレーション モードをイネーブルにします。
ステップ 5	`Router(config-ipc-protocol-sctp)# local-port` *local_port_num*	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 コンフィギュレーション モードをイネーブルにします。ローカル SCTP ポートは、冗長ピアとの通信に使用されます。 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）** ローカル ポート番号は、ピア ルータのリモート ポート番号と同じである必要があります。
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 アドレスと一致している必要があります。
ステップ 7	`Router(config-ipc-local-sctp)# keepalive` [*period* [*retries*]]	（任意）キープアライブ パケットをイネーブルにします。任意で、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 プロトコルをダウンする前に、Cisco IOS ソフトウェアが応答なしでキープアライブ パケットの送信を試みる回数を指定します。 *period* の有効な値は、0 より大きい整数値（秒数）です。デフォルトは 10 です。*retries* の有効な値は、1 より大きくかつ 355 より小さい整数値です。デフォルトは以前に使用された値です。以前に指定された値がない場合は 5 です。
ステップ 8	`Router(config-ipc-local-sctp)# retransmit-timeout` *interval*	（任意）メッセージ再送信時間を設定します。 有効な範囲は、300 ～ 60000 ミリ秒です。デフォルトは、最小が 300、最大が 600 です。
ステップ 9	`Router(config-ipc-local-sctp)# path-retransmit` *number*	（任意）対応する宛先アドレスに非アクティブのマークが付けられるまでのキープアライブ再試行の最大回数を設定します。 有効な範囲は、2 ～ 10 です。デフォルトは 4 です。
ステップ 10	`Router(config-ipc-local-sctp)# assoc-retransmit` *number*	（任意）アソシエーションが失敗と宣言されるまでの宛先アドレス全体に対する再送信の最大回数を定義します。 有効な範囲は、2 ～ 20 です。デフォルトは 4 です。

	コマンド	目的
ステップ 11	`Router(config-ipc-local-sctp)# max-inbound-streams max-streams`	（任意）ローカル ポートに許可されるインバウンド ストリームの最大数を設定します。 有効な範囲は、2 ～ 25 です。デフォルトは 17 ストリームです。
ステップ 12	`Router(config-ipc-local-sctp)# init-timeout msec`	（任意）init パケットの再送信タイムアウト値の最大間隔を設定します。 有効な範囲は、1000 ～ 60000 ミリ秒です。デフォルトは 1000 ミリ秒です。
ステップ 13	`Router(config-ipc-local-sctp)# exit`	IPC トランスポート - SCTP ローカル コンフィギュレーション モードを終了します。
ステップ 14	`Router(config-ipc-protocol-sctp)# remote-port port_nun`	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 モードをイネーブルにします。リモート SCTP ポートは、冗長 GGSN との通信に使用されます。 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 GGSN のローカル ポート番号と同じである必要があります。
ステップ 15	`Router(config-ipc-remote-sctp)# remote-ip ip_addr`	ローカル デバイスとの通信に使用される冗長 GGSN 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 アドレスで同じ GGSN を参照している必要があります。

アソシエーションを削除するには、コマンドの **no** フォームを使用します。

インターフェイスでのパッシブ ルート抑制の設定

地理的冗長性の実装では、アクティブ GGSN だけがルートをアドバタイズします。したがって、GGSN がスタンバイ GGSN になったときにはルートの再配信を停止するようにインターフェイスを設定する必要があります。

インターフェイスにパッシブ ルート抑制を設定するには、ルータ 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-router)# passive-interface [default] interface-type interface-number [on-standby]`	インターフェイスにルーティング アップデートの抑制を設定します（OSPF 隣接はスーパーバイザのネイバーでは形成されません）。任意で、**on-standby** キーワード オプションを指定して、スタンバイ モード時だけインターフェイスでのルーティング アップデートを抑制するように設定します。

次の例では、GGSN がスタンバイ GGSN の場合にルーティング アップデートを抑制するように 2 つの GigabitEthernet インターフェイスを設定しています。

```
router ospf 100
 router-id 30.30.30.30
 no log-adjacency-changes
 redistribute static subnets
 passive-interface GigabitEthernet0/0.100 on-standby
 network 10.0.0.0 0.0.0.255 area 0
 network 1.1.1.10.0.0.0 area 0
!
router ospf 200 vrf Gi-VRF
 no log-adjacency-changes
 redistribute static route-map xxx
 passive-interface GigabitEthernet0/0.200 on-standby
 network 11.0.0.0 0.0.0.255 area 1
```

GGSN での GTP-SR のイネーブル

GTP-SR をイネーブルにするには、各冗長 GGSN で、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)# gprs redundancy`	GGSN で GTP-SR をイネーブルにします。

GTP セッション冗長性のディセーブル

GTP-SR を（GGSN アプリケーション レベルとデバイス間インフラストラクチャ レベルの両方で）ディセーブルにするには、次の作業を記載されている順序で実行します。次の作業を開始するときには、GGSN がスタンバイ モードになっていることを確認してください。

1. GGSN がスタンバイ モードになっていることを確認して、GGSN アプリケーションレベルの冗長性をディセーブルにします。

   ```
   Router(config)# show gprs redundancy
   ...
   Router(config)# no gprs redundancy
   ```

   GGSN はスタンドアローンのアクティブ GGSN になります。

2. デバイス間コンフィギュレーション モードで、設定済みのスタンバイ スキームを削除します。

   ```
   Router(config)# redundancy inter-device
   Router(config-red-interdevice)# no scheme standby HSRP-Gn
   ```

3. 設定変更をメモリに保存します。

   ```
   Router(config)# write memory
   ```

4. ルータをリロードします。

   ```
   Router# reload
   ```

   GGSN が稼動状態に戻ったあと、GGSN をリロードせずにその他の設定変更を実行および保存できます。

5. 2 つのデバイス間のアソシエーションをディセーブルにし、SCTP の設定を解除することで、SCTP をディセーブルにします。

```
Router(config)# ip zone default
Router(config-ipczone)# association 1
Router(config-ipczone-assoc)# shutdown
...
Router(config-ipczone-assoc)# no protocol sctp
```

6. インターフェイスに関連付けられている HSRP 設定を削除するには、関連する HSRP コマンドの **no** フォームを使用します。クライアント グループの HSRP グループ設定を最初に削除します。

```
Router(config)# interface GigabitEthernet0/0.56001
Router(config-if)# no standby 52 ip 172.90.1.52
Router(config-if)# no standby 52 follow HSRP-Gn
Router(config-if)# no standby version 2
Router(config-if)# exit

Router(config)# interface GigabitEthernet0/0.401
Router(config-if)# no standby 52 ip 192.1268.1.52
Router(config-if)# no standby 52 name HSRP-Gn
Router(config-if)# no standby version 2
Router(config-if)# exit
```

7. 設定変更をメモリに保存します。

```
Router(config)# write memory
```

課金関連同期パラメータの設定

PDP コンテキストの課金の確立に必要な課金関連のデータは、スタンバイ GGSN と同期化されます。このデータには次の内容が含まれます。

- PDP コンテキストと関連付けられる Charging Identity（CID; 課金 ID）
- ローカル シーケンス番号
- レコード シーケンス番号
- GTP シーケンス番号
- サービスごとのローカル シーケンス番号

（注） 地理的冗長性の場合、アクティブ GGSN とスタンバイ GGSN の両方で同じ IP アドレスを使用して課金元インターフェイスを設定する必要があり、また、アドレスは OSPF ルーティング プロトコル経由で配信される必要があります。

課金 ID（CID）およびローカル レコード シーケンス番号

確立された PDP コンテキストが同期化されると、PDP コンテキストの呼詳細レコード（CDR）に割り当てられている CID もスタンバイ GGSN と同期化されます。スタンバイ GGSN で PDP コンテキストの同期化データを受信したときに、提供された CID 値がグローバル CID カウンタの現在値よりも大きかった場合、スタンバイ GGSN はグローバル CID カウンタにその値を書き込みます。スイッチオーバーが発生した場合、新しいアクティブ GGSN は、書き込み済みの最新の CID 値と、新しいアクティブ GGSN で作成される新しい PDP コンテキストすべてのウィンドウ / オフセットから開始されます。

アクティブ GGSN の CID タイマーがタイムアウトになり、アクティブ GGSN がグローバル CID カウンタ値をメモリに書き込むと、CID 値およびローカル レコード シーケンス（設定している場合）は、スタンバイ GGSN と同期化され、スタンバイ GGSN が情報をメモリに書き込みます。ローカル シーケンス番号も設定されている場合、ローカル シーケンス番号に関連付けられている書き込みタイマーがタイムアウトになると、CID とローカル シーケンス番号の両方がスタンバイ GGSN と同期化されます。スタンバイ GGSN がアクティブになると、ローカル レコード シーケンス番号、メモリに書き込まれている最新の CID 値、新しいアクティブ GGSN で作成される後続の PDP コンテキストのウィンドウ/オフセットが使用されます。

レコード シーケンス番号

課金ゲートウェイはレコード シーケンス番号を使用して、PDP コンテキストに関連付けられている重複 CDR を検出します。

スタンバイ GGSN と同期化されるデータ量を最小化するために、レコード シーケンス番号は CDR が閉じるたびに同期化されるわけではありません。代わりに、レコード シーケンス番号のウィンドウしきい値が、CDR が閉じるたびに同期化されます。

レコード シーケンス番号の現在値および最後に同期化された PDP コンテキストのレコード番号がチェックされます。これらの値の差がウィンドウ サイズに設定されている値の場合、現在のレコード シーケンス番号がスタンバイ GGSN と同期化されます。スタンバイ GGSN がアクティブ GGSN になると、同期化された最後の値とウィンドウ サイズから開始されます。

CDR レコード シーケンス番号がスタンバイ GGSN といつ同期化されるかを決定するウィンドウ サイズを設定するには、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# gprs redundancy charging sync-window cdr rec-seqnum size`	CDR レコード シーケンス番号がいつ同期化されるかを決定するために使用されるウィンドウ サイズを設定します。有効な範囲は、1 ～ 20 です。デフォルトは 10 です。

GTP シーケンス番号

課金ゲートウェイは、GTP シーケンス番号を使用して、パケットの重複を防ぎます。GGSN は、PDP コンテキストに関連付けられている符号化 CDR を GTP パケットに含めて課金ゲートウェイに送信します。課金ゲートウェイは GTP パケットを確認応答すると、メモリからパケットを削除します。確認応答されなかった場合、パケットは再送信されます。シーケンス番号が繰り返していた場合、課金ゲートウェイは GTP パケットを確認応答できません。

スタンバイ GGSN と同期化されるデータ量を最小化するために、GTP シーケンス番号は CDR が閉じるたびに同期化されるわけではありません。代わりに、GTP シーケンス番号のウィンドウしきい値が、CDR メッセージが送信されるたびに同期化されます。GTP シーケンス番号の現在値および最後に同期化された PDP コンテキストの GTP シーケンス番号がチェックされます。これらの値の差がウィンドウ サイズに設定されている値の場合、GTP プライム シーケンス番号がスタンバイ GGSN と同期化されます。スタンバイ GGSN がアクティブ GGSN になると、同期化された最後の値とウィンドウ サイズから開始されます。

GTP シーケンス番号がスタンバイ GGSN といつ同期化されるかを決定するウィンドウ サイズを設定するには、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# **gprs redundancy charging sync-window gtpp seqnum** size	GTP シーケンス番号がいつ同期化されるかを決定するウィンドウ サイズを設定します。有効な範囲は、5 ～ 65535 です。デフォルトは 10000 です。 **（注）** GGSN は、確認応答なしで 128 GTP パケットを送信できます。したがって、ウィンドウ サイズが 128 より大きくなるように設定することを推奨します。

サービスごとのローカル シーケンス番号

課金ゲートウェイはサービスごとのローカル シーケンス番号を使用して、PDP コンテキストに関連付けられている重複サービス コンテナを検出します。

スタンバイ GGSN と同期化されるデータ量を最小化するために、サービスごとのローカル シーケンス番号は拡張 GGSN CDR（eG-CDR）が閉じるたびに同期化されるわけではありません。代わりに、ローカル シーケンス番号の現在値および最後に同期化された PDP コンテキストのローカル シーケンス番号がチェックされ、その差が設定されているウィンドウ サイズよりも大きい場合、現在のローカル シーケンス番号がスタンバイ GGSN と同期化されます。スタンバイ GGSN がアクティブ GGSN になると、同期化された最後の値とウィンドウ サイズから開始されます。

サービスごとのローカル シーケンス番号がスタンバイ GGSN といつ同期化されるかを決定するウィンドウ サイズを設定するには、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# **gprs redundancy charging sync-window svc-seqnum** size	サービスごとのローカル シーケンス番号がスタンバイ GGSN といつ同期化されるかを決定するウィンドウ サイズを設定します。有効な値は、1 ～ 200 の数値です。デフォルトは 50 です。

GTP-SR のモニタリングおよびメンテナンス

次の特権 EXEC **show** コマンドを使用して、GTP-SR 設定のさまざまな要素をモニタリングできます。

コマンド	目的
Router# **show gprs redundancy**	GTP-SR に関連する統計情報を表示します。
Router# **show redundancy [clients | counters | events | history | states | switchovers]**	現在または過去のステータスや、計画または記録されているハンドオーバーの関連情報を表示します。
Router# **show standby**	HSRP 情報を表示します。

GTP-SR 環境での GGSN イメージのアップグレード

Cisco SAMI で新しい Cisco GGSN イメージにアップグレードするには、次の作業を実行します。

1. Link Control Protocol（LCP; リンク制御プロトコル）（PPC0）コンソールで **show version** コマンドを使用して、SAMI 上のすべてのアプリケーション エンティティ（GGSN イメージ）を識別します。
2. Cisco IOS SLB の **no inservice** コマンドを使用して、スーパーバイザの GTP Server Load Balancing（SLB; サーバ ロード バランシング）リストから Cisco SAMI プロセッサ上のすべての GGSN を削除します。これにより、GGSN は新しい PDP コンテキスト作成要求を受信しなくなりますが、既存の PDP コンテキストのサービスは続行できます。
3. すべての PDP コンテキストがクリアされるまで待つか、または **clear gprs gtp pdp-context** コマンドを使用して手動で PDP コンテキストをクリアします。
4. 新しいイメージを SAMI にロードし、『*Cisco Service and Application Module for IP User Guide*』の説明に従って SAMI をリセットします。
5. イメージのリロードが完了したあと、スーパーバイザで Cisco IOS SLB の **inservice** コマンドを使用して GGSN を GTP SLB リストに戻します。

Cisco SAMI でアプリケーション イメージをアップグレードする方法の詳細は、『*Cisco Service and Application Module for IP User Guide*』を参照してください。

設定例

ここでは、次の設定例を示します。

- 「ローカル GTP-SR の例」（P.5-19）
- 「地理的 GTP-SR の例」（P.5-25）

（注）　ここに示す設定例は、あくまでも設定のサンプルです。実際の設定は、ネットワーク設計によって異なります。

ローカル GTP-SR の例

ここでは、ローカル GTP-SR 実装の次の設定例を示します。

- 「プライマリ スーパーバイザの設定例」（P.5-19）
- 「プライマリ GGSN の設定例」（P.5-22）
- 「セカンダリ GGSN の設定例」（P.5-23）

プライマリ スーパーバイザの設定例

次の例は、プライマリ スーパーバイザの設定例の一部を示しています。GTP-SR の設定に使用するいくつかのコマンドは、太字で強調表示されています。

```
sup-primary# show running-config
Building configuration...

Current configuration : 7144 bytes
!
```

```
! Last configuration change at 12:28:26 UTC Tue Oct 21 2003
! NVRAM config last updated at 13:32:08 UTC Thu Oct 16 2003
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname sup-primary
!
...
!
svclc multiple-vlan-interfaces
svclc module 7 vlan-group 71,73
svclc vlan-group 71 71 svclc vlan-group 73 95,100,101
ip subnet-zero
!
no ip domain-lookup
!
interface GigabitEthernet2/1
 description "VLAN for Inter-dev SCTP"
 no ip address
 switchport
 switchport access vlan 498
 switchport mode access
 no cdp enable
!
...
!
interface FastEthernet3/25
 description "VLAN for Gn"
 no ip address
 duplex full
 switchport
 switchport access vlan 410
 switchport mode access
 no cdp enable
!
interface FastEthernet3/26
 description "VLAN for Gi"
 no ip address
 duplex full
 switchport
 switchport access vlan 420
 switchport mode access
!
...
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan410
 description "Virtual LAN for Gn interface for all GGSNs on an SAMI"
 ip address 10.20.21.1 255.255.255.0
 no ip redirects
!
interface Vlan420
 description "One Gi Vlan all GGSN images of mwmam"
 ip address 10.20.51.1 255.255.255.0
 no ip redirects
!
interface Vlan498
 description "VLAN for Inter-dev_SCTP"
```

```
 ip address 10.70.71.1 255.255.255.0
!
router ospf 1
 router-id 10.20.1.2
 log-adjacency-changes
 summary-address 10.20.30.0 255.255.255.0
 redistribute static subnets route-map GGSN-routes
 network 10.20.1.0 0.0.0.255 area 1
!
ip classless
ip route 0.0.0.0 0.0.0.0 128.107.234.100
ip route 1.8.0.0 255.255.0.0 1.8.0.1
ip route 1.12.0.0 255.255.0.0 1.12.0.1
ip route 10.2.5.0 255.255.255.0 10.2.15.1
ip route 10.20.30.11 255.255.255.255 10.20.21.81
ip route 10.20.30.12 255.255.255.255 10.20.21.82
ip route 10.20.30.13 255.255.255.255 10.20.21.83
ip route 10.20.30.14 255.255.255.255 10.20.21.84
ip route 10.20.30.15 255.255.255.255 10.20.21.85
ip route 110.1.0.0 255.255.0.0 10.20.51.91
ip route 120.1.0.0 255.255.0.0 10.20.51.92
ip route 128.107.241.185 255.255.255.255 128.107.234.161
ip route 130.1.0.0 255.255.0.0 10.20.51.93
ip route 140.1.0.0 255.255.0.0 10.20.51.94
ip route 150.1.0.0 255.255.0.0 10.20.51.95
ip route 172.19.23.55 255.255.255.255 172.19.24.1
ip route 223.0.0.0 255.0.0.0 1.8.0.1
ip route 223.0.0.0 255.0.0.0 1.12.0.1
no ip http server
no ip http secure-server
ip pim bidir-enable
!
!
access-list 1 permit 10.20.30.0 0.0.0.255
access-list 101 permit ip 128.107.234.160 0.0.0.31 any
access-list 102 permit ip any 128.107.234.160 0.0.0.31
arp 127.0.0.22 0000.2200.0000 ARPA
!
route-map GGSN-routes permit 10
 match ip address 1
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 exec-timeout 0 0
 password abc
 logging synchronous
 transport input lat pad mop telnet rlogin udptn nasi
line vty 5 15
 exec-timeout 0 0
 password abc
 logging synchronous
!
ntp master
end

sup-primary#
```

プライマリ GGSN の設定例

```
Active_GGSN# show running-config
Building configuration...

Current configuration : 2942 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service gprs ggsn
no service dhcp
!
hostname Act_GGSN
!
...
!
redundancy inter-device
 scheme standby Gn
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.70.71.5
    keepalive 3000
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 20
   remote-port 5000
    remote-ip 10.70.71.9
!
no aaa new-model
ip subnet-zero
!
!
no ip cef
no ip domain lookup
!
!
interface Loopback1
 description VT address of processor3:GGSN"
 ip address 10.20.30.12 255.255.255.255
!
interface Loopback2
 description "Loopback of GTP-SLB for dispatch mode"
 ip address 10.20.30.91 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 standby use-bia
!
interface GigabitEthernet0/0.3
 description "VLAN for Gn interface of UMTS"
 encapsulation dot1Q 410
 ip address 10.20.21.52 255.255.255.0
 no ip mroute-cache
 no keepalive
 no cdp enable
 standby version 2
 standby 7 ip 10.20.21.82
```

```
 standby 7 priority 190
 standby 7 name Gn
!
interface GigabitEthernet0/0.31
 description "VLAN for Gi interface of UMTS"
 encapsulation dot1Q 420
 ip vrf forwarding internet
 ip address 10.30.21.52 255.255.255.0
 standby 7 follow Gn
 standby 7 ip 10.30.21.82
!
interface GigabitEthernet0/0.71
 description "VLAN for inter-dev_SCTP"
 encapsulation dot1Q 498
 ip address 10.70.71.5 255.255.255.0
!
interface Virtual-Template1
 ip unnumbered Loopback1
 no ip redirects
 encapsulation gtp
 gprs access-point-list gprs
!
ip local pool APN1 110.1.0.1 110.1.10.255
ip classless
no ip http server
!
gprs access-point-list gprs
  access-point 1
   access-point-name apn1
   ip-address-pool local APN1
!
gprs gtp path-echo-interval 0
!
gprs charging disable
gprs redundancy
!
!
...
!
!
end

Active_GGSN-3#
```

セカンダリ GGSN の設定例

```
Standby_GGSN# show running config
Building configuration...

Current configuration : 2823 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Stby_GGSN
!
service gprs ggsn
!
...
!
```

```
redundancy inter-device
 scheme standby Gn
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.70.71.9
    keepalive 3000
    retransmit-timeout 300 10000
    path-retransmit 10
    assoc-retransmit 20
   remote-port 5000
    remote-ip 10.70.71.5
!
no aaa new-model
ip subnet-zero
!
!
no ip cef
!!
interface Loopback1
 description VT address of processor3:GGSN"
 ip address 10.20.30.12 255.255.255.255
!
interface Loopback2
 description "Loopback of GTP-SLB for dispatch mode"
 ip address 10.20.30.91 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 standby use-bia
!
interface GigabitEthernet0/0.3
 description "VLAN for Gn interface of UMTS"
 encapsulation dot1Q 410
 ip address 10.20.21.62 255.255.255.0
 no ip mroute-cache
 no keepalive
 no cdp enable
 standby version 2
 standby 7 ip 10.20.21.82
 standby 7 priority 160
 standby 7 name Gn
!
interface GigabitEthernet0/0.31
 description "VLAN for Gi interface of UMTS"
 encapsulation dot1Q 420
 ip vrf forwarding internet
 ip address 10.30.21.62 255.255.255.0
 standby 7 follow Gn
 standby 7 ip 10.30.21.82
!
interface GigabitEthernet0/0.71
 description "VLAN for inter-dev_SCTP"
 encapsulation dot1Q 498
 ip address 10.70.71.9 255.255.255.0
!
interface Virtual-Template1
 ip unnumbered Loopback1
 no ip redirects
 encapsulation gtp
 gprs access-point-list gprs
```

```
!
ip local pool APN1 110.1.0.1 110.1.10.255
ip classless
no ip http server
!
!
gprs access-point-list gprs
  access-point 1
   access-point-name apn1
   ip-address-pool local APN1
   !
  !
!
!
gprs charging disable
gprs redundancy
!
!
...
!
!
end

Stby_GGSN-3#
```

地理的 GTP-SR の例

ここでは、地理的 GTP-SR 実装の次の設定例を示します。

- 「GGSN インターフェイスの設定例」（P.5-25）
- 「セカンダリ GGSN インターフェイスの設定例」（P.5-26）
- 「スーパーバイザ ルーティングの設定例」（P.5-26）
- 「GGSN ルーティングの設定例」（P.5-27）

GGSN インターフェイスの設定例

プライマリ GGSN インターフェイスの設定例

```
!
interface Loopback1
 description GGSN Loopback i/f
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0.100
 description Gn VLAN
 encapsulation dot1Q 100
 ip address 10.0.0.1 255.255.255.0
 standby 1 ip none
 standby 1 name geo
 standby 1 unicast destination 20.0.0.2
!
interface GigabitEthernet0/0.200
 description Gi VLAN
 encapsulation dot1Q 200
 ip vrf forwarding Gi-VRF
 ip address 11.0.0.1 255.255.255.0
 standby 1 ip none
 standby 1 follow geo
```

```
!
interface Virtual-Template1
 ip unnumbered Loopback1
 encapsulation gtp
 gprs access-point-list APLIST
!
```

セカンダリ GGSN インターフェイスの設定例

```
!
interface Loopback1
 description GGSN Loopback i/f
 ip address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/0.300
 description Gn VLAN
 encapsulation dot1Q 300
 ip address 20.0.0.2 255.255.255.0
 standby 1 ip none
 standby 1 name geo
 standby 1 unicast destination 10.0.0.1
!
interface GigabitEthernet0/0.400
 description Gi VLAN
 encapsulation dot1Q 400
 ip vrf forwarding Gi-VRF
 ip address 21.0.0.2 255.255.255.0
 standby 1 ip none
 standby 1 follow geo
!
interface Virtual-Template1
 ip unnumbered Loopback1
 encapsulation gtp
gprs access-point-list APLIST
!
```

スーパーバイザ ルーティングの設定例

プライマリ スーパーバイザの設定例

```
ip vrf Gi-VRF
rd 200:1
!
interface Vlan200
description Gi-VRF
ip vrf forwarding Gi-VRF
ip address 11.0.0.10 255.255.255.0
end
!
router ospf 200 vrf Gi-VRF
log-adjacency-changes
network 11.0.0.0 0.0.0.255 area 1
```

セカンダリ スーパーバイザ ルーティングの設定例

```
ip vrf Gi-VRF
rd 200:1
!
interface Vlan400
description Gi-VRF
ip vrf forwarding Gi-VRF
ip address 21.0.0.20 255.255.255.0
end
```

```
!
router ospf 400 vrf Gi-VRF
log-adjacency-changes
network 21.0.0.0 0.0.0.255 area 3
!
```

GGSN ルーティングの設定例

プライマリ GGSN ルーティングの設定例

```
router ospf 10
router-id 30.30.30.30
no log-adjacency-changes
redistribute static subnets
passive-interface GigabitEthernet0/0.10 on-standby
network 10.0.0.0 0.0.0.255 area 0
network 1.1.1.1 0.0.0.0 area 0
!
router ospf 20 vrf Gi-VRF
no log-adjacency-changes
redistribute static route-map xxx
passive-interface GigabitEthernet0/0.20 on-standby
network 11.0.0.0 0.0.0.255 area 1
!
```

セカンダリ GGSN ルーティングの設定例

```
router ospf 30
router-id 40.40.40.40
no log-adjacency-changes
redistribute static subnets
passive-interface GigabitEthernet0/0.30 on-standby
network 20.0.0.0 0.0.0.255 area 2
network 2.2.2.2 0.0.0.0 area 2
!
router ospf 40 vrf Gi-VRF
no log-adjacency-changes
redistribute static route-map xxx
passive-interface GigabitEthernet0/0.40 on-standby
network 21.0.0.0 0.0.0.255 area 3
!
```

CHAPTER 6

GGSN での課金の設定

この章では、Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）に課金機能を設定する方法について説明します。

Cisco GGSN に課金ゲートウェイを少なくとも 1 つ定義していると、デフォルトでは GGSN で課金処理がイネーブルになります。

課金ゲートウェイとの通信をカスタマイズするには、いくつかの方法があります。課金オプションの多くは、デフォルト値のままでも問題ありません。ネットワークに関する知識が増えてから、課金インターフェイスのカスタマイズを検討してください。

（注） この章で説明するグローバル コンフィギュレーション課金コマンドは、コマンド説明に特に明記されていないかぎり、GGSN に設定されたすべての課金グループに適用され、影響を与えます。

この章に記載されている GGSN コマンドの詳細については、使用している Cisco GGSN リリースの『*Cisco GGSN Command Reference*』を参照してください。この章に記載されているその他のコマンドのマニュアルを参照するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

この章は、次の内容で構成されています。

課金ゲートウェイへのインターフェイスの設定

General Packet Radio Service（GPRS; グローバル パケット ラジオ サービス）/Universal Mobile Telecommunication System（UMTS）ネットワークの外部課金ゲートウェイへのアクセスを確立するには、課金ゲートウェイのネットワークに接続するためのインターフェイスを GGSN に設定する必要があります。

GPRS/UMTS では、GGSN と課金ゲートウェイ間のインターフェイスを *Ga インターフェイス*と呼びます。Cisco GGSN は、2.5G Ga インターフェイスと 3G Ga インターフェイスの両方をサポートしています。Cisco 7600 シリーズ ルータ プラットフォームでは、Ga インターフェイスはスーパーバイザ エンジンに設定されたレイヤ 3 ルーテッド Ga VLAN への論理的なインターフェイスとなります。この論理インターフェイスに IEEE 802.1Q カプセル化を設定する必要があります。

スーパーバイザ エンジン上の Ga VLAN の詳細については、「プラットフォームの前提条件」（P.2-2）を参照してください。インターフェイスの設定の詳細については、『*Cisco IOS Interface Configuration Guide*』および『*Cisco IOS Interface Command Reference*』を参照してください。

スーパーバイザ エンジン上の Ga VLAN へのサブインターフェイスを設定するには、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
ステップ 1	`Router(config)# interface gigabitethernet slot/port.subinterface-number`	サブインターフェイスを設定します。
ステップ 2	`Router(config-if)# encapsulation dot1q vlanid`	カプセル化形式を IEEE 802.1Q（dot1q）と定義し、VLAN 識別子を指定します。
ステップ 3	`Router(config-if)# ip address ip-address mask`	インターフェイスのプライマリ IP アドレスを設定します。

課金ゲートウェイへのインターフェイス設定の検証

課金ゲートウェイへのインターフェイスを検証するには、まず GGSN 設定を検証し、次にインターフェイスが使用できることを検証します。

ステップ 1　スーパーバイザ エンジンに Ga VLAN を正しく設定したことを検証するには、**show running-config** コマンドを使用します。次の例は、課金ゲートウェイへの Ga インターフェイスとなるギガビット イーサネット 8/22 物理インターフェイスの設定と、Ga VLAN の設定を表示するコマンドの出力を示しています。

```
Sup# show running-config
Building configuration...

Current configuration :12672 bytes
!
version 12.2
...
!
interface GigabitEthernet8/22
 no ip address
 switchport
 switchport access vlan 302
!
interface Vlan302
 description Vlan to GGSN for Ga
 ip address 40.40.40.100 255.255.255.0
```

ステップ 2　物理インターフェイスおよび Ga VLAN が利用可能であることを検証するには、スーパーバイザ エンジンで **show interface** コマンドを使用します。次の例は、課金ゲートウェイへのファスト イーサネット 8/22 物理インターフェイスが稼動していることを示しています。Ga VLAN である VLAN 101 が稼動しています。

```
Sup# show ip interface brief GigabitEthernet8/22
Interface                  IP Address      OK? Method Status                Protocol
GigabitEthernet8/22        unassigned      YES unset  up                    up

Sup# show ip interface brief Vlan302
Interface                  IP-Address      OK? Method Status                Protocol
Vlan302                    40.40.40.100    YES TFTP   up                    up

Sup#
```

ステップ 3　Ga VLAN の設定および可用性を検証するには、スーパーバイザ エンジンで **show vlan name** コマンドを使用します。Gn VLAN Gn_1 の例を次に示します。

```
Sup# show vlan name Ga_1

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
302  Ga_1                             active    Gi4/1, Gi4/2, Gi4/3, Gi7/1
                                                Gi7/2, Gi7/3, Fa8/22, Fa8/26

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
302  enet  100302     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ---------------- ------------------------------------------
```

ステップ 4　GGSN で、スーパーバイザ上の Ga VLAN への Ga サブインターフェイスを正しく設定したことを検証するには、**show running-config** コマンドを使用します。次の例は、Ga 課金ゲートウェイへのインターフェイスとなるギガビット イーサネット 0/0.2 サブインターフェイスの設定を表示するコマンドの出力を示しています。

```
GGSN# show running-config
Building configuration...

Current configuration : 5499 bytes
!
! Last configuration change at 20:38:31 PST Tue Oct 13 2009
!
version 12.4
!
.....
!
interface GigabitEthernet0/0.2
 description Ga Interface
 encapsulation dot1Q 302
 ip address 40.40.40.41 255.255.0.0
 no cdp enable
!
.....
ip route 40.1.2.1 255.255.255.255 10.1.1.1
```

ステップ 5　サブインターフェイスが利用可能であることを検証するには、**show ip interface brief** コマンドを使用します。次の例は、Ga VLAN へのギガビット イーサネット 0/0.2 サブインターフェイスが「稼動」し、プロトコルも「稼動」していることを示しています。

```
GGSN# show ip interface brief GigabitEthernet0/0.2
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0.2       40.40.40.41     YES NVRAM  up                    up
```

デフォルト課金ゲートウェイの設定

GGSN が課金情報をやり取りするためにデフォルトで使用する課金ゲートウェイを設定できます。また、セカンダリおよびターシャリの課金ゲートウェイをバックアップ課金ゲートウェイとして指定できます。すべての課金ゲートウェイが、同じグローバル課金パラメータを共有します。

（注）　Cisco GGSN リリース 9.0 以降では粒状課金機能を導入しており、このデフォルト課金ゲートウェイのセットは、課金グループ番号 0、つまりデフォルト課金グループであると見なされます。

GGSN のデフォルト課金ゲートウェイを設定するには、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)# **gprs default charging-gateway** {*ip-address* | *name*} [{*ip-address* | *name*}] [{*ip-address* | *name*}] [{*ip-address* | *name*}]	プライマリ課金ゲートウェイを指定します。任意で、セカンダリおよびターシャリのバックアップ課金ゲートウェイを指定することもできます。詳細は次のとおりです。 • *ip-address*：課金ゲートウェイの IP アドレスを指定します。第二および第三の *ip-address* 引数には、バックアップ課金ゲートウェイの IP アドレスを指定します。 • *name*：課金ゲートウェイのホスト名を指定します。第二および第三の *name* 引数には、バックアップ課金ゲートウェイのホスト名を指定します。

優先順位の最も高い課金ゲートウェイに切り替えるための GGSN の設定

gprs charging switchover priority コマンドを使用して GGSN にプライオリティ スイッチオーバーを設定した場合、現在のアクティブな課金ゲートウェイの状態に関係なく、プライオリティの高いゲートウェイが稼動すると、GGSN はその課金ゲートウェイに切り替えて G-CDR を送信します。

（注）　このコマンドは、デフォルト課金グループ（課金グループ 0）に属するグローバルに定義された課金ゲートウェイにだけ適用されます。1 ～ 29 の課金グループにプライオリティ スイッチオーバーを設定するには、課金グループ コンフィギュレーション モードで **switchover priority** コマンドを使用します。

GGSN でデフォルト課金グループのプライオリティ スイッチオーバーを設定するには、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
ステップ 1	`Router(config)# gprs charging switchover priority`	プライオリティの高いゲートウェイがアクティブになったときにそのゲートウェイに切り替わるように、GGSN を設定します。

デフォルト課金ゲートウェイの変更

GGSN のデフォルト課金ゲートウェイを変更するには、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
ステップ 1	`Router(config)# gprs default charging-gateway 10.9.0.2`	10.9.0.2 という IP アドレスにプライマリ課金ゲートウェイを指定します。
ステップ 2	`Router(config)#  no gprs default charging-gateway 10.9.0.2`	10.9.0.2 という IP アドレスにあるプライマリ課金ゲートウェイを除外します。
ステップ 3	`Router(config)# gprs default charging-gateway 10.9.0.3`	10.9.0.3 という IP アドレスにあるプライマリ課金ゲートウェイを新しいデフォルトに指定します。

課金元インターフェイスの設定

デフォルトでは、グローバル GTP 仮想テンプレート インターフェイスが、すべての課金メッセージに使用されます。Cisco GGSN リリース 8.0 以降では、課金メッセージの*課金元インターフェイス*を設定できます。

課金元インターフェイスはループバック インターフェイスであり、**gprs charging interface source loopback** コマンドを使用すると、GGSN は課金トラフィックにこのインターフェイスを使用するように設定されます。ループバック インターフェイスを課金元インターフェイスとして設定すると、どの課金メッセージでもそのループバック インターフェイスの IP アドレスが送信元アドレスとして使用されます。

課金元インターフェイス機能を使用すると、課金トラフィックを分離できます。任意で、課金トラフィックをプライベート VLAN に分離するように、ループバック インターフェイスに VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンスを設定することもできます。

課金元インターフェイスを設定する場合は、次の点に注意してください。

- ループバック インターフェイスは、いったん設定すると、課金元インターフェイス設定を削除しないかぎり、変更できません。すべての課金メッセージが、パス構造に基づいて新しいエンド ポイントを使用します。
- アクティブな PDP または Call Detail Record（CDR; 呼詳細レコード）が存在するかぎり、課金元インターフェイスは未設定にしておくことができません。

課金元インターフェイスを設定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# interface loopback number`	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、常に稼動している仮想インターフェイスです。
ステップ 2	`Router(config-if)# ip address ip-address mask`	ループバック インターフェイスに IP アドレスを割り当てます。
ステップ 3	`Router(cfg-acct-mlist)# exit`	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。

課金トラフィックにループバック インターフェイスを使用するように GGSN 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)# gprs charging interface source loopback number`	GGSN が課金メッセージに使用するループバック インターフェイスを指定します。 **（注）** 課金元インターフェイスは、ループバック インターフェイスである必要があり、有効な IP アドレスを使用して設定する必要があります。任意で、課金トラフィックをプライベート VLAN に分離するように、課金元インターフェイスに VRF インスタンスを設定することもできます。

GGSN メモリ保護モードしきい値の設定

GGSN メモリ保護機能を使用すると、異常な条件が発生している間、たとえば、すべての課金ゲートウェイがダウンし、GGSN が呼詳細レコード（CDR）をメモリにバッファリングしているときにも、プロセッサ メモリの枯渇を回避できます。

メモリしきい値は、イネーブルにすると、デフォルトでは **gprs ggsn service** コマンドで GGSN サービスがイネーブルになった場合に使用可能なメモリ総量の 10 % となります。

gprs memory threshold コマンドを使用すると、ルータのメモリとサイズに従ってしきい値を設定できます。この値を超えると、GGSN でメモリ保護モードがアクティブになります。

システムに残っているメモリ容量が定義したしきい値に達すると、メモリ保護機能がアクティブになり、GGSN はプロセッサ メモリがしきい値を下回らないように次の手順を実行します。

- 新規の PDP コンテキストの作成要求を理由種別「No Resource」で拒否します。
- PDP コンテキストの更新を受信している既存の PDP を理由種別「Management Intervention」で廃棄します。
- ボリューム トリガーが発生した PDP を廃棄します。

（注）　メモリ保護機能がアクティブである間、バイト カウントがトラッキングされ、GGSN が回復した時点で報告されます。ただし、変更条件の中には GGSN がメモリ保護モードのときには処理されないものもあるため、一部のカウント（たとえば、Quality of Service（QoS）やタリフ条件）には正確な課金条件が反映されません。

メモリしきい値を設定し、その値に達したときには GGSN でメモリ保護機能をアクティブにするには、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)# gprs memory threshold threshold`	GGSN にしきい値を設定し、その値に達したときにはメモリ保護機能をアクティブにします。有効な範囲は、0 ～ 1024 MB です。デフォルトは、GGSN サービスがイネーブルになったときに使用可能なメモリ総量の 10% です。

課金ゲートウェイの転送プロトコルの設定

課金ゲートウェイとの通信に使用するトランスポート パス プロトコルとして、Transport Control Protocol（TCP）または User Datagram Protocol（UDP; ユーザ データグラム プロトコル）をサポートするように、GGSN を設定できます。

GGSN のデフォルト トランスポート パス プロトコルは UDP です。UDP はコネクションレス型プロトコルで、信用性の低いトランスポート方式と見なされていますが、パフォーマンスは優れています。

課金ゲートウェイ パス プロトコルとしての TCP の設定

TCP は接続ベースのプロトコルであり、パケット確認応答によって信頼性の高い伝送を実現します。

TCP をトランスポート パス プロトコルとして指定するには、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
ステップ 1	`Router(config)# gprs charging cg-path-requests 1`	パス プロトコルとして TCP を指定した場合に、GGSN が課金ゲートウェイへの TCP パスを確立するまでに待機する時間（分）を指定します。デフォルトは 0 分で、タイマーは無効になっています。
ステップ 2	`Router(config)# gprs charging path-protocol tcp`	GGSN が TCP ネットワーク プロトコルを使用して課金データを送受信することを指定します。

課金ゲートウェイ パス プロトコルとしての UDP の設定

Cisco GGSN は、デフォルトで課金ゲートウェイへのトランスポート パス プロトコルとして UDP を使用します。課金ゲートウェイを UDP トランスポート用に再設定する必要がある場合は、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)# gprs charging path-protocol udp`	GGSN が UDP ネットワーク プロトコルを使用して課金データを送受信することを指定します。デフォルト値は UDP です。

課金リリースの設定

Cisco GGSN は、2.5G と 3G Ga の両方のインターフェイス、および GPRS（R97/R98）と UMTS（R99）の Quality of Service（QoS）プロファイル フォーマットをサポートします。3GPP TS 32.215 Release 4、Release 5、または Release 7 に準拠するように、Cisco GGSN を設定できます。

99 キーワードまたは **98** キーワードを指定するときは、次の手順を実行します。

- R97/R98 CDR を提示するように GGSN を設定する（**gprs charging release 98** を設定する）場合：
  - PDP コンテキストが R98 である場合、GGSN は R97/R98 G-CDR を提示します。
  - PDP コンテキストが R99 である場合、GGSN は R99 QoS プロファイルを R97/R98 QoS プロファイルに変換し、R97/R98 G-CDR を提示します。
- R99 CDR を提示するように GGSN を設定する（**gprs charging release 99** を設定する）場合：
  - PDP コンテキストが R99 である場合、GGSN は R99 G-CDR を提示します。
  - PDP コンテキストが R98 である場合、GGSN は QoS プロファイルを変換し、R99 CDR を提示します。

（注）　Cisco GGSN リリース 9.2 以降の場合、拡張 G-CDR（eG-CDR）を生成するには、GGSN に charging release 7 を設定する必要があります。eG-CDR を生成するように GGSN を設定する方法の詳細については、「拡張 G-CDR を生成するための GGSN の設定」（P.7-4）を参照してください。

G-CDR を提示するときに GGSN が準拠する課金リリースを設定するには、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)# gprs charging release {99 | 98 | 4 | 5 | 7}`	CDR に GGSN が提示するフォーマットを設定します。 • **99** : R97、R98、R99 の各 QoS プロファイル フォーマットを提示します。 • **98** : R97/R98 QoS プロファイル フォーマットを提示します。 • **4** : GGSN は、3GPP TS 32.215 Release 4 に準拠します。 • **5** : GGSN は、3GPP TS 32.215 Release 5 に準拠します。 • **7** : GGSN は、3GPP TS 32.215 Release 7 に準拠します。 デフォルトは 99 です。 **（注）** 99 を設定した場合、G-CDR には課金特性パラメータが含まれています。**4**、**5**、または **7** を設定した場合は、Charging Characteristics Selection Mode IE が含まれています。

課金リリース設定を検証するには、**show gprs charging parameters** コマンドを使用します。

ローミング ユーザ課金の設定

ローミング ユーザ課金機能を使用すると、ローミング モバイル加入者の G-CDR を生成するように Cisco GGSN を設定できます。

Cisco GGSN は、PDP コンテキストの作成要求を受信した場合、ローミング ユーザ課金機能がイネーブルになっていると、Routing Area Identity（RAI）情報要素（IE）をチェックして、GGSN と SGSN の Public Land Mobile Network（PLMN; パブリック ランド モバイル ネットワーク）ID がともに存在し、両者が一致しているかどうかを確認します。PLMN ID が存在しないか、または存在しても一致しない場合、GGSN は SGSN Signaling Address フィールドを含む IE を、**gprs plmn ip address** コマンドに **sgsn** キーワード オプションを指定して定義した PLMN IP アドレス範囲のリストと照合します。

GGSN は、PDP コンテキストの作成要求を送信した SGSN が自身と同じ PLMN 内に配置されていないことを確認すると、G-CDR を生成します。GGSN は、SGSN が自身と同じ PLMN 内に存在することを確認すると、SGSN を別の PLMN に移動したとの通知を受信するまで CDR を生成しません。

ローミング ユーザ課金機能をイネーブルにする場合には、次の点に注意してください。

- PDP コンテキストの作成要求の RAI IE を使用して、ローミング ユーザを検出するには、グローバル コンフィギュレーション モードで **gprs mcc mn** コマンドを使用して、有効なホーム PLMN を GGSN に設定する必要があります。

  有効なホーム PLMN が設定されているか、または PLMN が有効で信頼できる PLMN である場合でも、RAI がその設定したホーム PLMN または信頼できる PLMN に一致した場合、G-CDR は生成されません。G-CDR は、RAI がホーム PLMN にも信頼できる PLMN にも一致しないすべての PDP に対して作成されます。

- RAI フィールドが PDP コンテキストの作成要求に存在せず、**gprs plmn ip address** コマンドに **sgsn** キーワード オプションを指定してアドレス範囲を設定していない場合、PDP は「未知の」パケットに分類され、ローミング ユーザとして扱われます。

- **gprs charging roamers** コマンドを使用してローミング ユーザ課金機能をイネーブルにする場合は、まず **gprs plmn ip address** コマンドを使用して PLMN の一連の IP アドレス範囲を定義する必要があります。

gprs plmn ip address コマンドと **gprs charging roamers** コマンドは次のように正しい順序で設定してください。

a. **gprs plmn ip address** コマンドを使用して、PLMN の IP アドレス範囲を設定します。IP アドレス範囲を変更する場合は、**gprs plmn ip address** コマンドを再発行します。

b. **gprs charging roamers** コマンドを使用して、GGSN でローミング ユーザ課金機能をイネーブルにします。

GGSN でローミング ユーザ課金機能をイネーブルにするには、次の作業を実行します。

- 「PLMN IP アドレス範囲の設定」（P.6-10）
- 「ローミング ユーザ課金のイネーブル」（P.6-11）

設定を検証するには、**show gprs charging parameters** コマンドを使用します。PLMN IP アドレス範囲を検証するには、**show gprs plmn ip address** コマンドを使用します。

PLMN IP アドレス範囲の設定

PLMN IP アドレス範囲の設定内容に応じて、ローミング ユーザ課金機能は次のように動作します。

- **gprs plmn ip address** *start_ip end_ip* [**sgsn**] コマンドを使用して、PLMN IP アドレス範囲を設定していない場合、GGSN と SGSN が同じ PLMN 内に存在するかどうかに関係なく、GGSN はすでに開始したすべての PDP コンテキストの G-CDR を生成します。
- **gprs plmn ip address** *start_ip end_ip* [**sgsn**] コマンドを使用して、PLMN IP アドレス範囲のリストを設定し、**sgsn** キーワードを指定してその範囲の 1 つ以上を定義した場合、GGSN は **sgsn** キーワードで定義された範囲を使用して、SGSN が同じ PLMN 内に存在するかどうかを判断します。

  次のシナリオでは、この設定を使用して、ローミング ユーザ課金機能の仕組みについて説明します。

  - MS1 は PLMN1 に加入し、PLMN2 の SGSN に接続します。MS1 は、PLMN2 から PLMN1 の GGSN に関する PDP コンテキストを開始します。このシナリオでは、MS1 はローミング ユーザであり、GGSN は SGSN が別の PLMN に存在することを確認するため CDR を生成します。
  - MS1 は PLMN1 に加入し、PLMN2 の SGSN に接続します。MS1 は、PLMN2 から PLMN2 の GGSN に関する PDP コンテキストを開始します。このシナリオでは、MS1 はローミング デバイスではなく、GGSN は SGSN と同じ PLMN 内に存在することを確認するため G-CDR を生成しません。

PLMN IP アドレス範囲を設定するには、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)# gprs plmn ip address start_ip end_ip [sgsn]`	PLMN の IP アドレス範囲を指定します。任意で、**sgsn** キーワードで定義した PLMN IP アドレス範囲だけを使用して、SGSN が GGSN とは異なる PLMN に存在するかどうかを確認することを指定できます。

ローミング ユーザ課金のイネーブル

GGSN でローミング ユーザ課金機能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)# gprs charging roamers`	GGSN でローミング ユーザ課金をイネーブルにします。

課金オプションのカスタマイズ

GGSN 課金オプションでは、デフォルト値が推奨値となります。他の任意のコマンドも、デフォルト値に設定されています。ただし、必要に応じて、または使用しているハードウェアによっては、ネットワークを最適化するためにこれらのコマンドを変更することを推奨します。

GGSN は、エコー タイミングを使用して、SGSN と外部課金ゲートウェイ間のパスを維持します。ただし、実装できるエコー タイミングの方法は、維持の対象となるすべてのパスに対して 1 つだけです。GGSN のエコー タイミングの詳細を確認したり、エコー タイミング機能を変更したりするには、「GGSN での GTP サービスの設定」の「GGSN でのエコー タイミングの設定」（P.3-4）を参照してください。

（注）　次の課金オプションは、G-CDR でも eG-CDR でも使用できます。GGSN は、課金設定に応じて eG-CDR または G-CDR を生成します。このため、GGSN 課金オプションの説明で G-CDR に言及した場合、その説明は G-CDR または eG-CDR に適用されます。

GGSN の課金処理を微調整するには、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)# gprs charging cdr-aggregation-limit` *CDR_limit*	GGSN が課金ゲートウェイ宛の課金データ転送メッセージに集約する CDR の最大数を指定します。デフォルトは 255 個です。
`Router(config)# gprs charging cdr-option apn [virtual]`	G-CDR に Access Point Name（APN; アクセス ポイント ネーム）IE を含めるように指定します。任意で、**virtual** キーワードを指定して、仮想 APN を G-CDR、アカウンティング レコード、および Credit Control Request（CCR; クレジット制御要求）に含めることもできます。
`Router(config)# gprs charging cdr-option apn-selection-mode`	G-CDR でアクセス ポイント ネーム（APN）が選択された原因コードを GGSN で提供できるようにします。
`Router(config)# gprs charging cdr-option camel-charge-info`	SGSN の CDR から Customized Application for Mobile Enhanced Logic（CAMEL）のタグおよび長さをコピーして、G-CDR に含めるように指定します。
`Router(config)# gprs charging cdr-option chch-selection-mode`	課金特性選択モード パラメータを G-CDR に含めるように指定します。
`Router(config)# gprs charging cdr-option dynamic-address`	dynamic address flag IE を G-CDR に含めるように指定します。

コマンド	目的
Router(config)# **gprs charging cdr-option imeisv**	International Mobile Equipment Identity IMEI Software Version（IMEISV）IE を G-CDR に含めるように指定します。IMEISV は、加入者が使用している移動体を識別するための情報です。
Router(config)# **gprs charging cdr-option local-record-sequence-number**	GGSN で、local record sequence number IE を G-CDR で使用できるようにします。
Router(config)# **gprs charging cdr-option ms-time-zone**	MS Time Zone（MSTZ）IE を G-CDR に含めるように指定します。MSTZ IE は、世界時と現地時間の時差を示します。 更新要求で MSTZ を変更すると、（R7 32.251 の指定に従って）CDR が閉じ、新しい CDR が開きます。また、更新要求で MSTZ の変更が発生すると、中間アカウンティング レコードが生成されます。
Router(config)# **gprs charging cdr-option nip**	Network-Initiated PDP IE を G-CDR に含めるように指定します。
Router(config)# **gprs charging cdr-option no-partial-cdr-generation [all]**	GGSN で、完全修飾部分 G-CDR を作成しないようにします。 任意で、**all** キーワード オプションを指定して、SGSN 変更制限トリガーが正しく設定されている場合には Release 4 よりも前の課金リリースのために SGSN リストをコピーするように GGSN を設定することもできます。 デフォルトでは、完全修飾部分 G-CDR の作成はイネーブルになっています。 **（注）** アクティブな PDP コンテキストがないときにだけ、この機能をイネーブルにします。この機能をイネーブルにすると、後続のすべての PDP コンテキストが影響を受けます。
Router(config)# **gprs charging cdr-option node-id**	GGSN で、G-CDR の node ID フィールドに CDR を生成したノードを指定できるようにします。
Router(config)# **gprs charging cdr-option packet-count**	GGSN で、G-CDR の任意の record extension フィールドにアップリンクとダウンリンクのパケット カウントを提供できるようにします。
Router(config)# **gprs charging cdr-option pdp-address**	G-CDR に PDP address IE を含めるように指定します。
Router(config)# **gprs charging cdr-option pdp-type**	G-CDR に PDP type IE を含めるように指定します。
Router(config)# **gprs charging cdr-option rat-type**	Radio Access Technology（RAT; 無線アクセス テクノロジー）IE を G-CDR に含めるように指定します。 RAT は、SGSN が Universal Terrestrial Radio Access Network（UTRAN）と GSM/EDGE RAN（GERAN）のどちらを使用して、User Equipment（UE; ユーザ端末）にサービスを提供するのかを示します。 PDP コンテキストの更新要求で RAT を変更すると、（R7 32.251 の指定に従って）CDR が閉じ、新しい CDR が開きます。また、更新要求で RAT の変更が発生すると、中間アカウンティング レコードが生成されます。
Router(config)# **gprs charging cdr-option served-msisdn**	GGSN で、PDP コンテキストの作成要求から Mobile Station ISDN（MSISDN; モバイル ステーション ISDN）番号を G-CDR に提供できるようにします。

コマンド	目的
Router(config)# **gprs charging cdr-option service-record** [*value*]	GGSN で、サービス単位のレコードを生成できるようにします。任意で、CDR のサービス レコードの最大数を指定することもできます。この最大数に達すると、現在の G-CDR が閉じ、新しい部分 CDR が開きます。最大数を指定していないと、デフォルト（5）が使用されます。
Router(config)# **gprs charging cdr-option sgsn-plmn**	SGSN PLMN ID を G-CDR に含めるように GGSN を設定します。 **（注）** SGSN PLMN ID は、設定すると、PDP コンテキストの作成または更新要求で SGSN から任意の RAI IE を受信した場合にだけ表示されます。
Router(config)# **gprs charging cdr-option user-loc-info**	User Location Information（ULI）IE を G-CDR に含めるように指定します。ULI は、加入者位置の Cell Global Identity（CGI; セル グローバル ID）および Service Area Identity（SAI; サービス エリア ID）を提供します。
Router(config)# **gprs charging cg-path-requests** *minutes*	パス プロトコルとして TCP を指定した場合に、GGSN が課金ゲートウェイへのパスを確立するまでに待機する時間（分）を指定します。デフォルトは 0 分で、タイマーは無効になっています。
Router(config)# **gprs charging container change-limit** *number*	GGSN から送信する G-CDR ごとに含めることができる課金コンテナの最大数を指定します。有効な値は 1 ～ 100 の数値です。デフォルトは 5 です。
Router(config)# **gprs charging container sgsn-change-limit** *number*	特定の PDP コンテキストの G-CDR を閉じるまでに SGSN に加えることができる変更の最大数を指定します。有効な値は 0 ～ 15 の数値です。デフォルトは 0 で、タイマーは無効になっています。
Router(config)# **gprs charging container time-trigger** *number*	PDP コンテキストに関するグローバルな期限を指定します。PDP コンテキストがこの期限を過ぎると、GGSN はその特定の PDP コンテキストの G-CDR を閉じて更新します。有効な値は 5 ～ 429467295（分単位）です。デフォルトは 0 で、タイマーは無効になっています。
Router(config)# **gprs charging container volume-threshold** *threshold_value*	GGSN が G-CDR を閉じて更新するまでにユーザの課金コンテナに保持する最大バイト数を指定します。有効な値は 1 ～ 4264967295 の数値です。デフォルトは 1,048,576 バイト（1 MB）です。
Router(config)# **gprs charging flow-control private-echo**	課金ゲートウェイに送信されるパケットでフロー制御を維持できるように、エコー要求にプライベートな拡張を実装します。
Router(config)# **gprs charging header short**	GGSN で、GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）の詳細ヘッダーではなく、簡易ヘッダー（6 バイトのヘッダー）を使用できるようにします。
Router(config)# **gprs charging map data tos** *tos_value*	GPRS 課金パケットの IP Type of Service（ToS; タイプ オブ サービス）マッピングを指定します。デフォルトは 3 です。
Router(config)# **gprs charging message transfer-request command-ie**	GGSN が Packet Transfer Command IE を Data Record Transfer Request メッセージに含めることを指定します。
Router(config)# **gprs charging message transfer-request possibly-duplicate**	Packet Transfer Request IE の値を 2（Send Possibly Duplicate Data Record Packet）に設定して、GGSN が Data Record Transfer Request メッセージを（以前にアクティブな課金ゲートウェイに）再送信することを指定します。
Router(config)# **gprs charging message transfer-response number-responded**	GGSN が Data Record Transfer Response メッセージの Requests Responded IE では Length フィールドではなく Number of Requests Responded フィールドを使用することを指定します。

コマンド	目的
Router(config)# **gprs charging packet-queue-size** *queue_size*	GGSN が確認応答のない課金データ転送要求をキューに保持する最大数を指定します。デフォルトは 128 パケットです。
Router(config)# **gprs charging path-protocol** {**udp** | **tcp**}	GGSN が課金データの送受信に使用するプロトコルを指定します。デフォルトは UDP です。
Router(config)# **gprs charging port** *port-num*	課金ゲートウェイの宛先ポートを設定します。デフォルトは 3386 です。
Router(config)# **gprs charging send-buffer** *bytes*	GGSN で GTP PDU メッセージおよびシグナリング メッセージを格納するためのバッファのサイズを設定します。デフォルトは 1460 バイトです。
Router(config)# **gprs charging server-switch-timer** *seconds*	宛先課金ゲートウェイが見つからないか、または使用できなくなっていると GGSN が判断し、代替課金ゲートウェイの検索に移るまでのタイムアウト値を指定します。デフォルトは 60 秒です。
Router(config)# **gprs charging tariff-time** *time*	GPRS/UMTS 課金タリフの変更時刻を指定します。デフォルトのタリフ時間はありません。 **（注）** スーパーバイザ コンソール プロンプトで **clock set** 特権 EXEC コマンドを使用してシステム ソフトウェア クロックを手動で設定した場合は、タリフ変更の発生時間を再設定する必要があります。
Router(config)# **gprs charging message transfer-request command-ie**	GGSN が Packet Transfer Command 情報要素（IE）を Data Record Transfer Response メッセージに含めることを指定します。 **（注）** Cisco GGSN が Packet Transfer Command IE をサポートする場合でも、「Send Data Record Packet」値だけが使用されます。ただし、そのためにパケットが重複してしまう可能性もあります。Cisco GGSN は、「Send Possibly Duplicated Data Record Packet」、「Cancel Data Record Packet」、「Release Data Record Packet」のいずれの値もサポートしていません。このため、課金ゲートウェイまたは課金サーバには、CDR が重複しないようにするための機能が必要です。
Router(config)# **gprs charging message transfer-response number-responded**	GGSN が Data Record Transfer Response メッセージの Requests Responded IE では Length フィールドではなく Number of Requests Responded フィールドを使用するように設定します。
Router(config)# **gprs charging reconnect** *minutes*	到達不能となっている課金ゲートウェイへの再接続を定期的に試みて、リンクのバックアップ時期を判断するように GGSN を設定します。 **（注）** 到達不能な課金ゲートウェイへの再接続を自動的に試みるように GGSN を設定する必要があるのは、UDP を課金転送プロトコルとして使用し、課金ゲートウェイがエコー要求をサポートしていないときだけです。
Router(config)# **gprs charging transfer interval** *seconds*	GGSN が課金データを課金ゲートウェイに転送するまでに待機する秒数を指定します。デフォルトは 105 秒です。

GGSN GTP オプションの設定の詳細については、「GGSN での GTP サービスの設定」の「GGSN 設定のカスタマイズ」（P.3-14）を参照してください。

課金処理の無効化

注意　**gprs charging disable** コマンドは、GGSN での課金データ処理を排除します。つまり、カスタマーにネットワーク使用料を課金するために必要なデータが、GGSN によって収集されないか、または課金ゲートウェイに送信されません。このコマンドは、実稼動 GPRS/UMTS ネットワーク環境では使用しないことを推奨します。このコマンドを使用する必要があるときは、細心の注意を払い、実稼動以外のネットワークにかぎって使用してください。

GGSN での課金を無効にできるのは、開いているすべての CDR を処理し、課金ゲートウェイに送信したあとだけです。現在の GGSN CDR をクリアするには、**clear gprs charging cdr** 特権 EXEC コマンドを使用します。

GGSN で課金処理を無効にするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# gprs charging disable`	GGSN での課金トランザクションを無効にします。

課金プロファイルの使用

課金プロファイルを作成、カスタマイズ、および指定し、それを特定のタイプのユーザのデフォルト課金方法としてグローバル レベルや APN レベルで使用すると、PDP 単位で異なる課金方法を適用できます。課金プロファイルを使用すると、提供するサービスを加入者プリファレンスにあわせて柔軟にカスタマイズできます。

課金プロファイルを使用する場合は、GGSN を次のように設定する必要があります。

- **gprs charging cdr-option chch-selection-mode** コマンドを設定して、課金特性選択モード パラメータを CDR に含めます。
- **gprs charging release** コマンドを設定して、CDR で charging characteristics selection mode IE を受信します。

GGSN 課金プロファイルを使用して PDP 単位で異なる課金方法を適用するには、次の項で説明する作業を実行する必要があります。

- 「課金プロファイルの設定」（P.6-16）
- 「課金プロファイルの課金特性およびトリガーの定義」（P.6-17）
- 「デフォルト課金プロファイルの APN への適用」（P.6-19）
- 「デフォルト課金プロファイルのグローバルな適用」（P.6-20）
- 「課金プロファイルが一致しない PDP を GGSN で処理する方法の設定」（P.6-20）

課金プロファイルの設定

課金プロファイルには、特定のタイプの加入者（ホーム、ローミング ユーザ、ビジター）に適用する課金方法を定義します。

特定の加入者タイプのデフォルトの課金方法として、APN レベルまたはグローバル レベルで課金プロファイルを適用できます。

GGSN は、最大 256 個の課金プロファイルをサポートします。それぞれに 0 ～ 255 の番号が付与されます。プロファイル 0 は、常に GGSN に存在する設定済みプロファイルです。また、グローバルなデフォルト課金プロファイルでもあります。ユーザがプロファイル 0 を作成することはありませんが、charging-related グローバル コンフィギュレーション コマンドを使用すると変更を加えることができます。プロファイル 1 ～ 255 は、Cisco GGSN 課金プロファイル コンフィギュレーション コマンドを使用して、ユーザが定義し、カスタマイズできるプロファイルです。

GGSN は、PDP コンテキストの作成要求を受信すると、次の入力源に基づいて適切な課金プロファイルを選択します。

- Charging Characteristics Selection Mode IE を介した SGSN/HLR
- ローカルなデフォルト
- 課金プロファイル インデックス AAA アトリビュート

（注） AAA から受信した課金プロファイル インデックスが有効になるのは、サービス認識課金が、GGSN でグローバル コンフィギュレーション モードの **gprs service-aware** コマンドを使用してグローバルにイネーブルになっており、かつ **service-aware** アクセス ポイント コンフィギュレーション コマンドを使用して APN レベルでもイネーブルになっている場合だけです。

このサービス認識 GGSN の設定については、第 7 章「拡張サービス認識課金の実装」を参照してください。

GGSN が PDP コンテキストの課金プロファイルを選択する順序は次のとおりです。

1. APN のオーバーライド規則に定められた課金プロファイル インデックス：デフォルト課金プロファイルが APN とグローバルの両方のレベルで設定され、SGSN の指定を上書きするようになっている場合は、APN のデフォルト課金プロファイルが優先されます。
2. ボックスのオーバーライド規則に定められた課金プロファイル インデックス：APN にデフォルト課金プロファイルが設定されていない場合は、グローバルに設定されたデフォルト課金プロファイルが使用されます。
3. AAA からの課金プロファイル インデックス。
4. SGSN/HLR からの課金プロファイル インデックス。
5. APN の非オーバーライド規則からの課金プロファイル インデックス。
6. ボックスの非オーバーライド規則からの課金プロファイル インデックス。

上記のいずれも適用されない場合、**gprs charging characteristics reject** グローバル コンフィギュレーション コマンドが設定され、PDP コンテキストの作成要求が GTP v1 であると、PDP コンテキストは拒否されます。**gprs charging characteristics reject** コマンドが設定されていない場合は、課金プロファイル 0 を使用して GTPv1 PDP コンテキストが作成されます。

（注） サービス認識 PDP では、グローバルなデフォルト課金プロファイルである課金プロファイル 0 はサポートされません。このような PDP コンテキストの作成要求は、エラー コード 199 で拒否されます。

課金プロファイルを作成または変更するには、課金プロファイル コンフィギュレーション モードを開始し、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)# **gprs charging profile** *profile-num*	新しい課金プロファイルを作成するか、または既存の課金プロファイルを変更し、課金プロファイル コンフィギュレーション モードを開始します。有効な値は 1 ～ 255 です。

課金プロファイルの課金特性およびトリガーの定義

（注） Cisco GGSN リリース 9.2 以降では、拡張クォータ サーバ インターフェイスを設定すると、Cisco GGSN はサービス認識後払いユーザ向けのクォータ サーバとして機能しません。このため、Cisco IOS リリース 12.2(22)YE2 以降では、**content** 課金プロファイル コンフィギュレーション コマンドは無視されます。同じく、後払いユーザを対象にトリガー条件を設定して拡張クォータ サーバ インターフェイスの使用を禁止する課金プロファイル コンフィギュレーション コマンドも無視されます。

拡張サービス認識課金の設定の詳細については、『*Cisco GGSN リリース 9.2 コンフィギュレーション ガイド*』を参照してください。

課金プロファイルの課金特性およびトリガーを設定するには、課金プロファイル 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(ch-prof-conf)# **category** {**hot** | **flat** | **prepaid** | **normal**}	課金プロファイルを適用する加入者のカテゴリを識別します。
Router(ch-prof-conf)# **cdr suppression**	CDR を抑制することを指定します。
Router(ch-prof-conf)# **cdr suppression prepaid**	前払い加入者の CDR を抑制することを指定します。
Router(ch-prof-conf)# **content dcca profile** *profile-name*	DCCA サーバと通信するように DCCA プロファイルを指定します。 **（注）** この設定が課金プロファイルに存在する場合は、オンライン課金を適用する必要があることを示します。DCCA プロファイルには、DCCA サーバ グループを定義します。DCCA プロファイルが課金プロファイルに定義されている場合、課金プロファイルを使用する PDP は、まず DCCA サーバに問い合せて、オンライン課金を使用するかどうかを判断する必要があります。課金プロファイルに **content dcca profile** 設定が含まれていない場合は、課金プロファイルを使用するユーザは後払い（オフライン課金）ユーザとして扱われます。

コマンド	目的
Router(ch-prof-conf)# **content postpaid** {**plmn-change** | **qos-change** | **rat-change** | **sgsn-change** | **user-loc-info-change**}	後払い加入者の課金プロファイルに条件を設定します。その条件が満たされると、GGSN は PDP コンテキストのクォータ再認可を要求します。 • **plmn-change**：パブリック ランド モバイル ネットワーク（PLMN）を変更すると、クォータ再認可要求がトリガーされます。 • **qos-change**：Quality of Service（QoS）を変更すると、クォータ再認可要求がトリガーされます。 • **rat-change**：無線アクセス テクノロジー（RAT）を変更すると、クォータ再認可要求がトリガーされます。 • **sgsn-change**：SGSN を変更すると、クォータ再認可要求がトリガーされます。 • **user-loc-info-change**：ユーザ位置情報を変更すると、クォータ再認可がトリガーされます。 （注）　**plmn-change**、**rat-change**、**user-loc-info-change** の各キーワード オプションを機能させるには、グローバル コンフィギュレーション モードで **gprs charging service record include** コマンドを使用して、これらのフィールドを CDR の service-record IE に含めるように GGSN を設定する必要があります。
Router(ch-prof-conf)# **content postpaid time** *number*	サービス認識課金がイネーブルになっている場合、後払い加入者を対象に、期限を設定します。この期限を過ぎると、GGSN はアップストリームおよびダウンストリームのトラフィック バイト カウントを収集し、特定の PDP コンテキストの G-CDR を閉じて更新します。
Router(ch-prof-conf)# **content postpaid validity** *seconds*	サービス認識課金がイネーブルになっている場合、後払い加入者を対象に、ユーザに付与されているクォータが有効になる時間を設定します。
Router(ch-prof-conf)# **content postpaid volume** *threshold*	サービス認識課金がイネーブルになっている場合、後払い加入者を対象に、GGSN が特定の PDP コンテキストのコンテナ全体で保持する最大バイト数を設定します。この数を超えると、GGSN は G-CDR を閉じて更新します。
Router(ch-prof-conf)# **content rulebase** *id*	PDP コンテキストに適用するデフォルトのルールベース ID を定義します。
Router(ch-prof-conf)# **description**	課金プロファイルの名前または簡単な説明を指定します。
Router(ch-prof-conf)# **limit duration** *number* [**reset**]	GGSN がアップストリームおよびダウンストリームのトラフィック バイト カウントを収集し、特定の PDP コンテキストの G-CDR を閉じて更新するまでの期限（分単位）を設定します。 **reset** キーワード オプションを設定した場合、時間トリガーは CDR が他のトリガーによって閉じられると再起動されます。**reset** キーワードを指定しない場合（デフォルト）、時間トリガーは（**limit volume** コマンドで設定した）ボリューム トリガーの期限が切れても再起動されませんが、他のトリガーの期限が切れると再起動されます。
Router(ch-prof-conf)# **limit volume** *number* [**reset**]	アクティブな PDP コンテキストから各 CDR に報告できる最大バイト数を設定します。この数を超えると、GGSN は CDR を閉じて更新し、GGSN でのセッションが続く間 PDP コンテキストの部分 CDR を開きます。 **reset** キーワード オプションを設定した場合、ボリューム トリガーは CDR が他のトリガーによって閉じられると起動されます。**reset** キーワードを指定しない場合、ボリューム トリガーは（**limit duration** コマンドで設定した）時間トリガーの期限が切れても再起動されませんが、他のトリガーの期限が切れると再起動されます。

コマンド	目的
`Router(ch-prof-conf)# limit sgsn-change`	課金プロファイルが、**gprs charging tariff-time** コマンドを使用して設定されたグローバルなタリフ変更を使用することを指定します。
`Router(ch-prof-conf)# tariff-time`	課金プロファイルが、**gprs charging tariff-time** コマンドを使用して設定されたグローバルなタリフ変更時間を使用することを指定します。

デフォルト課金プロファイルの APN への適用

APN に特定のタイプのユーザのデフォルト課金プロファイルを設定するには、アクセス ポイント 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-access-point)# charging profile {home | roaming | visiting | any} [trusted] profile_num [override]`	SGSN から課金特性を受信していない場合には、APN で特定のタイプのユーザのデフォルト課金プロファイルを使用するように設定します。詳細は次のとおりです。 • **home**：課金プロファイルがホーム ユーザに適用されることを指定します。 • **roaming**：課金プロファイルがローミング ユーザ（サービング GPRS サポート ノード（SGSN）パブリック ランド モバイル ネットワーク（PLMN）ID がゲートウェイ GPRS サポート ノード（GGSN）のものとは異なるユーザ）に適用されることを指定します。 • **visiting**：課金プロファイルが訪問ユーザ（IMSI に外部 PLMN ID が含まれているユーザ）に適用されることを指定します。 • **any**：課金プロファイルがあらゆるタイプのユーザに適用されることを指定します。 • **trusted**：（任意）ユーザが訪問ユーザまたはローミング ユーザ（**roaming** と **visiting** のどちらを指定するかによって異なる）であり、その PLMN ID が（**gprs mcc mnc** コマンドで設定された）信頼できるものである場合に、課金プロファイルが適用されることを指定します。 • *profile-number*：アクセス ポイントに関連付けられる課金プロファイルの番号。有効な値は 0 ～ 15 です。0 を指定した場合、課金動作がグローバルな課金特性（課金プロファイルに定義されていないもの）で定義されます。 • **overide**：（任意）PDP コンテキストの作成要求で SGSN から受信した課金特性値を無視し、代わりに APN のデフォルトを使用することを指定します。

デフォルト課金プロファイルのグローバルな適用

グローバル レベルで適用されるデフォルト課金プロファイルは、APN にデフォルト課金プロファイルが指定されていないときに使用されます。

特定のタイプのユーザのデフォルト課金プロファイルをグローバルに設定するには、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)# gprs charging profile default {home | roaming | visiting | any} [trusted] chp_num [override]`	特定のタイプのユーザのデフォルト課金プロファイルをグローバルに適用します。

課金プロファイルが一致しない PDP を GGSN で処理する方法の設定

一致するプロファイルがない GTPv1 PDP コンテキストの作成要求を拒否または受け入れるように GGSN を設定できます。このような PDP コンテキスト要求を受け入れるように GGSN を設定した場合、課金プロファイル 0 で定義されている課金方法が適用されます。GGSN は、デフォルトでは PDP コンテキストの作成要求を受け入れ、課金プロファイル 0 で定義されている課金方法を適用します。

サービス認識 PDP に選択されている課金プロファイルには、次の制約が適用されます。

- 同じユーザに属するすべての PDP が、プライマリ PDP と同じ課金プロファイルを使用する必要があります。
- サービス認識 PDP では、グローバルなデフォルト課金プロファイルである課金プロファイル 0 はサポートされません。このような PDP コンテキストの作成要求は、エラー コード 199 で拒否されます。

一致する課金プロファイルがない PDP コンテキストの作成要求を拒否するように GGSN 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)# gprs charging characteristics reject`	課金プロファイルを選択できない GTPv1 PDP コンテキストの作成要求を拒否するように GGSN を設定します。

iSCSI を使用した G-CDR のバックアップおよび取得の設定

Cisco GGSN リリース 8.0 以降では、Cisco IOS ソフトウェアの Small Computer Systems Interface over IP（iSCSI）サポートを使用して、RFC 3720 の定義に従って、Storage Area Network（SAN; ストレージ エリア ネットワーク）のストレージ ターゲットに対して CDR の保管および取得を実現しています。

ここでは、GGSN での iSCSI サポートに関する次の内容について説明します。

iSCSI の概要

iSCSI 転送プロトコルは TCP/IP 上で動作するため、モバイル事業者およびサービス プロバイダーは iSCSI インターフェイスに接続した自社の SAN を使用して、閉じた CDR も含め Data Transfer Record（DTR; データ転送レコード）メッセージ全体を保存できます。

SAN テクノロジーは主に次の要素で構成されており、カスタマーはスケーラブルなストレージ ソリューションを構築できます。

- **SCSI**：同じシステムに複数のデバイスを設置するためのインターフェイス規格であり、ケーブルで各デバイスを鎖状に接続できます。各デバイスには一意の ID（番号）が割り当てられるため、バス上で各デバイスを識別できます。SCSI ID は Logical Unit Number（LUN; 論理ユニット番号）に分割できるため、数多くのデバイスが単一の SCSI ID を共有できます。I/O 要求を発信したデバイスはイニシエータと呼ばれ、応答を発信したデバイスはターゲットと呼ばれます。
- **SAN**：ストレージからなる独自のネットワークにネットワーク ストレージを移動できるようにするためのテクノロジー。ストレージ ネットワークはスイッチおよびハブを配置してストレージ デバイスを異種サーバに接続したものであり、ディスク、テープ、および光ストレージを接続できます。

  SAN システムでは、共有ストレージ アレイに存在するデータに専用のストレージ ネットワークを介してブロック レベルでアクセスできます。
- **iSCSI**：TCP 上で SCSI 要求および応答をマッピングし、SCSI イニシエータ（次の例では Cisco GGSN）とターゲット（SAN 上のストレージ デバイス）間でブロック レベルでデータを転送できる転送プロトコル。イニシエータは、I/O 要求を送信し、ターゲットは I/O 応答を送信します。

SAN トポロジの特徴として、次の機能があります。

- ストレージは、ネットワーク クライアントに直接には接続されません。
- ストレージは、サーバに直接には接続されません。
- ストレージ デバイスは、相互に接続されています。
- 複数のサーバが複数のストレージ デバイスを共有できます。

GGSN での iSCSI バックアップおよびストレージの設定

SCSI 環境では、GGSN は iSCSI イニシエータとして機能します。

iSCSI デバイスで G-CDR バックアップ ストレージをイネーブルにするには、次の作業を実行します。

1. GGSN で、ターゲットの名前および IP アドレスを含めた iSCSI ターゲット プロファイルと、iSCSI トラフィックを「リッスンする」TCP ポートを設定します。
2. 課金ゲートウェイが使用できない場合には、レコード保管用のインターフェイスを使用するように GGSN を設定します。

Cisco GGSN リリース 9.0 以降では、最大 30 個の iSCSI ターゲット プロファイルを設定し、課金グループ内の一意の課金ゲートウェイに関連付けることができます。

このようにする代わりに、iSCSI ターゲット プロファイルを CDR のプライマリ ストレージとして設定することもできます。そのためには、グローバル レベル（デフォルト課金グループ 0）で課金ゲートウェイではなく iSCSI ターゲット プロファイルだけを設定します。また、APN レベルで設定する場合は、APN に関連付けられた課金グループ（課金グループ 1 ～ 29）に iSCSI ターゲットだけを定義します。

GGSN から送信された I/O 要求は、SCSI 要求に変換され、TCP/IP 経由でリモート ストレージ ターゲットに転送されます。

iSCSI への書き込み時のレコード フォーマットの選択

DTR を iSCSI に書き込むとき、レコードを格納するためのフォーマットはデフォルトでは「GTP」であり、DTR 全体が iSCSI ターゲットに書き込まれます。この代わりに、iSCSI レコード フォーマットを ASN.1 に設定することもできます。そのためには、グローバル コンフィギュレーション モードで **gprs charging iscsi rec-format** コマンドを使用し、**asn.1** キーワード オプションを指定します。レコード フォーマットを ASN.1 に設定した場合、GGSN は DTR 情報要素をレコードに埋め込まず、ASN1 に従ってエンコードされた未加工の CDR だけを iSCSI に書き込みます。ASN.1 フォーマットは、FTP を使用して iSCSI からレコードを取得するときに有用です。

レコード フォーマットを設定するには、グローバル コンフィギュレーション モードで **gprs charging iscsi rec-format** コマンドを使用します。

（注） ASN.1 フォーマットのレコードが生成されるのは、**gprs auto-retrieve** が GGSN で無効になっている（デフォルトの動作）ときだけです。iSCSI ターゲットが課金レコードのプライマリ ストレージとして使用されるとき（課金ゲートウェイが設定されないとき）にだけ、ASN.1 フォーマットを使用してください。

iSCSI がバックアップ ストレージとして使用される場合の DTR の書き込み

- iSCSI バックアップ ストレージ設定が所定の場所に配置されており、課金ゲートウェイに到達できない場合、iSCSI への書き込みが開始されます。DTR メッセージ全体が、ターゲット プロファイルに定義された iSCSI ターゲットに送信されます。
- iSCSI をバックアップとして使用している場合に推奨する iSCSI レコード フォーマットは GTP（デフォルトのフォーマット）です。iSCSI の自動取得（**gprs auto-retrieve** グローバル コンフィギュレーション コマンド）がイネーブルになっている場合は、レコード フォーマットを GTP に設定する必要があります。
- iSCSI 自動取得がイネーブルになっている場合、GGSN は DTR メッセージ全体を送信するとともに、メッセージの前に 12 バイトのヘッダーを追加してから SAN に格納します。このヘッダーは、DTR を取得して課金ゲートウェイに送信するときに使用されます（また、RSM レイヤはメッセージに 12 バイトのヘッダーおよび 4 バイトのトレーラを追加して格納します）。

（注） FTP など他の手段で SAN から DTR を直接取得する場合は、レコードごとに 10 バイトのヘッダーをスキップして、エンコードされた CDR が含まれている実際の DTR を得る必要があります。

iSCSI がプライマリ ストレージとして使用される場合の DTR の書き込み

- 課金ゲートウェイが設定されておらず、iSCSI ターゲット プロファイルだけがグローバル課金レベル（課金グループ 0）または粒状課金レベル（課金グループ 1 ～ 29）で定義されている場合は、iSCSI が課金レコードを書き込むためのプライマリ ストレージとなります。
- iSCSI レコード フォーマットはどれでも使用できますが、ASN.1 iSCSI レコード フォーマットを使用すると、ヘッダーを追加することなく、ASN1 に従ってエンコードされた未加工の CDR を iSCSI に格納できます。

CDR の読み取り

- iSCSI バックアップ ストレージ設定が所定の場所にあると、課金ゲートウェイが稼動した場合、iSCSI イニシエータ（GGSN）は iSCSI ターゲットから iSCSI レコードを受信するように要求します。
- GGSN がレコードを受信すると、書き込みの処理時に GGSN が追加した 12 バイトのヘッダーが削除され、DTR 全体が課金ゲートウェイに送信されます。

DTR を課金ゲートウェイに送信する前に、重複の可能性ありとのマークを DTR に付与する場合は、次の課金コンフィギュレーション コマンドで GGSN を設定する必要があります。

- **gprs charging message transfer-request command-ie**
- **gprs charging message transfer-request possibly-duplicate**

iSCSI の制限

GGSN に iSCSI CDR バックアップおよびストレージを設定する場合は、次の点に注意してください。

- iSCSI ターゲットは動的に検出できません。
- iSCSI セッションあたりの TCP 接続の数は、1 つに制限されます。
- iSCSI ターゲット デバイスは、あらかじめフォーマットしておく必要があります。LUN ごとに、FAT32 パーティションを 1 つだけにする必要があります。
- LUN の最大サイズは、2TB までとする必要があります。これが、FAT32 ファイル システムでサポートされている最大ディスク サイズとなります。

GGSN に iSCSI CDR バックアップおよびストレージを設定する場合は、次の項の作業を実行します。

- 「iSCSI ターゲット プロファイルの設定」（P.6-23）
- 「iSCSI ターゲット プロファイルの関連付け」（P.6-24）
- 「iSCSI セッションの検証」（P.6-24）

iSCSI ターゲット プロファイルの設定

（注）　GGSN では、最大 30 個の iSCSI プロファイルを設定できます。ただし、プロファイルごとにターゲットを 1 つだけ定義できます。また、グローバル コンフィギュレーション モードで **gprs iscsi** コマンドを使用すると、GGSN にプロファイルを関連付けて iSCSI インターフェイスを使用できますが、一度に 1 つのプロファイルにかぎられます。

GGSN に iSCSI ターゲット プロファイルを設定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip iscsi target-profile target_profile_name`	GGSN でターゲットの iSCSI ターゲット プロファイルを作成し、iSCSI インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-iscsi)# name target name`	（必須）iSCSI ターゲットの名前。
ステップ 3	`Router(config-iscsi)# ip ip_address`	（必須）iSCSI ターゲットの IP アドレス。
ステップ 4	`Router(config-iscsi)# port tcp port`	（必須）ターゲット上の TCP「リスリング」ポートの番号。デフォルトは 3260 です。
ステップ 5	`Router(config-iscsi)# source-interface loopback_interface_number`	（任意）ループバック インターフェイスの番号（iSCSI トラフィックで別のソース インターフェイスを使用する場合）。
ステップ 6	`Router(config-iscsi)# vrf vrf_name`	（任意）VPN ルーティングおよび転送（VRF）インスタンスの名前（iSCSI トラフィックで Virtual Private Network（VPN; バーチャル プライベート ネットワーク）が必要になる場合）。
ステップ 7	`Router(config-iscsi)# exit`	iSCSI 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。

（注）　**name**、**ip**、**port** の各 iSCSI インターフェイス サブ設定は必須です。ターゲット プロファイルに設定できる任意の設定をすべて記載したリストについては、iSCSI インターフェイス コンフィギュレーション モードで「**?**」コマンドを発行するか、または『*Cisco GGSN Release 9.0 Command Reference*』で **ip iscsi target-profile** コマンドの説明を参照してください。

iSCSI ターゲット プロファイルの関連付け

使用できる課金ゲートウェイがない場合に CDR ストレージの iSCSI インターフェイスを使用するように GGSN 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)# gprs iscsi target_profile_name`	レコード保管用の iSCSI プロファイルを使用するように GGSN を設定します。 （注）　一度に 1 つのプロファイルだけを定義できます。 （注）　指定するプロファイル名は、**ip iscsi target-profile** コマンドを使用して設定したものと同じである必要があります。

iSCSI セッションの検証

iSCSI セッションが稼動していることを検証するには、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# show ip iscsi session`	iSCSI セッションのステータスを表示します。

iSCSI CDR バックアップおよびストレージのモニタリングおよびメンテナンス

GGSN で iSCSI バックアップおよびストレージ機能をモニタリングおよびメンテナンスするには、次のコマンドを使用できます。

コマンド	目的
`Router# clear gprs iscsi statistics`	GGSN iSCSI 処理統計情報をクリアします。
`Router# clear ip iscsi statistics`	iSCSI 処理統計情報をクリアします。
`Router# clear record-storage-module`	レコード保管モジュール統計情報をクリアします。
`Router# show ip iscsi name`	iSCSI イニシエータの名前を表示します。
`Router# show ip iscsi session`	iSCSI セッションのステータスを表示します。
`Router# show ip iscsi stats`	iSCSI および SCSI レイヤ統計情報を表示します。
`Router# show ip iscsi target`	iSCSI ターゲットの詳細を表示します。

コマンド	目的
Router# **show record-storage-module stats**	レコード保管モジュール統計情報を表示します。
Router# **show record-storage-module target-info** [**all** | **target-profile** *profile_name*]	使用可能なすべてのディスクとそのステータス、またはターゲット プロファイルで定義されているディスクを表示します。

粒状課金およびストレージの設定

Cisco GGSN は、デフォルトのグローバル課金設定に加えて、アクセス ポイント レベルの課金設定（粒状課金）もサポートします。

粒状課金では、GGSN ごとに最大 30 個の*課金グループ*を設定できます。課金グループごとに、APN、一意のプライマリ、セカンダリ、ターシャリの課金ゲートウェイ、および iSCSI ターゲットを定義し、割り当てることができます。課金グループを使用すると、課金レコードを所属先の APN ごとに異なる宛先に送信できます。

APN に課金グループを割り当てないと、デフォルト課金グループ（グローバル レベルで設定したプライマリ、セカンダリ、ターシャリの課金ゲートウェイ、iSCSI ターゲット、プライオリティ スイッチオーバーなど）が使用されます。

課金グループ 0 が、グローバル レベルで定義されるデフォルト課金グループです。課金グループ 1 ～ 29 を設定し、関連付けることができます。

使用上の注意

粒状課金およびストレージを設定する場合は、次の点に注意してください。

- GGSN ごとに最大 30 個の課金グループを設定し、APN に割り当てることができます。0 値は、グローバル課金ゲートウェイおよびグローバル iSCSI ターゲット（設定している場合）が含まれているデフォルトのグローバル課金グループ用に予約されています。他の課金グループを定義するには、値 1 ～ 29 を使用できます。
- デフォルトでは、APN に課金グループ（課金グループ 1 ～ 29）を割り当てていないかぎり、すべての APN がデフォルトのグローバル課金グループ 0 を使用します。
- 同じ課金グループを複数の APN に割り当てることができますが、APN ごとに 1 つの課金グループだけを割り当てることができます。
- 課金ゲートウェイは 1 つの課金グループだけに割り当てることができます。課金ゲートウェイは、プライマリ、セカンダリ、ターシャリのいずれのゲートウェイとして定義しているかどうかに関係なく、グループで共有できません。
- iSCSI ターゲットは 1 つの課金グループだけに割り当てることができます。iSCSI は、グループで共有できません。
- 1 つの課金グループ内で課金ゲートウェイのスイッチオーバーが発生した場合、グローバル設定（課金グループ 0）と同じ優先順位が保持されます。つまり、プライマリ課金ゲートウェイ、セカンダリ課金ゲートウェイ、ターシャリ課金ゲートウェイ、iSCSI ターゲットの順となります。
- APN に課金グループを割り当てると、課金グループ内でだけ APN のスイッチオーバーが発生します。APN は、グローバルに設定した課金ゲートウェイまたは iSCSI ターゲットにはフォールバックしません。
- APN に空の課金グループ（課金ゲートウェイも iSCSI ターゲットも定義していないグループ）を割り当てた場合、**service-mode maintenance** 課金グループ コンフィギュレーション コマンドで課金グループをメンテナンス モードにしないかぎり、その APN の CDR は生成されません。

- 課金グループに iSCSI ターゲットだけを定義した場合、グローバルに設定した iSCSI ターゲットへのフォールバックは発生しません。
- 割り当てた課金グループで APN に iSCSI ターゲットを定義していない場合、その APN はグローバルに設定した iSCSI プロファイルにフォールバックできません。このため、APN の iSCSI バックアップおよびストレージをイネーブルにするには、APN に割り当てた課金グループに iSCSI ターゲットが定義されていることを確認してください。
- iSCSI ターゲットをバックアップ デバイスとしてではなく、APN の課金レコードのプライマリ ストレージ デバイスとして使用するには、その APN に関連付けられた課金グループに iSCSI ターゲットだけを定義します。
- 自動取得（**gprs auto-retrieve** グローバル コンフィギュレーション コマンド）は、グローバル レベル（デフォルト課金グループ 0）でだけサポートされます。自動取得は、APN 課金グループ レベル（グループ 1 ～ 29）ではサポートされません。
- 設定した iSCSI レコード フォーマットは、すべての課金グループに適用されます。
- 各課金グループを個別にメンテナンス モードまたは運用モードにすることができます。課金グループを変更する場合（課金ゲートウェイまたは iSCSI ターゲットを追加または削除する場合）は、まず **service-mode** 課金グループ コンフィギュレーション コマンドを使用してそのグループをメンテナンス モードにします。
- 課金グループがメンテナンス モードになると、そのグループで保留中の DTR がグループの課金メンテナンス キューに移動します。課金グループが運用モードに戻ると、グループ メンテナンス キューに保留中のメッセージ、または課金グループを使用して APN 用に開いている CDR が、次の順序に基づいて課金パスまたは iSCSI キューに移動します。
  - 課金グループに課金ゲートウェイが定義されている場合、保留中のメッセージおよび開いている CDR は、プライオリティが最も高い課金ゲートウェイのパスに移動します。
  - 課金ゲートウェイは定義されていないものの、iSCSI ターゲットは定義されている場合、保留中のメッセージおよび開いている CDR は iSCSI 書き込みキューに移動します。
  - 課金ゲートウェイも iSCSI ターゲットも課金グループに定義されていない場合、そのグループの保留中のメッセージまたは開いている CDR があると、グループは運用モードに移行できません。

（注） 課金グループが空で運用モードになっている場合、そのグループの CDR は生成されません。

粒状課金を設定するには、次の項の作業を実行します。

- 「課金グループの設定」（P.6-27）
- 「課金グループのアクセス ポイントへの関連付け」（P.6-28）
- 「課金グループの変更」（P.6-28）
- 「粒状課金のモニタリングおよびメンテナンス」（P.6-28）

粒状課金およびストレージを設定するには、次の項の作業を実行します。

- 「課金グループの設定」（P.6-27）
- 「課金グループのアクセス ポイントへの関連付け」（P.6-28）
- 「課金グループの変更」（P.6-28）

課金グループの設定

課金グループを設定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# gprs charging group group-number`	課金グループを定義または変更します。 *group-number* は 1 ～ 29 の値です。 **（注）** 0 値は、グローバル課金ゲートウェイおよびグローバル iSCSI ターゲット（定義している場合）が含まれているデフォルト課金グループ用に予約されています。他の課金グループを定義するには、値 1 ～ 29 を使用できます。
ステップ 2	`Router(config-chrg-group)# description description`	課金ゲートウェイ グループの定義です。
ステップ 3	`Router(config-chrg-group)# primary {ip-address | name}`	グループのプライマリ課金ゲートウェイを指定します。詳細は次のとおりです。 • *ip-address*：プライマリ課金ゲートウェイの IP アドレスを指定します。 • *name*：プライマリ課金ゲートウェイのホスト名を指定します。
ステップ 4	`Router(config-chrg-group)# secondary {ip-address | name}`	グループのセカンダリ課金ゲートウェイを指定します。詳細は次のとおりです。 • *ip-address*：セカンダリ課金ゲートウェイの IP アドレスを指定します。 • *name*：セカンダリ課金ゲートウェイのホスト名を指定します。
ステップ 5	`Router(config-chrg-group)# tertiary {ip-address | name}`	グループのターシャリ課金ゲートウェイを指定します。詳細は次のとおりです。 • *ip-address*：ターシャリ課金ゲートウェイの IP アドレスを指定します。 • *name*：ターシャリ課金ゲートウェイのホスト名を指定します。
ステップ 6	`Router(config-chrg-group)# switchover priority`	プライオリティの高いゲートウェイがアクティブになったときには課金グループ内のそのゲートウェイに切り替わるように、GGSN を設定します。
ステップ 7	`Router(config-chrg-group)# iscsi iscsi-profile-name`	すべての課金ゲートウェイがダウンしている場合には、CDR バックアップの iSCSI ターゲットを指定します。
ステップ 8	`Router(config-chrg-group)# service-mode [maintenance | operational]`	課金グループをメンテナンス モードまたは運用モードにします。デフォルトは運用モードです。
ステップ 9	`Router(config-chrg-group)# exit`	課金グループ コンフィギュレーション モードを終了します。

課金グループのアクセス ポイントへの関連付け

課金グループの設定を終えたら、そのグループを APN に割り当てます。

課金グループを APN に割り当てるには、アクセス ポイント 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-access-point)# charging group chrg-group-number`	既存の課金グループを APN に割り当てます。*group-number* は 1 ～ 29 のいずれかの数字です。

課金グループの変更

課金グループを変更する場合は、まず課金グループをメンテナンス モードにします。

課金グループをメンテナンス モードにするには、課金グループ 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-chrg-group)# service-mode maintenance`	課金グループをメンテナンス モードにします。

変更後、課金グループを運用モードに戻すには、課金グループ 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-chrg-group)# service-mode operational`	課金グループを運用モードにします。

粒状課金のモニタリングおよびメンテナンス

GGSN で粒状課金をモニタリングおよびメンテナンスするために使用できるコマンドを次に示します。

コマンド	目的
`Router# clear gprs charging cdr charging-group`	CDR をクリアします。
`Router# clear gprs iscsi statistics`	現在の GPRS 関連の iSCSI 統計情報をクリアします。
`Router# show gprs access-point`	GGSN のアクセス ポイントに関する情報を表示します。
`Router# show gprs charging parameters charging-group`	GGSN の累積課金統計情報を表示します。
`Router# show gprs charging statistics`	GGSN の現在の課金統計情報を表示します。
`Router# show gprs charging status`	GGSN の現在の課金統計情報を表示します。
`Router# show gprs charging summary`	GGSN に定義されているすべての課金グループの概要を表示します。

（注）　上記に挙げた **clear** と **show** のコマンドの多くが、課金グループに固有の情報をクリアおよび表示できるように、**charging-group** キーワード オプションで拡張されています。

GGSN での課金機能のモニタリングおよびメンテナンス

ここでは、GGSN の課金機能をモニタリングするために使用できる **show** コマンドの要約を示します。

GGSN での課金をモニタリングおよびメンテナンスするには、次の特権 EXEC コマンドを使用します。

コマンド	目的
Router# **show gprs charging parameters**	現在の GGSN 課金設定に関する情報を表示します。
Router# **show gprs service-mode**	GGSN の現在のグローバル サービス モード状態と、状態の最終変更時刻を表示します。
Router# **show gprs charging statistics**	GGSN と課金ゲートウェイ間での課金パケットの転送に関する累積統計情報を表示します。

設定例

GGSN に実装した課金設定の例を次に示します。

グローバル課金設定

GGSN 設定

```
Router# show running-config
Building configuration...

Current configuration :7390 bytes
!
! Last configuration change at 16:56:05 UTC Wed Jun 25 2003
! NVRAM config last updated at 23:40:27 UTC Fri Jun 13 2003
!
version 12.3
.....
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
.....
ip route 40.1.2.1 255.255.255.255 10.1.1.1
!
gprs access-point-list gprs
  access-point 1
   access-point-name auth-accounting
   access-mode non-transparent
   aaa-group authentication first
   aaa-group accounting second
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.60.0.1
   dhcp-gateway-address 10.60.0.1
   exit
   !
. . .
!
gprs default charging-gateway 10.9.0.2
```

```
gprs charging send-buffer 1000
gprs charging container volume-threshold 500000
gprs charging container change-limit 3
gprs charging cdr-aggregation-limit 10
gprs charging cdr-option apn-selection-mode
gprs charging cdr-option served-msisdn
!
gprs memory threshold 512
!
. . .
!
end
```

スーパーバイザ エンジン設定

```
Sup# show running-config
Building configuration...

Current configuration :12672 bytes
!
version 12.2
...
interface FastEthernet8/22
 no ip address
 switchport
 switchport access vlan 302
!
interface Vlan101
 description Vlan to GGSN for GA/GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
```

課金プロファイル設定

次の設定例は、GGSN に設定された課金プロファイルを 2 つ示しています（課金プロファイル 1 と課金プロファイル 2）。課金プロファイル 1 は、課金プロファイルが APN に指定されていない場合に、「あらゆる」タイプのユーザに使用されるグローバルなデフォルト課金プロファイルとして設定されています。

```
Router# show running-config
Building configuration...

Current configuration :7390 bytes
!
! Last configuration change at 16:56:05 UTC Wed Jun 25 2003
! NVRAM config last updated at 23:40:27 UTC Fri Jun 13 2003
!
version 12.3
.....
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
.....
ip route 40.1.2.1 255.255.255.255 10.1.1.1
!
```

```
!
. . .
!
gprs charging profile default any 1

gprs charging profile 1
 description "roamer_profile"
 limit volume 500000 reset
 limit duration 30 reset
!
gprs charging profile 2
 description "any_unmatched"
 limit volume 1000000 reset
 limit duration 60 reset
. . .
!
. . .
!
end
```

粒状課金およびストレージ設定

次の設定例は、GGSN に設定された課金グループを 2 つ示しています（課金グループ 1 と課金グループ 2）。iSCSI ターゲットが課金グループ 1 に定義されています。課金グループ 1 は、アクセス ポイント 4 およびアクセス ポイント 5 に関連付けられています。

```
Router# show running-config
Building configuration...

Current configuration :7390 bytes
.....
!
gprs access-point-list gprs
access-point 4
access-point-name test2
charging group 1
!
access-point 5
access-point-name pppregen
charging group 1
ppp-regeneration
!
!
!
gprs charging group 2
primary 66.66.66.1
secondary 66.66.66.2
tertiary 66.66.66.3
!
gprs charging group 1
primary 55.55.55.1
secondary 55.55.55.2
tertiary 55.55.55.3
iscsi ISCSI_TARGET1
switchover priority
!
gprs iscsi TARGET_LINUX
```

CHAPTER 7

拡張サービス認識課金の実装

この章では、Cisco Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）をサービス認識 GGSN として実装する方法について説明します。サービス認識 GGSN では、前払い加入者のリアルタイムのクレジット制御、および前払い加入者と後払い加入者のサービス認識課金が可能になります。

（注） サービス認識 GGSN 機能は、IPv4 Packet Data Protocol（PDP; パケット データ プロトコル）コンテキストだけでサポートされます。

この章に記載されている GGSN コマンドの詳細については、使用している Cisco GGSN リリースの『*Cisco GGSN Command Reference*』を参照してください。この章に記載されているその他のコマンドのマニュアルを参照するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

この章は、次の内容で構成されています。

サービス認識 GGSN の概要

Cisco GGSN と Cisco Content Services Gateway - 2nd Generation（CSG2）を一緒に実装すると、サービス認識 GGSN として機能します。

サービス認識 GGSN を実装する方法は 2 つあります。1 つは、Cisco IOS Diameter プロトコル/Diameter Credit Control Application（DCCA）サポートによる Cisco GGSN と Cisco CSG2 設定を GGSN 上で使用する方法です。もう 1 つは、Online Charging Service（OCS; オンライン課金サービス）アドレス サポートによる Cisco GGSN と Cisco CSG2 設定を使用してサービス認識 GGSN を GGSN で実装する方法です。

サービス認識 GGSN 実装では、Cisco CSG2 および GGSN は次の機能を提供します。

- Cisco CSG2
  - パケットの検査、およびトラフィックの分類
  - クォータの要求、および使用状況の報告
  - 課金プラン、サービス名、およびコンテンツ定義の提供
  - 非 DCCA トラフィック用の Remote Authentication Dial-In User Service（RADIUS）プロキシとして機能
  - 各サービス フロー課金記録の前払いモードで機能

  Cisco CSG2 の設定の詳細については、『*Cisco Content Services Gateway - 2nd Generation Installation and Configuration Guide*』を参照してください。

  http://www.cisco.com/en/US/products/sw/wirelssw/ps779/products_configuration_guide_book09186a0080856678.html
- Diameter/DCCA を使用して実装した場合の GGSN
  - Cisco CSG2 へのクォータ サーバとして機能
  - クォータ要求および応答用の Diameter インターフェイスを DCCA サーバに提供
  - Cisco CSG2 によって要求され、DCCA サーバから受信したクォータの管理
  - Cisco CSG2 課金プランへの DCCA サーバ ルールベースのマッピング
  - Cisco CSG2 サービス クォータへの DCCA サーバ カテゴリ クォータのマッピング
- OCS アドレス選択サポートとともに実装した場合、GGSN は後払い加入者のクォータ サーバとしてだけ機能します。OCS アドレス選択サポートによって、Cisco CSG2 が直接接続する外部 OCS は、前払い加入者のオンライン クレジット制御を提供できます。

サービス認識 GGSN を実装するには、次の項の作業を実行します。

- 「制限事項および制約事項の確認」（P.7-3）
- 「サービス認識課金のサポートのイネーブル」（P.7-3）（必須）
- 「待機アカウンティングの設定」（P.7-4）（サービス認識課金サポートが Access Point Name（APN; アクセス ポイント ネーム）でイネーブルになっている場合は必須）
- 「拡張 G-CDR を生成するための GGSN の設定」（P.7-4）（必須）
- 「Cisco GGSN でのクォータ サーバ サポートの設定」（P.7-5）（必須）
- 「Diameter/DCCA サポートによるサービス認識課金の実装」（P.7-12）
  （OCS アドレス選択サポートがイネーブルになっていない場合は必須）
- 「OCS アドレス選択サポートによるサービス認識課金の実装」（P.7-28）
  （Diameter/DCCA サポートが設定されていない場合は必須）
- 「課金プロファイルの拡張課金パラメータの設定」（P.7-25）（必須）
- 「サービス認識 PDP の GTP セッション冗長性の概要」（P.7-33）

制限事項および制約事項の確認

拡張サービス認識課金を実装する前に、次の点に注意してください。

- セッション冗長性が必要な場合、GGSN では、ユーザごとに最大 21 のカテゴリがサポートされます。
- Known User Table（KUT）エントリに PDP コンテキスト ユーザ情報を読み込むには、RADIUS アカウンティングを Cisco CSG と GGSN 間でイネーブルにする必要があります。
- Cisco CSG2 は、すべての GGSN インスタンスのクォータ サーバ アドレスを使用して設定する必要があります。
- DCCA を使用する場合、Cisco CSG 上のサービス ID は、DCCA サーバ上のカテゴリ ID と一致する数値ストリングとして設定する必要があります。
- RADIUS を使用しない場合、Cisco CSG2 を GGSN 上の RADIUS プロキシとして設定する必要があります。
- Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）では、GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）N3 要求と T3 再送信の数に設定されている値は、使用可能なすべてのサーバ タイマー（RADIUS、DCCA、および Cisco CSG2）の合計よりも大きい必要があります。

  特に、SGSN N3*T3 は次の値よりも大きい必要があります。

  2 x RADIUS タイムアウト + *N* x DCCA タイムアウト + Cisco CSG2 タイムアウト

  上記の意味を次に示します。

  - 2 は、認証とアカウンティングの両方を示します。
  - *N* は、サーバ グループで設定されている Diameter サーバの数を示します。
- APN でサービス認識課金サポートをイネーブルにする場合は、PDP コンテキストの作成応答を SGSN に送信する前に RADIUS アカウンティング応答を待機するように GGSN を設定する必要があります。

サービス認識課金のサポートのイネーブル

Cisco GGSN でサービス認識課金機能を実装する前に、GGSN で拡張サービス認識課金サポートをイネーブルにする必要があります。

GGSN でサービス認識課金サポート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 モードで次の作業を実行します。

コマンド	目的
`Router(config)# gprs service-aware`	GGSN がサービス認識課金をサポートできるようにします。

特定のアクセス ポイントでサービス認識課金サポートをイネーブルにするには、アクセス ポイント コンフィギュレーション モードで次の作業を実行します。

コマンド	目的
`Router(access-point-config)# service-aware`	APN がサービス認識課金をサポートできるようにします。

（注）　APN でサービス認識課金サポートをイネーブルにする場合は、PDP コンテキストの作成応答を SGSN に送信する前に RADIUS アカウンティング応答を待機するように GGSN を設定する必要があります。RADIUS アカウンティング応答を待機するように GGSN を設定する方法については、「待機アカウンティングの設定」（P.7-4）を参照してください。

待機アカウンティングの設定

サービス認識課金が APN でイネーブルになっている場合は、GGSN で待機アカウンティングを設定する必要があります。待機アカウンティングを GGSN で設定した場合、GGSN は、PDP コンテキストの作成応答を SGSN に送信する前に、RADIUS アカウンティング応答を待機します。

GGSN で待機アカウンティ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 モードで次の作業を実行します。

コマンド	目的
`Router(config)# gprs gtp response-message wait-accounting`	PDP コンテキストの作成応答を SGSN に送信する前に RADIUS アカウンティング応答を待機するように GGSN を設定します。

（注）　待機アカウンティングは、eGGSN 実装の場合は必須ですが、スタンドアローン GGSN クォータ実施の場合は任意です。

拡張 G-CDR を生成するための GGSN の設定

G-Call Detail Record（CDR; 呼詳細レコード）には、PDP コンテキストの全期間または一部の期間に関する情報が含まれています。G-CDR には、加入者（MSISDN、IMSI）、使用されている APN、適用される Quality of Service（QoS）、SGSN ID（モバイル アクセスの場所として）、タイム スタンプと期間、アップストリームとダウンストリームの方向別に記録されるデータ量、および中間 CDR 生成の量しきい値やタリフ時間切り替えなどの情報が含まれています。

enhanced G-CDR（eG-CDR; 拡張 G-CDR）には、上記の情報以外に、カテゴリ ID で指定された、PDP セッションで使用される各サービス フローの使用状況データを含むサービス レコード Information Element（IE; 情報エレメント）も含まれています。たとえば、アップストリームとダウンストリームの量、および期間がサービス フローごとに記録されます。

デフォルトでは、GGSN では G-CDR にサービス レコードは組み込まれません。サービル認識 GGSN 実装をサポートするには、G-CDR を生成するように GGSN を設定する必要があります。これを行うには、G-CDR にサービス レコードを組み込むように GGSN を設定します。

（注）　Cisco GGSN リリース 9.2 以降では、拡張 G-CDR（eG-CDR）を生成する場合、**gprs charging release 7** グローバル コンフィギュレーション コマンドを使用して、GGSN で charging release 7 が設定されている必要があります。

G-CDR にサービス レコードを含めるように GGSN 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)# gprs charging cdr-option service-record [1-100]`	G-CDR にサービス レコード IE を含めるように GGSN を設定し、G-CDR を閉じて G-CDR の一部を開くまでに G-CDR が保持できる最大サービス レコード数を指定します。有効な値は 1 ～ 100 の数値です。デフォルトは 5 です。

eG-CDR にサービス レコード IE の Public Land Mobile Network（PLMN; パブリック ランド モバイル ネットワーク）ID、Radio Access Technology（RAT; 無線アクセス テクノロジー）、または User Location Info の各フィールドを含めるように GGSN 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)# gprs charging service-record include [plmn-id | rat | user-loc-info-change]`	eG-CDR にサービス レコード IE の特定のフィールドを含めるように GGSN を設定します。それぞれの意味を次に示します。 • **plmn-id**：PLMN-ID フィールドを含めるように GGSN を設定します。 • **rat**：RAT フィールドを含めるように GGSN を設定します。RAT は、SGSN が User Equipment（UE; ユーザ端末）Universal Mobile Telecommunication System（UMTS）または Global System for Mobile communication（GSM）/EDGE RAN（GERAN）にサービスを提供するかどうかを示します。 • **user-loc-info-change**：User-Location-Info フィールドを含めるように GGSN を設定します。

Cisco GGSN でのクォータ サーバ サポートの設定

GGSN でクォータ サーバ サポートを設定するには、次の項の作業を実行します。

- 「Cisco CSG2 サーバ グループの設定」（P.7-6）（必須）
- 「GGSN でのクォータ サーバ インターフェイスの設定」（P.7-6）（必須）
- 「Cisco CSG2 を認証およびアカウンティング プロキシとして使用するための GGSN の設定」（P.7-10）（RADIUS が使用されていない場合は必須）
- 「クォータ サーバから CSG2 への設定のモニタリングとメンテナンス」（P.7-11）

Cisco CSG2 サーバ グループの設定

GGSN 上でクォータ サーバ プロセスと対話する場合は、2 つの Cisco CSG2（1 つはアクティブ、もう 1 つはスタンバイ）を 1 つとして機能させることを推奨します。

GGSN クォータ サーバ インターフェイスが Cisco CSG2 との通信に使用する Cisco CSG2 グループを設定する場合、冗長ペアを構成する各 Cisco CSG2 の実 IP アドレスとともに、仮想 IP アドレスを指定する必要があります。GGSN 上のクォータ サーバ プロセスは仮想アドレスと通信し、アクティブ Cisco CSG2 はその仮想 IP アドレスをリッスンします。

GGSN で Cisco CSG2 グループを設定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ggsn csg csg-group-name`	Cisco CSG2 サーバ グループの名前を指定し、Cisco CSG2 グループ コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-csg-group)# virtual-address ip-address`	Cisco CSG2 グループの仮想 IP アドレスを指定します。これは、GGSN 上のクォータ サーバ プロセスが Cisco CSG2 との通信に使用する IP アドレスです。
ステップ 3	`Router(config-csg-group)# port port-number`	（任意）クォータ サーバからの通信を Cisco CSG2 が受信するポートを設定します。デフォルトは 3386 です。 **（注）** Cisco CSG2 は、常にポート 3386 でクォータ サーバにメッセージを送信します。
ステップ 4	`Router(config-csg-group)# real-address ip-address`	Cisco CSG2 からの着信メッセージの発信元チェック用に実 Cisco CSG2 の IP アドレスを設定します。冗長ペアを構成している各 Cisco CSG2 の実 IP アドレスを設定します。

GGSN でのクォータ サーバ インターフェイスの設定

Cisco GGSN リリース 9.2 以前のリリースでは、GGSN は、クォータ サーバ インターフェイスを Cisco CSG2 とのクォータ サーバ メッセージ交換に使用して使用状況情報を取得し、次のタイプのユーザの eG-CDR を生成します。

- サービス認識前払い（Gy）ユーザおよびサービス認識後払い（QS）ユーザ

  前払い加入者、または CSG2 で前払いとして設定されている後払い加入者の場合、GGSN はクォータ サーバとして機能し、クォータ サーバ インターフェイスを介して CSG2 から使用状況を受信するたびにサービス コンテナを eG-CDR に追加します。

Cisco GGSN リリース 9.2 以降では、**ggsn quota-server** コマンドの **service-msg** キーワード オプションを指定して、GGSN と Cisco CSG2 との間に*拡張*クォータ サーバ インターフェイスを設定できます。拡張クォータ サーバ インターフェイスは、サービス コントロール メッセージの交換をサポートします。サービス コントロール メッセージに含まれるサービス使用状況情報を使用して、GGSN では、次の追加タイプのユーザ用 eG-CDR を生成できます。

- サービス認識前払い（GTP）ユーザ

  OCS アドレス選択を使用して実装されたサービス認識 GGSN では、GGSN は前払いユーザのクォータ サーバとして機能しません。OCS アドレス選択サポートによって、Cisco CSG2 は、GTP による直接接続が可能な外部 OCS からクォータを取得できます。GGSN は、拡張クォータ サーバ インターフェイス経由でサービス使用状況を取得して、eG-CDR を生成します。

- サービス認識後払いユーザ

  GGSN は、サービス認識後払いユーザのクォータ サーバとして機能しません。GGSN は、拡張クォータ サーバ インターフェイスを使用して、Cisco CSG2 から使用状況を取得し、その使用状況を eG-CDR に追加します。

- Policy and Charging Control（PCC; ポリシー / 課金制御）対応（Gx）ユーザ

  Gx 対応ユーザが前払い（Gy）ユーザでもある場合は、eG-CDR 生成のサポートが Cisco IOS リリース 12.4(22)YE2 以前のリリースに存在しており、クォータ サーバ メッセージで受信した使用状況に基づいてサービス コンテナが eG-CDR に追加されます。

  Gx ユーザが、CSG2 と OCS の直接インターフェイスが存在する実装での前払いユーザ、または（サービス認識または非サービス認識の）後払いユーザでもある場合、GGSN は拡張クォータ サーバ インターフェイス経由で CSG2 から使用状況を取得し、その使用状況を eG-CDR に追加します。

（注）　Cisco IOS リリース 12.4(22)YE2 以降では、拡張クォータ サーバ インターフェイスが GGSN でイネーブルになっている場合、GGSN はサービス認識後払いユーザまたは Gx 後払いユーザのクォータ サーバとして機能しないため、これらのユーザは Cisco CSG2 で後払いとして設定する必要があります。Cisco CSG2 の設定の詳細については、『*Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide*』を参照してください。

クォータ サーバ インターフェイス

GGSN のクォータ サーバ インターフェイスでは、次のことがサポートされています。

- Cisco CSG2 への RADIUS アカウンティング開始メッセージのアトリビュート
  - 課金プラン ID：DCCA サーバから受信するルールベース ID に対応します。GGSN のクォータ サーバ プロセスによって、ルールベース ID が課金プラン ID にマップされます。
  - クォータ サーバ アドレスおよびポート：Cisco CSG2 がユーザに使用する、クォータ サーバの IP アドレスおよびポートです。
  - OCS アドレス選択サポートが GGSN でイネーブルになっている場合を除いて、デフォルトは GGSN の IP アドレスになります。GGSN での OCS アドレス選択サポートのイネーブル方法については、「OCS アドレス選択サポートによるサービス認識課金の実装」（P.7-28）を参照してください。
  - ダウンリンク ネクストホップ アドレス：（Cisco CSG2 から GGSN への）ダウンリンク トラフィック用のネクストホップ アドレス（ユーザ アドレス）です。
- Threshold Limit Value（TLV）
  - Quota Consumption Timer（QCT）。QCT はゼロと見なされます。
  - Quota Holding Timer（QHT）
  - クォータしきい値

クォータ サーバ インターフェイス、課金プラン、および QCT と QHT については、『*Cisco Content Services Gateway Installation and Configuration Guide*』を参照してください。

拡張クォータ サーバ インターフェイス

拡張クォータ サーバ インターフェイスでは、追加で次のことがサポートされています。

- サービス コントロール メッセージ
  - Service Control Request（SCR）
  - Service Control Request Ack
  - Service Control Usage（SCU）
  - Service Control Usage Ack
- Cisco CSG2 への RADIUS アカウンティング メッセージと停止メッセージのアトリビュート
  - クォータ サーバ モード：拡張クォータ サーバ インターフェイスの機能（オンライン課金がイネーブルにされるか、またはオフライン課金がイネーブルにされるか）を指定します。
  - eG-CDR コリレータ ID：Service Control Usage を Service Control Request と一致させるために GGSN が使用する識別情報です。

拡張クォータ サーバ インターフェイスを設定する場合は、次の点に注意してください。

- サービス コントロール メッセージをトリガーするために、APN をサービス認識課金サポート（**service-aware** コマンド）または PCC 対応（**pcc** コマンド）用にイネーブルにする必要があります。
- GPRS Charging Release 7 は、「課金リリースの設定」（P.6-8）の説明に従って設定する必要があります。
- 「APN での課金レコード タイプの設定」（P.7-32）の説明に従って、参加している APN 用の課金レコード タイプを設定します。
- 「サービスごとのローカル シーケンス番号の同期の設定」（P.7-35）の説明に従って、サービスごとのローカル シーケンス番号の同期を設定します。
- GGSN ごとに 1 つのクォータ サーバ インターフェイスを設定できます。複数のクォータ サーバ インターフェイスを設定すると、既存のインターフェイスが上書きされます。

GGSN でクォータ サーバ インターフェイスを設定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# ggsn quota-server server-name [service-msg]`	GGSN でクォータ サーバ プロセスをイネーブルにし、クォータ サーバ コンフィギュレーション モードを開始します。任意で、**service-msg** キーワード オプションを指定して、クォータ サーバ プロセスがサービス コントロール メッセージを交換できるようにします。
ステップ 2	`Router(config-quota-server)# interface interface-name`	使用するクォータ サーバに対して、論理インターフェイスを名前で指定します。ループバック インターフェイスをクォータ サーバ インターフェイスとして使用することを推奨します。 **（注）** クォータ サーバは、GTP 仮想テンプレート アドレスとは異なるアドレスを使用する必要があります。

	コマンド	目的
ステップ 3	`Router(config-quota-server)# echo-interval [ 0 | 60-65535]`	エコー要求メッセージを Cisco CSG に送信する前にクォータ サーバが待機する秒数を指定します。有効な値は 0（エコー メッセージはディセーブル）、または 60 ～ 65535 の値です。デフォルトは 60 です。
ステップ 4	`Router(config-quota-server)# n3-requests number`	クォータ サーバが Cisco CSG へのシグナリング要求の送信を試行する最大回数を指定します。有効な値は 2 ～ 65535 の数値です。デフォルトは 5 です。
ステップ 5	`Router(config-quota-server)# t3-response number`	要求への応答を受信していない場合に、シグナリング要求メッセージを再送する前にクォータ サーバが待機する最初の時間を指定します。有効な値は 2 ～ 65535 の数値です。デフォルトは 1 です。
ステップ 6	`Router(config-quota-server)# csg-group csg-group-name`	クォータ サーバ プロセスが Cisco CSG2 との通信に使用する Cisco CSG2 グループを指定します。 （注）　クォータ サーバ プロセスは Cisco CSG2 へのパスを 1 つだけサポートしているため、一度に 1 つの Cisco CSG2 グループだけを指定できます。
ステップ 7	`Router(config-quota-server)# scu-timeout csg-group-name`	GGSN が、SCR を廃棄する前に Cisco CSG2 からの SCU の受信を待機する時間（秒単位）を指定します。有効な値は 1 ～ 1000 の数値です。デフォルトは 30 です。
ステップ 8	`Router(config-quota-server)# exit`	クォータ サーバ コンフィギュレーション モードを終了します。

ダウンリンク トラフィックのネクストホップ アドレスのアドバタイズ

（Cisco CSG2 から GGSN への）ダウンリンク トラフィックのネクストホップ アドレス（ユーザ アドレス）が RADIUS エンドポイントへのアカウンティング開始要求でアドバタイズされるように設定するには、アクセス ポイント コンフィギュレーション モードで次の作業を実行します。

コマンド	目的
`GGSN(access-point-config)# advertise downlink next-hop ip-address`	GGSN 宛てのダウンリンク トラフィックのルーティング先となるネクストホップ アドレスがアカウンティング開始要求でアドバタイズされるように設定します。

Cisco CSG2 を認証およびアカウンティング プロキシとして使用するための GGSN の設定

RADIUS を使用していない場合は、Cisco CSG2 を RADIUS プロキシとして設定する必要があります。

Cisco CSG2 を RADIUS プロキシとして使用するように GGSN を設定するには、次の作業を実行する必要があります。

- 「グローバル RADIUS サーバの設定」（P.7-10）
- 「Cisco CSG2 を含む AAA RADIUS サーバ グループの設定」（P.7-10）
- 「方式リストを使用したサポート対象サービスの指定」（P.7-11）
- 「APN の方式リストの指定」（P.7-11）

グローバル RADIUS サーバの設定

RADIUS サーバをグローバルに設定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]`	RADIUS サーバ ホストを指定します。
ステップ 2	`Router(config)# radius-server key {0 string | 7 string | string}`	GGSN と RADIUS デーモン間のすべての RADIUS 通信に対して認証および暗号鍵を設定します。

Cisco CSG2 を含む AAA RADIUS サーバ グループの設定

AAA RADIUS サーバ グループを定義し、このサーバ グループに Cisco CSG2 をサーバとして含めるには、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# aaa group server radius group-name`	AAA RADIUS サーバ グループを指定し、選択したサーバ グループを認証サービス用に割り当てます。
ステップ 2	`Router(config-sg-radius)# server ip_address [auth-port port-number] [acct-port port-number]`	サーバ グループの RADIUS エンドポイントの IP アドレスを設定します。
ステップ 3	`Router(config-sg-radius)# exit`	サーバ グループ コンフィギュレーション モードを終了します。

方式リストを使用したサポート対象サービスの指定

AAA 方式リストを使用して、グループがサポートするサービスのタイプを指定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# aaa authentication ppp list-name group group-name`	PPP を実行しているシリアル インターフェイスで使用する、1 つ以上の AAA 認証方式を指定します。
ステップ 2	`Router(config)# aaa authorization network list-name group group-name`	ネットワーク アクセスをユーザに制限するパラメータを設定します。
ステップ 3	`Router(config)# aaa accounting network list-name start-stop group group-name`	RADIUS を使用する場合、課金およびセキュリティのために、要求されたサービスの AAA アカウンティングをイネーブルにします。

APN の方式リストの指定

Cisco CSG2 を RADIUS プロキシとして使用する APN の方式リストを参照するには、アクセス ポイント コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(access-point-config)# aaa-group authentication server-name`	AAA サーバ グループを指定し、選択したサーバ グループをアクセス ポイント上の認証サービス用に割り当てます。
ステップ 2	`Router(access-point-config)# aaa-group accounting server-name`	使用するクォータ サーバに対して、論理インターフェイスを名前で指定します。

クォータ サーバから CSG2 への設定のモニタリングとメンテナンス

次のコマンドを特権 EXEC モードで使用して、クォータ サーバから Cisco CSG2 への設定をモニタリングおよびメンテナンスします。

コマンド	目的
`Router# clear ggsn quota-server statistics`	クォータ サーバ関連の統計情報（メッセージおよびエラー数）をクリアします。
`Router# show ggsn quota-server [parameters | statistics]`	クォータ サーバのパラメータ、またはクォータ サーバのメッセージとエラー数に関する統計情報を表示します。
`Router# show ggsn csg [parameters | statistics]`	Cisco CSG2 グループで使用するパラメータ、またはクォータ サーバで送受信されるパスとクォータ管理メッセージの数を表示します。

Diameter/DCCA サポートによるサービス認識課金の実装

Diameter/DCCA サポートを使用してサービス認識 GGSN を実装するには、次の項の作業を実行します。

DCCA/Diameter によるサービス認識課金の確認

DCCA によるサービス認識 GGSN の実装では、Cisco CSG はトラフィックを分類し、使用状況を報告し、クォータを管理します。GGSN は、DCCA サーバと通信する DCCA クライアントとして機能することで、次の機能を提供します。

- DCCA サーバへの Diameter インターフェイス（Gy）。これを使用して、Cisco CSG はクォータを要求し、使用状況を報告します。
- クォータのネゴシエーション。これは、Cisco CSG2 から DCCA サーバにクォータ要求を送信し、DCCA サーバから Cisco CSG2 にクォータ応答をプッシュすることで行います。
- DCCA サーバ ルールベースから Cisco CSG2 課金プランへのマッピング。
- Cisco CSG2 サービス クォータへの DCCA サーバ カテゴリ クォータのマッピング。
- PDP メンテナンス、および PDP が前払いであるか後払いであるかの識別。

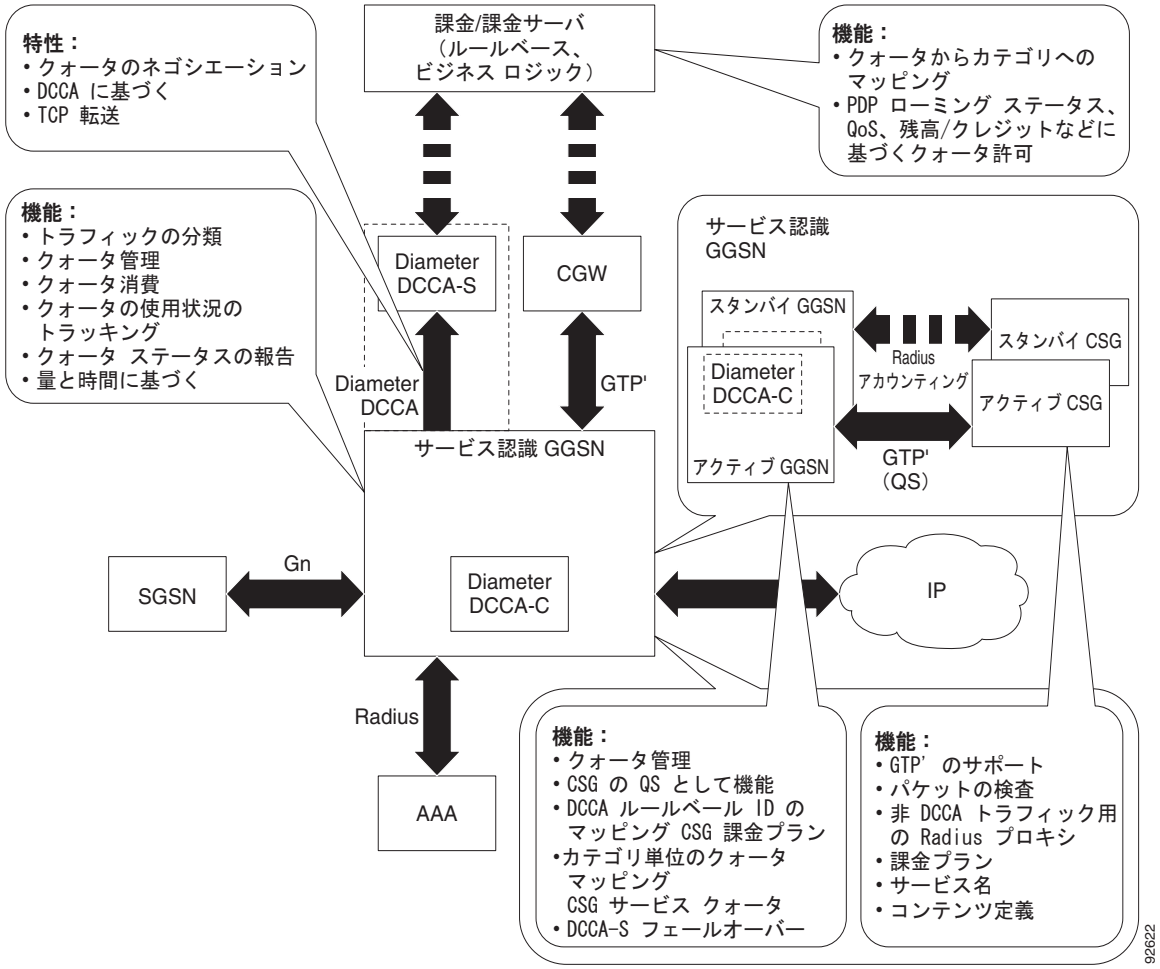
前払いサービスベースの課金、または後払いサービスベースの課金が必要な場合、エントリが Cisco CSG に作成されます。Cisco CSG はサービス カテゴリを調べ、使用状況を GGSN に報告します。ユーザが後払い加入者（オフライン課金）として処理される場合、GGSN は、Cisco CSG によって報告される使用状況情報を eG-CDR に記録します。ユーザが前払い加入者（オンライン課金）として処理される場合、GGSN は報告された使用状況情報を eG-CDR に記録し、その情報を変換して DCCA サーバに送信します。

GGSN は、クォータの再認可、サーバにより開始された再認可、または終了要求の Gn 側トリガーも処理します。Cisco CSG は、認可要求、クォータ レポート、およびサービス停止を GGSN に送信します。GGSN は、Cisco CSG が、Diameter インターフェイス経由のトランスポートに対する DCCA メッセージで何を送信したかを解釈します。DCCA サーバが追加クォータを戻した場合、GGSN はそのクォータを Cisco CSG にプッシュします。

（注）　RADIUS を使用しない場合、Cisco CSG は RADIUS プロキシとして設定する必要があります。

図 7-1 に、DCCA サポートによるサービス認識 GGSN の実装の機能および特性を示します。

図 7-1　DCCA サポートによる実装でのサービス認識 GGSN 機能の概要



サポートされる機能

DCCA を使用してサービス認識 GGSN を実装できるようにするために、Cisco GGSN では次の機能がサポートされています。

- 前払い加入者のオンライン/リアルタイム クレジット制御のための Diameter/DCCA クライアント インターフェイス サポート（IP PDP コンテキストの場合だけ）
- サービス単位課金のための、Cisco CSG に対するクォータ サーバ機能およびインターフェイス
- 前払い加入者と後払い加入者のための、サービス認識 CDR の拡張 G-CDR
- AAA 認証インターフェイス：DCCA ルールベース サポートおよび課金プロファイル選択
- AAA アカウンティング インターフェイス：Cisco CSG Known User Table（KUT）の読み込みおよび Cisco CSG ベースのプロキシ
- オフライン課金用の拡張 Ga インターフェイス

サポートされない機能

次の機能は、DCCA によるサービス認識 GGSN の実装でサポートされていません。

- セカンダリ PDP コンテキストでの課金の相違
- PPP PDP コンテキスト
- PPP 再生成
- ネットワーク管理
- セル ID
- オンライン DCCA 交換とオフライン サービスベース使用状況の両方に対する PDP コンテキスト
- クォータの再認可待機時の、トラフィックのブロッキング/フォワーディングのダイナミック コンフィギュレーション
- Diameter プロキシ、リレー、またはリダイレクション
- Diameter トランスポート レイヤ セキュリティ
- SCTP トランスポート
- （量と時間のクォータを受信するための）二重クォータ サポート

メッセージ サポート

Diameter 経由のクレジット制御をサポートするために、GGSN 上の DCCA クライアント プロセスと DCCA サーバは、次のメッセージを交換します。

- Credit Control Request（CCR; クレジット制御要求）: 開始、更新、および最終
- Credit Control Answer（CCA; クレジット制御応答）: 開始、更新、および最終

また、GGSN Diameter インターフェイスでは、次の基本 Diameter メッセージがサポートされています。

- Capability Exchange Request（CER）および Capability Exchange Answer（CEA）: GGSN は、CER メッセージで DCCA サポートをアドバタイズします。また、グローバル コンフィギュレーション モードで **diameter vendor support** コマンドを使用して、ベンダー固有の attribute value pair（AVP; アトリビュート値ペア）のサポートをアドバタイズするように GGSN を設定できます。
- Disconnect Peer Request（DPR）および Disconnect Peer Answer（DPA）: Diameter ピアとの CER が失敗した場合、または設定されている Diameter サーバがない場合、GGSN は DPR メッセージを送信します。
- Device Watchdog Request（DWR）および Device Watchdog Answer（DWA）: GGSN は DWR メッセージと DWA メッセージを使用して、Diameter ピアでのトランスポート障害を検出します。**timer watchdog** Diameter ピア コンフィギュレーション コマンドを使用して、ウォッチドッグ タイマーを各 Diameter ピアに設定できます。
- Re-auth Request（RAR）および Re-auth Answer（RAA）
- Abort Session Request（ASR）/Abort Session Answer（ASA）: 正しくない ASR が DCCA サーバから送信された場合、No Failed-AVP が ASA で送信されます。

DCCA クライアントとして、GGSN は Cisco IOS AAA から次の通知も受け取ります。

- CCA メッセージの受信
- 非同期セッション終了要求
- サーバにより開始された RAR

DCCA データ フローを伴うサービス認識課金

次に、DCCA を使用する拡張サービス認識課金実装での前払い加入者の PDP コンテキスト作成時のトラフィック フローの概要を示します。

前払い加入者の PDP コンテキスト作成のデータ フロー

1. SGSN はサービス認識 GGSN に PDP コンテキストの作成要求を送信します。
2. GGSN は、Access-Request メッセージを RADIUS（サーバまたは RADIUS プロキシとして設定されている Cisco CSG2）に送信します。
3. RADIUS は Access-Accept 応答を返します。GGSN は、この Access-Accept 応答からデフォルトのルールベース ID を取得します。また、応答にデフォルトのルールベース ID が含まれていない場合、GGSN は、PDP コンテキストの作成要求で選択された課金プロファイル内のローカルに設定された値から、ルールベース ID を取得します。
4. サービス認識 GGSN は、Diameter クレジット制御要求（CCR）を DCCA サーバに送信します。
5. DCCA サーバは、クレジット制御応答（CCA）を GGSN に返します。この CCA には、ルールベースとクォータ要求が含まれている場合があります。
6. CCA にルールベースが含まれている場合、GGSN は選択したルールベースとともにアカウンティング開始要求を RADIUS に送信します。
7. RADIUS は GGSN からアカウンティング開始要求を受信し、ユーザの KUT を作成します。
8. RADIUS はアカウンティング開始応答を GGSN に送信します。
9. DCCA サーバが CCA のクォータ要求を GGSN に送信します。
10. GGSN はクォータ要求を Cisco CSG2 にプッシュします。
11. GGSN は、Cisco CSG2 からクォータ プッシュ応答を受信すると、PDP コンテキストの作成応答を SGSN に送信し、コンテキストが確立されます。

後払い加入者の PDP コンテキスト作成のデータ フロー

1. SGSN はサービス認識 GGSN に PDP コンテキストの作成要求を送信します。
2. GGSN は、選択したルールベースを含むアカウンティング開始要求を RADIUS（サーバまたは RADIUS プロキシとして設定された Cisco CSG2）に送信します。
3. RADIUS プロキシはアカウンティング開始要求を受信し、ユーザの KUT を作成します。
4. RADIUS プロキシはアカウンティング開始応答を GGSN に送信します。
5. RADIUS プロキシからアカウンティング開始応答を受信すると、GGSN が PDP コンテキストの作成応答を SGSN に送信し、コンテキストが確立されます。

Diameter ベースの設定

Diameter プロトコル ベースを設定するには、次の項の作業を実行します。

- 「Diameter ピアの設定」（P.7-16）
- 「Diameter AAA のイネーブル」（P.7-17）
- 「Diameter プロトコル パラメータのグローバル設定」（P.7-18）
- 「Diameter ベースのモニタリングとメンテナンス」（P.7-20）

Diameter ピアの設定

Diameter ピアを設定するには、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
ステップ 1	`Router(config)# diameter peer name`	デバイスを Diameter プロトコル ピアとして設定し、Diameter ピア コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-dia-peer)# address ipv4 ip-address`	IPv4 を使用して、Diameter ピアのホストへのルートを定義します。
ステップ 3	`Router(config-dia-peer)# transport {tcp | sctp} port port-num`	Diameter ピアに接続するためのトランスポート プロトコルを設定します。 **（注）**　Cisco GGSN では、TCP がサポートされています。
ステップ 4	`Router(config-dia-peer)# security ipsec`	IPSec を Diameter ピアツーピア接続のセキュリティ プロトコルとして設定します。
ステップ 5	`Router(config-dia-peer)# source interface interface`	Diameter ピアに接続するようにインターフェイスを設定します。
ステップ 6	`Router(config-dia-peer)# timer {connection | transaction | watchdog} value`	Diameter ベース プロトコル タイマーをピアツーピア接続用に設定します。有効な秒数の範囲は、1 ～ 1000 です。デフォルトは 30 です。 • **connection**：転送障害が原因でピアへの接続が停止したあとに、GGSN が Diameter ピアへの再接続を試行する最大時間。値 0 の場合は、再接続を試行しないように GGSN が設定されます。 • **transaction**：GGSN が別のピアを試行する前に Diameter ピアの応答を待機する最大時間。 • **watchdog**：GGSN がウォッチドッグ パケットへの Diameter ピアの応答を待機する最大時間。 ウォッチドッグ タイマーが期限切れになると、DWR が Diameter ピアに送信され、ウォッチドッグ タイマーがリセットされます。ウォッチドッグ タイマーの次の期限切れまでに DWA が受信されない場合は、その Diameter ピアに転送障害が発生しています。 タイマーを設定する場合、トランザクション タイマーの値は TX タイムアウト値よりも大きい必要があり、SGSN では、GTP N3 要求と T3 再送信の数に設定された値は、使用可能なすべてのサーバ タイマー（RADIUS、DCCA、および Cisco CSG2）の合計よりも大きい必要があります。特に、SGSN N3*T3 は、2 x RADIUS タイムアウト + *N* x DCCA タイムアウト + Cisco CSG2 タイムアウトよりも大きい必要があります。それぞれの意味を次に示します。 • 2 は、認証とアカウンティングの両方を示します。 • *N* は、サーバ グループで設定されている Diameter サーバの数を示します。

	コマンド	目的
ステップ 7	`Router(config-dia-peer)# destination host string`	Diameter ピアの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を設定します。
ステップ 8	`Router(config-dia-peer)# destination realm string`	Diameter ピアの宛先レルム（ドメイン「*@realm*」の一部）を設定します。 このレルムは、AAA への要求の送信時に AAA クライアントによって追加されることがあります。ただし、クライアントがこのアトリビュートを追加しなかった場合は、Diameter ピア コンフィギュレーション モード時に設定した値が、宛先 Diameter ピアにメッセージを送信するときに使用されます。 Diameter ピア コンフィギュレーション モード時に値を設定しなかった場合は、**diameter destination realm** コマンドを使用してグローバルに設定した値が使用されます。
ステップ 9	`Router(config-dia-peer)# ip vrf forwarding name`	VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンスを Diameter ピアに関連付けます。 **（注）** VRF 名が Diameter サーバに設定されていない場合は、グローバル ルーティング テーブルが使用されます。

Diameter AAA のイネーブル

Diameter AAA をイネーブルにするには、次の項の作業を実行します。

- 「Diameter AAA サーバ グループの定義」（P.7-17）
- 「前払い加入者用の認可方式リストの定義」（P.7-18）

Diameter AAA サーバ グループの定義

冗長性を確保するために、複数の Diameter サーバをプライマリ サーバとセカンダリ サーバで構成される Diameter AAA サーバ グループとして設定します。

Diameter AAA サーバ グループを定義するには、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
ステップ 1	`Router(config)# aaa new-model`	AAA をイネーブルにします。

	コマンド	目的
ステップ 2	`Router(config)# aaa group server diameter group-name`	さまざまな Diameter サーバ ホストを個別のリストおよび方式にグループ化します。 AAA サーバ グループを設定することで、さまざまなサーバを AAA の各要素に使用できます。また、1 つの冗長サーバ セットを各要素に定義することもできます。
ステップ 3	`Router(config-sg-diameter)# server name auth-port 1645 acct-port 1646`	グループ サーバの Diameter サーバの名前を設定します。 このコマンドに指定した名前は、**diameter peer** コマンドを使用して定義した Diameter ピアの名前と一致する必要があります。 **（注）** ポート番号 1645 と 1646 は、それぞれ認可およびアカウンティングのデフォルトです。デフォルト以外のポート番号を使用する場合にだけ、明示的なポート番号が必要となります。

前払い加入者用の認可方式リストの定義

アクセスを前払い加入者のネットワークに制限するパラメータを適用するには、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)# aaa authorization prepaid method_list group server_group [group server_group]`	前払い加入者用の認可方式リストを定義し、レコードを送信する Diameter AAA グループを定義します。

Diameter プロトコル パラメータのグローバル設定

Diameter パラメータを Diameter ピア レベルで定義していない場合、GGSN はグローバル Diameter プロトコル パラメータを使用します。

グローバル Diameter 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 モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# diameter timer {connection | transaction | watchdog} value`	Diameter ピア レベルで何も設定されていない場合に使用する Diameter ベース プロトコル タイマーを設定します。有効な秒数の範囲は 0 ～ 1000 です。デフォルトは 30 です。 • **connection**：転送障害が原因で切断されたあとに、GGSN が Diameter ピアへの再接続を試行する最大時間。値 0 の場合は、再接続を試行しないように GGSN が設定されます。 • **transaction**：GGSN が別のピアを試行する前に Diameter ピアの応答を待機する最大時間。 • **watchdog**：GGSN がウォッチドッグ パケットへの Diameter ピアの応答を待機する最大時間。 ウォッチドッグ タイマーが期限切れになると、DWR が Diameter ピアに送信され、ウォッチドッグ タイマーがリセットされます。ウォッチドッグ タイマーの次の期限切れまでに DWA が受信されない場合は、その Diameter ピアに転送障害が発生しています。 タイマーを設定する場合、トランザクション タイマーの値は TX タイマーの値よりも大きい必要があり、SGSN では、GTP N3 要求と T3 再送信の数に設定された値は、使用可能なすべてのサーバ タイマー（RADIUS、DCCA、および Cisco CSG2）の合計よりも大きい必要があります。特に、SGSN N3*T3 は、2 x RADIUS タイムアウト + *N* x DCCA タイムアウト + Cisco CSG2 タイムアウトよりも大きい必要があります。それぞれの意味を次に示します。 • 2 は、認証とアカウンティングの両方を示します。 • *N* は、サーバ グループで設定されている Diameter サーバの数を示します。
ステップ 2	`Router(config)# diameter redundancy`	Diameter ノードが Cisco IOS Redundancy Facility（RF; 冗長ファシリティ）クライアントとなり、セッション状態を追跡できるようにします。 Diameter ベースは、スタンバイ モードの Diameter ピアへの接続を開始しません。スタンバイ モードからアクティブ モードへの移行時に、新たにアクティブになったピアへの接続が確立されます。 **（注）** このコマンドは、サービス認識 PDP セッションの冗長性を確保するために必要です。サービス認識 PDP セッションの冗長性の詳細については、「サービス認識 PDP の GTP セッション冗長性の概要」（P.7-33）を参照してください。
ステップ 3	`Router(config)# diameter origin realm string`	Diameter ノードが配置されている元のレルム（ドメイン「*@realm*」の一部）を設定します。 元のレルム情報は、Diameter ピアへの要求で送信されます。

	コマンド	目的
ステップ 4	`Router(config)# diameter origin host string`	Diameter ノードのホストの完全修飾ドメイン名（FQDN）を設定します。 元のホスト情報は、Diameter ピアへの要求で送信されます。
ステップ 5	`Router(config)# diameter vendor support {Cisco | 3gpp | Vodafone}`	Diameter ノードが Diameter ピアとの Capability Exchange メッセージでサポートしているベンダー AVP をアドバタイズするように Diameter ノードを設定します。 ベンダー ID が異なる場合は、このコマンドの複数インスタンスを設定できます。

Diameter ベースのモニタリングとメンテナンス

次のコマンドを特権 EXEC モードで使用して、Diameter ピア コンフィギュレーションのモニタリングとメンテナンスを行います。

コマンド	目的
`Router# show diameter peer`	Diameter ピア関連情報を表示します。

GGSN での DCCA クライアント プロセスの設定

クォータを取得および要求するために DCCA サーバと対話する場合、GGSN は DCCA クライアントとして機能します。GGSN は DCCA クライアントとして、クレジット制御セッション（PDP セッションごとに 1 つのクレジット制御セッション）の間、DCCA サーバに CCR メッセージを送信し、DCCA サーバから CCA を受信します。また、DCCA クライアント プロファイルで設定したデフォルトは、サーバ フェールオーバーが発生し、サーバから指示が送信されなかった場合に GGSN がクレジット制御セッションを処理する方法を示します。

DCCA クライアントでのデフォルトの障害処理

次の 2 つの AVP によって、障害発生時の CC（クレジット制御）セッションの処理方法が決定されます。

- CC-Session-Failover AVP：CC セッションが代替 Diameter サーバにフェールオーバーする必要があることを示します。この AVP は、**session-failover** DCCA クライアント プロファイル コンフィギュレーション コマンドを使用して設定します。
- Credit-Control-Failure-Handling（CCFH）AVP：障害発生時の GGSN の動作を決定します。この AVP は、**ccfh** DCCA クライアント プロファイル コンフィギュレーション コマンドを使用して設定します。

障害処理用にこれらの AVP のデフォルトを DCCA クライアント プロファイルで設定できますが、DCCA サーバから受信した値によって GGSN で設定したデフォルトは上書きされます。

次の障害状態が発生した場合は、CCFH AVP によって、DCCA クライアントがセッションで実行する処理が決定されます。

- Tx タイムアウトが期限切れになった。
- プロトコル エラー（結果コード 3xxx）を含む CCA メッセージを受信した。
- CCA の失敗（永久障害の通知（結果コード 5xxx）を含む CCA など）を受信した。

- 送信障害の状態が存在する（DCCA クライアントが目的の宛先に接続できない）。
- 無効な応答を受信した。

DCCA クライアント プロファイル（DCCA クライアント プロセスの特性を設定する）を設定し、課金プロファイルからその DCCA クライアント プロファイルを参照するには、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
ステップ 1	`Router(config)# gprs dcca profile name`	GGSN で DCCA クライアント プロセスを定義し、DCCA クライアント プロファイル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-dcca-profile)# authorization method_list_name`	Diameter AAA サーバ グループを指定するために使用する方式リストを定義します。
ステップ 3	`Router(config-dcca-profile)# tx-timeout seconds`	DCCA クライアントが CCR と Diameter サーバ間の通信をモニタリングするために使用する TX タイムアウト値を秒数で設定します。 有効な範囲は 1 ～ 1000 秒です。デフォルトは 10 です。 タイマーを設定する場合、トランザクション タイマーの値は TX タイムアウト値よりも大きい必要があり、SGSN では、GTP N3 要求と T3 再送信の数に設定された値は、使用可能なすべてのサーバ タイマー（RADIUS、DCCA、および Cisco CSG2）の合計よりも大きい必要があります。特に、SGSN N3*T3 は、2 x RADIUS タイムアウト + *N* x DCCA タイムアウト + Cisco CSG2 タイムアウトよりも大きい必要があります。それぞれの意味を次に示します。 • 2 は、認証とアカウンティングの両方を示します。 • *N* は、サーバ グループで設定されている Diameter サーバの数を示します。

	コマンド	目的
ステップ 4	`Router(config-dcca-profile)# ccfh {continue | terminate | retry_terminate}`	障害状態が発生した場合に PDP コンテキストで実行するデフォルトの Credit Control Failure Handling（CCFH）処理を設定します。 • **continue**：中断にかかわらず、関連カテゴリ（複数可）の PDP コンテキストおよびユーザ トラフィックの続行を許可します。他のカテゴリのクォータ管理には影響しません。 • **terminate**：PDP コンテキストおよび CC セッションを終了します。 • **retry_terminate**：関連カテゴリ（複数可）の PDP コンテキストおよびユーザ トラフィックの続行を許可します。最初の DCCA サーバが使用できなくなると、ハードコードされたクォータ（1 GB）が CSG2 に渡されます。 DCCA クライアントは、代替サーバへの CRR の送信を再試行し、その代替サーバで送信障害の状態が発生した場合は PDP コンテキストが終了します。 デフォルトは terminate です。 DCCA サーバからの CCA の値によって、デフォルトが上書きされます。
ステップ 5	`Router(config-dcca-profile)# session-failover`	DCCA サーバからの CCA メッセージに CCSF AVP の値が含まれていない場合は、代替 DCCA サーバの Configures Credit Control Session Failover（CCSF）AVP サポートへのセッション フェールオーバーが必要であることを指定します。 デフォルトでは、セッション フェールオーバーはサポートされていません。
ステップ 6	`Router(config-dcca-profile)# destination-realm` *string*	DCCA サーバへの最初の CCR 要求で送信される宛先レルムを指定します。後続の CCR では、最後の CCA で受信された元のレルム AVP が宛先レルムとして使用されます。

	コマンド	目的
ステップ 7	`Router(config-dcca-profile)# trigger {plmn-change | qos-change | rat-change | sgsn-change | user-loc-info-change}`	どのような変更が発生した場合に GGSN（DCCA クライアントとして機能する）がトリガーされ、クォータ再認可が要求されて、eG-CDR が生成されるかを設定します。 • **plmn-id**：PLMN ID の変更によって、クォータ再認可要求がトリガーされます。 • **qos-change**：QoS の変更によって、クォータ再認可要求がトリガーされます。 • **rat**：RAT の変更によって、クォータ再認可要求がトリガーされます。RAT は、SGSN が UE UMTS または GERAN にサービスを提供するかどうかを示します。 • **sgsn-change**：SGSN の変更によって、クォータ再認可要求がトリガーされます。 • **user-loc-info-change**：ユーザ位置の変更によって、クォータ再認可要求がトリガーされます。 このコマンドを変更しても、DCCA クライアント プロファイルを使用する既存の PDP コンテキストには影響しません。**plmn-change**、**rat-change**、および **user-loc-info-change** の各キーワード オプションでは、**gprs charging service record include** コマンドを使用して、サービス レコード IE のこれらのフィールドを CDR に含めるように GGSN を設定する必要があります。 トリガーを設定する場合は、次の点に注意してください。 • このコマンドは、汎用 DCCA クライアントおよび 3GPP Gy-DCCA だけでサポートされています。 • 前払いユーザと後払いユーザの両方に対して明示的にすべてのトリガーをイネーブルにする必要があります。 • 設定された前払いトリガーは、PDP コンテキストを流れるすべてのサービスに適用されます。OCS サーバから特定のサービス用に受信されたトリガーは、**trigger** コマンドを使用して設定されたものよりも優先されます。

DCCA メッセージのベンダー固有 AVP のサポートのイネーブル

Cisco GGSN では、次の DCCA 実装がサポートされています。

- IETF RFC-4006 に基づく汎用実装
- VF_CLCI（Vodafone）を使用する統合 eGGSN
- 3GPP Gy 準拠（3GPP）

デフォルトのサポート モードは、汎用実装です。Gy 準拠実装では、標準の DCCA アトリビュート以外に、一部の追加 3GPP Vendor Specific Attribute（VSA; ベンダー固有アトリビュート）がサポートされています。VF_CLCI 準拠実装では、Vodafone 固有の VSA、3GPP VSA（必要な場合）、および標準 DCCA アトリビュートがサポートされています。

Cisco GGSN では、CER メッセージの DCCA アプリケーション（認可アプリケーション ID 4）だけのサポートがアドバタイズされます。また、次に示すベンダー ID のサポートが（ベンダー固有の AVP の認識のために）アドバタイズされます。

- Cisco（ベンダー ID = 9）
- 3GPP（ベンダー ID = 10415）
- Vodafone（ベンダー ID = 12645）

Cisco GGSN が DCCA メッセージの標準 DCCA アトリビュートに加えて追加の 3GPP VSA を DCCA サーバに送信できるようにするには、グローバル コンフィギュレーション モードで次の作業を実行します。

コマンド	目的
`Router(config)# gprs dcca 3gpp`	DCCA メッセージ内の追加 3GPP VSA をサーバに送信するように GGSN を設定します。

GGSN が標準 DCCA アトリビュートおよび追加の 3GPP VSA に加えて、DCCA メッセージ内の Vodafone VSA を DCCA サーバに送信できるようにするには、グローバル コンフィギュレーション モードで次の作業を実行します。

コマンド	目的
`Router(config)# gprs dcca clci`	DCCA メッセージ内の Vodafone ベンダー固有 AVP をサーバに送信するように GGSN を設定します。

Gy ベース、VF-CLCI、および汎用 DCCA の各実装に関してサポートされている AVP のリストについては、『*Diameter Credit Control Application on the Cisco GGSN*』テクニカル ホワイトペーパーを参照してください。

課金プロファイルの拡張課金パラメータの設定

GGSN は、最大 256 個の課金プロファイルをサポートします。それぞれに 0 ～ 255 の番号が付与されます。プロファイル 0 は、常に GGSN に存在する設定済みプロファイルです。また、グローバルなデフォルト課金プロファイルでもあります。ユーザがプロファイル 0 を作成することはありませんが、charging-related グローバル コンフィギュレーション コマンドを使用すると変更を加えることができます。プロファイル 1 ～ 255 は、Cisco GGSN 課金プロファイル コンフィギュレーション コマンドを使用して、ユーザが定義し、カスタマイズできるプロファイルです。

サービス認識課金をサポートするために、すべての課金またはオンライン課金だけに対して eG-CDR を許可および抑制するように、課金プロファイルを設定できます。

次のサービス認識課金特性を課金プロファイルに設定することもできます。

- ユーザに適用されるデフォルトのルールベース ID
- デフォルトの課金タイプ（主に前払い加入者または後払い加入者に使用）
- クォータ要求を問い合せるデフォルト DCCA サーバ（存在する場合はオンライン課金を示します）

サービス認識課金特性を課金プロファイルに設定するには、次の項の作業を実行します。

- 「デフォルト ルールベース ID の指定」（P.7-25）
- 「オンライン課金の DCCA クライアント プロファイルの指定」（P.7-26）
- 「前払い加入者の CDR の抑制」（P.7-26）
- 「後払い加入者のトリガー条件の設定」（P.7-27）

デフォルト ルールベース ID の指定

Diameter/DCCA によるサービス認識実装（「Diameter/DCCA サポートによるサービス認識課金の実装」（P.7-12）を参照）では、トラフィックのカテゴリを定義するためのルールが含まれています。これらのカテゴリに基づいて、トラフィックを許可または拒否するかどうか、およびトラフィックをどのように測定するかが決定されます。GGSN によって、Diameter ルールベース ID が Cisco CSG2 課金プランにマップされます。

特定の課金プロファイルを使用して PDP コンテキストに適用するデフォルト ルールベース ID を設定するには、課金プロファイル 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(ch-prof-conf)# content rulebase id`	この課金プロファイルを使用して、PDP コンテキストに適用するデフォルトのルールベース ID を定義します。

（注）　RADIUS Access Accept メッセージのルールベース値によって、課金プロファイルに設定されたデフォルト ルールベース ID が上書きされます。DCCA サーバからの最初の CCA メッセージで受信したルールベース ID によって、RADIUS サーバから受信したルールベース ID および課金プロファイルに設定されているデフォルト ルールベース ID が上書きされます。

Gy : DCCA 前払いソリューションの場合、ルールベース ID は DCCA で受信されず、ルールベース ID はスタンドアローン前払いソリューションには適用されません。

オンライン課金の DCCA クライアント プロファイルの指定

プライマリ PDP コンテキストが作成されると、課金プロファイルが選択されます。

DCCA プロファイルを課金プロファイルで定義すると、オンライン課金はその PDP を示します。したがって、ユーザが前払いであるか後払いであるかに関係なく、**content dcca profile** 設定が存在する場合、GGSN は DCCA サーバにアクセスします。

（注）　この課金プロファイル設定では、サービス認識課金が Diameter/DCCA を使用して実装されている必要があります（「Diameter/DCCA サポートによるサービス認識課金の実装」（P.7-12）を参照）。

ユーザが後払い加入者として処理されている場合、DCCA サーバは結果コード CREDIT_CONTROL_NOT_APPLICABLE（4011）とともに CAA を返し、そのユーザは後払い加入者として処理されます。

課金プロファイルに DCCA プロファイル設定が含まれていない場合、ユーザは後払い（オフライン課金）として処理されます。

DCCA サーバと通信する DCCA クライアント プロファイルを指定するには、課金プロファイル 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(ch-prof-conf)# content dcca profile profile-name`	DCCA サーバと通信するプロファイルを指定します。

前払い加入者の CDR の抑制

Diameter/DCCA によるサービス認識実装（「Diameter/DCCA サポートによるサービス認識課金の実装」（P.7-12）を参照）では、前払い加入者の課金は DCCA クライアントによって処理されるため、eG-CDR が前払い加入者用に生成される必要はありません。

DCCA サーバへのアクティブな接続を持つユーザについて eG-CDR を抑制するように GGSN を設定するには、課金プロファイル 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(ch-prof-conf)# cdr suppression prepaid`	前払い加入者の CDR を抑制することを指定します。

（注）　イネーブルである場合、セッションがアクティブであるときに Diameter サーバでエラーが発生すると、ユーザは後払いステータスに戻されますが、PDP コンテキストの CDR は生成されません。

後払い加入者のトリガー条件の設定

ユーザが拡張クォータ サーバ インターフェイスを使用していない前払い加入者である場合、すべてのクレジット制御が DCCA サーバによって実行されます。ユーザが拡張クォータ サーバ インターフェイスを使用していない後払い加入者であり、かつサービス認識課金がイネーブルである場合、課金プロファイルで設定されたデフォルト値によって、使用状況の報告頻度を制御する条件が定義されます。

（注） 前払い加入者と後払い加入者の両方に対してトリガーが明示的にイネーブルにされている必要があります。

後払い加入者の課金プロファイルでトリガー条件を定義するには、課金プロファイル 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
ステップ 1	`Router(ch-prof-conf)# content postpaid {qos-change | sgsn-change | plmn-change | rat-change}`	条件を設定します。この条件が発生すると、GGSN によって PDP コンテキストのクォータ再認可が要求されます。 • **qos-change**：Quality of Service（QoS）の変更によって、クォータ再認可要求がトリガーされます。 • **sgsn-change**：SGSN の変更によって、クォータ再認可要求がトリガーされます。 • **plmn-change**：パブリック ランド モバイル ネットワーク（PLMN）の変更によって、クォータ再認可要求がトリガーされます。 • **rat-change**：無線アクセス テクノロジー（RAT）の変更によって、クォータ再認可要求がトリガーされます。 **（注）** **plmn-change** および **rat-change** のキーワード オプションでは、**gprs charging service record include** コマンドを使用して、サービス レコード IE の RAT フィールドや PLMN ID フィールドが CDR に含まれるように GGSN を設定する必要があります。 **（注）** 前払い加入者と後払い加入者の両方に対して明示的にトリガーをイネーブルにする必要があります。
ステップ 2	`Router(ch-prof-conf)# content postpaid time value`	期間制限を指定します。これを超えると、GGSN によって、アップストリームとダウンストリームのトラフィック バイト カウントが収集され、特定の PDP コンテキストの G-CDR が閉じて更新されます。 有効な値は 300 ～ 4294967295 秒です。デフォルトは 1048576 です。

	コマンド	目的
ステップ 3	`Router(ch-prof-conf)# content postpaid validity seconds`	後払い加入者に許可されているクォータが有効な時間（秒単位）を指定します。有効な範囲は 900 ～ 4294967295 秒です。デフォルトでは、検証タイマーは設定されていません。
ステップ 4	`Router(ch-prof-conf)# content postpaid volume value`	G-CDR を終了および更新する前に特定の PDP コンテキストのすべてのコンテナにわたって GGSN が保持する最大バイト数を指定します。 有効な値は 1 ～ 4294967295 です。デフォルトは 1,048,576 バイト（1 MB）です。

OCS アドレス選択サポートによるサービス認識課金の実装

DCCA オンライン課金ソリューションを使用する GGSN の代わりに、OCS アドレス選択をサポートするように GGSN を設定できます。OCS アドレス選択を使用すると、前払い加入者のオンライン クレジット制御を、Cisco CSG2 がダイレクト GTP インターフェイスを持つ外部 OCS によって指定できます。OCS アドレス選択をサポートするように GGSN を設定する場合、GGSN は後払い加入者に対してだけクォータ サーバとして機能します。GGSN は後払い加入者の拡張 G-CDR（eG-CDR）は生成しません。

デフォルトでは、GGSN はアカウンティング開始メッセージで自身の IP アドレスを（RADIUS プロキシとして機能する）Cisco CSG2 に送信して、GGSN 自身を前払い加入者と後払い加入者のクォータ サーバとして確立します。OCS アドレス選択サポートが設定されている場合は、OCS の IP アドレスが AAA サーバからの Access-Accept メッセージ内の「csg:quota_server」アトリビュートで返されると、GGSN はアカウンティング開始メッセージ内の同じアトリビュートのアドレスを Cisco CSG2 に転送します。これにより、外部 OCS を PDP コンテキストのクォータ サーバとして使用するように Cisco CSG2 に通知します。OCS アドレス選択を使用するサービス認識 GGSN 実装では、GGSN は後払い加入者に対してだけクォータ サーバとして機能します。

OCS アドレス選択によるサービス認識課金のデータ フロー

次に、OCS アドレス選択を使用する拡張サービス認識課金実装での前払い加入者の PDP コンテキスト作成時のトラフィック フローの概要を示します。

1. SGSN はサービス認識 GGSN に PDP コンテキストの作成要求を送信します。
2. GGSN は、Access-Request メッセージを RADIUS エンドポイント（サーバまたは RADIUS プロキシとして設定された Cisco CSG2）に送信します。
3. RADIUS エンドポイントは、ユーザが前払いであるかどうかを判別し、前払いである場合は、外部 OCS の IP アドレスやポートなどの「csg:quota_server」アトリビュートを含む Access-Accept メッセージを使用して Access-Request メッセージに応答します。
4. APN がサービス認識として設定されており、eG-CDR を生成するように GGSN が設定されている場合、GGSN は RADIUS エンドポイントから Access-Accept を受信し、そこに csg_quota_server アトリビュートが存在し、OCS の IP アドレスが含まれていることから、GGSN はそのユーザが前払い加入者であることを識別し、次のアトリビュートを含むアカウンティング開始要求を返します。
   - csg:billing_plan
   - csg:quota_server アトリビュート : csg:quota_server アトリビュートには、Cisco CSG2 に対する OCS IP アドレスおよびポートが含まれています。含まれていない場合、GGSN は csg:quota_server フィールド内の自身の IP アドレスを転送します。

- csg:eggsn_qs：拡張クォータ サーバ インターフェイスの IP アドレスとポート番号です。
- csg:eggsn_qs_mode：拡張クォータ サーバ インターフェイスが、サービス コントロール メッセージを CSG2 と交換できるかどうかを示します。

5. アカウンティング開始要求を受信すると、RADIUS エンドポイントは次のことを実行します。
   a. KUT エントリを作成します。
   b. GGSN が eG-CDR を生成したことを識別し、そのユーザのサービス レベル CDR 生成をディセーブルにします。
   c. ユーザが、受信した課金プランに基づく前払いユーザであることを識別します。
   d. 指定した OCS アドレスとのクォータ サーバ メッセージ交換をイネーブルにします。
   e. GGSN とのサービス コントロール メッセージ交換をイネーブルにします。
   f. アカウンティング開始応答を GGSN に送信します。
6. GGSN は PDP コンテキストの作成応答を SGSN に送信し、コンテキストが確立されます。
7. トリガー条件が発生すると、Service Control Request（SCR）メッセージと Service Control Usage（SCU）メッセージが GGSN と CSG2 間で交換されて、サービス コンテナが eG-CDR に追加されるか、eG-CDR が閉じます（あるいはその両方が行われます）。
8. GGSN は eG-CDR を生成し、それらを課金ゲートウェイに送信します。

（注） 外部 OCS が前払い加入者のクォータ サーバとして使用される場合、GGSN は後払い加入者のサービス レベル使用状況報告を Cisco CSG2 から受信し、それに応じて eG-CDR を生成します。「GGSN でのクォータ サーバ インターフェイスの設定」（P.7-6）での説明どおりに拡張クォータ インターフェイスが設定されている場合を除いて、GGSN は前払い加入者の eG-CDR を生成しません。

GGSN での OCS アドレス選択サポートでは、次の条件が満たされている必要があります。

- サービス認識課金のサポートが、グローバルに、かつ APN レベル（「サービス認識課金のサポートのイネーブル」（P.7-3）を参照）でイネーブルになっている。
- （「待機アカウンティングの設定」（P.7-4）を使用して）待機アカウンティングがイネーブルになっている。
- Cisco CSG2 と通信するように GGSN が設定されている（「Cisco GGSN でのクォータ サーバ サポートの設定」（P.7-5）を参照）。
- eG-CDR を生成するように GGSN が設定されている（「拡張 G-CDR を生成するための GGSN の設定」（P.7-4）を参照）。
- 正しい設定が AAA サーバ上に存在する。

GGSN で OCS アドレス選択サポート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
ステップ 1	`Router(conf)# gprs radius attribute quota-server ocs-address`	アカウンティング開始メッセージ内の csg:quota server アトリビュートの RADIUS サーバから Access-Accept 応答で受信した OCS IP アドレスを Cisco CSG2 に送信するように GGSN を設定します。

APN での PCC のイネーブル

Gx インターフェイスは、Policy and Charging Rules Function（PCRF; ポリシー / 課金ルール機能）と Policy and Charging Enforcement Function（PCEF; ポリシー / 課金実施機能）間の参照ポイントです。ポリシー / 課金制御（PCC）ファイルを PCRF から PCEF にプロビジョニングおよび削除するために使用されます。

PDP コンテキストの作成要求が、PCC 対応 APN 上の SGSN から受信された場合：

1. 認証後、GGSN は、（他の標準 3GPP アトリビュートに加えて）次の Cisco AVP を含む CSG2 にアカウンティング開始メッセージを送信します。
   - pcc_enabled：加入者が Gx ユーザであるかどうかを示します。イネーブルである場合、CSG2 は加入者を Gx ユーザとしてマーキングし、加入者セッションを確立するために PCRF と通信します（イネーブルでない場合、CSG2 は加入者を非 Gx 加入者としてマーキングし、PCRF とは通信しません）。
   - coa_flags：GGSN が、RADIUS CoA メッセージング経由の Gx 更新をサポートするかどうかを示します。イネーブルである場合、GGSN は、RADIUS CoA Gx メッセージング経由の更新をサポートします（イネーブルでない場合は、Mobile Station（MS; モバイル ステーション）によって開始された QoS 更新を示します）。
2. eG-CDR を生成するように GGSN が設定されている場合、GGSN は、アカウンティング開始メッセージに次の追加アトリビュートを含めます。
   - csg:eggsn_qs：拡張クォータ サーバ インターフェイスの IP アドレスとポート番号です。
   - csg:eggsn_qs_mode：拡張クォータ サーバ インターフェイスが、サービス コントロール メッセージを CSG2 と交換できるかどうかを示します。
3. アカウンティング開始要求を受信すると、CSG2 は次のことを実行します。
   a. KUT エントリを作成します。
   b. 受信したアトリビュートに基づいて、Gx ユーザであるかどうかを識別します。
   c. GGSN が eG-CDR を生成したことを識別し、そのユーザのサービス レベル CDR 生成をディセーブルにします。
   d. アカウンティング開始メッセージ内の csg:eggsn_qs アトリビュートで定義されている拡張クォータ サーバ インターフェイスとサービス コントロール メッセージとの交換をイネーブルにします。
4. CSG2 は PCRF と通信して、課金ルールおよび認可された QoS アトリビュートをプロビジョニングします。
5. CSG2 は、認可ステータスおよび認可された QoS アトリビュートの GGSN を通知する CoA 要求を GGSN に送信し、アカウンティング開始応答を GGSN に送信します。
6. Cisco GGSN は、CoA 要求を受信し、認可ステータスに基づいて、PDP コンテキストの作成要求応答を SGSN に送信し、PDP コンテキストが作成されます。
7. トリガー条件が発生すると、SCR メッセージと SCU メッセージが GGSN と CSG2 間で交換されて、サービス コンテナが eG-CDR に追加されるか、eG-CDR が閉じます（あるいはその両方が行われます）。
8. GGSN は eG-CDR を生成し、それらを課金ゲートウェイに送信します。

（注）　APN が PCC 対応である場合、PDP コンテキストの作成応答を SGSN に送信する前に、RADIUS アカウンティング開始応答を待機するように GGSN を設定する必要があります。待機アカウンティングの設定については、「待機アカウンティングの設定」（P.7-4）を参照してください。

APN を PCC 対応 APN として設定するには、アクセス ポイント 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-access-point)# pcc`	APN を PCC 対応 APN として設定します。

スタンドアローン GGSN の前払いクォータ実施の設定

拡張課金サービスを提供するために一緒に実装されたサービス認識 GGSN、Cisco GGSN、および CSG2 を使用して、前払いクォータ実施を実装できます。または、スタンドアローン モードで動作する Cisco GGSN を使用して前払いクォータ実施を実装できます。

スタンドアローン モードで動作する Cisco GGSN を使用して前払い機能を実装した場合、GGSN は、量単位、時間単位、またはその両方を使用して前払い加入者ごとにデータ パケットをモニタリングします。GGSN を量と時間の両方のクォータ用に設定している場合、GGSN は両方の使用状況を検査し、いずれかの使用状況がしきい値に達するか、または期限切れになるとただちに追加クォータを要求します。

スタンドアローン GGSN の前払いクォータ実施を設定する場合は、次の点に注意してください。

- **gprs service-aware** グローバル コンフィギュレーション コマンドを使用して、サービス認識課金のサポートを GGSN でイネーブルにする必要があります。
- 時間の測定は、セッションの確立と同時に開始されます。
- GGSN は、サービス単位ではなく、ユーザ単位でモニタリングします。
- 冗長な設定では、イベント トリガーが発生すると（各クォータの許可時など）、アクティブ GGSN は、クォータ情報をスタンバイ GGSN と同期化します。クォータの使用状況情報の定期的な同期は、実行されません。ユーザへの過剰請求を確実に回避するために、スタンバイ GGSN とアクティブ GGSN は、各クォータ許可とともに CC 要求番号の同期を維持します。
- GGSN はユーザごとにクォータをモニタリングします。したがって、スタンドアローン GGSN がクォータを要求した場合、MSCC AVP で予期されるサービスは 1 つだけとなります。CCA に複数のサービスが含まれているか、または MSCC AVP にサービスが含まれていない場合、CCA は無効な応答であると見なされ、CCFH によって処理が決定されます。
- 単一サービスだけがサポートされています。複数のサービスが設定されている場合は、CCFH によって、GGSN が PDP を拒否するか、または後払いに変換するかが決定されます。
- 二重クォータでは、Quota Holding Timer（QHT）は、Quota Consumption Timer（QCT）のあとに開始されます。QCT は量クォータには適用されず、この動作は時間クォータによって発生します。時間クォータでは、QHT は、QCT のあとに発生する、クォータ消費の停止後に開始されます。
- DCCA プロファイルが課金プロファイルで設定されていない場合、その PDP は拒否されます。
- PDP が後払いに変換されると、拡張 G-CDR は生成されなくなり、G-CDR だけが生成されます。
- 冗長設定では、Quota Validity Timer（QVT）を除くすべてのタイマー（QHT、QCT、時間しきい値など）が、スタンバイ GGSN がアクティブになると再開されます。QVT タイムスタンプが同期化され、スタンバイ GGSN がアクティブになると、その新たにアクティブになった GGSN は、タイマーを再開する代わりに、残りの時間が経過するのを待機します。

スタンドアローン モードで前払い加入者のクォータ実施を実行するように GGSN 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)# **gprs prepaid stand-alone**	スタンドアローン モードで前払いクォータ実施を実行するように GGSN を設定します。

受信した量/時間クォータのパーセンテージとして、量/時間クォータしきい値の最大制限を設定するには、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)# **gprs prepaid quota threshold** *percentage*	DCCA サーバから受信した量/時間クォータ許可のパーセンテージとして、量/時間クォータしきい値の最大制限を設定します。有効な値は 0 ～ 100% です。デフォルトは 80% です。

前払いクォータしきい値を設定する場合、GGSN で使用されるしきい値は次の値よりも小さくなります。

- CCA で受信されるしきい値
- クォータ許可の設定済みパーセンテージ

スタンドアローン クォータ実施をモニタリングするには、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# **clear gprs prepaid quota sanity**	GPRS クォータ許可パラメータの健全性統計情報をクリアします。
Router# **clear gprs prepaid statistics**	GGSN クォータ マネージャ統計情報をクリアします。
Router# **show gprs prepaid quota sanity**	GPRS クォータ許可パラメータの健全性統計情報を表示します。
Router# **show gprs prepaid statistics**	GGSN クォータ マネージャ統計情報を表示します。

APN での課金レコード タイプの設定

Cisco GGSN リリース 9.2 以降では、APN の課金レコード タイプを設定できます。このコマンドは、次のいずれかの条件が存在する場合にサポートされます。

- サービス認識（「サービス認識課金のサポートのイネーブル」（P.7-3）を参照）または PCC 対応（「APN での PCC のイネーブル」（P.7-30）を参照）となるように APN を設定している。
- 交換サービス コントロール メッセージをサポートするようにクォータ サーバ インターフェイスを設定している（「GGSN でのクォータ サーバ インターフェイスの設定」（P.7-6）を参照）。
- GPRS Charging Release 7 が設定されている（「課金リリースの設定」（P.6-8）を参照）。

APN の課金レコード タイプを設定するには、アクセス ポイント 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(access-point-config)# charging record type [gcdr | egcdr | none]`	APN の課金レコード タイプを設定します。それぞれの意味を次に示します。 • **gcdr**：G-CDR が生成されます。 • **egcdr**：eG-CDR が生成されます。 • **none**：レコードは生成されません。 デフォルトでは、G-CDR の生成がイネーブルになっていますが、**cdr suppression** アクセス ポイント コンフィギュレーション コマンドを使用してディセーブルにすることができます。

課金レコード タイプは、次のモードで設定できます。

- グローバル コンフィギュレーション
- 課金プロファイル コンフィギュレーション
- アクセス ポイント コンフィギュレーション

APN レベルで課金レコード タイプを設定する場合は、課金プロファイル コンフィギュレーションによってグローバル コンフィギュレーションが上書きされること、および APN レベル コンフィギュレーションによって課金プロファイル コンフィギュレーションが上書きされることに注意してください。

たとえば、**gprs charging cdr-option service-record** コマンドを使用して、eG-CDR の生成をグローバルにイネーブルにしてから、APN で **charging record type gcdr** コマンドを設定して、G-CDR を生成する APN のユーザを制限できます。残りのサービス認識ユーザは、eG-CDR を生成します。

課金レコード タイプ コマンドが APN レベルで設定されていない場合、デフォルトの動作は、**gprs charging cdr-option service-record** コマンドを使用して設定された既存の eG-CDR 生成グローバル設定に基づきます。

サービス認識 PDP の GTP セッション冗長性の概要

GTP-Session Redundancy（GTP-SR; GTP セッション冗長性）を使用すると、アクティブ GGSN に障害が発生した場合でも、PDP コンテキストに関する必要なすべての情報をスタンバイ GGSN が所有して、サービスを中断することなく続行できます。これは、拡張サービス認識課金環境では、サービス関連の情報についてもアクティブからスタンバイのサービス認識 GGSN に同期化される必要があることを意味します。したがって、GGSN リリース 5.2 以降では、サービス認識 PDP セッションの課金の確立に必要なサービス認識データが、スタンバイ GGSN と同期化されます。

スタンバイ GGSN と同期化されるサービス認識データを次に示します。

- PDP コンテキスト単位のサービス：ルールベース ID および DCCA の障害処理設定（CCSF AVP と CCSH AVP）。
- カテゴリ単位の情報：カテゴリ ID、Cisco CSG2 セッション、およびカテゴリ状態とイベント トリガー。多くのカテゴリ状態は、中間状態であるため、スタンバイのサービス認識 GGSN とは同期化されません。ブラックリスト、アイドル、および認可のカテゴリ状態は同期化されます。

すべてのイベント トリガーが記録されます。アクティブ GGSN でのイベント処理の最後に、イベントのトリガーの消去がスタンバイ GGSN に同期化されます。スイッチオーバーが発生した場合、イベント トリガーがカテゴリ上に存在していると、新たにアクティブになった GGSN がイベントを再開します。

- パス状態：アクティブ GGSN 上のクォータ サーバ プロセスは、Cisco CSG2 へのパスの状態を、スタンバイ GGSN 上のクォータ サーバ プロセスに同期化します。スタンバイ クォータ サーバ上のパス エコー タイマーは、スタンバイ クォータ サーバがアクティブにならないと開始されません。パス シーケンス番号は同期化されません。スイッチオーバーの発生後、新たにアクティブとなったクォータ サーバの番号は 0 から始まります。

（注）　カテゴリ使用状況データは、アクティブ GGSN からスタンバイ GGSN に同期化されません。これにより、スイッチオーバーが発生した場合に使用状況の過剰報告を防ぐことができます。

サービス認識 PDP セッションの GTP-SR のガイドライン

第 5 章「ゲートウェイ GPRS サポート ノード（GGSN）の GPRS トンネリング プロトコル（GTP）セッション冗長性の設定」に記載している、サービス認識 PDP セッションのセッション冗長性を実現するための前提条件に加えて、冗長に設定されたサービス認識 GGSN で次の設定が存在することを確認します。

- グローバル コンフィギュレーション モードで **gprs redundancy** コマンドを使用して、GGSN で GTP-SR がイネーブルになっている。また、GGSN が Diameter ノードとして機能している場合は、グローバル コンフィギュレーション モードで **diameter redundancy** コマンドを使用してセッション状態を追跡できるようになっていることを確認します。Diameter の冗長性の設定については、「Diameter ベースの設定」（P.7-15）を参照してください。
- クォータ サーバ プロセスが、アクティブ GGSN とスタンバイ GGSN の両方で同一に設定されている。特に、アクティブ/スタンバイの各ペアで、クォータ サーバ アドレスが同じであることが必要です。Cisco CSG2 がアクティブなクォータ サーバ プロセスだけと対話するようにするには、クォータ サーバへのメッセージを Gi インターフェイスの仮想 HSRP アドレス経由で常にルーティングするように Cisco CSG2 を設定します。反対に、GGSN は仮想 Cisco CSG2 アドレスを使用して、冗長ペアのアクティブな Cisco CSG2 にメッセージを送信します。仮想 Cisco CSG2 アドレスの設定の詳細については、「Cisco CSG2 サーバ グループの設定」（P.7-6）を参照してください。
- Diameter を使用している場合は、DCCA クライアントの送信元アドレスをアクティブ GGSN とスタンバイ GGSN の両方に設定する必要があります。DCCA クライアントの送信元アドレスは、DCCA サーバへの TCP 接続で使用されるローカル アドレスです。アクティブ GGSN とスタンバイ GGSN 間の仮想 HRSP アドレス経由でルーティング可能な論理インターフェイスを使用することを推奨します。

Cisco IOS HRSP の設定については、『Cisco IOS IP Configuration Guide, Release 12.3』の「*Configuring the Hot Standby Router Protocol*」の項を参照してください。GTP-SR の詳細については、第 5 章「ゲートウェイ GPRS サポート ノード（GGSN）の GPRS トンネリング プロトコル（GTP）セッション冗長性の設定」を参照してください。

Cisco CSG2 での耐障害性については、『*Cisco Content Services Gateway - 2nd Generation Installation and Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/wirelssw/ps779/products_configuration_guide_book09186a0080856678.html

サービスごとのローカル シーケンス番号の同期の設定

課金ゲートウェイはサービスごとのローカル シーケンス番号を使用して、PDP コンテキストに関連付けられている重複サービス コンテナを検出します。

スタンバイ GGSN と同期化されるデータ量を最小化するために、サービスごとのローカル シーケンス番号は拡張 GGSN CDR（eG-CDR）が閉じるたびに同期化されるわけではありません。代わりに、ローカル シーケンス番号の現在値および最後に同期化された PDP コンテキストのローカル シーケンス番号がチェックされ、その差が設定されているウィンドウ サイズよりも大きい場合、現在のローカル シーケンス番号がスタンバイ GGSN と同期化されます。スタンバイ GGSN がアクティブ GGSN になると、同期化された最後の値とウィンドウ サイズから開始されます。

サービスごとのローカル シーケンス番号がスタンバイ GGSN といつ同期化されるかを決定するウィンドウ サイズを設定するには、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# gprs redundancy charging sync-window svc-seqnum size`	サービスごとのローカル シーケンス番号がスタンバイ GGSN といつ同期化されるかを決定するウィンドウ サイズを設定します。有効な値は、1 ～ 200 の数値です。デフォルトは 50 です。

拡張クォータ サーバ インターフェイス ユーザのトリガー条件

Cisco GGSN は、Cisco CSG2 と OCS との直接インターフェイスが存在する場合、加入者が Gx ユーザである場合、またはユーザが後払いである場合に、次のタイプのトリガー条件が発生すると eG-CDR を生成します。

- 「PDP コンテキストの変更」（P.7-36）
- 「タリフ時間の変更」（P.7-36）
- 「サービス フロー レポート」（P.7-36）
- 「eG-CDR の終了」（P.7-37）

（注）　次のトリガー条件では、GGSN での特別な設定は必要ありません。量と期間、およびサービス フローのトリガーが Cisco CSG2 で設定されている必要があります。Cisco CSG2 の設定の詳細については、『*Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide*』を参照してください。

PDP コンテキストの変更

次のいずれかの PDP コンテキスト変更トリガーが発生した場合、GGSN は次の処理を実行します。

- RAT タイプ、PLMN 変更、または MS タイム ゾーンの変更
  - 量コンテナを追加し、そのあとにサービス コンテナのリストを追加します。
  - eG-CDR を閉じます。
  - SVC レコードの制限に達した場合は、eG-CDR を閉じ、一部の CDR を開き、残りの SVC レコードを新しい eG-CDR に追加します。
- QoS の変更またはユーザ位置の変更
  - 量コンテナを追加し、そのあとにサービス コンテナのリストを追加します。
  - 課金条件の最大制限に達した場合は、eG-CDR を閉じます。
  - SVC レコードの制限に達した場合は、eG-CDR を閉じ、一部の CDR を開き、残りの SVC レコードを新しい eG-CDR に追加します。
- SGSN の変更
  - 量コンテナを追加し、そのあとにサービス コンテナのリストを追加します。
  - 最大 SGSN 制限に達した場合は、eG-CDR を閉じます。
  - それ以外の場合は、変更条件の最大制限に達した場合に eG-CDR を閉じます。
  - この中間の場合、SVC レコード制限に達した場合は、eG-CDR を閉じ、一部の CDR を開き、残りの SVC レコードを新しい eG-CDR に追加します。

タリフ時間の変更

タリフ時間が変更されると、GGSN は、次の処理を実行します。

- 量コンテナを追加します。
- 最大変更制限に達した場合は、eG-CDR を閉じます。
- 前払い GTP ユーザの場合、Cisco CSG2 はサービス使用状況メッセージを送信し、GGSN がそのメッセージを eG-CDR に追加する場合があります。

サービス フロー レポート

次のサービス フロー トリガー条件が発生した場合、GGSN はサービスごとにサービス コンテナを生成します。

- 時間制限の期限切れ
- 量制限の期限切れ
- サービス フローの終了

量と期間、およびサービス フローのトリガーが Cisco CSG2 で設定されている必要があります。Cisco CSG2 で量と期間のトリガー、およびサービス フロー トリガーを設定する方法については、『*Cisco Content Services Gateway 2nd Generation - Release 3.5 Installation and Configuration Guide*』を参照してください。

また、GGSN は、前払い GTP ユーザに関して、同じトリガーが Cisco CSG2 に設定されている場合に次のトリガー条件が発生すると、サービス コンテナを生成します。

- 時間しきい値に到達した
- 量しきい値に到達した
- 時間クォータが使い果たされた
- 量クォータが使い果たされた
- サービス データ フローの終了またはサービスのアイドル アウト時

eG-CDR の終了

次の eG-CDR 終了トリガー条件が発生すると、GGSN は、CDR が手動でクリアされた場合を除いて、量コンテナを追加してからサービス コンテナを追加します。

- PDP コンテキストの終了
- 一部のレコードの原因
  - データ量制限
  - 時間制限
  - 変更条件（QoS、タリフ時間、ユーザ位置情報の変更）の最大変更数
  - 管理の介入
  - MS タイム ゾーンの変更
  - PLMN 間の SGSN 変更
  - RAT の変更

設定例

GGSN で設定された拡張サービス認識課金サポートの 1 例を次に示します。

```
Current configuration :3537 bytes
!
! Last configuration change at 15:26:45 UTC Fri Jan 7 2005
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service gprs ggsn
!
hostname sup-samiA
!
boot-start-marker
boot-end-marker
!
enable password abc
!
aaa new-model
!
!
!Configures the CSG2 RADIUS server group
!
aaa group server radius CSG-group
```

```
server 10.10.65.100 auth-port 1812 acct-port 1813
!
!Configures the Diameter server group
!
aaa group server diameter DCCA
server name DCCA
!
!
!Assigns AAA services to the CSG2 RADIUS and Diameter server groups
!
aaa authentication ppp CSG-list group CSG-group
aaa authorization prepaid DCCA group DCCA
aaa authorization network CSG-list group CSG
aaa accounting network CSG-list start-stop group CSG-group
aaa session-id common
ip subnet-zero
!
!
ip cef
!
!
...
!
!
gprs access-point-list gprs
!
...
!
!
!Enables service-aware billing on the GGSN
!
gprs service-aware
!
gprs access-point-list gprs
 access-point 10
  access-point-name cisco.com
  access-mode non-transparent
  aaa-group authentication CSG-list
  aaa-group accounting CSG-list
  gtp response-message wait-accounting
  charging profile any 1 override
  service-aware
  advertise downlink next-hop 10.10.150.2
  !
 access-point 20
  access-point-name yahoo.com
  access-mode non-transparent
  aaa-group authentication CSG
  aaa-group accounting CSG
  gtp response-message wait-accounting
  charging profile any 1 override
  service-aware
  !
 !
!
!Configures a DCCA client profile
!
gprs dcca profile 1
  ccfh continue
  authorization CSG-list
  destination-realm cisco.com
  trigger sgsn-change
  trigger qos-change
!
```

```
gprs charging profile 1
  limit volume 64000
  limit duration 64000
  content rulebase PREPAID
  content dcca profile 1
  content postpaid volume 64000
  content postpaid time 1200
  content postpaid qos-change
  content postpaid sgsn-change
!
!Congigures the quota server
!
ggsn quota-server qs
 interface Loopback2
 csg group csg_1
 !
!
!Configures a CSG2 group
!
ggsn csg-group csg_1
 virtual-address 10.10.65.10
 port 4386
 real-address 10.10.65.2
 !
tftp-server abcbar
!
radius-server host 10.10.65.100 auth-port 1812 acct-port 1813
radius-server host 10.20.154.201 auth-port 1812 acct-port 1813
radius-server key abc
radius-server vsa send accounting
radius-server vsa send accounting 3gpp2
!
!configures Diameter global parameters
!
diameter origin realm corporationA.com
diameter origin host sup-sami42.corporationA.com
diameter vendor supported cisco
!
!configures Diameter peer
!
diameter peer DCCA
 address ipv4 172.18.43.59
 transport tcp port 4100
 timer connection 20
 timer watchdog 25
 destination realm corporationA.com
!
!
...
!
end
```

CHAPTER 8

GGSN へのネットワーク アクセスの設定

この章では、Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）から Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）、Public Data Network（PDN; 公衆データ網）、および任意で Virtual Private Network（VPN; バーチャル プライベート ネットワーク）へのアクセスを設定する方法について説明します。また、GGSN にアクセス ポイントを設定する方法についても説明します。

この章に記載されている GGSN コマンドの詳細については、使用している Cisco GGSN リリースの『*Cisco GGSN Command Reference*』を参照してください。この章に記載されているその他のコマンドのマニュアルを参照するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

この章は、次の内容で構成されています。

SGSN へのインターフェイスの設定

SGSN へのアクセスを確立するには、SGSN へのインターフェイスを設定する必要があります。General Packet Radio Service（GPRS; グローバル パケット ラジオ サービス）/Universal Mobile Telecommunication System（UMTS）では、GGSN と SGSN 間のインターフェイスは *Gn インターフェイス*と呼ばれています。Cisco GGSN では、2.5G と 3G の両方の Gn インターフェイスがサポートされています。

Cisco 7600 シリーズ ルータ プラットフォームでは、Gn インターフェイスはスーパーバイザ エンジンに設定されたレイヤ 3 ルーテッド Gn VLAN への論理インターフェイスとなります（ここに IEEE 802.1Q カプセル化が設定されます）。

スーパーバイザ エンジン上の Gn VLAN の詳細については、「プラットフォームの前提条件」（P.2-2）を参照してください。

インターフェイスの設定の詳細については、『*Cisco IOS Interface Configuration Guide*』および『*Cisco IOS Interface Command Reference*』を参照してください。

802.1Q カプセル化サブインターフェイスの設定

Gn VLAN に対する IEEE 802.1Q カプセル化をサポートするサブインターフェイスを設定するには、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
ステップ 1	`Router(config)# interface gigabitethernet slot/port.subinterface-number`	IEEE 802.1Q が使用されるサブインターフェイスを指定します。
ステップ 2	`Router(config-if)# encapsulation dot1q vlanid`	カプセル化形式を IEEE 802.1Q（dot1q）と定義し、VLAN 識別子を指定します。
ステップ 3	`Router(config-if)# ip address ip-address mask`	インターフェイスのプライマリ IP アドレスを設定します。

SGSN へのインターフェイスの設定の検証

ステップ 1　スーパーバイザ エンジンに Gn インターフェイスを適切に設定したことを検証するには、**show running-config** コマンドを使用します。ファスト イーサネット 8/22 物理インターフェイス設定（太字部分を参照）を SGSN への Gn インターフェイスとして表示するコマンドの出力例を次に示します。

```
Sup# show running-config
Building configuration...

Current configuration :12672 bytes
!
version 12.x
...
interface FastEthernet8/22
 no ip address
 switchport
 switchport access vlan 302
!
interface Vlan101
 description Vlan to GGSN for GA/GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
```

ステップ 2　物理インターフェイスおよび Gn VLAN が利用可能であることを検証するには、スーパーバイザ エンジンで **show interface** コマンドを使用します。次に、課金ゲートウェイへのファスト イーサネット 8/22 物理インターフェイスが稼動している例を示します。Gn VLAN である VLAN 101 が稼動しています。

```
Sup# show ip interface brief FastEthernet8/22
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet8/22           unassigned      YES unset  up                    up
```

```
Sup# show ip interface brief Vlan302
Interface                  IP-Address      OK? Method Status                Protocol
Vlan302                    40.0.2.1        YES TFTP   up                    up

Sup#
```

ステップ 3　Gn VLAN の設定および可用性を検証するには、スーパーバイザ エンジンで **show vlan name** コマンドを使用します。Gn VLAN Gn_1 の例を次に示します。

```
Sup# show vlan name Gn_1

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
302  Gn_1                             active    Gi4/1, Gi4/2, Gi4/3, Gi7/1
                                                Gi7/2, Gi7/3, Fa8/22, Fa8/26

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
302  enet  100302     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

ステップ 4　GGSN で、Gn VLAN への Gn サブインターフェイスを適切に設定したことを検証するには、**show running-config** コマンドを使用します。ギガビット イーサネット 0/0.2 物理インターフェイス設定を課金ゲートウェイへの Gn インターフェイスとして表示するコマンドの出力例を次に示します。

```
GGSN# show running-config
Building configuration...

Current configuration :7390 bytes
!
! Last configuration change at 16:56:05 UTC Wed Jun 25 2003
! NVRAM config last updated at 23:40:27 UTC Fri Jun 13 2003
!
version 12.3
.....
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
.....
ip route 40.1.2.1 255.255.255.255 10.1.1.1
```

ステップ 5　サブインターフェイスが利用可能であることを検証するには、**show ip interface brief** コマンドを使用します。Gn VLAN へのギガビット イーサネット 0/0.2 サブインターフェイスが「稼動」し、プロトコルも「稼動」している例を次に示します。

```
GGSN# show ip interface brief GigabitEthernet0/0.2
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0.2       10.1.1.72       YES NVRAM  up                    up
```

SGSN へのルートの設定

SGSN との通信には、スタティック ルートか、または Open Shortest Path First（OSPF）などのルーティング プロトコルを使用できます。

（注）　SGSN が GGSN と正常に通信するには、SGSN にスタティック ルートを設定するか、または SGSN から GGSN インターフェイスの IP アドレスではなく、GGSN *仮想テンプレート*の IP アドレスに動的にルーティングできるようにする必要があります。

ここでは、スタティック ルートを設定したり、GGSN で OSPF ルーティングをイネーブルにしたりするための基本的なコマンドについて説明します。IP ルートの設定の詳細については、『*Cisco IOS IP Configuration Guide*』および『*Cisco IOS IP Command References*』を参照してください。

この項は、次の内容で構成されています。

SGSN へのスタティック ルートの設定

スタティック ルートは SGSN への固定ルートで、ルーティング テーブルに格納されます。OSPF などのルーティング プロトコルを実装しない場合は、SGSN へのスタティック ルートを設定して、ネットワーク デバイス間のパスを確立できます。

インターフェイスから SGSN へのスタティック ル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
`Router(config)# ip route prefix mask {ip-address | interface-type interface-number} [distance] [tag tag] [permanent]`	スタティック IP ルートを設定します。 • *prefix*：宛先の IP ルート プレフィクスを指定します（これは、SGSN の IP アドレスです）。 • *mask*：宛先のプレフィクス マスクを指定します（これは、SGSN ネットワークのサブネット マスクです）。 • *ip-address*：宛先ネットワークに到達するために使用できるネクストホップの IP アドレスを指定します。 • *interface-type interface-number*：宛先ネットワークに到達するために使用できるネットワーク インターフェイスのタイプとインターフェイス番号を指定します（これは、GGSN で Gn インターフェイスとなるインターフェイスです）。 • *distance*：ルートの管理ディスタンスを指定します。 • **tag** *tag*：ルート マップ経由で再配布を制御するための「一致」値として使用できるタグ値を指定します。 • **permanent**：インターフェイスがシャットダウンした場合でも、ルートを削除しないことを指定します。

OSPF の設定

他のルーティング プロトコルと同じく、OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、そのルーティング プロセスに関連付ける IP アドレスの範囲を指定し、その IP アドレス範囲に関連付けるエリア ID を割り当てる必要があります。

（注）　Cisco 7600 シリーズ ルータ プラットフォームでは、OSPF ルーティング プロセスがスーパーバイザ エンジンに設定されており、GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）Server Load Balancing（SLB; サーバ ロード バランシング）仮想サーバと GGSN 仮想テンプレート アドレスだけをアドバタイズするようになっています。

OSPF 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
ステップ 1	`Router(config)# router ospf process-id`	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。*process-id* には、OSPF ルーティング プロセスのために内部で使用する識別パラメータを指定します。 *process-id* はローカルで割り当てられ、任意の正の整数を指定できます。OSPF ルーティング プロセスごとに一意の値を割り当てます。
ステップ 2	`Router(config-router)# network ip-address wildcard-mask area area-id`	OSPF が動作するインターフェイスを定義し、そのインターフェイスのエリア ID を定義します。 • *ip-address* : OSPF ネットワーク エリアに関連付ける IP アドレスを指定します。 • *wildcard-mask* : OSPF ネットワーク エリアの「don't care」ビットが含まれている IP アドレス マスクを指定します。 • *area-id* : OSPF アドレス範囲に関連付けるエリアを指定します。10 進値または IP アドレスを指定できます。エリアを IP サブネットに関連付ける場合は、エリア ID としてサブネット アドレスを指定できます。

SGSN へのルートの検証

SGSN へのルートを検証するには、まず GGSN 設定を検証し、ルートが確立されていることを検証します。

ステップ 1　スーパーバイザ エンジン設定を検証するには、**show running-config** コマンドを使用し、SGSN に対して設定したルートを検証します。SGSN に対する設定の一部を次に示します。

```
Sup# show running-config
Building configuration...

Current configuration :3642 bytes
!
version 12.3
...
```

```
ip slb vserver V0-GGSN
 virtual 10.10.10.10 udp 3386 service gtp

!
vlan 101
 name Internal_Gn/Ga
!
vlan 302
 name Gn_1
!
vlan 303
 name Ga_1
!
interface FastEthernet8/22
 no ip address
 switchport
 switchport access vlan 302
!
interface FastEthernet8/23
 no ip address
 switchport
 switchport access vlan 302
!
interface FastEthernet8/24
 no ip address
 switchport
 switchport access vlan 303
!
interface Vlan101
 description Vlan to GGSN for GA/GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
!
interface Vlan303
 ip address 40.0.3.1 255.255.255.0
!
router ospf 300
 log-adjacency-changes
 summary-address 9.9.9.0 255.255.255.0
 redistribute static subnets route-map GGSN-routes
 network 40.0.2.0 0.0.0.255 area 300
 network 40.0.3.0 0.0.0.255 area 300
!
ip route 9.9.9.42 255.255.255.255 10.1.1.42
ip route 9.9.9.43 255.255.255.255 10.1.1.43
ip route 9.9.9.44 255.255.255.255 10.1.1.44
ip route 9.9.9.45 255.255.255.255 10.1.1.45
ip route 9.9.9.46 255.255.255.255 10.1.1.46
ip route 9.9.9.72 255.255.255.255 10.1.1.72
ip route 9.9.9.73 255.255.255.255 10.1.1.73
ip route 9.9.9.74 255.255.255.255 10.1.1.74
ip route 9.9.9.75 255.255.255.255 10.1.1.75
ip route 9.9.9.76 255.255.255.255 10.1.1.76
!
access-list 1 permit 9.9.9.0 0.0.0.255
!
route-map GGSN-routes permit 10
 match ip address 1
```

ステップ 2　GGSN 設定を検証するには、**show running-config** コマンドを使用します。SGSN に対する設定の一部を次に示します。

```
Sup# show running-config
Building configuration...

Current configuration :3642 bytes
!
version 12.3
!
...

interface GigabitEthernet0/0
 no ip address
!

interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
ip route 40.1.2.1 255.255.255.255 10.1.1.1
ip route 40.2.2.1 255.255.255.255 10.1.1.1
ip route 40.1.3.10 255.255.255.255 10.1.1.1
ip route 40.2.3.10 255.255.255.255 10.1.1.1
```

ステップ 3　スーパーバイザ エンジンが SGSN へのルートを確立したことを検証するには、次の例に太字で示すように、**show ip route** コマンドを使用します。

```
Sup# show ip route ospf 300
9.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
O       9.9.9.0/24 is a summary, 1w1d, Null0
!

Sup# show ip route 9.9.9.72
Routing entry for 9.9.9.72/32
  Known via "static", distance 1, metric 0
  Redistributing via ospf 300
  Routing Descriptor Blocks:
  * 10.1.1.72
      Route metric is 0, traffic share count is 1
!
```

GGSN でのアクセス ポイントの設定

GGSN にアクセス ポイントを正しく設定するには、モバイル セッションで外部の PDN およびプライベート ネットワークに適切なアクセスを確立できるように、慎重に検討および計画する必要があります。

この項は、次の内容で構成されています。

また、サポート対象の Dynamic Host Configuration Protocol（DHCP）サーバおよび Remote Authentication Dial-In User Service（RADIUS）サーバを使用する場合には、それぞれのサーバとの通信を適切に確立して、アクセス ポイントでダイナミック IP アドレッシング機能およびユーザ認証機能を提供する必要もあります。

アクセス ポイントで DHCP や RADIUS など他のサービスを設定する方法については、「GGSN でのダイナミック アドレッシングの設定」と「GGSN でのセキュリティの設定」の各章で詳しく説明します。

アクセス ポイントの概要

この項は、次の内容で構成されています。

GPRS/UMTS ネットワークのアクセス ポイントの説明

GPRS と UMTS の規格では、Access Point Name（APN; アクセス ポイント ネーム）と呼ばれるネットワーク ID を定義しています。APN は、ネットワークのどの部分にユーザ セッションが確立されるかを識別するための情報です。GPRS/UMTS バックボーンでは、APN は GGSN を参照する情報となります。APN は、GPRS/UMTS ネットワークの GGSN に設定され、GGSN からアクセスできます。

APN を使用すると、公衆データ網（PDN）、プライベート ネットワーク、または企業ネットワークにアクセスできるようになります。また、APN をインターネット アクセスや Wireless Application Protocol（WAP）など特定のタイプのサービスに関連付けることができます。

ユーザがセッションの確立を要求すると、Packet Data Protocol（PDP; パケット データ プロトコル）コンテキストの作成要求メッセージを介して APN が Mobile Station（MS; モバイル ステーション）または SGSN から GGSN に提供されます。

APN を識別するため、次の 2 つの要素からなる論理名が定義されています。

- ネットワーク ID：APN の必須要素で、GGSN が接続される外部のネットワークを識別します。ネットワーク ID は、長さが最大 63 バイトで、ラベルが少なくとも 1 つ含まれている必要があります。複数のラベルが含まれているネットワーク ID は、インターネット ドメイン名であると解釈されます。たとえば、「corporate.com」はネットワーク ID です。
- オペレータ ID：APN の任意の要素であり、GGSN が存在する Public Land Mobile Network（PLMN; パブリック ランド モバイル ネットワーク）を識別します。オペレータ ID は小数点で区切られた 3 つのラベルからなり、最後のラベルは常に「gprs」とする必要があります。たとえば、「mnc10.mcc200.gprs」というようになります。

  オペレータ ID は、存在する場合には、ネットワーク ID のあとに配置されます。この ID は、GGSN の Domain Name System（DNS; ドメイン ネーム システム）名に相当します。APN の最大長は 100 バイトです。オペレータ ID が存在しない場合は、International Mobile Subscriber Identity（IMSI）に含まれる Mobile Network Code（MNC; モバイル ネットワーク コード）および Mobile Country Code（MCC; モバイル国コード）情報から、デフォルトのオペレータ ID が取得されます。

Cisco GGSN でのアクセス ポイントの実装

アクセス ポイントの設定は、Cisco GGSN で中心となる設定作業の 1 つです。GPRS/UMTS ネットワークに GGSN を適切に実装するには、アクセス ポイントを適切に設定する必要があります。

APN を設定する場合、Cisco GGSN ソフトウェアでは次の設定要素を使用します。

- アクセス ポイント リスト：Cisco GGSN の仮想テンプレートに関連付けられる論理インターフェイス。アクセス ポイント リストには、1 つ以上のアクセス ポイントが含まれています。
- アクセス ポイント：APN およびそれに関連付けられたアクセス特性を定義します。アクセス特性には、セキュリティやダイナミック アドレッシング方式などがあります。Cisco GGSN のアクセス ポイントは、仮想アクセス ポイントまたは実アクセス ポイントのいずれかにできます。
- アクセス ポイント インデックス番号：GGSN 設定内の APN を識別するために APN に割り当てられる整数。GGSN コンフィギュレーション コマンドの中には、インデックス番号を使用して APN を参照するものがあります。
- アクセス グループ：ルータに追加で設定可能なルータ セキュリティ。アクセス ポイントに設定して、PDN とのアクセスを制御できます。従来の IP アクセス リストの定義に従って MS から GGSN へのアクセスを許可する場合、IP アクセス グループには（アクセス ポイントで）PDN へのアクセスを許可するかどうかも定義します。IP アクセス グループ設定では、PDN から MS へのアクセスを許可するかどうかも定義できます。

GGSN でのアクセス ポイント タイプ

Cisco IOS GGSN リリース 3.0 以降は、次のアクセス ポイント タイプをサポートしています。

- 実：インターフェイス経由で特定のターゲット ネットワークに直接アクセスするように GGSN を設定するには、実アクセス ポイント タイプを使用します。GGSN は、常に実アクセス ポイントを使用して外部のネットワークに到達します。

  GGSN に実アクセス ポイントを設定する方法の詳細については、「GGSN での実アクセス ポイントの設定」（P.8-11）を参照してください。

- 仮想：GGSN に仮想 APN アクセス ポイントを設定して複数のターゲット ネットワークへのアクセスを統合するには、仮想アクセス ポイント タイプを使用します。GGSN では常に実アクセス ポイントを使用して外部のネットワークに到達するため、GGSN の仮想アクセス ポイントは、実アクセス ポイントと組み合せて使用する必要があります。

  GGSN に仮想アクセス ポイントを設定する方法の詳細については、「GGSN での仮想アクセス ポイントの設定」（P.8-32）を参照してください。

（注）　GGSN リリース 1.4 以前では、実アクセス ポイントだけがサポートされています。PLMN のプロビジョニングの問題に対処するため、GGSN リリース 3.0 以降では、仮想アクセス ポイント タイプもサポートされています。また、GGSN リリース 6.0 と Cisco IOS リリース 12.3(14)YU 以降では、「事前認証」フェーズ中に、ユーザごとにターゲット APN に動的にマッピングされるように仮想 APN を設定できます。詳細については、「GGSN での仮想アクセス ポイントの設定」（P.8-32）を参照してください。

基本的なアクセス ポイント設定の作業リスト

この項では、GGSN にアクセス ポイントを設定するために必要となる、基本的な作業について説明します。仮想 APN アクセスなど特殊な機能向けにアクセス ポイントを設定する方法については、この章の別の項で詳しく説明します。

GGSN にアクセス ポイントを設定するには、次の基本的な作業を実行します。

- 「GGSN での GPRS アクセス ポイント リストの設定」（P.8-10）（必須）
- 「GGSN でのアクセス ポイントの作成およびそのタイプの指定」（P.8-10）（必須）

GGSN での GPRS アクセス ポイント リストの設定

GGSN ソフトウェアでは、*アクセス ポイント リスト*と呼ばれるエンティティを設定する必要があります。GPRS アクセス ポイント リストには、GGSN に設定する仮想アクセス ポイントおよび実アクセス ポイントの集合を定義します。

グローバル コンフィギュレーション モードでアクセス ポイント リストを設定した場合は、GGSN ソフトウェアがアクセス ポイント リストを GGSN の仮想テンプレート インターフェイスに自動的に関連付けます。このため、GGSN では、アクセス ポイント リストは 1 つだけ使用できます。

（注）　GPRS/UMTS アクセス ポイント リストと IP アクセス リストとでは、Cisco IOS ソフトウェアのエンティティが異なることに注意してください。GPRS/UMTS アクセス ポイント リストはアクセス ポイントおよびその関連する特性を定義するものであり、IP アクセス リストは IP アドレスによるルータへのアクセスの許可を制御するものです。アクセス ポイントに対する権限を定義するには、グローバル設定に IP アクセス リストを設定し、アクセス ポイント設定に **ip-access-group** コマンドを設定します。

GPRS/UMTS アクセス ポイント リストを設定し、リスト内にアクセス ポイントを設定するには、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
`Router(config)# gprs access-point-list list-name`	新しいアクセス ポイント リストの名前を指定するか、既存のアクセス ポイント リストの名前を参照し、アクセス ポイント リスト コンフィギュレーション モードを開始します。

GGSN でのアクセス ポイントの作成およびそのタイプの指定

GGSN のアクセス ポイント リストにアクセス ポイントを定義する必要があります。このため、アクセス ポイントを作成するには、まず GGSN に新しいアクセス ポイント リストを定義するか、または既存のアクセス ポイント リストを指定して、アクセス ポイント リスト コンフィギュレーション モードにする必要があります。

アクセス ポイントを作成する場合は、インデックス番号をアクセス ポイントに割り当て、アクセス ポイントのドメイン名（ネットワーク ID）を指定し、アクセス ポイントのタイプ（仮想または実）を指定する必要があります。アクセス ポイントに設定できる他のオプションについては、「追加の実アクセス ポイント オプションの設定」（P.8-20）にまとめます。

アクセス ポイントを作成し、そのタイプを指定するには、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
ステップ 1	`Router(config)# gprs access-point-list list-name`	新しいアクセス ポイント リストの名前を指定するか、既存のアクセス ポイント リストの名前を参照し、アクセス ポイント リスト コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-ap-list)# access-point access-point-index`	新しいアクセス ポイント定義のインデックス番号を指定するか、既存のアクセス ポイント定義を参照し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-access-point)# access-point-name apn-name`	定義されたアクセス ポイントでユーザが GGSN からアクセスできる PDN のネットワーク（またはドメイン）名を指定します。 （注）　*apn-name* は、MS、Home Location Register（HLR; ホーム ロケーション レジスタ）、および DNS サーバでプロビジョニングされる APN に一致する必要があります。
ステップ 4	`Router (config-access-point)# access-type {virtual [pre-authenticate [default-apn apn-name]]| real}`	（任意）アクセス ポイントのタイプを指定します。使用できるオプションは次のとおりです。 • **virtual**：GGSN の特定の物理ターゲット ネットワークに関連付けられていない APN タイプ。任意で、ユーザごとにターゲット APN に動的にマッピングされるように設定することもできます。 • **real**：GGSN の外部ネットワークへのインターフェイスに対応する APN タイプ。これはデフォルト値です。 （注）　デフォルトのアクセス タイプは実です。このため、このコマンドを設定する必要があるのは、APN が仮想アクセス ポイントである場合だけです。

GGSN での実アクセス ポイントの設定

GGSN は、実アクセス ポイントを使用して、GGSN の Gi インターフェイス経由で使用可能な PDN またはプライベート ネットワークと通信します。インターフェイス経由で特定のターゲット ネットワークに直接アクセスするように GGSN を設定するには、実アクセス ポイント タイプを使用します。

仮想アクセス ポイントを設定した場合は、ターゲット ネットワークに到達するための実アクセス ポイントも設定する必要があります。

GGSN は、公衆データ網およびプライベート ネットワークへのアクセス ポイントの設定をサポートしています。ここでは、次のような多様な実アクセス ポイントの設定方法について説明します。

- 「PDN アクセス設定の作業リスト」（P.8-12）
- 「VRF を使用した VPN アクセスの設定の作業リスト」（P.8-13）

PDN アクセス設定の作業リスト

PDN への接続を設定する場合は、次の作業を実行します。

- PDN へのインターフェイスの設定（Gi インターフェイス）（必須）
- PDN のアクセス ポイントの設定（必須）

PDN へのインターフェイスの設定

GPRS/UMTS ネットワークの PDN へのアクセスを確立するには、PDN に接続するように GGSN 上のインターフェイスを設定する必要があります。このインターフェイスは、*Gi インターフェイス*と呼ばれています。

Cisco 7600 シリーズ ルータ プラットフォームでは、このインターフェイスはスーパーバイザ エンジンに設定されたレイヤ 3 ルーテッド Gi VLAN への論理インターフェイスとなります（ここに IEEE 802.1Q カプセル化が設定されます）。

スーパーバイザ エンジン上の Gi VLAN の詳細については、「プラットフォームの前提条件」（P.2-2）を参照してください。

インターフェイスの設定の詳細については、『*Cisco IOS Interface Configuration Guide*』および『*Cisco IOS Interface Command Reference*』を参照してください。

（注）　VPN アクセスに VPN Routing And Forwarding（VRF; VPN ルーティングおよび転送）を使用している場合は、GGSN で Cisco Express Forwarding（CEF）スイッチングをイネーブルにする必要があります。グローバル設定レベルで CEF スイッチングをイネーブルにした場合は、個別のインターフェイスで特にディセーブルにしていないかぎり、どのインターフェイスでも自動的にイネーブルになります。

802.1Q カプセル化サブインターフェイスの設定

Gi VLAN に対する IEEE 802.1Q カプセル化をサポートするサブインターフェイスを設定するには、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
ステップ 1	`Router(config)# interface gigabitethernet slot/port.subinterface-number`	IEEE 802.1Q が使用されるサブインターフェイスを指定します。
ステップ 2	`Router(config-if)# encapsulation dot1q vlanid`	カプセル化形式を IEEE 802.1Q（dot1q）と定義し、VLAN 識別子を指定します。
ステップ 3	`Router(config-if)# ip address ip-address mask`	インターフェイスのプライマリ IP アドレスを設定します。

PDN のアクセス ポイントの設定

PDN のアクセス ポイントを設定するには、GPRS アクセス ポイント リストに実アクセス ポイントを定義する必要があります。

GGSN に実アクセス ポイントを設定するには、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
ステップ 1	`Router(config)# gprs access-point-list list-name`	新しいアクセス ポイント リストの名前を指定するか、既存のアクセス ポイント リストの名前を参照し、アクセス ポイント リスト コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-ap-list)# access-point access-point-index`	新しいアクセス ポイント定義のインデックス番号を指定するか、既存のアクセス ポイント定義を参照し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-access-point)# access-point-name apn-name`	定義されたアクセス ポイントでユーザが GGSN からアクセスできる PDN のネットワーク（またはドメイン）名を指定します。 （注）　*apn-name* は、MS、HLR、および DNS サーバでプロビジョニングされる APN に一致する必要があります。
ステップ 4	`Router(config-access-point)# access-type real`	GGSN の外部ネットワークへのインターフェイスに対応する APN タイプを指定します。デフォルト値は実です。

GPRS アクセス ポイントの設定例については、「アクセス ポイント リスト設定の例」（P.8-52）を参照してください。

VRF を使用した VPN アクセスの設定の作業リスト

Cisco IOS GGSN ソフトウェアは、VPN ルーティングおよび転送（VRF）を使用した VPN への接続をサポートしています。

（注）　VRF は、IPv6 PDP ではサポートされていません。このため、VRF がイネーブルになっている APN に **ipv6** コマンドを設定した場合、IPv4 PDP は VRF でルーティングされますが、IPv6 PDP はグローバル ルーティング テーブルでルーティングされます。

GGSN ソフトウェアでは、数種類の方法で VPN へのアクセスを設定できます。どの方法を使用するかは、稼動中のプラットフォーム、GGSN と PDN 間の Gi インターフェイスに対するネットワーク設定、およびアクセス先の VPN によって異なります。

GGSN で VRF を使用して VPN アクセスを設定するには、次の作業を実行します。

- 「CEF スイッチングのイネーブル」（P.8-14）（必須）
- 「GGSN での VRF ルーティング テーブルの設定」（P.8-14）（必須）
- 「VRF を使用した VPN へのルートの設定」（P.8-14）（必須）
- 「VRF を使用した PDN へのインターフェイスの設定」（P.8-16）（必須）
- 「VPN へのアクセスの設定」（P.8-16）（必須）

設定例については、「VRF トンネル設定の例」（P.8-53）を参照してください。

CEF スイッチングのイネーブル

CEF スイッチングを GGSN でグローバルにイネーブルにすると、GGSN のすべてのインターフェイスで CEF スイッチングが自動的にイネーブルになります。

（注）　CEF スイッチングを適切に機能させるには、**no ip cef** コマンドを使用して CEF スイッチングをディセーブルにしたあと、少し待ってから CEF スイッチングをイネーブルにします。

GGSN 上のどのインターフェイスでも CEF スイッチ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)#` **`ip cef`**	プロセッサで CEF をイネーブルにします。

GGSN での VRF ルーティング テーブルの設定

GGSN に VRF ルーティング テーブルを設定するには、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
ステップ 1	`Router(config)#` **`ip vrf`** *`vrf-name`*	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-vrf)#` **`rd`** *`route-distinguisher`*	VRF のルーティング テーブルおよび転送テーブルを作成し、VPN のデフォルトのルート識別子を指定します。

VRF を使用した VPN へのルートの設定

GGSN とアクセス先のプライベート ネットワークとの間にルートが存在することを確認してください。GGSN からプライベート ネットワーク アドレスに対して **ping** コマンドを使用して、接続性を検証できます。ルートを設定するには、スタティック ルートまたはルーティング プロトコルを使用できます。

VRF を使用したスタティック ルートの設定

VRF を使用してスタティック ル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
Router(config)# **ip route vrf** *vrf-name prefix mask* [*next-hop-address*] [*interface* {*interface-number*}] [**global**] [*distance*] [**permanent**] [**tag** *tag*]	スタティック IP ルートを設定します。 • *vrf-name*：スタティック ルート用の VPN ルーティングおよび転送インスタンス（VRF）の名前を指定します。 • *prefix*：宛先の IP ルート プレフィクスを指定します。 • *mask*：宛先のプレフィクス マスクを指定します。 • *next-hop-address*：宛先ネットワークに到達するために使用できるネクストホップの IP アドレスを指定します。 • *interface interface-number*：宛先ネットワークに到達するために使用できるネットワーク インターフェイスのタイプとインターフェイス番号を指定します。 • **global**：指定のネクストホップ アドレスが VRF ルーティング テーブル以外のテーブルにあることを指定します。 • *distance*：ルートの管理ディスタンスを指定します。 • **permanent**：インターフェイスがシャットダウンした場合でも、ルートを削除しないことを指定します。 • **tag** *tag*：ルート マップ経由で再配布を制御するための「一致」値として使用できるタグ値を指定します。

VRF を使用したスタティック ルートの検証

設定したスタティック VRF ルートが GGSN によって確立されたことを検証するには、次の例に示すように、**show ip route vrf** 特権 EXEC コマンドを使用します。

```
GGSN# show ip route vrf vpn1 static
     172.16.0.0/32 is subnetted, 1 subnets
U       172.16.0.1 [1/0] via 0.0.0.0, Virtual-Access2
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
S       10.100.0.3/32 [1/0] via 10.110.0.13
```

VRF を使用した OSPF ルートの設定

VRF を使用して OSPF ル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
Router(config)# **router ospf** *process-id* [**vrf** *vrf-name*]	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。 • *process-id*：OSPF ルーティング プロセスのために内部で使用する識別パラメータを指定します。*process-id* はローカルで割り当てられ、任意の正の整数を指定できます。OSPF ルーティング プロセスごとに一意の値を割り当てます。 • **vrf** *vrf-name*：VPN ルーティングおよび転送インスタンスの名前を指定します。

VRF を使用した PDN へのインターフェイスの設定

PDN へのアクセスを確立するには、PDN に接続するためのインターフェイスが GGSN 上に必要です。このインターフェイスは、Gi インターフェイスと呼ばれています。

Cisco 7600 シリーズ ルータ プラットフォームでは、このインターフェイスはスーパーバイザ エンジンに設定されたレイヤ 3 ルーテッド Gi VLAN への論理インターフェイスとなります（ここに IEEE 802.1Q カプセル化が設定されます）。

スーパーバイザ エンジン上の Gi VLAN の詳細については、「プラットフォームの前提条件」（P.2-2）を参照してください。

インターフェイスの設定の詳細については、『*Cisco IOS Interface Configuration Guide*』および『*Cisco IOS Interface Command Reference*』を参照してください。

（注）　VPN アクセスに VRF を使用している場合は、GGSN で CEF スイッチングをイネーブルにする必要があります。グローバル設定レベルで CEF スイッチングをイネーブルにした場合は、個別のインターフェイスで特にディセーブルにしていないかぎり、どのインターフェイスでも自動的にイネーブルになります。

802.1Q カプセル化サブインターフェイスの設定

Gi VLAN に対する IEEE 802.1Q カプセル化をサポートするサブインターフェイスを設定するには、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
ステップ 1	`Router(config)# interface gigabitethernet slot/port.subinterface-number`	IEEE 802.1Q が使用されるサブインターフェイスを指定します。
ステップ 2	`Router(config-if)# encapsulation dot1q vlanid`	カプセル化形式を IEEE 802.1Q（dot1q）と定義し、VLAN 識別子を指定します。
ステップ 3	`Router(config-if)# ip address ip-address mask`	インターフェイスのプライマリ IP アドレスを設定します。

VPN へのアクセスの設定

前提となる設定作業を完了したあと、トンネルを使用する、または使用しない VPN へのアクセスを設定できます。

ここでは、VPN へのアクセスを設定するためのさまざまな方法について説明します。

トンネルのない VPN へのアクセスの設定

トンネルのある VPN へのアクセスの設定

（注）　GGSN リリース 5.0 以降では、複数の APN を同じ VRF に割り当てることができます。

トンネルのない VPN へのアクセスの設定

複数の Gi インターフェイスを異なる PDN に設定し、そのうちの 1 つの PDN から VPN にアクセスする必要がある場合、IP トンネルを設定しなくても、その VPN へのアクセスを設定できます。このような場合に VPN へのアクセスを設定するには、**vrf** アクセス ポイント コンフィギュレーション コマンドを設定する必要があります。

GPRS アクセス ポイント リストに VPN へのアクセスを設定するには、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
ステップ 1	`Router(config)# gprs access-point-list list-name`	新しいアクセス ポイント リストの名前を指定するか、既存のアクセス ポイント リストの名前を参照し、アクセス ポイント リスト コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-ap-list)# access-point access-point-index`	新しいアクセス ポイント定義のインデックス番号を指定するか、既存のアクセス ポイント定義を参照し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-access-point)# access-point-name apn-name`	定義されたアクセス ポイントでユーザが GGSN からアクセスできる PDN のネットワーク（またはドメイン）名を指定します。 （注）　*apn-name* は、MS、HLR、およびドメイン ネーム システム（DNS）サーバでプロビジョニングされる APN に一致する必要があります。
ステップ 4	`Router(config-access-point)# access-type real`	GGSN の外部ネットワークへのインターフェイスに対応する APN タイプを指定します。デフォルト値は実です。
ステップ 5	`Router(config-access-point)# vrf vrf-name`	GGSN アクセス ポイントで VRF を設定し、アクセス ポイントを特定の VRF インスタンスに関連付けます。
ステップ 6	`Router(config-access-point)# exit`	アクセス ポイント コンフィギュレーション モードを終了します。

他のアクセス ポイント設定オプションの詳細については、「追加の実アクセス ポイント オプションの設定」（P.8-20）を参照してください。

トンネルのある VPN へのアクセスの設定

PDN から 1 つ以上の VPN にアクセスする必要があるものの、その PDN への Gi インターフェイスが 1 つだけである場合は、それらのプライベート ネットワークにアクセスするための IP トンネルを設定できます。

トンネルを使用する VPN へのアクセスを設定するには、次の作業を実行します。

- VPN アクセス ポイントの設定（必須）
- IP トンネルの設定（必須）

VPN アクセス ポイントの設定

GPRS アクセス ポイント リストに VPN へのアクセスを設定するには、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
ステップ 1	`Router(config)# gprs access-point-list` *list-name*	新しいアクセス ポイント リストの名前を指定するか、既存のアクセス ポイント リストの名前を参照し、アクセス ポイント リスト コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-ap-list)# access-point` *access-point-index*	新しいアクセス ポイント定義のインデックス番号を指定するか、既存のアクセス ポイント定義を参照し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-access-point)# access-point name` *apn-name*	アクセス ポイント ネットワーク ID を指定します。これには、インターネット ドメイン名が広く使用されています。 **（注）** *apn-name* は、MS、HLR、および DNS サーバでプロビジョニングされる APN に一致する必要があります。
ステップ 4	`Router(config-access-point)# access-mode` {**transparent** | **non-transparent**}	（任意）GGSN では PDN へのアクセス ポイントでユーザ認証を要求するかどうかを指定します。使用できるオプションは次のとおりです。 • **transparent**：このアクセス ポイントに対しては、セキュリティ認証および認可のいずれも GGSN によって要求されません。これはデフォルト値です。 • **non-transparent**：GGSN は、認証を実施するプロキシとして機能します。
ステップ 5	`Router(config-access-point)# access-type real`	GGSN の外部ネットワークへのインターフェイスに対応する APN タイプを指定します。デフォルト値は実です。

	コマンド	目的
ステップ 6	`Router(config-access-point)# ip-address-pool {dhcp-proxy-client | radius-client | local pool-name | disable}`	（任意）IP アドレス プールを使用するダイナミック アドレス割り当て方法を現在のアクセス ポイントのために指定します。使用できるオプションは次のとおりです。 • **dhcp-proxy-client**：DHCP サーバが IP アドレス プールを提供します。 • **radius-client**：RADIUS サーバが IP アドレス プールを提供します。 • **local**：ローカル プールが IP アドレスを提供することを指定します。このオプションを機能させるには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用して、ローカル プールを設定する必要があります。 • **disable**：ダイナミック アドレス割り当てをオフにします。 **（注）** ダイナミック アドレス割り当て方法を使用している場合は、適切な IP アドレス プール ソースに従ってこのコマンドを設定する必要があります。
ステップ 7	`Router(config-access-point)# vrf vrf-name`	GGSN アクセス ポイントで VPN ルーティングおよび転送を設定し、アクセス ポイントを特定の VRF インスタンスに関連付けます。
ステップ 8	`Router(config-access-point)# exit`	アクセス ポイント コンフィギュレーション モードを終了します。

他のアクセス ポイント設定オプションの詳細については、「追加の実アクセス ポイント オプションの設定」（P.8-20）を参照してください。

IP トンネルの設定

トンネルを設定する場合は、ループバック インターフェイスを実インターフェイスではなく、トンネル エンドポイントとして使用することを推奨します。これは、ループバック インターフェイスが常に稼動しているためです。

プライベート ネットワークへの IP トンネルを設定するには、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
ステップ 1	`Router(config)# interface tunnel number`	論理トンネル インターフェイス番号を設定します。
ステップ 2	`Router(config-if)# ip vrf forwarding vrf-name`	VRF インスタンスをインターフェイスに関連付けます。
ステップ 3	`Router(config-if)# ip address ip-address mask [secondary]`	トンネル インターフェイスの IP アドレスを指定します。 **（注）** この IP アドレスは、GGSN に関する他の設定では使用されません。

	コマンド	目的
ステップ 4	`Router(config-if)# tunnel source {ip-address | type number}`	PDN またはループバック インターフェイスへの Gi インターフェイスの IP アドレス（またはインターフェイス タイプと、ポート番号かカード番号）を指定します。
ステップ 5	`Router(config-if)# tunnel destination {hostname | ip-address}`	このトンネルからアクセスできるプライベート ネットワークの IP アドレス（またはホスト名）を指定します。

追加の実アクセス ポイント オプションの設定

この項では、GGSN アクセス ポイントに対して指定できる設定オプションの要約を示します。

これらのオプションの中には、GGSN を設定する他のグローバル ルータ設定と組み合せて使用されるものがあります。一部のオプションの設定については、この章の他のトピックおよびこのマニュアルの他の章でさらに詳しく説明します。

（注） Cisco IOS ソフトウェアでは仮想アクセス ポイントで他のアクセス ポイント オプションを設定することもできますが、仮想アクセス ポイントには **access-point-name** コマンドと **access-type** コマンドだけを適用できます。他のアクセス ポイント コンフィギュレーション コマンドは、設定しても無視されます。

GGSN アクセス ポイントのオプションを設定するには、アクセス ポイント リスト 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
ステップ 1	`Router(config-access-point)# aaa-accounting {enable | disable}`	GGSN の特定のアクセス ポイントに対するアカウンティングをイネーブルまたはディセーブルにします。 （注） 透過的アクセスの APN を設定し、その APN でアカウンティングを提供する場合は、APN で **aaa-accounting enable** コマンドを設定する必要があります。
ステップ 2	`Router(config-access-point)# aaa-group {authentication | accounting} server-group`	認証、認可、アカウンティング（AAA）を担当するデフォルトのサーバ グループを指定し、そのサーバ グループでサポートする AAA サービスのタイプを GGSN の特定のアクセス ポイントに対して割り当てます。詳細は次のとおりです。 • **authentication**：選択したサーバ グループを APN での認証サービスに割り当てます。 • **accounting**：選択したサーバ グループを APN でのアカウンティング サービスに割り当てます。 • *server-group*：APN での AAA サービスに使用される AAA サーバ グループの名前を指定します。 （注） 指定する AAA サーバ グループの名前は、**aaa group server** コマンドを使用して設定するサーバ グループに対応している必要があります。

	コマンド	目的
ステップ 3	`Router(config-access-point)# access-mode {transparent | non-transparent}`	（任意）GGSN では PDN へのアクセス ポイントでユーザ認証を要求するかどうかを指定します。使用できるオプションは次のとおりです。 • **transparent**：このアクセス ポイントに対しては、セキュリティ認証および認可のいずれも GGSN によって要求されません。これはデフォルト値です。 • **non-transparent**：GGSN は、認証を実施するプロキシとして機能します。
ステップ 4	`Router(config-ap-list)# access-point access-point-index`	新しいアクセス ポイント定義のインデックス番号を指定するか、既存のアクセス ポイント定義を参照し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 5	`Router(config-access-point)# access-point-name apn-name`	定義されたアクセス ポイントでユーザが GGSN からアクセスできる PDN のネットワーク（またはドメイン）名を指定します。 **（注）** *apn-name* は、MS、HLR、および DNS サーバでプロビジョニングされる APN に一致する必要があります。
ステップ 6	`Router(config-access-point)# access-type {virtual | real}`	（任意）アクセス ポイントのタイプを指定します。使用できるオプションは次のとおりです。 • **virtual**：特定の物理ターゲット ネットワークに関連付けられていない APN タイプ。 • **real**：GGSN の外部ネットワークへのインターフェイスに対応する APN タイプ。これはデフォルト値です。 **（注）** デフォルトのアクセス タイプは実です。このため、このコマンドを設定する必要があるのは、APN が仮想アクセス ポイントである場合だけです。
ステップ 7	`Router(config-access-point)# access-violation deactivate-pdp-context}`	（任意）ユーザがアクセス ポイント経由で PDN への不正アクセスを試みた場合は、ユーザのセッションを終了し、ユーザ パケットを廃棄することを指定します。
ステップ 8	`Router(config-access-point)# aggregate {auto | ip-network-prefix{/mask-bit-length | ip-mask}}`	（任意）指定のネットワークの MS から GGSN の特定のアクセス ポイント経由で PDP 要求を受信した場合は、IP ルーティング テーブルに集約ルートを作成するように GGSN を設定します。 **（注）** ローカル IP アドレス プールを使用している場合、**aggregate auto** コマンドではルートは集約されません。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 9	`Router(config-access-point)# anonymous user username [password]`	（任意）アクセス ポイントに匿名ユーザ アクセスを設定します。

	コマンド	目的
ステップ 10	`Router(config-access-point)# block-foreign-ms`	（任意）モバイル ユーザのホーム PLMN に基づいて、特定のアクセス ポイントで GGSN アクセスを制限します。
ステップ 11	`Router(config-access-point)# cac-policy`	（任意）Call Admission Control（CAC; コール アドミッション制御）機能の最大 QoS ポリシー機能をイネーブルにし、ポリシーをアクセス ポイントに適用します。
ステップ 12	`Router(config-access-point)# charging group` *chrg-group-number*	既存の課金グループを APN に関連付けます。*group-number* は 1 から 29 までのいずれかの数字です。
ステップ 13	`Router(config-access-point)# dhcp-gateway-address` *ip-address*	（任意）モバイル ステーション（MS）ユーザが特定の PDN アクセス ポイントに入ることができるよう、DHCP 要求を処理する DHCP ゲートウェイを指定します。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 14	`Router(config-access-point)# dhcp-server` {*ip-address*} [*ip-address*] [**vrf**]	（任意）特定の PDN アクセス ポイントに入ろうとしている MS ユーザに IP アドレスが割り当てられるよう、プライマリ（およびバックアップ）DHCP サーバを指定します。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 15	`Router(config-access-point)# dns primary` *ip-address* **secondary** *ip-address*	（任意）アクセス ポイントから PDP コンテキストの作成応答で送信されるプライマリ（およびバックアップ）DNS を指定します。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。

	コマンド	目的
ステップ 16	`Router(config-access-point)# gtp pdp-context single pdp-session [mandatory]`	（任意）PDP セッションがハングした場合には、プライマリ PDP コンテキストと、（関連付けられていれば）セカンダリ PDP コンテキストを削除するように、GGSN を設定します。実際にこの削除が行われるのは、同じ MS から、ハングしている PDP コンテキストと同じ IP アドレスを共有する作成要求を新たに受信したときです。 ハングしている PDP コンテキストとは、GGSN 上の PDP コンテキストのうち、何らかの理由で SGSN 上の対応する PDP コンテキストがすでに削除されたもののことです。 PDP セッションがハングし、**gtp pdp-context single pdp-session** コマンドが設定されていない場合、（同じ APN の）同じ MS から、Network Service Access Point Identifiers（NSAPI; ネットワーク サービス アクセス ポイント ID）は異なるものの、ハングした PDP セッションで使用されているのと同じ IP アドレスが割り当てられている PDP コンテキストの作成要求が新たに送信されると、GGSN ではその PDP コンテキストの作成要求を拒否します。 この機能は、**mandatory** キーワードを指定せずに設定すると、シスコ Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）「gtp-pdp-session=single-session」が RADIUS ユーザ プロファイルに定義されているユーザにだけ適用されます。 この機能をイネーブルにし、RADIUS ユーザ プロファイルに関係なく APN のすべてのユーザに適用するには、**mandatory** キーワード オプションを指定します。 **（注）** この機能を GTP ロード バランシングとともに使用すると、正常に機能しない場合があります。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 17	`Router(config-access-point)# gtp response-message wait-accounting`	（任意）PDP コンテキストの作成応答を SGSN に送信する前に RADIUS アカウンティング応答を待機するように、GGSN を設定します。
ステップ 18	`Router(config-access-point)# gtp pdp-context timeout idle` *interval* `[uplink]`	（任意）特定のアクセス ポイントでセッションがアイドル状態のままで存続できる時間を秒単位で指定します。この時間を過ぎると、GGSN はセッションを終了します。
ステップ 19	`Router(config-access-point)# gtp pdp-context timeout session` *interval* `[uplink]`	（任意）任意のアクセス ポイントにセッションが存在できる時間を秒単位で指定します。この時間を過ぎると、GGSN はセッションを終了します。

	コマンド	目的
ステップ 20	Router(config-access-point)# **ip-access-group** *access-list-number* {**in** | **out**}	（任意）特定のアクセス ポイントに MS から GGSN を経由して PDN に至るアクセスの権限を指定します。*access-list-number* には、アクセス ポイントで使用する IP アクセス リスト定義を指定します。使用できるオプションは次のとおりです。 • **in** : PDN から MS までの IP アクセス リスト定義を適用します。 • **out** : MS から PDN までの IP アクセス リスト定義を適用します。 **（注）** ICMP メッセージの送信をディセーブルにするには、**no ip unreachable** インターフェイス コンフィギュレーション コマンドを仮想テンプレート インターフェイスに設定します。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 21	Router(config-access-point)# **ip-address-pool** {**dhcp-proxy-client** | **radius-client** | **local** *pool-name* | **disable**}	（任意）IP アドレス プールを使用するダイナミック アドレス割り当て方法を現在のアクセス ポイントのために指定します。使用できるオプションは次のとおりです。 • **dhcp-proxy-client** : DHCP サーバが IP アドレス プールを提供します。 • **radius-client** : RADIUS サーバが IP アドレス プールを提供します。 • **local** : ローカル プールが IP アドレスを提供することを指定します。このオプションを機能させるには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用して、ローカル プールを設定する必要があります。 • **disable** : ダイナミック アドレス割り当てをオフにします。 **（注）** ダイナミック アドレス割り当て方法を使用している場合は、適切な IP アドレス プール ソースに従ってこのコマンドを設定する必要があります。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 22	Router(config-access-point)# **ip probe path** *ip_address* **protocol udp** [**port** *port* **ttl** *ttl*]	（任意）APN に正常に確立されている PDP コンテキストごとに、GGSN から特定の宛先に probe パケットを送信できるようにします。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 23	Router(config-access-point)# **ipv6 ipv6-access-group** *ACL-name* [**up** | **down**]	（任意）Access-Control List（ACL; アクセス コントロールリスト）設定をアップリンクまたはダウンリンクの IPv6 ペイロード パケットに適用します。

	コマンド	目的
ステップ 24	`Router(config-access-point)# ipv6 ipv6-address-pool {local pool-name | radius-client}`	（任意）アクセス ポイントにダイナミック IPv6 プレフィクス割り当て方法を設定します。
ステップ 25	`Router(config-access-point)# ipv6 base-vtemplate number`	（任意）仮想テンプレート インターフェイスを指定します。IPv6 Routing Advertisement（RA; ルーティング アドバタイズメント）パラメータが含まれており、APN にコピーして IPv6 PDP コンテキスト用の仮想サブインターフェイスを作成できるようになっています。
ステップ 26	`Router(config-access-point)# ipv6 dns primary ipv6-address [secondary ipv6-address]`	（任意）アクセス ポイントから IPv6 PDP コンテキストの作成応答で送信されるプライマリ（およびバックアップ）IPv6 DNS のアドレスを指定します。
ステップ 27	`Router(config-access-point)# ipv6 [enable | exclusive]`	（任意）IPv6 と IPv4 の両方の PDP コンテキストを許可したり、IPv6 PDP コンテキストだけを許可したりするように、アクセス ポイントを設定します。
ステップ 28	`Router(config-access-point)# ipv6 redirect [all | intermobile] ipv6-address`	（任意）IPv6 トラフィックを外部の IPv6 デバイスにリダイレクトするように、GGSN を設定します。使用できるオプションは次のとおりです。 • **all**：すべての IPv6 トラフィックを APN の外部の IPv6 デバイスにリダイレクトします。 • **intermobile**：モバイル間 IPv6 トラフィックを外部の IPv6 デバイスにリダイレクトします。 • *ipv6-address*：IPv6 トラフィックのリダイレクト先となる IPv6 外部デバイスの IP アドレス。
ステップ 29	`Router(config-access-point)# ipv6 security verify source`	（任意）GGSN で、MS に以前に割り当てられていたアドレスと照合して、アップストリーム TPDU の IPv6 送信元アドレスを検証できるようにします。
ステップ 30	`Router(config-access-point)# msisdn suppression [value]`	（任意）GGSN では、Mobile Station ISDN（MSISDN; モバイル ステーション ISDN）番号を、RADIUS サーバへの認証要求に事前設定された値で上書きすることを指定します。
ステップ 31	`Router(config-access-point)# nbns primary ip-address secondary ip-address`	（任意）アクセス ポイントから PDP コンテキストの作成応答で送信されるプライマリ（およびバックアップ）NetBIOS Name Service（NBNS）を指定します。 **（注）**　この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 32	`Router(config-access-point)# network-behind-mobile`	アクセス ポイントが、モバイル ステーション（MS）背後へのルーティングをサポートできるようにします。 **（注）**　この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 33	`Router(config-access-point)# pcc`	APN を Policy and Charging Control（PCC; ポリシー/課金制御）対応 APN として設定します。

	コマンド	目的
ステップ 34	`Router(config-access-point)# ppp-regeneration [max-session number | setup-time seconds | verify-domain | fixed-domain | allow-duplicate]`	（任意）アクセス ポイントが、PPP 再生成をサポートできるようにします。 • **max-session** *number* : アクセス ポイントで許可されている PPP 再生成セッションの最大数を指定します。デフォルト値はデバイスに依存し、ルータでサポート可能な最大 IDB によって決まります。 • **setup-time** *seconds* : PPP 再生成セッションの確立に許可されている最大時間（1 から 65535 秒）を指定します。デフォルト値は 60 秒です。 • **verify-domain** : PPP 再生成が使用されている場合には、PDP コンテキストの作成要求で送信された Protocol Configuration Option（PCO; プロトコル設定オプション）Information Element（IE; 情報エレメント）に含まれるドメインを、ユーザが送信した APN と照合して検証するように、GGSN を設定します。 不一致が発生した場合、PDP コンテキストの作成要求は原因コード「Service not supported」で拒否されます。 • **fixed-domain** : PPP 再生成が使用されている場合、アクセス ポイント ネームを、ユーザまでの L2TP トンネルを開始するドメイン名として使用するように、GGSN を設定します。 **ppp-regeneration fixed-domain** と **ppp-regeneration verify-domain** コマンド設定は、相互に排他的です。**ppp-regeneration fixed-domain** コマンドが設定されている場合、ドメイン検証は実行できません。 • **allow-duplicate** : PPP 生成 PDP コンテキストの場合は IP アドレスの重複をチェックしないように、GGSN を設定します。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 35	`Router(config-access-point)# radius attribute acct-session-id charging-id`	（任意）アクセス要求に Acct-Session-ID（アトリビュート 44）の課金 ID が含まれることを指定します。
ステップ 36	`Router(config-access-point)# radius attribute nas-id format`	（任意）GGSN が APN でのアクセス要求に NAS-Identifier を含めて送信することを指定します。*format* はアトリビュート 32 で送信される文字列で、IP アドレス（%i）、ホスト名（%h）、およびドメイン名（%d）が含まれています。

	コマンド	目的
ステップ 37	`Router(config-access-point)# radius attribute suppress [imsi | qos | sgsn-address]`	（任意）GGSN が RADIUS サーバへの認証要求およびアカウンティング要求で次の情報を抑制することを指定します。 • **imsi**：3GPP-IMSI 番号を抑制します。 • **qos**：3GPP-GPRS-QoS プロファイルを抑制します。 • **sgsn-address**：3GPP-GPRS-SGSN-Address を抑制します。
ステップ 38	`Router(config-access-point)# radius attribute user-name msisdn`	（任意）アクセス要求の User-Name（アトリビュート 1）フィールドに MSISDN が含まれることを指定します。
ステップ 39	`Router(config-access-point) redirect all ip ip address`	（任意）すべてのトラフィックを外部デバイスにリダイレクトするように、GGSN を設定します。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 40	`Router(config-access-point) redirect intermobile ip ip address`	（任意）モバイル間トラフィックを外部デバイスにリダイレクトするように、GGSN を設定します。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 41	`Router(config-access-point) security verify {source | destination}`	GGSN が、Gn インターフェイスから受信した Transport Protocol Data Unit（TPDU; 転送プロトコル データ ユニット）の送信元アドレスまたは宛先アドレスを検証することを指定します。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。
ステップ 42	`Router(config-access-point)# session idle-timer number`	（任意）GGSN が現在のアクセス ポイントでアイドル状態のモバイル セッションを終了するまでに待機する時間（1 から 168 時間）を指定します。
ステップ 43	`Router(config-access-point)# subscription-required`	（任意）アクセス ポイント経由で PDN にアクセスするには加入が必要かどうかを判断するために、GGSN が PDP コンテキスト要求の選択モードの値をチェックすることを指定します。
ステップ 44	`Router(config-access-point)# vrf vrf-name`	（任意）GGSN アクセス ポイントで VPN ルーティングおよび転送を設定し、アクセス ポイントを特定の VRF インスタンスに関連付けます。 **（注）** この設定は、IPv4 PDP コンテキストに適用されます。

実アクセス ポイント設定の検証

この項では、GGSN にアクセス ポイントを適切に設定したことを検証する方法について説明します。このための作業は次のとおりです。

- 「GGSN 設定の検証」（P.8-28）
- 「アクセス ポイント経由でのネットワークの到達可能性の検証」（P.8-30）

GGSN 設定の検証

GGSN にアクセス ポイントを適切に設定したことを検証するには、**show running-config** コマンドおよび **show gprs access-point** コマンドを使用します。

（注）　**show running-config** コマンドの出力では、まず、仮想テンプレート インターフェイスの下に **gprs access-point-list** コマンドが出力されます。このことは、GPRS アクセス ポイント リストが設定されており、かつ仮想テンプレートに関連付けられていることを示します。GPRS アクセス ポイント リスト内の、特定のアクセス ポイントの設定を検証するには、**show** コマンドの出力の、さらに下の部分を参照します。**gprs access-point-list** コマンドが再び出力されており、そのあとに個々のアクセス ポイント設定が続きます。

ステップ 1　グローバル コンフィギュレーション モードから、次の例に示すように、**show running-config** コマンドを使用します。**gprs access-point-list** コマンドが仮想テンプレート インターフェイスの下に出力されていることを検証し、**gprs access-point-list** セクション内で太字で示された個々のアクセス ポイントの設定を検証します。

```
Router# show running-config
Building configuration...

Current configuration : 3521 bytes
!
version 12.x
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service gprs ggsn
!
hostname ggsn
!
ip cef
!
...
!
interface loopback 1
 ip address 10.40.40.3 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
. . .
!
gprs access-point-list gprs
!
  access-point 1
   access-point-name gprs.cisco.com
```

```
   access-mode non-transparent
   aaa-group authentication abc
   network-request-activation
   exit
!
  access-point 2
   access-point-name gprt.cisco.com
   exit
!
  access-point 3
   access-point-name gpru.cisco.com
   ip-address-pool radius-client
   access-mode non-transparent
   aaa-group authentication abc
   exit
!
gprs maximum-pdp-context-allowed 90000
gprs gtp path-echo-interval 0
gprs default charging-gateway 10.15.15.1
!
gprs memory threshold 512
!
...
radius-server host 172.18.43.7 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 3
radius-server key 7 12150415
call rsvp-sync
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
gatekeeper
 shutdown
end
```

ステップ 2　GGSN の特定のアクセス ポイントの設定をさらに詳しく表示するには、次の例に示すように、**show gprs access-point** コマンドを使用し、アクセス ポイントのインデックス番号を指定します。

```
Router# show gprs access-point 2
    apn_index 2          apn_name = gprt.cisco.com
    apn_mode: transparent
    apn-type: Real
    accounting: Disable
    wait_accounting: Disable
    dynamic_address_pool: not configured
    apn_dhcp_server: 0.0.0.0
    apn_dhcp_gateway_addr: 0.0.0.0
    apn_authentication_server_group:
    apn_accounting_server_group:
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: No
    network_activation_allowed: No
    Block Foreign-MS Mode: Disable
    VPN: Disable
    GPRS vaccess interface: Virtual-Access1
    number of ip_address_allocated 0

    Total number of PDP in this APN :1
```

```
    aggregate:
    In APN:    Disable

    In Global: Disable
```

ステップ 3　GGSN に設定されている各アクセス ポイントの概要を表示するには、次の例に示すように、**show gprs access-point all** コマンドを使用します。

```
Router# show gprs access-point all

There are 3 Access-Points configured

Index   Mode            Access-type    AccessPointName      VRF Name
-------------------------------------------------------------------------
1       non-transparent    Real       gprs.cisco.com
-------------------------------------------------------------------------
2       transparent        Real       gprt.cisco.com
-------------------------------------------------------------------------
3       non-transparent    Real       gpru.cisco.com
-------------------------------------------------------------------------
```

アクセス ポイント経由でのネットワークの到達可能性の検証

次の手順では、MS から宛先ネットワークまでの到達可能性を検証するための基本的な方法を示します。

（注）　宛先ネットワークに正常に到達できるかどうかには、多くの要因が影響を及ぼします。この手順はどの要因にも全面的に対処しようとするものではありませんが、GGSN の APN、IP ルーティング、および物理接続に関する特定の設定が、ホストと MS 間のエンドツーエンド接続に影響を及ぼすことに注意してください。

MS からネットワークに到達できることを検証するには、次のステップを実行します。

ステップ 1　MS から（たとえば、ハンドセットを使用して）、接続先となる APN を指定して、GGSN を含めた PDP コンテキストを作成します。次の例では、APN *gprt.Cisco.com* を指定します。

ステップ 2　GGSN でグローバル コンフィギュレーション モードから、**show gprs access-point** コマンドを使用し、作成されたネットワーク PDP コンテキストの数を検証します（この APN 出力フィールドで PDP の総数を確認します）。

正常に作成された PDP コンテキスト要求の例を次に示します。

```
Router# show gprs access-point 2
    apn_index 2          apn_name = gprt.cisco.com
    apn_mode: transparent
    apn-type: Real
    accounting: Disable
    wait_accounting: Disable
    dynamic_address_pool: not configured
    apn_dhcp_server: 0.0.0.0
    apn_dhcp_gateway_addr: 0.0.0.0
    apn_authentication_server_group:
    apn_accounting_server_group:
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: Yes
    network_activation_allowed: No
    Block Foreign-MS Mode: Disable
```

```
VPN: Disable
GPRS vaccess interface: Virtual-Access1
number of ip_address_allocated 0

Total number of PDP in this APN :1

aggregate:
In APN:    Disable

In Global: Disable
```

ステップ 3　さらにテストするには、ネットワークへのトラフィックを生成します。このことを行うには、次の例に示すように、ハンドセットまたはハンドセットに接続されているラップトップから宛先ネットワーク上のホストまで、**ping** コマンドを使用します。

```
ping 192.168.12.5
```

（注）　DNS の設定に関する問題が発生しないようにするため、宛先ネットワーク内で到達できると推定されるホストの（ホスト名ではなく）IP アドレスを使用します。このテストを機能させるには、選択するホストの IP アドレスが GGSN によって正常にルーティングできるものである必要があります。

また、APN が設定され、Gi インターフェイス経由の宛先ネットワークへの物理接続が確立されている必要があります。たとえば、到達しようとしているホストが VPN 内にある場合、VPN へのアクセスが提供されるように、APN を適切に設定する必要があります。

ステップ 4　PDP コンテキストによるトラフィックの生成を開始したあと、**show gprs gtp pdp-context** コマンドを使用して、送信バイト、受信バイト、パケットのカウントなど詳細な統計情報を表示します。

ヒント　APN で特定の PDP コンテキストの Terminal Identifier（TID; 端末識別子）を見つけるには、**show gprs gtp pdp-context access-point** コマンドを使用します。

TID 81726354453647FA という PDP コンテキストの出力例を次に示します。

```
Router# show gprs gtp pdp-context tid 81726354453647FA

TID              MS Addr         Source  SGSN Addr       APN
81726354453647FA 10.2.2.1        Static  172.16.44.1     gprt.cisco.com

    current time :Dec 06 2001 13:15:34
    user_name (IMSI): 18273645546374     MS address: 10.2.2.1
    MS International PSTN/ISDN Number (MSISDN): 243926901
    sgsn_addr_signal: 172.16.44.1        ggsn_addr_signal: 10.30.30.1
    signal_sequence:  7                  seq_tpdu_up:      0
    seq_tpdu_down:    5380
    upstream_signal_flow:   371          upstream_data_flow:   372
    downstream_signal_flow: 1            downstream_data_flow: 1
    RAupdate_flow:          0
    pdp_create_time:   Dec 06 2001 09:54:43
    last_access_time:  Dec 06 2001 13:15:21
    mnrgflag:          0                 tos mask map: 00
    gtp pdp idle time: 72
    gprs qos_req: 091101                 canonical Qos class(req.): 01
    gprs qos_neg: 25131F                 canonical Qos class(neg.): 01
    effective bandwidth: 0.0
    rcv_pkt_count:       10026           rcv_byte_count:    1824732
    send_pkt_count:      5380            send_byte_count:   4207160
```

```
cef_up_pkt:           10026          cef_up_byte:        1824732
cef_down_pkt:         5380           cef_down_byte:      4207160
cef_drop:             0
charging_id:          12321224
pdp reference count: 2
ntwk_init_pdp:        0
single pdp-session: Disabled
.
.
.
absolute session start time: NOT SET
Accounting Session ID: 5D04010E82AD7CD3
Periodic accounting interval: NOT SET
Direct Tunnel: Enabled
```

GGSN での仮想アクセス ポイントの設定

この項は、次の内容で構成されています。

- 「仮想アクセス ポイント機能の概要」（P.8-32）
- 「仮想アクセス ポイント設定の作業リスト」（P.8-35）
- 「仮想アクセス ポイント設定の検証」（P.8-37）

設定例については、「仮想 APN 設定の例」（P.8-54）を参照してください。

仮想アクセス ポイント機能の概要

GGSN リリース 3.0 以降は、GGSN の仮想アクセス ポイント タイプを使用した PLMN からの仮想 APN アクセスをサポートしています。GGSN の仮想 APN 機能を使用すると、GGSN の共有 APN アクセス ポイント経由で、複数のユーザがそれぞれ異なる物理ターゲット ネットワークにアクセスできます。

GPRS/UMTS ネットワークでは、ホーム ロケーション レジスタ（HLR）や DNS サーバなど複数の GPRS/UMTS ネットワーク エンティティに、ユーザ APN 情報を設定する必要があります。HLR では、ユーザ加入データによって、IMSI（ユーザごとに一意）が、アクセスを許可されている各 APN に関連付けられています。DNS サーバでは、APN が GGSN IP アドレスと相互に関連付けられています。DHCP サーバまたは RADIUS サーバを使用中である場合は、それぞれのサーバまで APN 設定を広げることができます。

仮想 APN 機能は、GGSN に設定した単一の仮想 APN を介してすべての実 APN へのアクセスを統合することによって、APN プロビジョニングの所要量を削減します。このため、HLR および DNS サーバでは、到達しようとする実 APN がそれぞれプロビジョニングされるのではなく、仮想 APN だけがプロビジョニングされます。また、仮想 APN 向けに GGSN を設定する必要があります。

（注）　Cisco 7600 シリーズ ルータ プラットフォームでは、仮想サーバによってロード バランシングされる各 GGSN に、同じ仮想 APN 設定が存在する必要があります。

仮想 APN 機能の利点

仮想 APN 機能には、次の利点があります。

- APN 情報のプロビジョニングを簡素化します。
- スケーラビリティが高く、多数の企業ネットワーク、ISP、およびサービスに対応できます。
- アクセス ポイントを柔軟に選択できます。
- 新しい APN およびサービスを容易に配置できます。
- AAA サーバから APN（事前認証ベースの仮想 APN）を設定することによって、オペレータはハンドセットからワイルドカード APN（*）を含めどの APN でも操作できます。ユーザが接続されていないターゲット APN はユーザ プロビジョニングに基づくためです。

仮想 APN 機能の一般的な制限

仮想 APN 機能には、次の制限があります。

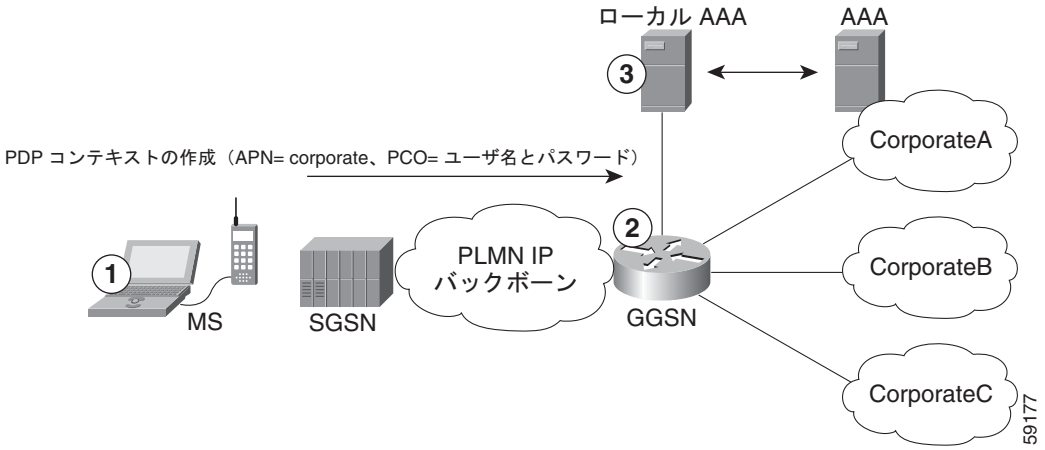
- Call Detail Record（CDR; 呼詳細レコード）にはドメイン情報が含まれません。仮想 APN の場合、Username アトリビュートからドメイン情報が削除されるためです。デフォルトでは、CDR および仮想 APN に対する認証要求には、その仮想 APN に関連付けられた実 APN 名が使用されます。ただし、**gprs charging cdr-option** コマンドに **apn virtual** キーワード オプションを指定して、CDR で仮想 APN を送信するように GGSN を設定できます。
- Cisco IOS ソフトウェアでは仮想アクセス ポイントに他のアクセス ポイント オプションを設定できますが、たとえ設定しても、これらのアクセス ポイント オプションはいずれも適用されません。

ドメイン ベースの仮想アクセス ポイント

デフォルトでは、GGSN が仮想アクセス ポイントで PDP コンテキストの作成要求を受信し、ドメイン名を抽出してパケットを適切な実 APN に向けて送信することによって、セッションの最終的なターゲット ネットワークを決定します。実 APN は、実際の宛先ネットワークです。ドメイン ベースの APN 解決がデフォルトの動作です。

図 8-1 に、MS から送信された PDP コンテキストの作成要求が、デフォルトで、GGSN の仮想 APN を経由してどのように処理されるかを示します。

図 8-1　GGSN でのデフォルトの仮想 APN PDP コンテキストのアクティベーション



1. MS で、ユーザが ciscouser@CorporateA.com などの login@domain 形式のユーザ名でネットワークに接続します。SGSN が、「corporate」の仮想 APN を使用して、PDP コンテキストの作成要求を GGSN に送信します。また、PDP コンテキストの作成要求では、ユーザ名が login@domain という形式でプロトコル設定オプション（PCO）情報要素に含まれています。
2. GGSN が、PCO の情報からドメインを抽出します。これは、GGSN の実ターゲット ネットワークに対応します。次の例では、GGSN が CorporateA.com をドメインと認識し、ターゲット ネットワークの適切な実 APN に向けてセッションを送信します。この場合、実 APN は corporateA.com です。GGSN が、完全な形のユーザ名を使用して認証を行います。
3. ユーザ名のドメイン部分、この例では CorporateA.com に基づいて、ローカル サーバまたは企業 AAA サーバが選択されます。

事前認証ベースの仮想アクセス ポイント

事前認証ベースの仮想 APN 機能は、AAA サーバを使用して、仮想 APN からターゲット（実）APN へのマッピングをユーザ単位で動的に実施します。

仮想 APN の設定時に **pre-authenticate** キーワード オプションを指定した場合、事前認証フェーズは、受信した PDP コンテキストの作成要求のうち、APN 情報要素に仮想 APN が含まれているものにだけ適用されます。

事前認証ベースの仮想 APN を機能させるには、ユーザ プロファイルをプロビジョニングしてターゲット APN を含めるように AAA サーバを設定する必要があります。AAA では、IMSI、ユーザ名、MSISDN などのユーザ ID を使用して、ユーザをターゲットにマッピングします。また、GGSN で、ターゲット APN をローカルで設定する必要があります。

仮想 APN が関連する場合の外部の AAA サーバに関する一般的なコール フローを次に示します。

1. GGSN が、仮想 APN が含まれている PDP コンテキストの作成要求を受信します。GGSN は Access-Request メッセージを AAA サーバに送信して仮想 APN を特定し、PDP コンテキストの事前認証フェーズを開始します。
2. AAA サーバでは、Access-Request メッセージに含まれているユーザ ID（ユーザ名、MSISDN、IMSI など）に基づいて検索を実行し、ユーザ プロファイルに基づいてそのユーザのターゲット APN を判断します。ターゲット APN が、Access-Accept メッセージの Radius アトリビュートとして GGSN に返されます。
3. GGSN は、ローカルで設定された APN の中に、Access-Accept メッセージのターゲット APN アトリビュートの APN 名に一致するものがないかをチェックします。
   - 一致したものが見つかると、仮想 APN が解決され、PDP コンテキストの作成要求がターゲット APN にリダイレクトされます。この要求の処理は、ターゲット APN を使用して（ターゲット APN が元の PDP コンテキストの作成要求に含まれていたかのように）さらに続行されます。実 APN が透過的でない場合は、別の Access-Request が送信されます。一般的に、AAA サーバと送信元は異なります。
   - 一致しているものが見つからない場合は、PDP コンテキストの作成要求が拒否されます。
   - GGSN への Access-Accept メッセージの RADIUS アトリビュートにターゲット APN が含まれていないか、またはターゲット APN がローカルで設定されていない場合は、PDP コンテキストの作成要求が拒否されます。
4. GGSN が、2 回目の認証用に AAA サーバから Access-Accept を受信します。

事前認証ベースの仮想 APN 機能の制限

事前認証ベースの仮想 APN 機能を設定する場合は、「仮想 APN 機能の一般的な制限」（P.8-33）に記載されている制限以外に、次のことに注意してください。

- AAA サーバ上のユーザ プロファイルがターゲット APN を含むように設定されている場合、ターゲット APN は実 APN であり、かつ、GGSN で設定されている必要があります。
- 1 つの APN は、ドメイン ベースの仮想 APN 機能または事前認証ベースの APN 機能のいずれかに対してだけ設定でき、両方に対して設定することはできません。
- AAA から返されたターゲット APN は、実 APN である必要があります。また、複数の APN が返された場合は、最初の APN が使用され、他の APN は無視されます。
- （**anonymous user** アクセス ポイント コンフィギュレーション コマンドを使用して）仮想 APN の下にモバイル ステーション（MS）への匿名ユーザ アクセスを設定します。ユーザ名およびパスワードを指定しなくてもアクセスできるようになります（GGSN は APN に設定された共通パスワードを使用します）。
- 少なくとも、仮想 APN の下、またはグローバルに、AAA アクセス方法を設定する必要があります。方法が設定されていない場合、PDP コンテキストの作成要求は拒否されます。

仮想アクセス ポイント設定の作業リスト

仮想 APN アクセスをサポートするように GGSN を設定するには、1 つ以上の仮想アクセス ポイントを設定する必要があります。また、VPN または外部の PDN の物理ネットワークへの接続に必要な情報を提供する実アクセス ポイントを設定する必要があります。

GGSN での設定以外に、必要に応じて、他の GPRS/UMTS ネットワーク エンティティも適切にプロビジョニングして、GPRS/UMTS ネットワークに仮想 APN 機能を正しく実装する必要があります。

GGSN に仮想 APN アクセスを設定するには、次の作業を実行します。

- 「GGSN での仮想アクセス ポイントの設定」（P.8-35）（必須）
- 「GGSN での実アクセス ポイントの設定」（P.8-11）（必須）
  - 「PDN アクセス設定の作業リスト」（P.8-12）
  - 「VRF を使用した VPN アクセスの設定の作業リスト」（P.8-13）
- 「仮想 APN での他の GPRS/UMTS ネットワーク エンティティの設定」（P.8-36）（任意）

設定例については、「仮想 APN 設定の例」（P.8-54）を参照してください。

GGSN での仮想アクセス ポイントの設定

複数の実ターゲット ネットワークへのアクセスを GGSN に統合するには、仮想アクセス ポイント タイプを使用します。GGSN では常に実アクセス ポイントを使用して外部ネットワークに到達するため、GGSN の仮想アクセス ポイントは、実アクセス ポイントと組み合せて使用します。

GGSN には、複数の仮想アクセス ポイントを設定できます。複数の仮想アクセス ポイントを使用して、同じ実ネットワークにアクセスできます。1 つの仮想アクセス ポイントを使用して、異なる実ネットワークにアクセスできます。

（注）　HLR をプロビジョニングし、GGSN に設定した仮想 APN ドメインに適切に対応するように DNS サーバを設定していることを確認してください。詳細については、「仮想 APN での他の GPRS/UMTS ネットワーク エンティティの設定」（P.8-36）を参照してください。

GGSN に仮想アクセス ポイントを設定するには、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
ステップ 1	`Router(config)# gprs access-point-list list-name`	新しいアクセス ポイントのリストの名前を指定するか、または既存のアクセス ポイントのリストの名前を参照し、アクセス ポイント リスト コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-ap-list)# access-point access-point-index`	新しいアクセス ポイント定義のインデックス番号を指定するか、既存のアクセス ポイント定義を参照し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-access-point)# access-point-name apn-name`	定義されたアクセス ポイントでユーザが GGSN からアクセスできる PDN のネットワーク（またはドメイン）名を指定します。 （注）　*apn-name* は、MS、HLR、および DNS サーバでプロビジョニングされる APN に一致する必要があります。
ステップ 4	`Router (config-access-point)# access-type virtual [pre-authenticate [default-apn apn-name]]`	GGSN の特定の物理ターゲット ネットワークに関連付けられていない APN タイプを指定します。任意で、ユーザごとにターゲット（デフォルト）APN に動的にマッピングされるように設定することもできます。 デフォルトのアクセス タイプは実です。

（注）　Cisco IOS ソフトウェアでは仮想アクセス ポイントに追加のアクセス ポイント オプションを設定できますが、たとえ設定していても、どのアクセス ポイント オプションも適用されません。

仮想 APN での他の GPRS/UMTS ネットワーク エンティティの設定

仮想 APN アクセスをサポートするように GGSN を設定した場合は、他の GPRS/UMTS ネットワーク エンティティを適切に設定して、仮想 APN の実装がサポートされるようにするために必要な要件が、すべて満たされていることも確認してください。

仮想 APN サポートを適切に実装するには、次の GPRS/UMTS ネットワーク エンティティをプロビジョニングする必要があります。

- DHCP サーバ：実 APN を設定する必要があります。
- DNS サーバ：SGSN が GGSN のアドレスを解決するために使用する DNS サーバでは、GGSN の GTP 仮想テンプレートの IP アドレスで仮想 APN を識別する必要があります。GTP SLB を実装する場合は、SLB ルータ上の GTP ロード バランシング仮想サーバ インスタンスの IP アドレスに仮想 APN を関連付ける必要があります。
- HLR：加入ユーザの許可内容に従って、加入データに仮想 APN の名前を含める必要があります。
- RADIUS サーバ：実 APN を設定する必要があります。
- SGSN：APN がユーザ加入データに含まれていない場合は、（必要に応じて）デフォルトの APN として仮想 APN の名前を指定する必要があります。

仮想アクセス ポイント設定の検証

この項では、GGSN に仮想 APN サポートを適切に設定したことを検証する方法について説明します。このための作業は次のとおりです。

- 「GGSN 設定の検証」（P.8-37）
- 「仮想アクセス ポイント経由でのネットワークの到達可能性の検証」（P.8-40）

GGSN 設定の検証

GGSN にアクセス ポイントを適切に設定したことを検証するには、**show running-config** コマンドおよび **show gprs access-point** コマンドを使用します。

（注）　**show running-config** コマンドの出力では、**gprs access-point-list** まず、仮想テンプレート インターフェイスの下にコマンドが出力されます。このことは、GPRS アクセス ポイント リストが設定されており、かつ仮想テンプレートに関連付けられていることを示します。GPRS アクセス ポイント リスト内の、特定のアクセス ポイントの設定を検証するには、**show** コマンドの出力の、さらに下の部分を参照します。**gprs access-point-list** コマンドが再び出力されており、そのあとに個々のアクセス ポイント設定が続きます。

ステップ 1　特権 EXEC モードから、次の例に示すように、**show running-config** コマンドを使用します。インターフェイス設定、仮想アクセス ポイント、および実アクセス ポイントを検証します。

```
Router# show running-config
Building configuration...

Current configuration : 3521 bytes
!
version 12.x
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enable the router for GGSN services
!
service gprs ggsn
!
hostname ggsn
!
ip cef
!
no logging buffered
logging rate-limit console 10 except errors
aaa new-model
aaa group server radius abc
 server 172.18.43.7 auth-port 1645 acct-port 1646
aaa authentication ppp abc group abc
aaa authorization network abc group abc
aaa accounting network abc start-stop group abc

!
ip subnet-zero
!
...
!
interface loopback 1
 ip address 10.40.40.3 255.255.255.0
```

```
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
...
!
gprs access-point-list gprs
!
! Configure a domain-based virtual access point called corporate
!
 access-point 1
   access-point-name corporate
    access-type virtual
    exit
!
! Configure three real access points called corporatea.com,
! corporateb.com, and corporatec.com
!
 access-point 2
    access-point-name corporatea.com
    access-mode non-transparent
    aaa-group authentication abc
    exit
!
 access-point 3
    access-point-name corporateb.com
   exit
    !
 access-point 4
    access-point-name corporatec.com
    access-mode non-transparent
    aaa-group authentication abc
    exit
    !
! Configure a pre-authentication-based virtual access point called virtual-apn-all
!
 access-point 5
    access-point-name virtual-apn-all
    access-mode non-transparent
    access-type virtual pre-authenticate default-apn a1b1c1.com
    anonymous user anyone 1z1z1z
    radius attribute user-name msisdn
    exit
!
gprs maximum-pdp-context-allowed 90000
gprs gtp path-echo-interval 0
gprs default charging-gateway 10.15.15.1
!
gprs memory threshold 512
radius-server host 172.18.43.7 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 3
radius-server key 7 12150415
call rsvp-sync
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
gatekeeper
 shutdown
!
end
```

ステップ 2　GGSN の特定のアクセス ポイントの設定をさらに詳しく表示するには、次の例に示すように、**show gprs access-point** コマンドを使用し、アクセス ポイントのインデックス番号を指定します。

次の出力は、実アクセス ポイントに関する情報を示しています。

```
Router# show gprs access-point 2
    apn_index 2          apn_name = corporatea.com
    apn_mode: non-transparent
    apn-type: Real
    accounting: Disable
    wait_accounting: Disable
    dynamic_address_pool: not configured
    apn_dhcp_server: 0.0.0.0
    apn_dhcp_gateway_addr: 0.0.0.0
    apn_authentication_server_group: abc
    apn_accounting_server_group:
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: No
    network_activation_allowed: No
    Block Foreign-MS Mode: Disable
    VPN: Disable
    GPRS vaccess interface: Virtual-Access1
    number of ip_address_allocated 0

    Total number of PDP in this APN :1

    aggregate:
    In APN:    Disable

    In Global: Disable
```

次の出力は、仮想アクセス ポイントに関する情報を示しています。

```
Router# show gprs access-point 1
    apn_index 1          apn_name = corporate
    apn_mode: transparent
    apn-type: Virtual
    accounting: Disable
    wait_accounting: Disable
    dynamic_address_pool: not configured
    apn_dhcp_server: 0.0.0.0
    apn_dhcp_gateway_addr: 0.0.0.0
    apn_authentication_server_group:
    apn_accounting_server_group:
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: No
    network_activation_allowed: No
    Block Foreign-MS Mode: Disable
    VPN: Disable
    GPRS vaccess interface: Virtual-Access2
    number of ip_address_allocated 0

    Total number of PDP in this APN :0

    aggregate:
    In APN:    Disable

    In Global: Disable
```

次の出力は、事前認証ベースの仮想アクセス ポイントに関する情報を示しています。このアクセス ポイントは、a1b1c1.com というデフォルトの APN に動的にマッピングするように設定されています。

```
Router# show gprs access-point 5
    apn_index 1          apn_name = corporate
    apn_mode: non-transparent
    apn-type: Virtual pre-authenticate default-apn a1b1c1.com
    accounting: Disable
    interim newinfo accounting: Disable
    interim periodic accounting: Enable (20 minutes)
    wait_accounting: Disable
    input ACL: None, output ACL: None
    dynamic_address_pool: not configured
    apn_dhcp_server: 0.0.0.0
    apn_dhcp_gateway_addr: 0.0.0.0
    apn_authentication_server_group:
    apn_accounting_server_group:
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: No
    network_activation_allowed: No
    Block Foreign-MS Mode: Disable
    VPN: Disable
    GPRS vaccess interface: Virtual-Access2
    number of ip_address_allocated 0

    Total number of PDP in this APN :0

    aggregate:
    In APN:    Disable

    In Global: Disable
```

ステップ 3　GGSN に設定されている各アクセス ポイントの概要を表示するには、次の例に示すように、**show gprs access-point all** コマンドを使用します。

```
Router# show gprs access-point all

There are 4 Access-Points configured

Index   Mode            Access-type    AccessPointName      VRF Name
-------------------------------------------------------------------------
1       transparent        Virtual    corporate
-------------------------------------------------------------------------
2       non-transparent    Real       corporatea.com
-------------------------------------------------------------------------
3       transparent        Real       corporateb.com
-------------------------------------------------------------------------
4       non-transparent    Real       corporatec.com
-------------------------------------------------------------------------
```

仮想アクセス ポイント経由でのネットワークの到達可能性の検証

仮想アクセス ポイントを経由した実宛先ネットワークへの到達可能性を検証するには、「アクセス ポイント経由でのネットワークの到達可能性の検証」（P.8-30）で説明しているのと同じ手順を使用できます。

また、仮想アクセス ポイントのテスト作業に関する次のガイドラインを満たす必要があります。

- MS で PDP コンテキスト アクティベーションを開始する場合は、（PDP コンテキストの作成要求に login@domain 形式で）指定するユーザ名が、GGSN に設定した実 APN に対応していることを確認してください。
- ネットワークへのトラフィックを生成する場合、実宛先ネットワーク上にあって、GGSN での APN サポート用に設定されているいずれかのホストを選択してください。

外部サポート サーバへのアクセスの設定

外部サポート サーバにアクセスし、Dynamic Host Configuration Protocol（DHCP）または Remote Authentication Dial-In User Service（RADIUS）を使用して、MS のダイナミック IP アドレッシング向けにサービスを提供するように GGSN を設定できます。また、APN のネットワークにアクセスするユーザの認証などセキュリティを確保するように、GGSN に RADIUS サービスを設定することもできます。

GGSN では、すべてのアクセス ポイントを対象に DHCP サーバおよび RADIUS サーバへのアクセスをグローバルに設定したり、特定のアクセス ポイントを対象に特定のサーバへのアクセスを設定したりできます。GGSN での DHCP の設定の詳細については、「GGSN でのダイナミック アドレッシングの設定」を参照してください。GGSN での RADIUS の設定の詳細については、「GGSN でのセキュリティの設定」を参照してください。

外部モバイル ステーションから GGSN へのアクセスのブロック

この項では、ホーム PLMN の外部にあるモバイル ステーションから GGSN へのアクセスを制限する方法について説明します。内容は次のとおりです。

外部モバイル ステーションのブロックの概要

GGSN では、PLMN の外部にあるモバイル ステーションからのアクセスをブロックできます。外部モバイル ステーションのブロックをイネーブルにした場合、GGSN ではモバイル国コード（MCC）およびモバイル ネットワーク コード（MNC）に基づいて、MS が PLMN の内部にあるか、外部にあるかを判断します。GGSN に MCC コードおよび MNC コードを指定して、Home Public Land Mobile Network（HPLMN; ホーム パブリック ランド モバイル ネットワーク）値を適切に設定する必要があります。

アクセス ポイントで外部 MS アクセス機能のブロックをイネーブルにした場合、GGSN では PDP コンテキストの作成要求を受信するたびに、TID の MCC および MNC を、GGSN に設定したホーム オペレータ コードと比較します。MS モバイル オペレータ コードが GGSN の一致基準を満たさない場合、GGSN は PDP コンテキストの作成要求を拒否します。

外部モバイル ステーションのブロックの設定の作業リスト

GGSN に外部モバイル ステーションのブロックを実装するには、ブロック機能をイネーブルにし、MS がホーム PLMN の外部にあるかどうかを判断するためのサポート基準を指定する必要があります。

GGSN に外部モバイル ステーションのブロックを設定するには、次の作業を実行します。

- 「MCC 値および MNC 値の設定」（P.8-42）（必須）
- 「GGSN での外部モバイル ステーションのブロックのイネーブル」（P.8-43）（必須）
- 「外部モバイル ステーション設定のブロックの検証」（P.8-43）

MCC 値および MNC 値の設定

MCC および MNC はともに、パブリック ランド モバイル ネットワーク（PLMN）を識別する働きをします。その値は、**trusted** キーワード オプションを指定しない **gprs mcc mnc** コマンドを使用して設定し、GGSN が属する PLMN を指すホーム PLMN ID の値となります。

GGSN に一度に定義できるホーム PLMN は 1 つだけです。GGSN は、PDP コンテキストの作成要求の IMSI とこのコマンドで設定された値とを比較して、要求が外部 MS からのものであるかどうかを判断します。

また、**gprs mcc mnc** コマンドを発行するときに **trusted** キーワードを指定して、*信頼できる* PLMN を最大 5 つ設定することもできます。信頼できる PLMN にある MS から送信された PDP コンテキストの作成要求は、ホーム PLMN にある MS から送信された PDP コンテキストの作成要求と同じように扱われます。

要求がローミング MS からのものであるかどうかを判断するために GGSN が使用する MCC 値および MNC 値を設定するには、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)# gprs mcc mcc-num mnc mnc-num [trusted]`	PDP コンテキストの作成要求が外部 MS からのものであるかどうかを判断するために GGSN が使用するモバイル国コードおよびモバイル ネットワーク ノードを設定します。任意で、**trusted** キーワードを使用して、信頼できる PLMN を最大 5 つ定義します。 **（注）** 信頼できる PLMN から送信された PDP コンテキストの作成要求は、ホーム PLMN から送信されたものと同様に扱われます。

（注） GGSN は、MCC および MNC の値として 000 を自動的に指定します。ただし、GGSN でローミング ユーザ用の CDR を作成できるようにするには、MCC と MNC のいずれにも非ゼロの値を設定する必要があります。

GGSN での外部モバイル ステーションのブロックのイネーブル

GGSN で外部モバイル ステーションによる PDP コンテキストの作成をブロックできるようにするには、アクセス ポイント 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-access-point)# **block-foreign-ms**	モバイル ユーザの HPLMN に基づいて、特定のアクセス ポイントで GGSN アクセスを制限します。

（注）　GGSN で外部モバイル ステーションをブロックできるようにするには、要求がローミング MS からのものであるかどうかを判断するために使用される MCC 値および MNC 値を設定する必要があります。

外部モバイル ステーション設定のブロックの検証

ここでは、GGSN での外部モバイル ステーション設定のブロックを検証する方法について説明します。内容は次のとおりです。

- 「アクセス ポイントでの外部モバイル ステーションのブロックの検証」（P.8-43）
- 「GGSN での MCC 設定および MNC 設定の検証」（P.8-44）

アクセス ポイントでの外部モバイル ステーションのブロックの検証

GGSN が特定のアクセス ポイントで外部モバイル ステーションのブロックをサポートするように設定されているかどうかを検証するには、**show gprs access-point** コマンドを使用します。次の例に太字で示すように、Block Foreign-MS Mode 出力フィールドの値に注意してください。

```
Router# show gprs access-point 1
    apn_index 1          apn_name = gprs.corporate.com
    apn_mode: transparent
    apn-type: Real
    accounting: Disable
    interim newinfo accounting: Disable
    interim periodic accounting: Enable (20 minutes)
    wait_accounting: Disable
    input ACL: None, output ACL: None
    dynamic_address_pool: dhcp-proxy-client
    apn_dhcp_server: 10.99.100.5
    apn_dhcp_gateway_addr: 10.27.1.1
    apn_authentication_server_group: abc
    apn_accounting_server_group: abc1
    apn_username: , apn_password:
    subscribe_required: No
    deactivate_pdp_context_on violation: Yes
    network_activation_allowed: Yes
    Block Foreign-MS Mode: Enable
    VPN: Enable  (VRF Name : vpn1)
    GPRS vaccess interface: Virtual-Access2
    number of ip_address_allocated 0
```

```
Total number of PDP in this APN :0

aggregate:
In APN:    auto

In Global: 30.30.0.0/16
           21.21.0.0/16
```

GGSN での MCC 設定および MNC 設定の検証

要求が外部モバイル ステーションから送信されたものであるかどうかを判断するために GGSN が一致基準として使用する設定要素を検証するには、**show gprs plmn** 特権 EXEC コマンドを使用します。次の例に太字で示されている出力フィールドの値に注意してください。この例では、GGSN が USA 国コード（310）および Bell South ネットワーク コード（15）用に設定され、信頼できる PLMN が 4 つ設定されています。

```
Router# show gprs plmn
Home PLMN
  MCC = 302  MNC = 678
Trusted PLMN
  MCC = 346  MNC = 123
  MCC = 234  MNC = 67
  MCC = 123  MNC = 45
  MCC = 100  MNC = 35
```

IP アドレスが重複する MS による GGSN へのアクセスの制御

MS は、別の GPRS/UMTS ネットワーク エンティティと同じ IP アドレスを保有できません。GPRS/UMTS ネットワーク用に特定の IP アドレス範囲を予約し、MS がその範囲の IP アドレスを使用できないように GGSN を設定できます。

PDP コンテキストの作成要求を受信すると、GGSN は MS の IP アドレスが指定の除外範囲内にあるかどうかを検証します。MS IP アドレスが除外範囲と重なる場合、PDP コンテキストの作成要求は拒否されます。この基準によって、ネットワーク内で IP アドレッシングが重複するのを防ぐことができます。

最大 100 個の IP アドレス範囲を設定できます。範囲には、1 つ以上のアドレスを含めることができます。ただし、1 つのコマンド エントリで設定できる IP アドレス範囲は 1 つだけです。IP アドレスを 1 つだけ除外する場合は、start-ip 引数と end-ip 引数でその IP アドレスを繰り返すことができます。IP アドレスは、32 ビット値です。

（注） Cisco 7600 シリーズ ルータ プラットフォームでは、仮想サーバによってロード バランシングされる各 GGSN に、同じ設定が存在する必要があります。

GPRS/UMTS ネットワーク用に IP アドレス範囲を予約し、MS でその範囲の IP アドレスを使用できないようにするには、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)# **gprs ms-address exclude-range** *start-ip end-ip*	GPRS/UMTS ネットワークで使用し、MS の IP アドレス範囲から除外する IP アドレス範囲を指定します。

APN でのモバイル ステーション背後へのルーティングの設定

MS 背後へのルーティング機能を使用することによって、PDP コンテキスト（MS）に属していないものの、その背後にある IPv4 アドレスにパケットをルーティングできます。宛先のネットワーク アドレスは、MS アドレスと異なる場合があります。

MS 背後へのルーティングをイネーブルにするには、次の要件が満たされている必要があります。

- MS では、認証および認可に RADIUS を使用する必要があります。
- Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）の規格 RFC 2865 で定義されている Framed-Route（アトリビュート 22）をユーザのプロファイルに設定し、MS 背後へのルーティング機能を使用する MS ごとに少なくとも 1 個、最大で 16 個のルートを含める必要があります。

  設定された Framed-Route アトリビュートは、PDP コンテキスト作成の RADIUS 認証および認可フェーズ中に GGSN に自動的にダウンロードされます。**network-behind-mobile** アクセス ポイント コンフィギュレーション コマンドを使用しても MS 背後へのルーティングがイネーブルにならない場合、GGSN では Framed-Route アトリビュートが無視されます。

  MS セッションがアクティブではなくなっている場合、ルートは削除されます。
- PPP 再生成セッションまたは L2TP による PPP セッションの場合、Framed-Route アトリビュートは LNS の RADIUS サーバに設定する必要があります。
- PPP 再生成セッションでは、**security verify source** コマンドを設定した場合、Framed-Route アトリビュートも GGSN RADIUS サーバのユーザ プロファイルに設定する必要があります。
- スタティック ルートは設定しません。モバイル ステーション背後へのルーティング機能の設定（Framed Route、アトリビュート 22）およびスタティック ルートは、同時にはサポートされません。

モバイル ステーション背後へのルーティングのイネーブル

MS 背後へのルーティングをイネーブルにするには、アクセス ポイント 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-access-point)# network-behind-mobile [max-subnets number]`	アクセス ポイントが、MS 背後へのルーティングをサポートできるようにします。任意で、MS 背後で許可されるサブネットの最大数を指定します。有効な値は、1 から 16 までのいずれかの数字です。

（注）　MS 背後へのルーティングは、IPv4 PDP コンテキストでだけサポートされます。

MS 背後にルーティングされるパケットは、MS と同じ Third Generation Partnership Project（3GPP; 第 3 世代パートナーシップ プロジェクト）QoS 設定を共有します。

ルーティング テーブルの現在の状態を表示するには、特権 EXEC モードで **show ip route** コマンドを使用します。現在アクティブなモバイル セッションのリストを表示するには、**show pdp** コマンドを使用します。

モバイル ステーション背後へのルーティング設定の検証

モバイル ステーション背後へのルーティング設定を検証するには、次の **show** コマンドを使用します。

ステップ 1　PDP コンテキストの IP アドレスをゲートウェイ アドレスとして使用するフレーム化ルートおよびフレーム化ルート用に追加されるスタティック ルートを表示するには、特権 EXEC モードから **show gprs gtp pdp-context tid** コマンドおよび **show ip route** コマンドを使用します。

```
Router#show gprs gtp pdp-context tid 1234567809000010
TID              MS Addr               Source  SGSN Addr       APN
1234567809000010 83.83.0.1             Static  2.1.1.1         ippdp1

    current time :Feb 09 2004 12:52:49
    user_name (IMSI):214365879000000    MS address:83.83.0.1
    MS International PSTN/ISDN Number (MSISDN):123456789
    sgsn_addr_signal:2.1.1.1            sgsn_addr_data:  2.1.1.1
    control teid local: 0x637F00EC
    control teid remote:0x01204611
    data teid local:    0x637DFF04
    data teid remote:   0x01204612
    primary pdp:Y           nsapi:1
    signal_sequence: 11                 seq_tpdu_up:     0
    seq_tpdu_down:   0
    upstream_signal_flow:  0            upstream_data_flow:  0
    downstream_signal_flow:0            downstream_data_flow:0
    RAupdate_flow:         0
    pdp_create_time:  Feb 09 2004 12:50:41
    last_access_time: Feb 09 2004 12:50:41
    mnrgflag:         0                tos mask map:00
    gtp pdp idle time:72
    gprs qos_req:000000               canonical Qos class(reg.):03
    gprs qos_neg:000000               canonical Qos class(neg.):03
    effective bandwidth:0.0
    rcv_pkt_count:    0             rcv_byte_count:  0
    send_pkt_count:   0             send_byte_count: 0
    cef_up_pkt:       0             cef_up_byte:     0
    cef_down_pkt:     0             cef_down_byte:   0
    cef_drop:         0             out-sequence pkt:0
    charging_id:        736730069
    pdp reference count:2
    primary dns:        0.0.0.0
    secondary dns:      0.0.0.0
    primary nbns:       0.0.0.0
    secondary nbns:     0.0.0.0
    ntwk_init_pdp:      0
    Framed_route 5.5.5.0 mask 255.255.255.0
Router#

Router#show ip route
Codes:C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
C    2.0.0.0/8 is directly connected, FastEthernet6/0
     5.0.0.0/24 is subnetted, 1 subnets
U       5.5.5.0 [1/0] via 83.83.0.1
```

```
     83.0.0.0/32 is subnetted, 1 subnets
U       83.83.0.1 [1/0] via 0.0.0.0, Virtual-Access2
     8.0.0.0/32 is subnetted, 1 subnets
C       8.8.0.1 is directly connected, Loopback0
Router#

Router#show ip route vrf vpn4

Routing Table:vpn4
Codes:C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     80.0.0.0/16 is subnetted, 1 subnets
C       80.1.0.0 is directly connected, FastEthernet3/0
     5.0.0.0/24 is subnetted, 1 subnets
U       5.5.5.0 [1/0] via 123.123.123.123
     123.0.0.0/32 is subnetted, 1 subnets
U       123.123.123.123 [1/0] via 0.0.0.0, Virtual-Access9
Router#
```

ステップ 2　network-behind-mobile-station 統計情報（次の例に太字で表示されている情報）を表示するには、特権 EXEC モードから **show gprs gtp statistics** コマンドを使用します。

```
Router#show gprs gtp statistics
GPRS GTP Statistics:
  version_not_support        0            msg_too_short              0
  unknown_msg                0            unexpected_sig_msg         0
  unexpected_data_msg        0            unsupported_comp_exthdr    0
  mandatory_ie_missing       0            mandatory_ie_incorrect     0
  optional_ie_invalid        0            ie_unknown                 0
  ie_out_of_order            0            ie_unexpected              0
  ie_duplicated              0            optional_ie_incorrect      0
  pdp_activation_rejected    2            tft_semantic_error         0
  tft_syntactic_error        0            pkt_ftr_semantic_error     0
  pkt_ftr_syntactic_error    0            non_existent               0
  path_failure               0            total_dropped              0
  signalling_msg_dropped     0            data_msg_dropped           0
  no_resource                0            get_pak_buffer_failure     0
  rcv_signalling_msg         7            snd_signalling_msg         7
  rcv_pdu_msg                0            snd_pdu_msg                0
  rcv_pdu_bytes              0            snd_pdu_bytes              0
  total created_pdp          3            total deleted_pdp          2
  total created_ppp_pdp      0            total deleted_ppp_pdp      0
  ppp_regen_pending          0            ppp_regen_pending_peak     0
  ppp_regen_total_drop       0            ppp_regen_no_resource      0
  ntwk_init_pdp_act_rej      0            total ntwkInit created pdp 0
GPRS Network behind mobile Statistics:
  network_behind_ms APNs     1          total_download_route       5
  save_download_route_fail   0          insert_download_route_fail 2
  total_insert_download_route 3
```

APN での Proxy-CSCF 検出サポートの設定

PCO に「P-CSCF Address Request」フィールドが含まれている PDP コンテキストの作成要求を受信した場合は、APN 用に事前に設定された Proxy Call Session Control Function（P-CSCF）サーバ アドレスのリストを返すように GGSN を設定できます。

MS は、PDP コンテキストの有効化要求に PCO の P-CSCF Address Request フィールドを設定します。この要求は、SGSN から PDP コンテキストの作成要求で GGSN に転送されます。GGSN では、受信すると、PCO の「P-CSCF Address」フィールドにすべての設定済みの P-CSCF アドレスを返します。

PDP コンテキストの作成要求に PCO の P-CSCF Address Request フィールドが含まれていない場合、または P-CSCF アドレスが事前に設定されていない場合、PDP コンテキストの作成応答では P-CSCF アドレスを返しません。エラー メッセージは生成されず、PDP コンテキストの作成要求は処理されます。

任意で、Cisco GGSN で P-CSCF ロード バランシングをイネーブルにできます。

P-CSCF ロード バランシングがイネーブルになっている場合、Cisco GGSN では、PDP コンテキストの作成要求で送信されたプロトコル設定オプション（PCO）IE の、P-CSCF Address Request フィールドへの応答として送信する Proxy-CSCF サーバを、ラウンドロビン アルゴリズムを使用して選択します。

P-CSCF ロード バランシングがイネーブルになっていない場合、Cisco GGSN は事前に設定されたすべての P-CSCF サーバのリストを送信します。

（注）　PCO の「P-CSCF Address」フィールドに返されるアドレスの順序は、各アドレスが P-CSCF サーバ グループに定義され、そのグループが APN に関連付けられる順序と同じです。

APN での P-CSCF 検出サポートをイネーブルにするには、次の作業を実行します。

- 「GGSN での P-CSCF サーバ グループの作成」（P.8-48）
- 「APN への P-CSCF サーバ グループの関連付け」（P.8-49）

GGSN での P-CSCF サーバ グループの作成

P-CSCF サーバ グループには、最大 10 個の P-CSCF サーバを定義できます。

サーバ グループには、IPv6 サーバと IPv4 P-CSCF サーバの両方を定義できます。PDP タイプは、どのサーバに IP アドレスが送信されるかを示します。

GGSN に P-CSCF サーバ グループを設定するには、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
ステップ 1	`Router(config)# gprs pcscf group-name`	GGSN に P-CSCF サーバ グループを設定し、P-CSCF グループ コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-pcscf-group)# server [ipv6] ip-address`	IP アドレスで IPv4 P-CSCF サーバを定義します。 任意で、**ipv6** キーワード オプションを指定して、IPv6 P-CSCF サーバを P-CSCF サーバ グループに定義できます。

APN への P-CSCF サーバ グループの関連付け

APN に P-CSCF グループを関連付けるには、グローバル コンフィギュレーション モードで **gprs pcscf** コマンドを使用して、そのグループをグローバルに設定する必要があります。

（注）　定義できる P-CSCF グループは APN ごとに 1 つだけですが、1 つの P-CSCF グループを複数の APN に関連付けることができます。

APN の P-CSCF サーバ グループを指定するには、アクセス ポイント 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。

APN に P-CSCF サーバ グループを関連付けるには、アクセス ポイント 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-access-point)# pcscf group-name [load-balance]`	APN による P-CSCF 検出に使用する P-CSCF サーバ グループを指定します。任意で、**load-balance** キーワードを指定して、APN で P-CSCF ロード バランシングをイネーブルにできます。

P-CSCF 検出設定の検証

P-CSCF 検出設定を検証するには、次の show コマンドを使用します。

コマンド	目的
`Router# show gprs pcscf`	GGSN に設定されている各 P-CSCF サーバ グループの概要を表示します。
`Router# show gprs access-point [group-name]`	GGSN に設定されている 1 つ以上の P-CSCF サーバ グループの概要を表示します。

GGSN でのアクセス ポイントのモニタリングおよびメンテナンス

ここでは、GGSN 上のアクセス ポイントをモニタリングするために使用できる **clear** コマンドおよび **show** コマンドの要約を示します。

GGSN 上のアクセス ポイントをモニタリングおよびメンテナンスするには、次の特権 EXEC コマンドを使用します。

コマンド	目的
Router# **clear gprs access-point statistics** {*access-point-index* | all}	GGSN 上の特定のアクセス ポイントまたはすべてのアクセス ポイントの統計情報カウンタをクリアします。
Router# **clear gprs gtp pdp-context pdp-type** [**ipv6** | **ipv4**]	IP Version 4（IPv4）または IP Version 6（IPv6）の PDP であるパケット データ プロトコル（PDP）コンテキスト（モバイル セッション）をすべてクリアします。
Router# **show gprs access-point** {*access-point-index* | **all**}	GGSN のアクセス ポイントに関する情報を表示します。
Router# **show gprs access-point statistics** {*access-point-index* | **all**}	GGSN 上のアクセス ポイントに関するデータ ボリュームと、PDP のアクティベーションと非アクティベーションの統計情報を表示します。
Router# **show gprs access-point-name status**	アクセス ポイントでアクティブな PDP の数、およびそのうちの IPv4 PDP の数と IPv6 PDP の数を表示します。
Router# **show gprs gtp pdp-context** {**tid** *tunnel_id* [service [all | id *id_string*]] | ms-address *ip_address* [**access-point** *access-point-index*] | **imsi** *imsi* [**nsapi** *nsapi* [**tft**]] | **path** *ip-address* [*remote-port-num*] | **access-point** *access-point-index* | **pdp-type** {**ip** [**v6** | **v4**] | **ppp**} | qos-umts-class {background | conversational | interactive | streaming} | **qos-precedence** {**low** | **normal** | **high**} | **qos-delay** {**class1** | **class2** | **class3** | **classbesteffort**} | **version** *gtp-version*} | **msisdn** [*msisdn*] | ms-ipv6-addr *ipv6-address* | all}	現在アクティブな PDP コンテキスト（モバイル セッション）のリストを表示します。
Router# **show gprs gtp statistics**	ゲートウェイ GGSN に関する現在の GTP 統計情報（IE、GTP シグナリング、GTP PDU 統計情報など）を表示します。
Router# **show gprs gtp status**	GGSN 上の GTP の現在のステータスに関する情報を表示します。

設定例

この項では、GGSN へのさまざまなタイプのネットワーク アクセスを設定する例をいくつか示します。

- 「SGSN へのスタティック ルートの例」（P.8-51）
- 「アクセス ポイント リスト設定の例」（P.8-52）
- 「VRF トンネル設定の例」（P.8-53）
- 「仮想 APN 設定の例」（P.8-54）
- 「外部モバイル ステーション設定によるアクセスのブロックの例」（P.8-57）
- 「重複 IP アドレス保護設定の例」（P.8-58）
- 「P-CSCF 検出設定の例」（P.8-58）

SGSN へのスタティック ルートの例

（注）　SGSN が GGSN と正常に通信するには、SGSN にスタティック ルートを設定するか、または GGSN 仮想テンプレートで使用されている IP アドレスに動的にルーティングできるようにします。

GGSN 設定：

```
!
...
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
ip route 40.1.2.1 255.255.255.255 10.1.1.1
ip route 40.1.3.10 255.255.255.255 10.1.1.1
ip route 40.2.2.1 255.255.255.255 10.1.1.1
ip route 40.2.3.10 255.255.255.255 10.1.1.1
!
...
!
```

スーパーバイザ エンジン設定

```
!
...
!
interface FastEthernet8/22
 no ip address
 switchport
 switchport access vlan 302
!
interface FastEthernet9/41
 no ip address
 switchport
 switchport access vlan 303
!
interface Vlan101
 description Vlan to GGSN for GA/GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
!
interface Vlan303
 ip address 40.0.3.1 255.255.255.0
!

ip route 9.9.9.72 255.255.255.255 10.1.1.72
```

```
ip route 9.9.9.73 255.255.255.255 10.1.1.73
ip route 9.9.9.74 255.255.255.255 10.1.1.74
ip route 9.9.9.75 255.255.255.255 10.1.1.75
ip route 9.9.9.76 255.255.255.255 10.1.1.76
ip route 40.1.2.1 255.255.255.255 40.0.2.11
ip route 40.1.3.10 255.255.255.255 40.0.3.10
ip route 40.2.2.1 255.255.255.255 40.0.2.11
ip route 40.2.3.10 255.255.255.255 40.0.3.10
!
...
!
```

アクセス ポイント リスト設定の例

GPRS アクセス ポイント リストの GGSN 設定の一部を次に例示します。

```
!
interface virtual-template 1
 ip unnumber loopback 1
 no ip directed-broadcast
 encapsulation gtp
 gprs access-point-list abc
!
! Defines a GPRS access point list named abc
! with 3 access points
!
gprs access-point-list abc
 access-point 1
  access-point-name gprs.pdn1.com
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.102.100.3
  dhcp-gateway-address 10.30.30.30
  exit
!
 access-point 2
  access-point-name gprs.pdn2.com
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.60.0.1
  dhcp-gateway-address 10.27.27.27
  exit
!
 access-point 3
  access-point-name www.pdn3.com
  access-mode non-transparent
  dhcp-gateway-address 10.25.25.25
  aaa-group authentication abc
  exit
!
...
```

VRF トンネル設定の例

次の例では、2 つの VPN（vpn1 と vpn2）およびその関連する GRE トンネル（Tunnel1 と Tunnel2）の設定の一部を示します。

GGSN 設定

```
service gprs ggsn
!
hostname 7600-7-2
!
ip cef
!
ip vrf vpn1
 description GRE Tunnel 1
 rd 100:1
!
ip vrf vpn2
 description GRE Tunnel 3
 rd 101:1
!
interface Loopback1
 ip address 150.1.1.72 255.255.0.0
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface Tunnel1
 description VRF-GRE to PDN 7500(13) Fa0/1
 ip vrf forwarding vpn1
 ip address 50.50.52.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 165.2.1.13
!
interface Tunnel2
 description VRF-GRE to PDN PDN x(12) Fa3/0
 ip vrf forwarding vpn2
 ip address 80.80.82.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 167.2.1.12
!
interface GigabitEthernet0/0.1
 description Gi
 encapsulation dot1Q 100
 ip address 10.1.2.72 255.255.255.0
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
ip local pool vpn1_pool 100.2.0.1 100.2.255.255 group vpn1
ip local pool vpn2_pool 100.2.0.1 100.2.255.255 group vpn2
ip route vrf vpn1 0.0.0.0 0.0.0.0 Tunnel1
ip route vrf vpn2 0.0.0.0 0.0.0.0 Tunnel2

gprs access-point-list gprs
  access-point 1
   access-point-name apn.vrf1.com
   access-mode non-transparent
   aaa-group authentication ipdbfms
```

```
   ip-address-pool local vpn1_pool
   vrf vpn1
   !
  access-point 2
   access-point-name apn.vrf2.com
   access-mode non-transparent
   aaa-group authentication ipdbfms
   ip-address-pool local vpn2_pool
   vrf vpn2
   !
```

スーパーバイザ エンジン設定

```
interface FastEthernet9/5
 no ip address
 switchport
 switchport access vlan 167
 no cdp enable
!
interface FastEthernet9/10
 no ip address
 switchport
 switchport access vlan 165
 no cdp enable
!
interface Vlan165
 ip address 165.1.1.1 255.255.0.0
!
interface Vlan167
 ip address 167.1.1.1 255.255.0.0
!
! provides route to tunnel endpoints on GGSNs
!
ip route 150.1.1.72 255.255.255.255 10.1.2.72
!
! routes to tunnel endpoints on PDN
!
ip route 165.2.0.0 255.255.0.0 165.1.1.13
ip route 167.2.0.0 255.255.0.0 167.1.1.12
```

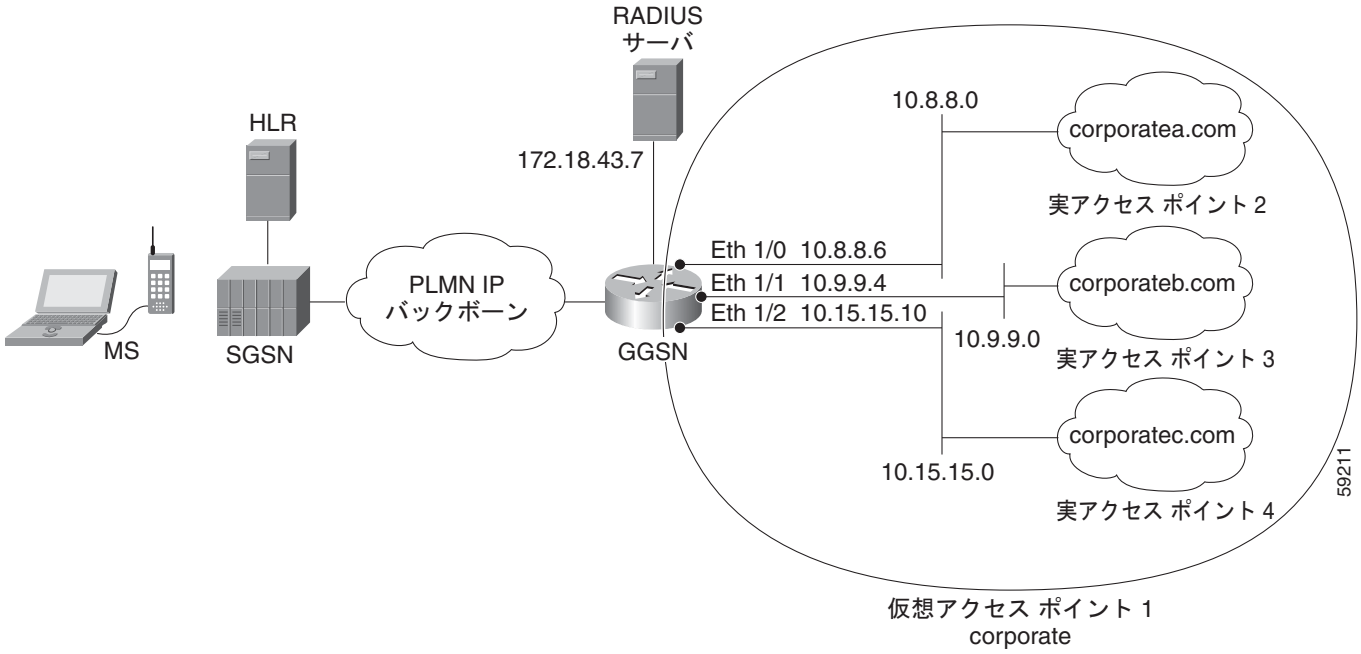
仮想 APN 設定の例

次の例では、1 つの仮想 APN アクセス ポイントを 3 種類の実企業ネットワークのフォーカルな接続として機能させるように設定されている GGSN を示します。

この例で示す GGSN 設定では、次のことに注意してください。

- 実企業ネットワークへのアクセスを確立するために、Ethernet 1/0、Ethernet 1/1、Ethernet 1/2 の 3 つの物理インターフェイス（Gi インターフェイス）が定義されています。
- アクセス ポイントが 4 つ設定されています。
  - アクセス ポイント 1 は、*corporate* という APN を持つ仮想アクセス ポイントとして設定されています。他の設定オプションは、仮想アクセス ポイントには適用されません。「corporate」仮想 APN は、HLR および DNS サーバでプロビジョニングされる APN です。
  - アクセス ポイント 2、3、および 4 は、それぞれ corporatea.com、corporateb.com、corporatec.com の各実ネットワーク ドメインに対して設定されています。実ネットワーク ドメインは、PDP コンテキスト要求の PCO に示されています。

図 8-2　仮想 APN 設定の例



GGSN 設定

```
!
version 12.x
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enable the router for GGSN services
!
service gprs ggsn
!
hostname ggsn
!
ip cef
!
no logging buffered
logging rate-limit console 10 except errors
aaa new-model
aaa group server radius abc
 server 172.18.43.7 auth-port 1645 acct-port 1646
aaa authentication ppp abc group abc
aaa accounting network abc start-stop group abc

!
ip subnet-zero
!
!
no ip dhcp-client network-discovery
!
!
interface Loopback1
 ip address 10.2.3.4 255.255.255.255
!
```

```
interface FastEthernet0/0
 ip address 172.18.43.174 255.255.255.240
 duplex half
!
interface FastEthernet2/0
 description Gn interface
 ip address 192.168.10.56 255.255.255.0
!
! Define Gi physical interfaces to real networks
!
interface Ethernet1/0
 description Gi interface to corporatea.com
 ip address 10.8.8.6 255.255.255.0
 no ip mroute-cache
 duplex half
!
interface Ethernet1/1
 description Gi interface to corporateb.com
 ip address 10.9.9.4 255.255.255.0
 no ip mroute-cache
 duplex half
!
interface Ethernet1/2
 description Gi interface to corporatec.com
 ip address 10.15.15.10 255.255.255.0
 no ip mroute-cache
 duplex half
!
interface loopback 1
 ip address 10.40.40.3 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
ip default-gateway 172.18.43.161
ip kerberos source-interface any
ip classless
ip route 10.7.7.0 255.255.255.0 10.8.8.2
ip route 10.21.21.0 255.255.255.0 Ethernet1/1
ip route 10.102.82.0 255.255.255.0 172.18.43.161
ip route 192.168.1.1 255.255.255.255 FastEthernet2/0
ip route 172.18.0.0 255.255.0.0 172.18.43.161
no ip http server
!
gprs access-point-list gprs
!
! Configure a virtual access point called corporate
!
 access-point 1
   access-point-name corporate
   access-type virtual
   exit
!
! Configure three real access points called corporatea.com,
! corporateb.com, and corporatec.com
!
 access-point 2
   access-point-name corporatea.com
   access-mode non-transparent
   aaa-group authentication abc
   exit
 access-point 3
```

```
   access-point-name corporateb.com
   access-mode transparent
   ip-address-pool dhcp-client
   dhcp-server 10.21.21.1
  exit
   !
 access-point 4
   access-point-name corporatec.com
   access-mode non-transparent
   aaa-group authentication abc
   exit
   !
 !
gprs maximum-pdp-context-allowed 90000
gprs gtp path-echo-interval 0
gprs default charging-gateway 10.15.15.1
!
gprs memory threshold 512
!
radius-server host 172.18.43.7 auth-port 1645 acct-port 1646 non-standard
radius-server retransmit 3
radius-server key 7 12150415
call rsvp-sync
!
no mgcp timer receive-rtcp
!
mgcp profile default
!
!
gatekeeper
 shutdown
!
end
```

外部モバイル ステーション設定によるアクセスのブロックの例

次の例では、アクセス ポイント 100 が外部モバイル ステーションによるアクセスをブロックする設定の一部を示します。

```
!
version 12.x
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enables the router for GGSN services
!
service gprs ggsn
!
hostname ggsn
!
ip cef
!
gprs access-point-list gprs
!
access-point 100
 access-point-name blocking
!
! Enables blocking of MS to APN 100
! that are outside ! of the PLMN
```

```
!
 block-foreign-ms
exit
!
. . .
!
! Configures the MCC and MNC codes
!
gprs mcc 123 mnc 456
```

重複 IP アドレス保護設定の例

次の例では、GPRS/UMTS ネットワーク用の IP アドレス範囲を 3 種類指定する設定の一部を示します（これらの範囲内にある IP アドレスは、MS IP アドレス範囲から除外されます）。

```
gprs ms-address exclude-range 10.0.0.1 10.20.40.50
gprs ms-address exclude-range 172.16.150.200 172.30.200.255
gprs ms-address exclude-range 192.168.100.100 192.168.200.255
```

P-CSCF 検出設定の例

次の例では、P-CSCF サーバ グループをいくつか GGSN に設定し、その 1 つをアクセス ポイントに割り当てる設定の一部を示します。

```
!
version 12.x
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enables the router for GGSN services
!
service gprs ggsn
!
hostname ggsn
!
ip cef
!
gprs pcscf groupA
server 172.10.1.1
server 10.11.1.2
server ipv6 2001:999::9
!
gprs pcscf groupB
server 172.20.2.1
server 10.21.2.2
gprs access-point-list gprs
!
access-point 100
access-point-name pcscf
pcscf groupA
!
```

CHAPTER 9

GGSN での PPP サポートの設定

Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）では、Point to Point Protocol（PPP; ポイントツーポイント プロトコル）を使用した 3 種類の GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）がサポートされています。GGSN での PPP サポートのタイプは、ネットワーク内の PPP エンドポイントの場所、Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）が使用されるかどうか、および IP パケット サービスが行われる場所によって異なります。この章では、GGSN でのさまざまな PPP サポート方式、およびこれらの方式の設定方法について説明します。

この章に記載されている GGSN コマンドの詳細については、使用している Cisco GGSN リリースの『*Cisco GGSN Command Reference*』を参照してください。この章に記載されているその他のコマンドのマニュアルを参照するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

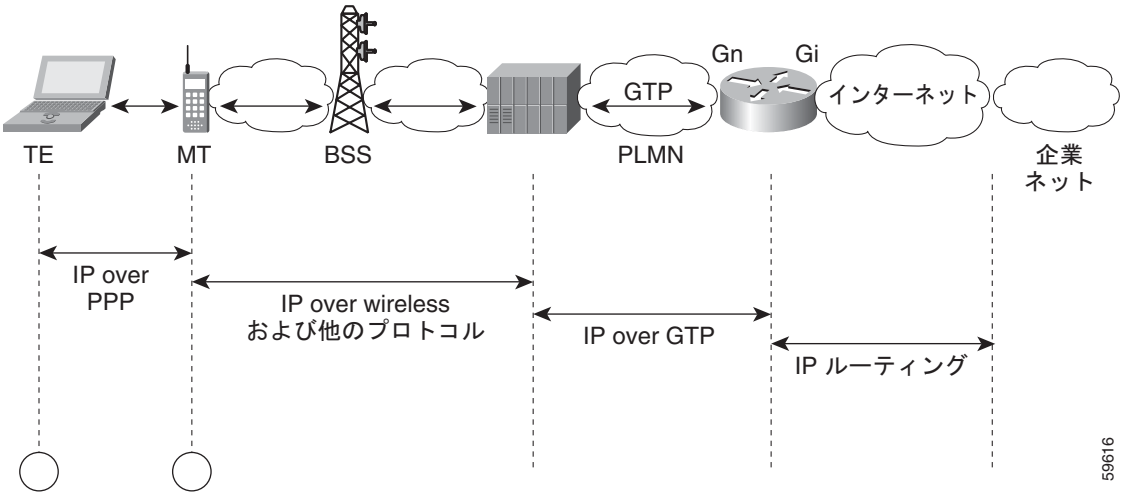
この章は、次の内容で構成されています。

GGSN での PPP サポートの概要

GGSN リリース 3.0 よりも前のリリースの場合、GGSN では、Terminal Equipment（TE; 端末装置）と Mobile Termination（MT; モバイル ターミネーション）間の IP over PPP のトポロジがサポートされていました。MT から Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）を経由し、Gn インターフェイスおよび GTP トンネルを介して GGSN に到達するまで、および Gi インターフェイスを介して企業ネットワークに到達するまでの間では、IP パケット サービスとルーティングだけがサポートされていました。GTP トンネル上、または GGSN と企業ネットワークとの間では、PPP トラフィック フローはサポートされていませんでした。

図 9-1 に、GPRS ネットワーク内で PPP がサポートされていない場合の IP over GTP の実装を示します。

図 9-1　GGSN で PPP がサポートされていない場合の IP over GTP トポロジ



GSM 04.08 バージョン 7.4.0 および GSM 09.60 バージョン 7.0.0 で、GSM 規格に PPP Packet Data Protocol（PDP; パケット データ プロトコル）タイプが追加されました。PPP は、フレーム リレー、ATM、X.25 などのネットワークを含む、さまざまな WAN 環境で幅広く使用されているレイヤ 2 プロトコルです。

PPP では、Password Authentication Protocol（PAP; パスワード認証プロトコル）および Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）によるセキュリティ チェックが提供されており、IP アドレスのネゴシエーションに IP Control Protocol（IPCP; IP コントロール プロトコル）サブレイヤが使用されます。General Packet Radio Service（GPRS; グローバル パケット ラジオ サービス）/Universal Mobile Telecommunication System（UMTS）ネットワーク内での PPP サポートで最も重要な特性は、L2TP を使用した Virtual Private Data Network（VPDN; バーチャル プライベート データ ネットワーク）による PPP のトンネリング機能です。トンネリングによって、公衆網を経由して PPP セッションをプライベート企業ネットワークに転送でき、セキュリティを確保できます。企業ネットワークの境界では、認証およびダイナミック IP アドレス割り当てを実行できます。

Cisco GGSN では、次の 3 つの PPP サポート方式が GGSN で提供されています。

- GTP-PPP
- L2TP を使用した GTP-PPP
- GTP-PPP 再生成

（注） GTP-PPP および GTP-PPP 再生成方式の IPv6 PDP コンテキストはサポートされていません。

（注） 最適な条件の下でいずれかの PPP 方式が設定された場合、GGSN は 8000 の PDP コンテキストをサポートします。ただし、この数は、プラットフォーム、インストールされているメモリ量、設定された PPP サポート方式、設定された PDP コンテキスト作成レートなどによる影響を受けます。

この章の次の項では、それぞれの方式についてより詳細に説明し、GGSN でのそれぞれのタイプの PPP サポートの設定方法および検証方法について説明します。

GGSN での GTP-PPP ターミネーションの設定

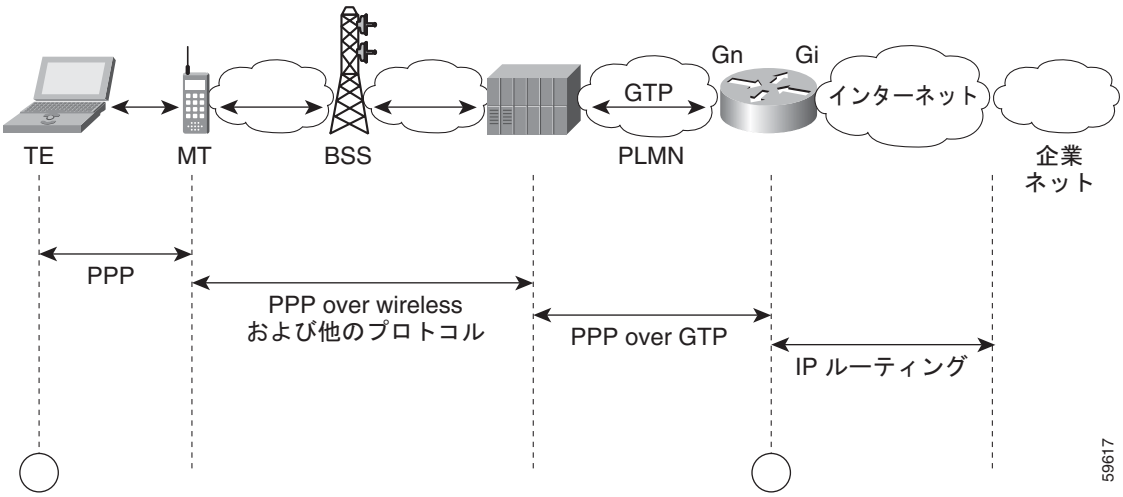
この項では、GGSN での PPP over GTP の概要および設定方法について説明します。内容は次のとおりです。

GGSN での GTP-PPP ターミネーションの概要

GGSN では、L2TP を使用しない GTP 上の PPP PDP タイプがサポートされています。このトポロジでは、GGSN によって、端末装置（TE）およびモバイル ターミネーション（MT）または Mobile Station（MS; モバイル ステーション）から、SGSN を経由し、Gn インターフェイスおよび GTP トンネルを介して GGSN に到達するまでの間の PPP サポートが提供されます。PPP エンドポイントは、端末装置（TE）および GGSN になります。IP ルーティングは、Gi インターフェイスを介して GGSN から企業ネットワークに対して行われます。

図 9-2 に、GPRS ネットワーク内の、L2TP を使用しない PPP over GTP のサポートの実装を示します。

図 9-2　GGSN で PPP ターミネーションが行われる、PPP over GTP トポロジ



利点

GGSN での PPP over GTP のサポートには、次の利点があります。

- GTP 上で、さまざまなトラフィック タイプをサポートできます。
- PPP エンドポイントで PPP オプションの正式なネゴシエーションを実行できます（プロキシ PPP ネゴシエーションは必要ありません）。
- GTP と、L2TP などの他の PPP ネットワーキング プロトコルとのインターワーキングの土台が提供されます。

- MT インテリジェンスの要件が簡素化され、MT で PPP スタックをサポートする必要がありません。
- 追加のセッション セキュリティが提供されます。
- TE に対してより柔軟に IP アドレスを割り当てることができます。

GGSN での PPP over GTP の設定の準備

GGSN で PPP over GTP のサポートの設定を開始する前に、ユーザに IP アドレスを割り当てるために GGSN で使用する方法を決定する必要があります。サポートする IP アドレス割り当て方法によって、設定に特定の依存関係が生じます。

ネットワークで使用されている IP アドレス割り当てのタイプをサポートするには、次の設定ガイドラインが満たされていることを確認してください。

- RADIUS IP アドレス割り当て
  - 完全な username@domain フォーマットを使用して、RADIUS サーバにユーザを設定します。
  - PPP 仮想テンプレート インターフェイスで、**no peer default ip address** コマンドを指定します。
  - GGSN での RADIUS サービスの設定の詳細については、このマニュアルの「GGSN でのセキュリティの設定」を参照してください。
- DHCP IP アドレス割り当て
  - ループバック インターフェイスと同じサブネットに対して、割り当て対象のアドレスの範囲を設定してください。
  - RADIUS サーバのユーザ用の IP アドレスを設定しないでください。
  - PPP 仮想テンプレート インターフェイスで、**peer default ip address dhcp** コマンドを指定します。
  - GGSN で、**aaa authorization network** *method_list* **none** コマンドを指定します。
  - GGSN での DHCP サービスの設定の詳細については、このマニュアルの「GGSN でのダイナミック アドレッシングの設定」を参照してください。
- ローカル プール IP アドレス割り当て
  - **ip local pool** コマンドを使用してローカル プールを設定してください。
  - GGSN で、**aaa authorization network** *method_list* **none** コマンドを指定します。
  - **peer default ip address pool** *pool-name* コマンドを指定します。

GTP-PPP ターミネーション設定の作業リスト

GGSN で PPP over GTP のサポートを設定するには、次の作業を実行します。

- 「ループバック インターフェイスの設定」（P.9-5）（推奨）
- 「PPP 仮想テンプレート インターフェイスの設定」（P.9-5）（必須）
- 「GGSN での PPP 用の仮想テンプレート インターフェイスの関連付け」（P.9-7）（必須）

ループバック インターフェイスの設定

仮想テンプレート インターフェイスには番号を付けず、その IP 番号をループバック インターフェイスに関連付けることを推奨します。

ループバック インターフェイスは、常に稼動しているインターフェイスをエミュレートするソフトウェア専用インターフェイスであり、すべてのプラットフォームでサポートされている仮想インターフェイスです。interface-number は、作成または設定を行うループバック インターフェイスの番号です。作成できるループバック インターフェイスの数に制限はありません。GGSN では、いくつかの異なる機能の設定をサポートするために、ループバック インターフェイスが使用されます。

GGSN でループバック インターフェイスを設定するには、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
ステップ 1	`Router(config)# interface loopback interface-number`	GGSN でループバック インターフェイスを定義します。*interface-number* によって、ループバック インターフェイスが識別されます。
ステップ 2	`Router(config-if)# ip address ip-address mask [secondary]`	インターフェイスの IP アドレスを指定します。 • *ip-address*：インターフェイスの IP アドレスをドット付き 10 進表記で指定します。 • *mask*：サブネット マスクをドット付き 10 進表記で指定します。 • **secondary**：セカンダリ IP アドレスとしてアドレスを設定することを指定します。このキーワードを省略すると、設定したアドレスがプライマリ IP アドレスになります。

PPP 仮想テンプレート インターフェイスの設定

PPP over GTP をサポートするには、PPP カプセル化をサポートする仮想テンプレート インターフェイスを GGSN で設定する必要があります。したがって、GGSN は、GTP カプセル化に 1 つ、PPP カプセル化に 1 つの合計 2 つの仮想テンプレート インターフェイスを持つことになります。GGSN では、GGSN での PPP セッションのすべての PPP 仮想アクセス インターフェイスを作成するために、PPP 仮想テンプレート インターフェイスが使用されます。

仮想テンプレート インターフェイスには番号を付けず、その IP 番号をループバック インターフェイスに関連付けることを推奨します。

PPP カプセル化はデフォルトであるため、インターフェイスに対する **show running-config** の出力には表示されません。

GGSN で PPP 仮想テンプレート インターフェイスを設定するには、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
ステップ 1	`Router(config)# interface virtual-template number`	仮想テンプレート インターフェイスを作成します。*number* によって、仮想テンプレート インターフェイスが識別されます。このコマンドによって、インターフェイス コンフィギュレーション モードが開始されます。 **（注）** この番号は、対応する **gprs gtp ppp vtemplate** コマンドで設定された *number* と同じである必要があります。
ステップ 2	`Router(config-if)# ip unnumbered type number`	インターフェイスに IP アドレスを明示的に割り当てずに、仮想テンプレート インターフェイスで IP 処理をイネーブルにします。*type* および *number* では、ルータに IP アドレスが割り当てられている他のインターフェイスを指定します。 GGSN では、Gi インターフェイスまたはループバック インターフェイスを指定できます。ループバック インターフェイスを使用することを推奨します。

ステップ 3	`Router(config-if)# no peer default ip address`
	（RADIUS サーバの場合）
	または
	`Router(config-if)# peer default ip address dhcp`
	（DHCP サーバの場合）
	または
	`Router(config-if)# peer default ip address pool pool-name`
	（ローカル プールの場合）
		以前に設定したピア IP アドレス プーリング設定をインターフェイスに指定します。
		IP アドレス割り当てに RADIUS サーバを使用している場合は、ピア IP アドレス プーリングをディセーブルにする必要があります。

ステップ 4	`Router(config-if)# encapsulation ppp`	（任意）仮想テンプレート インターフェイス経由で送信されるパケットのカプセル化タイプとして PPP を指定します。PPP は、デフォルトのカプセル化タイプです。 **（注）** PPP はデフォルトのカプセル化タイプであるため、手動でコマンドを設定しないかぎり、仮想テンプレート インターフェイスに対する **show running-config** コマンドの出力には表示されません。
ステップ 5	`Router(config-if)# ppp authentication {pap [chap]} [default]`	CHAP、PAP、またはその両方をイネーブルにして、インターフェイスで CHAP および PAP 認証が選択される順序を指定します。それぞれの意味を次に示します。 • **pap** [**chap**]：インターフェイスで CHAP、PAP、またはその両方をイネーブルにします。 • **default**：**aaa authentication ppp** コマンドによって作成された方式のリストの名前です。

GGSN での PPP 用の仮想テンプレート インターフェイスの関連付け

PPP 用の仮想テンプレート インターフェイスを関連付ける前に、仮想テンプレート インターフェイスを設定する必要があります。仮想テンプレート インターフェイスに設定する番号は、**gprs gtp ppp vtemplate** コマンドで指定する番号と同じである必要があります。

GGSN 用の仮想テンプレート インターフェイスを関連付けるには、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)# gprs gtp ppp vtemplate number`	PPP 特性を定義した仮想テンプレート インターフェイスを、GGSN での GTP 上の PPP PDP タイプのサポートと関連付けます。 **（注）** この番号は、対応する **interface virtual-template** コマンドで設定された *number* と同じである必要があります。

GGSN での L2TP を使用した GTP-PPP の設定

この項では、GGSN での L2TP を使用した PPP over GTP のサポートの概要および設定方法について説明します。内容は次のとおりです。

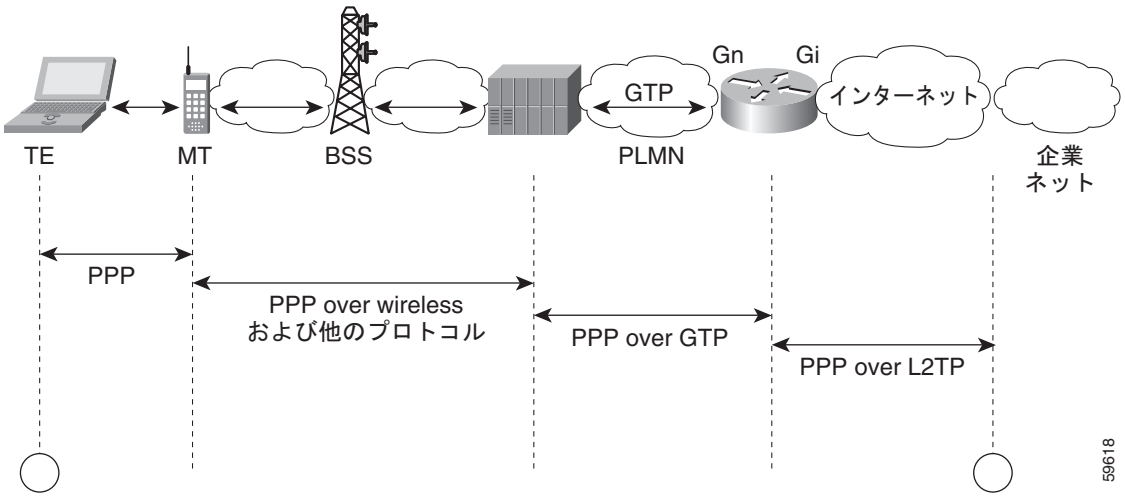
GGSN での L2TP を使用した GTP-PPP の概要

GGSN では、IP ルーティングは使用せず、L2TP を使用した PPP over GTP がサポートされています。GGSN では、TE および MT から SGSN を経由して、Gn インターフェイスおよび GTP トンネルを介して GGSN に到達するまで、および Gi インターフェイスおよび L2TP トンネルを介して企業ネットワークに到達するまでの間で PPP サポートが提供されています。このシナリオでは、PPP ターミネーション エンドポイントは TE と企業ネットワークの L2TP Network Server（LNS; L2TP ネットワーク サーバ）になります。

L2TP がサポートされている場合、パケットは、L2TP および PPP によってカプセル化された IP ペイロードをルーティングすることによって LNS に配信されます。L2TP がサポートされていない場合は、純粋な IP ペイロードが企業ネットワークの LNS にルーティングされます。

図 9-3 に、GPRS ネットワーク内の、L2TP を使用した PPP over GTP のサポートの実装を示します。

図 9-3　GGSN での L2TP を使用した PPP over GTP トポロジ



利点

GGSN での L2TP を使用した PPP over GTP のサポートには、次の利点があります。

- L2TP トンネルを使用した VPN セキュリティでは、公衆網を経由して企業ネットワークまでユーザ データを安全に配信できます。
- 認証、およびアドレスのネゴシエーションと割り当てを使用した、正式なエンドツーエンドの PPP セッションが使用されます。
- ネットワーク内のサーバへのアクセスは、企業ネットワークで引き続き制御できます。GGSN からこれらのサーバへのアクセスを提供する必要はありません。
- GGSN を更新することなく、企業サーバの設定を変更できます。

制約事項

GGSN での L2TP を使用した PPP over GTP のサポートには、次の制約事項があります。

- **ppp authentication** インターフェイス コンフィギュレーション コマンドを使用して、少なくとも 1 つの PPP 認証プロトコルをイネーブルにする必要があります。

L2TP を使用した GTP-PPP の設定の作業リスト

L2TP を使用した GTP over PPP を設定するには、L2TP を使用しない GTP over PPP を設定する場合と同じ設定作業の多くが必要になります。それ以外に、L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）としての GGSN の設定、および Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サービスの設定のためのいくつかの追加作業が必要です。

GGSN で L2TP を使用した PPP over GTP のサポートを設定するには、次の作業を実行します。

- 「LAC としての GGSN の設定」（P.9-9）（必須）
- 「L2TP 用の AAA サービスのサポートの設定」（P.9-10）（必須）

- 「ループバック インターフェイスの設定」（P.9-12）（推奨）
- 「PPP 仮想テンプレート インターフェイスの設定」（P.9-12）（必須）
- 「GGSN での PPP 用の仮想テンプレート インターフェイスの関連付け」（P.9-13）（必須）

LAC としての GGSN の設定

企業ネットワークの LNS への L2TP サービスを GGSN で使用する場合は、GGSN で VPDN サービスをイネーブルにすることによって、GGSN を LAC として設定する必要があります。

Cisco IOS ソフトウェアでの VPDN 設定およびコマンドの詳細については、資料『*Cisco IOS Dial Technologies Configuration Guide*』および『*Command Reference*』を参照してください。

GGSN を LAC として設定し、GGSN にトンネル パラメータをローカルに設定するには、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
ステップ 1	`Router(config)# vpdn enable`	ルータまたは Cisco IOS ソフトウェアのインスタンスで VPDN をイネーブルにし、ローカル データベースおよび存在する場合にはリモート認可サーバ（ホーム ゲートウェイ）でトンネル定義を検索するようにルータに指示します。 **（注）** RADIUS サーバを使用してトンネル パラメータを提供する場合は、このステップだけが必要です。
ステップ 2	`Router(config)# vpdn-group group-number`	VPDN グループを定義して、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-vpdn)# request-dialin`	ルータまたは Cisco IOS ソフトウェアのインスタンスでダイヤルイン トンネルの要求をイネーブルにし、ダイヤルイン VPDN サブグループ要求コンフィギュレーション モードを開始します。
ステップ 4	`Router(config-vpdn-req-in)# protocol l2tp`	ダイヤルイン トンネルに L2TP プロトコルを指定します。
ステップ 5	`Router(config-vpdn-req-in)# domain domain-name`	このドメイン名を持つユーザがトンネリングされることを指定します。トンネリングするすべてのドメイン名に対してこのコマンドを設定します。
ステップ 6	`Router(config-vpdn-req-in)# exit`	VPDN グループ コンフィギュレーション モードに戻ります。
ステップ 7	`Router(config-vpdn)# initiate-to ip ip-address [limit limit-number] [priority priority-number]`	トンネルの宛先 IP アドレスを指定します。
ステップ 8	`Router(config-vpdn)# local name name`	トンネルの認証に使用されるローカル名を指定します。

（注） L2TP トンネル パラメータは、GGSN にローカルで設定したり、RADIUS サーバで提供することができます。RADIUS サーバでトンネル パラメータを提供する場合、この手順で必要となるのは、GGSN に対して **vpdn enable** コマンドを設定することだけです。

L2TP 用の AAA サービスのサポートの設定

GGSN 上の VPDN スタックで LNS への L2TP トンネルが開かれる前に、まずトンネルの認可が試行されます。GGSN では、ローカル データベースに問い合せてこの認可が実行されます。したがって、L2TP トンネルの認可をサポートするためには、GGSN に対して適切な AAA サービスを設定する必要があります。これは、トンネル自体の認可であり、ユーザの認可ではありません。

この項では、GGSN で L2TP の認可のサポートを実装するために必要なコマンドだけを説明します。GGSN での RADIUS および AAA のサポートを設定するために必要なすべての作業について説明するわけではありません。GGSN での AAA サービスのイネーブルおよび AAA サーバ グループの設定の詳細については、このマニュアルの「GGSN でのセキュリティの設定」を参照してください。

（注） GGSN で L2TP 用の認証および認可サービスのサポートを正しく実装するには、両方に対して同じ方式およびサーバ グループを設定する必要があります。

GGSN で L2TP の認可のサポ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
ステップ 1	`Router(config)# aaa authorization network default local`	（任意）GGSN が、トンネルの認可において、**username** コマンドでの定義に従ってローカル データベースに問い合せることを指定します。

	コマンド	目的
ステップ 2	`Router(config)# aaa authorization network {default | list-name} group group-name [group group-name...]`	PPP を実行するインターフェイスで使用する 1 つ以上の AAA 方式を指定します。それぞれの意味を次に示します。 • **network**：SLIP1、PPP2、PPP NCPs3、ARA4 など、ネットワーク関連のすべてのサービス リクエストで認可を実行します。 • **default**：この引数のあとに指定された認証方式を、ユーザがログインするときのデフォルトの方式リストとして使用します。 • *list-name*：ユーザのログイン時に試行される認証方式のリストを指定するための文字列を指定します。 • **group** *group-name* : **aaa group server radius** コマンドで定義されている RADIUS サーバのサブセットを認証に使用します。 （注）　方式リストを必ず使用してください。**aaa authorization network default group radius** 形式のコマンドは使用しないでください。L2TP のサポートでは、*group-name* は **aaa authentication ppp** コマンドで指定するグループと同じである必要があります。
ステップ 3	`Router(config)# username name password secret`	CHAP 発信者識別で使用するパスワードを指定します。*name* はトンネルの名前です。 （注）　*ciscouser*、*ciscouser@corporate1.com*、および *ciscouser@corporate2.com* の形式のユーザ名は、それぞれ 3 つの異なるエントリであると見なされます。 このステップを繰り返して、ローカル ルータまたはアクセス サーバが認証を行う各リモート システムに対してユーザ名エントリを追加します。

（注）　L2TP トンネル パラメータは、GGSN にローカルで設定したり、RADIUS サーバで提供することができます。RADIUS サーバでトンネル パラメータを提供する場合、この手順で必要となるのは、GGSN に対して **username** コマンドを設定することだけです。

ループバック インターフェイスの設定

仮想テンプレート インターフェイスには番号を付けず、その IP 番号をループバック インターフェイスに関連付けることを推奨します。

ループバック インターフェイスは、常に稼動しているインターフェイスをエミュレートするソフトウェア専用インターフェイスであり、すべてのプラットフォームでサポートされている仮想インターフェイスです。インターフェイス数は、作成または設定するループバック インターフェイスの数です。作成できるループバック インターフェイスの数に制限はありません。GGSN では、いくつかの異なる機能の設定をサポートするために、ループバック インターフェイスが使用されます。

GGSN でループバック インターフェイスを設定するには、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
ステップ 1	`Router(config)# interface loopback` *interface-number*	GGSN でループバック インターフェイスを定義します。*interface-number* によって、ループバック インターフェイスが識別されます。
ステップ 2	`Router(config-if)# ip address` *ip-address mask* [**secondary**]	インターフェイスの IP アドレスを指定します。 • *ip-address*：インターフェイスの IP アドレスをドット付き 10 進表記で指定します。 • *mask*：サブネット マスクをドット付き 10 進表記で指定します。 • **secondary**：セカンダリ IP アドレスとしてアドレスを設定することを指定します。このキーワードを省略すると、設定したアドレスがプライマリ IP アドレスになります。

（注）　ループバック インターフェイスの IP アドレスは、L2TP を使用しない PPP PDP でだけ必要です。PPP PDP の宛先が、L2TP が設定されていないドメインである場合は、IP アドレスを使用することを推奨します。

PPP 仮想テンプレート インターフェイスの設定

PPP over GTP をサポートするには、PPP カプセル化をサポートする仮想テンプレート インターフェイスを GGSN で設定する必要があります。したがって、GGSN は、GTP カプセル化に 1 つ、PPP カプセル化に 1 つの合計 2 つの仮想テンプレート インターフェイスを持つことになります。GGSN では、GGSN での PPP セッションのすべての PPP 仮想アクセス インターフェイスを作成するために、PPP 仮想テンプレート インターフェイスが使用されます。

（注）　GTP-PPP および GTP-PPP-L2TP の両方をサポートする計画である場合（L2TP を使用する PPP PDP と L2TP を使用しない PPP PDP をサポートする場合）、PPP に同じ仮想テンプレート インターフェイスを使用する必要があります。

仮想テンプレート インターフェイスには番号を付けず、その IP 番号をループバック インターフェイスに関連付けることを推奨します。

PPP はデフォルトのカプセル化タイプであるため、明示的に設定する必要はなく、インターフェイスに対する **show running-config** の出力には表示されません。

GGSN で PPP 仮想テンプレート インターフェイスを設定するには、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
ステップ 1	`Router(config)# interface virtual-template number`	仮想テンプレート インターフェイスを作成します。*number* によって、仮想テンプレート インターフェイスが識別されます。このコマンドによって、インターフェイス コンフィギュレーション モードが開始されます。 （注）　この番号は、対応する **gprs gtp ppp vtemplate** コマンドで設定された *number* と同じである必要があります。
ステップ 2	`Router(config-if)# ip unnumbered type number`	インターフェイスに IP アドレスを明示的に割り当てずに、仮想テンプレート インターフェイスで IP 処理をイネーブルにします。*type* および *number* では、ルータに IP アドレスが割り当てられている他のインターフェイスを指定します。 GGSN では、Gi インターフェイスまたはループバック インターフェイスを指定できます。シスコでは、ループバック インターフェイスを使用することを推奨します。
ステップ 3	`Router(config-if)# encapsulation ppp`	仮想テンプレート インターフェイス経由で送信されるパケットのカプセル化タイプとして PPP を指定します。PPP は、デフォルトのカプセル化タイプです。 （注）　PPP はデフォルトのカプセル化タイプであるため、手動でコマンドを設定しないかぎり、仮想テンプレート インターフェイスに対する **show running-config** コマンドの出力には表示されません。
ステップ 4	`Router(config-if)# ppp authentication {protocol1 [protocol2...]} [if-needed] [list-name | default] [callin] [one-time] [optional]`	少なくとも 1 つの PPP 認証プロトコルをイネーブルにして、インターフェイスでプロトコルが選択される順序を指定します。

GGSN での PPP 用の仮想テンプレート インターフェイスの関連付け

PPP 用の仮想テンプレート インターフェイスを関連付ける前に、仮想テンプレート インターフェイスを設定する必要があります。仮想テンプレート インターフェイスに設定する番号は、**gprs gtp ppp vtemplate** コマンドで指定する番号と同じである必要があります。

GGSN 用の仮想テンプレート インターフェイスを関連付けるには、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)# gprs gtp ppp vtemplate number`	PPP 特性を定義した仮想テンプレート インターフェイスを、GGSN での GTP 上の PPP PDP タイプのサポートと関連付けます。 （注）　この番号は、対応する **interface virtual-template** コマンドで設定された *number* と同じである必要があります。

GGSN での GTP-PPP 再生成の設定

この項では、GGSN での L2TP を使用した PPP over GTP のサポートの概要および設定方法について説明します。内容は次のとおりです。

GGSN での GTP-PPP 再生成の概要

GGSN では、ネットワークの 2 つの異なる領域で、PPP エンドポイントの 2 つの異なるセットを使用した PPP がサポートされており、それらの間では IP over GTP がサポートされています。最初に、TE と MT との間では IP over PPP が使用されます。MT から SGSN を経由して、Gn インターフェイスおよび GTP トンネルを介して GGSN に到達するまでの間では IP パケットがサポートされます。Gi インターフェイス上で L2TP トンネルを介して企業ネットワークに到達するまでの間では、GGSN によって新たな PPP セッションが開始されます。つまり、2 番めの PPP エンドポイントのセットは、GGSN と企業ネットワークの LNS との間に位置します。

GGSN での PPP 再生成では、IP PDP タイプと PPP および L2TP を組み合せて使用できます。PPP 再生成をサポートするように設定されているアクセス ポイントで GGSN が受信する各 IP PDP コンテキストに対して、GGSN は PPP セッションを再生成します。GGSN では、すべての Tunnel Packet Data Unit（TPDU; トンネル パケット データ ユニット）が PPP ヘッダーおよび L2TP ヘッダーにデータ トラフィックとしてカプセル化されて、LNS に転送されます。

GGSN での PPP 再生成では、重複する IP アドレスを処理するために VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）が実装されます。PPP 再生成が設定された各 Access Point Name（APN; アクセス ポイント ネーム）では、VRF ルーティング テーブルが自動的にイネーブルになります。

Cisco GGSN リリース 8.0 以降の場合、GGSN では、ソフトウェア Interface Description Block（IDB; インターフェイス デスクリプション ブロック）上で動作する PPP セッションに PDP を再生成できます。これにより、サポートされるセッション数が増加します。

制約事項

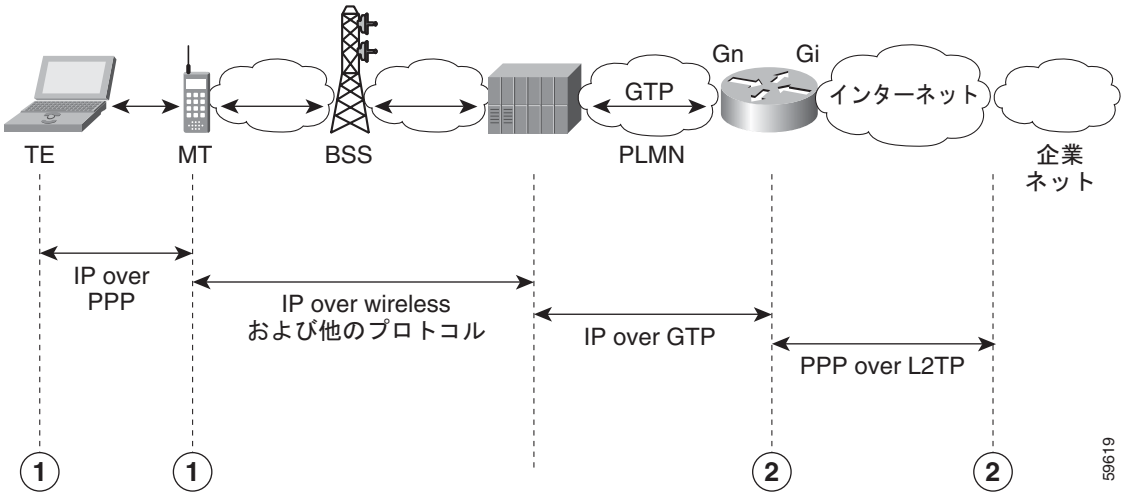
GGSN での PPP 再生成のサポートには、次の制約事項があります。

- VRF の手動設定はサポートされていません。
- **ppp authentication** インターフェイス コンフィギュレーション コマンドを使用して、少なくとも 1 つの PPP 認証プロトコルをイネーブルにする必要があります。
- PPP 再生成仮想テンプレートに、**no peer default ip address** コマンドが設定されている必要があります。

注意　コンソール ロギングがイネーブルになっており（**logging console** コマンド）、PPP 再生成仮想テンプレートでリンク ステータス ログがオフになっていない場合に GGSN で PPP 再生成コンテキストを作成すると、GGSN での CPU 利用率が通常よりも高くなることがあります。

図 9-4 に、GPRS ネットワーク内の、GGSN での PPP 再生成を使用した PPP サポートの実装を示します。

図 9-4　GGSN での PPP 再生成トポロジ



GTP-PPP 再生成設定の作業リスト

GGSN で PPP 再生成を行う IP over GTP を設定するには、L2TP を使用した GTP over PPP の設定に必要な設定作業と同様の作業が必要になります。ただし、実装にいくつかの例外があります。

GGSN で GTP-PPP 再生成のサポートを設定するには、次の作業を実行します。

- 「LAC としての GGSN の設定」（P.9-16）（必須）
- 「L2TP 用の AAA サービスのサポートの設定」（P.9-17）（必須）
- 「PPP 仮想テンプレート インターフェイスの設定」（P.9-19）（必須）
- 「GGSN での PPP 再生成用の仮想テンプレート インターフェイスの関連付け」（P.9-20）（必須）
- 「アクセス ポイントでの PPP 再生成の設定」（P.9-20）（必須）

LAC としての GGSN の設定

企業ネットワークの LNS への L2TP サービスを GGSN で使用する場合は、GGSN で VPDN サービスをイネーブルにすることによって、GGSN を LAC として設定する必要があります。

Cisco IOS ソフトウェアでの VPDN 設定およびコマンドの詳細については、資料『*Cisco IOS Dial Technologies Configuration Guide*』および『*Command Reference*』を参照してください。

GGSN を LAC として設定し、GGSN にトンネル パラメータをローカルに設定するには、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
ステップ 1	`Router(config)# vpdn enable`	ルータまたは Cisco IOS ソフトウェアのインスタンスで VPDN をイネーブルにし、ローカル データベースおよび存在する場合にはリモート認可サーバ（ホーム ゲートウェイ）でトンネル定義を検索するようにルータまたはインスタンスに指示します。 **（注）** RADIUS サーバを使用してトンネル パラメータを提供する場合は、このステップだけが必要です。
ステップ 2	`Router(config)# vpdn domain-delimiter` *characters* [**suffix** | **prefix**]	（任意）ドメイン プレフィクスまたはドメイン サフィクスを区切るために使用する文字を指定します。使用可能な文字は、%、-、@、\、#、および / です。デフォルトは @ です。 **（注）** バックスラッシュ（\）がコマンド ラインの最後のデリミタである場合は、二重のバックスラッシュ（\\）として入力してください。
ステップ 3	`Router(config)# vpdn-group` *group-number*	VPDN グループを定義して、VPDN グループ コンフィギュレーション モードを開始します。
ステップ 4	`Router(config-vpdn)# request-dialin`	ルータまたは Cisco IOS ソフトウェアのインスタンスでダイヤルイン トンネルの要求をイネーブルにし、ダイヤルイン VPDN サブグループ要求コンフィギュレーション モードを開始します。
ステップ 5	`Router(config-vpdn-req-in)# protocol l2tp`	ダイヤルイン トンネルでの L2TP プロトコルの使用を指定します。
ステップ 6	`Router(config-vpdn-req-in)# domain` *domain-name*	このドメイン名を持つユーザがトンネリングされることを指定します。トンネリングするすべてのドメイン名に対してこのコマンドを設定します。
ステップ 7	`Router(config-vpdn-req-in)# exit`	VPDN グループ コンフィギュレーション モードに戻ります。
ステップ 8	`Router(config-vpdn)# initiate-to ip` *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]	トンネルの宛先 IP アドレスを指定します。
ステップ 9	`Router(config-vpdn)# local name` *name*	トンネルの認証に使用されるローカル名を指定します。

（注） L2TP トンネル パラメータは、GGSN にローカルで設定したり、RADIUS サーバで提供することができます。RADIUS サーバでトンネル パラメータを提供する場合、この手順で必要となるのは、GGSN に対して **vpdn enable** コマンドを設定することだけです。

L2TP 用の AAA サービスのサポートの設定

GGSN 上の VPDN スタックで LNS への L2TP トンネルが開かれる前に、まずトンネルの認可が試行されます。GGSN では、ローカル データベースに問い合せてこの認可が実行されます。したがって、L2TP トンネルの認可をサポートするためには、GGSN に対して適切な AAA サービスを設定する必要があります。これは、トンネル自体の認可であり、ユーザの認可ではありません。

この項では、GGSN で L2TP の認可のサポートを実装するために必要なコマンドだけを説明します。GGSN での RADIUS および AAA のサポートを設定するために必要なすべての作業について説明するわけではありません。GGSN での AAA サービスのイネーブルおよび AAA サーバ グループの設定の詳細については、このマニュアルの「GGSN でのセキュリティの設定」を参照してください。

（注） GGSN で L2TP 用の認証および認可サービスのサポートを正しく実装するには、両方に対して同じ方式およびサーバ グループを設定する必要があります。

GGSN で L2TP の認可のサポ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
ステップ 1	`Router(config)# aaa authorization network default local`	（任意）GGSN が、トンネルの認可において、**username** コマンドでの定義に従ってローカル データベースに問い合せることを指定します。

	コマンド	目的
ステップ 2	`Router(config)# aaa authorization network {default | list-name} group group-name [group group-name...]`	PPP を実行するインターフェイスで使用する 1 つ以上の AAA 方式を指定します。それぞれの意味を次に示します。 • **network**：SLIP1、PPP2、PPP NCPs3、ARA4 など、ネットワーク関連のすべてのサービス リクエストで認可を実行します。 • **default**：この引数のあとに指定された認証方式を、ユーザがログインするときのデフォルトの方式リストとして使用します。 • *list-name*：ユーザのログイン時に試行される認証方式のリストを指定するための文字列を指定します。 • **group** *group-name*：**aaa group server radius** コマンドで定義されている RADIUS サーバのサブセットを認証に使用します。 **（注）** 方式リストを必ず使用してください。**aaa authorization network default group radius** 形式のコマンドは使用しないでください。L2TP のサポートでは、*group-name* は **aaa authentication ppp** コマンドで指定するグループと同じである必要があります。
ステップ 3	`Router(config)# username name password secret`	CHAP 発信者識別で使用するパスワードを指定します。*name* はトンネルの名前です。 **（注）** *ciscouser*、*ciscouser@corporate1.com*、および *ciscouser@corporate2.com* の形式のユーザ名は、それぞれ 3 つの異なるエントリであると見なされます。 このステップを繰り返して、ローカル ルータまたはアクセス サーバが認証を行う各リモート システムに対してユーザ名エントリを追加します。

（注） L2TP トンネル パラメータは、GGSN にローカルで設定したり、RADIUS サーバで提供することができます。RADIUS サーバでトンネル パラメータを提供する場合、この手順で必要となるのは、GGSN に対して **username** コマンドを設定することだけです。

PPP 仮想テンプレート インターフェイスの設定

PPP 再生成を行う IP over GTP をサポートするには、GGSN で、PPP カプセル化をサポートする仮想テンプレート インターフェイスを設定する必要があります。したがって、GGSN は、GTP カプセル化に 1 つ、PPP カプセル化に 1 つの合計 2 つの仮想テンプレート インターフェイスを持つことになります。GGSN では、GGSN での PPP セッションのすべての PPP 仮想アクセス インターフェイスを作成するために、PPP 仮想テンプレート インターフェイスが使用されます。

PPP はデフォルトのカプセル化タイプであるため、明示的に設定する必要はなく、インターフェイスに対する **show running-config** の出力には表示されません。

GGSN で PPP 再生成をサポートするために PPP 仮想テンプレート インターフェイスに対して使用するコンフィギュレーション コマンドは、前述の GTP over PPP サポートで示したコマンドとは異なります。

GGSN で PPP 仮想テンプレート インターフェイスを設定するには、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
ステップ 1	`Router(config)# interface virtual-template number`	仮想テンプレート インターフェイスを作成します。*number* によって、仮想テンプレート インターフェイスが識別されます。このコマンドによって、インターフェイス コンフィギュレーション モードが開始されます。 **（注）** この番号は、対応する **gprs gtp ppp-regeneration vtemplate** コマンドで設定された *number* と同じである必要があります。
ステップ 2	`Router(config-if)# ip address negotiated`	特定のインターフェイスの IP アドレスが、PPP/IPCP（IP コントロール プロトコル）アドレス ネゴシエーションによって取得されることを指定します。
ステップ 3	`Router(config-if)# no peer neighbor-route`	近接ルートの作成をディセーブルにします。
ステップ 4	`Router(config-if)#no peer default ip address`	このインターフェイスに接続しているリモート ピアに対して IP アドレスが返されないようにします。
ステップ 5	`Router(config-if)# encapsulation ppp`	（任意）仮想テンプレート インターフェイス経由で送信されるパケットのカプセル化タイプとして PPP を指定します。PPP は、デフォルトのカプセル化タイプです。 **（注）** PPP はデフォルトのカプセル化タイプであるため、手動でコマンドを設定しないかぎり、仮想テンプレート インターフェイスに対する **show running-config** コマンドの出力には表示されません。
ステップ 6	`Router(config-if)# ppp authentication {protocol1 [protocol2...]} [if-needed] [list-name | default] [callin] [one-time] [optional]`	少なくとも 1 つの PPP 認証プロトコルをイネーブルにして、インターフェイスでプロトコルが選択される順序を指定します。

GGSN での PPP 再生成用の仮想テンプレート インターフェイスの関連付け

PPP 再生成用の仮想テンプレート インターフェイスを関連付ける前に、仮想テンプレート インターフェイスを設定する必要があります。仮想テンプレート インターフェイスに設定する番号は、**gprs gtp ppp-regeneration vtemplate** コマンドで指定する番号と同じである必要があります。

PPP 再生成用の仮想テンプレート インターフェイスを関連付けるには、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)# gprs gtp ppp-regeneration vtemplate` *number*	PPP 特性を定義した仮想テンプレート インターフェイスを、GGSN での PPP 再生成のサポートと関連付けます。 **（注）** この番号は、対応する **interface virtual-template** コマンドで設定された *number* と同じである必要があります。

アクセス ポイントでの PPP 再生成の設定

GGSN で PPP 再生成をイネーブルにするには、PPP 再生成をサポートする各アクセス ポイントを設定する必要があります。GGSN のすべてのアクセス ポイントに対して PPP 再生成をイネーブルにするグローバル コンフィギュレーション コマンドはありません。

アクセス ポイントを作成し、そのタイプを指定するには、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
ステップ 1	`Router(config)# gprs access-point-list` *list-name*	新しいアクセス ポイント リストの名前を指定するか、既存のアクセス ポイント リストの名前を参照し、アクセス ポイント リスト コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-ap-list)# access-point` *access-point-index*	新しいアクセス ポイント定義のインデックス番号を指定するか、既存のアクセス ポイント定義を参照し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-access-point)# access-point-name` *apn-name*	アクセス ポイント ネットワーク ID を指定します。これには、インターネット ドメイン名が広く使用されています。 **（注）** *apn-name* は、MS、Home Location Register（HLR; ホーム ロケーション レジスタ）、および Domain Name System（DNS; ドメイン ネーム システム）サーバにプロビジョニングされた APN と一致する必要があります。

	コマンド	目的
ステップ 4	`Router(config-access-point)# access-mode transparent`	（任意）このアクセス ポイントに対して、GGSN によってセキュリティ認可または認証が要求されていないことを指定します。 **（注）** 透過的アクセスがデフォルト値ですが、アクセス モードが以前は非透過であった場合は、アクセス ポイントで PPP 再生成をサポートするために、透過的アクセスを *手動* で設定する必要があります。
ステップ 5	`Router(config-access-point)# ppp-regeneration [max-session number | setup-time seconds | verify-domain | fixed-domain]`	アクセス ポイントで PPP 再生成のサポートをイネーブルにします。それぞれの意味を次に示します。 • **max-session** *number*：アクセス ポイントで許可されている PPP 再生成セッションの最大数を指定します。デフォルト値は 65535 です。 • **setup-time** *seconds*：PPP 再生成セッションの確立に許可されている最大時間（1 から 65535 秒）を指定します。デフォルト値は 60 秒です。 • **verify-domain**：PPP 再生成が使用されている場合には、PDP コンテキストの作成要求で送信された Protocol Configuration Option（PCO; プロトコル設定オプション）Information Element（IE; 情報エレメント）に含まれるドメインを、ユーザが送信した APN と照合して検証するように、GGSN を設定します。 不一致が発生した場合、PDP コンテキストの作成要求は原因コード「Service not supported」で拒否されます。 • **fixed-domain**：PPP 再生成が使用されている場合、アクセス ポイント ネームを、ユーザまでの L2TP トンネルを開始するドメイン名として使用するように、GGSN を設定します。 **ppp-regeneration fixed-domain** と **ppp-regeneration verify-domain** コマンド設定は、相互に排他的です。**ppp-regeneration fixed-domain** コマンドが設定されている場合、ドメイン検証は実行できません。

GGSN での PPP のモニタリングおよびメンテナンス

この項では、GGSN でのさまざまな PPP 設定をモニタリングするために使用できる **show** コマンドの概要リストを示します。すべての **show** コマンドをすべての設定方法に適用できるわけではありません。

GGSN において PPP ステータスをモニタリングおよびメンテナンスするには、次の特権 EXEC コマンドを使用します。

コマンド	目的
Router# **show derived-config interface virtual-access** *number*	PPP 再生成セッションの仮想アクセス インターフェイス上の、GTP によって設定されている PPP オプションを表示します。
Router# **show gprs gtp pdp-context all**	現在アクティブなすべての PDP コンテキストを表示します。
Router# **show gprs gtp pdp-context path** *ip-address*	指定した SGSN パスの現在アクティブなすべての PDP コンテキストを表示します。
Router# **show gprs gtp pdp-context pdp-type ppp**	PPP を使用して送信される現在アクティブなすべての PDP コンテキストを表示します。
Router# **show gprs gtp status**	GGSN 上の GTP の現在のステータスに関する情報を表示します。
Router# **show interfaces virtual-access** *number* [**configuration**]	指定した仮想アクセス インターフェイスのステータス、トラフィック データ、および設定情報を表示します。
Router# **show vpdn session** [**all** | **packets** | **sequence** | **state** | **timers** | **window**] [**interface** | **tunnel** | **username**]	インターフェイス、トンネル、ユーザ名、パケット、ステータス、ウィンドウ統計情報などの VPN セッション情報を表示します。
Router# **show vpdn tunnel** [**all** | **packets** | **state** | **summary** | **transport**] [**id** | **local-name** | **remote-name**]	トンネル プロトコル、ID、ローカル トンネル名、リモート トンネル名、送受信パケット、トンネル、転送ステータスなどの VPN トンネル情報を表示します。

設定例

この項では、GGSN でのさまざまなタイプの PPP サポートの設定例を示します。次のような例があります。

- 「GGSN での GTP-PPP ターミネーションの設定例」（P.9-23）
- 「GTP-PPP-over-L2TP の設定例」（P.9-24）
- 「GTP-PPP 再生成の設定例」（P.9-25）
- 「L2TP 用の AAA サービスの設定例」（P.9-26）

GGSN での GTP-PPP ターミネーションの設定例

次の例は、PAP 認証を使用し、IP アドレスの割り当てに 172.16.0.2 の RADIUS サーバを使用する、GGSN での GTP over PPP の設定を示しています。

```
Router# show running-config
Building configuration...
Current configuration : 3521 bytes
!
version 12.2
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
! Enables the router for GGSN services
!
service gprs ggsn
!
ip cef
!
no logging buffered
logging rate-limit console 10 except errors
!
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius gtp_ppp
 server 172.16.0.2 auth-port 2001 acct-port 2002
!
! Configures authentication and authorization
! methods for PPP support.
!
aaa authentication ppp gtp_ppp group gtp_ppp
aaa authorization network gtp_ppp group gtp_ppp
aaa accounting network default start-stop group gtp_ppp
!
ip subnet-zero
!
! Configures a loopback interface
! for the PPP virtual template interface
!
interface Loopback2
 ip address 10.88.0.4 255.255.0.0
!
...
!
! Configures a VT interface for
! GTP encapsulation
!
interface loopback 1
 ip address 10.30.30.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
! Configures a VT interface for
```

```
! PPP encapsulation
!
interface Virtual-Template2
 ip unnumbered Loopback2
 no peer default ip address
 ppp authentication pap
!
...
!
gprs access-point-list gprs
  access-point 1
   access-point-name gprs.cisco.com
   aaa-group authentication gtp_ppp
   aaa-group accounting gtp_ppp
   exit
   !
! Associates the PPP virtual template
! interface for use by the GGSN
!
gprs gtp ppp-vtemplate 2
gprs default charging-gateway 10.7.0.2
!
gprs memory threshold 512
!
! Configures a global RADIUS server host
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 172.16.0.2 auth-port 2001 acct-port 2002
radius-server retransmit 3
radius-server key cisco
!
!
end
```

GTP-PPP-over-L2TP の設定例

次の例は、GGSN での L2TP を使用した PPP over GTP のサポートの設定の一部を示しています。トンネル パラメータは GGSN でローカルに設定され、RADIUS サーバからは提供されません。

```
. . .
!
! Enables AAA globally
!
aaa new-model
!
aaa authorization network default local
!
vpdn enable
!
! Configures a VPDN group
!
vpdn-group 1
  request-dialin
  protocol l2tp
  domain ppp-lns
  initiate-to ip 4.0.0.78 priority 1
  local name nas
!
! Configures a loopback interface
! for the PPP virtual template interface
```

```
!
interface Loopback2
 ip address 10.88.0.1 255.255.255.255
!
interface Virtual-Template2
 description VT for PPP L2TP
 ip unnumbered Loopback2
 no peer default ip address
 no peer neighbor-route
 ppp authentication pap chap
!
gprs access-point-list gprs
 access-point 15
 access-point-name ppp-lns
 exit
!
! Associates the PPP virtual template
! interface for use by the GGSN
!
gprs gtp ppp vtemplate 2
!
. . .
!
```

GTP-PPP 再生成の設定例

次の例は、GGSN での PPP 再生成を行う IP over GTP のサポートの設定の一部を示しています。トンネル パラメータは GGSN でローカルに設定され、RADIUS サーバからは提供されません。

```
!
. . .
!
! Enables AAA globally
!
vpdn enable
!
! Configures a VPDN group
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain ppp_regen1
 initiate-to ip 4.0.0.78 priority 1
 l2tp tunnel password 7 0114161648
!
! Configures a virtual template
! interface for PPP regeneration
!
interface Virtual-Template2
 description VT for PPP Regen
 ip address negotiated
 no peer neighbor-route
 no peer default ip address
 ppp authentication pap chap
!
gprs access-point-list gprs
 access-point 6
  access-point-name ppp_regen1
  ppp-regeneration
  exit
!
! Associates the PPP-regeneration
```

```
! virtual template interface for use by the GGSN
!
gprs gtp ppp-regeneration vtemplate 2
```

L2TP 用の AAA サービスの設定例

GGSN では、PPP-over-GTP テクノロジーおよび PPP 再生成を行う IP-over-GTP テクノロジーの両方のサポートにおいて、L2TP サポートが使用されます。次の例は、GGSN で L2TP サポートを提供するための RADIUS および AAA サービスの設定の一部を示しています。

```
!
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius gtp_ppp
 server 172.16.0.2 auth-port 2001 acct-port 2002
!
! Configures authentication and authorization
! method gtp_ppp and AAA server group gtp_ppp
! for PPP support.
!
! NOTE: You must configure the same methods and groups
! to support L2TP as shown by the
! aaa authentication ppp gtp_ppp
! and aaa authorization network gtp_ppp commands.
!
aaa authentication ppp gtp_ppp group gtp_ppp
aaa authorization network default local
aaa authorization network gtp_ppp group gtp_ppp
aaa accounting network default start-stop group radius
username nas password 0 lab
username hgw password 0 lab
!
. . .
!
! Configures a global RADIUS server host
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 172.16.0.2 auth-port 2001 acct-port 2002
radius-server retransmit 3
radius-server key cisco
!
. . .
!
```

CHAPTER 10

GGSN での QoS の設定

この章では、Quality of Service（QoS）機能を設定し、Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）でトラフィック フローを識別する方法について説明します。

この章に記載されている GGSN コマンドの詳細については、使用している Cisco GGSN リリースの『*Cisco GGSN Command Reference*』を参照してください。この章に記載されているその他のコマンドのマニュアルを参照するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

この章は、次の内容で構成されています。

GGSN での QoS サポートの概要

Cisco GGSN ソフトウェアでは、3G Universal Mobile Telecommunication System（UMTS）QoS がサポートされています。各 GPRS/UMTS Packet Data Protocol（PDP; パケット データ プロトコル）のコンテキスト要求には、UMTS QoS プロファイルが含まれています。

GPRS/UMTS Public LAN Mobile Network（PLMN; パブリック LAN モバイル ネットワーク）での QoS サポートの実装は、サービス プロバイダーや、ネットワークで使用可能なリソースによって異なります。Third Generation Partnership Project（3GPP; 第 3 世代パートナーシップ プロジェクト）規格では、UMTS MS で定義可能な UMTS QoS クラスが定義されます。ただし、サービス プロバイダーでの実装に応じて、実行される QoS はネゴシエーションされ、GPRS/UMTS ネットワーク バックボーン内で変動します。

UMTS QoS

異なるレベルの QoS を管理するために、UMTS では、遅延、ジッタ、帯域幅、および信頼性の各要因に基づいて、次の 4 つの QoS トラフィック クラスが定義されています。

- Conversational
- Streaming

- Interactive
- Background

Cisco GGSN では、Cisco IOS QoS Differentiated Services（Diffserv; ディファレンシエーテッド サービス）を使用して実装することにより、エンドツーエンドの UMTS QoS が提供されています。

この章では、GGSN が UMTS QoS クラスに提供する QoS サポートについて説明します。

GGSN での UMTS QoS の設定

ここでは、GGSN で UMTS QoS を設定する方法について説明します。内容は次のとおりです。

UMTS QoS の概要

3GPP 規格では、UMTS の遅延、ジッタ、帯域幅、および信頼性に基づいて、4 つの QoS トラフィック クラスが定義されています。表 10-1 は、これらの UMTS トラフィック クラスとその特性、アプリケーション、およびマッピングされている Cisco IOS QoS Diffserv クラスを示しています。

表 10-1　UMTS トラフィック クラス

トラフィック クラス	Conversational（リアルタイム）	Streaming（リアルタイム）	Interactive（ベストエフォート）	Background（ベストエフォート）
特性	ストリームの情報エンティティ間で時間関係（バリエーション）を保持します。 したがって、会話パターンの遅延とジッタが大幅に低くなります。	ストリームの情報エンティティ間で時間関係（バリエーション）を保持します。 遅延とジッタの要件は、conversational クラスほど厳密ではありません。	要求/応答パターン。 ペイロード コンテンツ インルートの再送信。	宛先で期待されるデータの時間は厳密ではありません。 ペイロード コンテンツ インルートの再送信が発生する可能性があります。

表 10-1　UMTS トラフィック クラス （続き）

トラフィック クラス	Conversational（リアルタイム）	Streaming（リアルタイム）	Interactive（ベストエフォート）	Background（ベストエフォート）
アプリケーションの例	Voice over IP	オーディオやビデオのストリーミング	Web ブラウズ	電子メールのダウンロード
Diffserv クラス / DSCP へのマッピング	緊急転送クラス	確認転送 2 クラス	確認転送 3 クラス	ベストエフォート

Cisco GGSN では、Cisco IOS Differentiated Services（Diffserv）モデルを使用して実装することにより、エンドツーエンドの UMTS QoS がサポートされています。DiffServ モデルは、異なる QoS 要件を満たすことが可能な複数サービス モデルです。ネットワークでは、DiffServ を使用し、パケットごとに指定された QoS に基づいて特定の種類のサービスを提供しようとします。この仕様は、IP パケットまたは送信元アドレスと宛先アドレスでの 6 ビット Differentiated Services Code Point（DSCP; DiffServ コード ポイント）設定の使用など、さまざまな方法で使用されます。ネットワークでは、この QoS 仕様に基づいてトラフィックのマーキング、形成、およびポリシングを行い、インテリジェント キューイングを実行します。

Cisco IOS QoS および DiffServ サービス モデルの詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』を参照してください。

UMTS QoS の設定の作業リスト

GGSN で UMTS QoS 方式を実装するには、最初にこの機能をイネーブルにする必要があります。その後、ネットワークのニーズがサポートされるように、UMTS QoS オプションを変更できます。

Cisco 7600 プラットフォームでの GGSN UMTS QoS の設定の作業リスト

Cisco 7600 プラットフォームで GGSN の UMTS QoS を設定する場合は、次の作業を実行します。

- 「GGSN での UMTS QoS マッピングのイネーブル」（P.10-3）（必須）
- 「DiffServ PHB グループへの UMTS QoS トラフィック クラスのマッピング」（P.10-4）（任意）
- 「DiffServ PHB グループへの DSCP への割り当て」（P.10-5）（任意）
- 「加入者データグラムでの DSCP の設定」（P.10-6）（任意）
- 「Cisco 7600 プラットフォームでの GGSN UMTS QoS 要件の設定」（P.10-7）（必須）
- 「GGSN でのコール アドミッション制御の設定」（P.10-12）（任意）
- 「UMTS QoS 設定の確認」（P.10-10）

GGSN での UMTS QoS マッピングのイネーブル

デフォルトでは、GGSN で UMTS QoS はイネーブルではありません。GGSN でモバイル UMTS QoS 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)# gprs qos map umts`	GGSN で UMTS QoS マッピングをイネーブルにします。

DiffServ PHB グループへの UMTS QoS トラフィック クラスのマッピング

UMTS QoS トラフィック クラスから DiffServ Per-Hop Behavior（PHB）グループへの QoS マッピングを指定する前に、グローバル コンフィギュレーション モードで **gprs qos map umts** コマンドを使用して UMTS QoS マッピングをイネーブルにする必要があります。

UMTS QoS トラフィック クラスのデフォルトのマッピング値は、次のとおりです。

- conversational トラフィック クラスと ef-class DiffServ PHB グループ
- streaming トラフィック クラスと af2-class DiffServ PHB グループ
- interactive トラフィック クラスと af3-class DiffServ PHB グループ
- background トラフィック クラスと best-effort DiffServ PHB グループ

これらのデフォルト以外のマッピング値を使用する場合は、**gprs umts-qos map traffic-class** コマンドを使用して、UMTS トラフィック クラスを別の DiffServ PHB グループにマッピングできます。

（注） UMTS QoS トラフィック クラスを DiffServ PHB に正常にマッピングするには、Cisco IOS ソフトウェア コマンドである **class map** および **match ip dscp** を使用して、クラス マップを設定する必要があります。クラス マップの設定の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』を参照してください。

UMTS トラフィック クラスを DiffServ PHB グループにマッピングするには、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)# gprs umts-qos map traffic-class` *traffic-class diffserv-phb-group*	DiffServ PHB への UMTS QoS トラフィック クラスのマッピングをイネーブルにします。UMTS トラフィック クラスは次のとおりです。 • signalling • conversational • streaming • interactive • background DiffServ PHB グループは次のとおりです。 • signalling-class • ef-class • af1-class • af2-class • af3-class • af4-class • best-effort

DiffServ PHB グループへの DSCP への割り当て

デフォルトでは、PHB クラスに関連付けられているデフォルトの DiffServ コード ポイント（DSCP）値が使用されます。表 10-2 は、各 PHB グループに対する DSCP のデフォルト値を示しています。

表 10-2　PHB グループに対する DSCP のデフォルト値

PHB グループ	DSCP 値
EF	101110
AF11	001010
AF12	001100
AF13	001110
AF21	010010
AF22	010100
AF23	010110
AF31	011010
AF32	011100
AF33	011110
AF41	100010
AF42	100100
AF43	100110
Best Effort	000000

ただし、1 つの DSCP を複数の PHB グループに割り当てることができます。

Assured Forwarding（AF; 確認転送）PHB グループの場合は、廃棄優先順位ごとに最大 3 つの DSCP を指定できます。signalling、EF、および best-effort の各クラスには廃棄優先順位がないため、最初の DSCP 値だけが使用されます。これらのクラスの引数 *dscp2* または *dscp3* に値を入力した場合、この値は無視されます。

（注） 廃棄優先順位は、ネットワークで輻輳が発生した場合にパケットが廃棄される順序を示しています。

（注） UMTS QoS トラフィック クラスを DiffServ PHB に正常にマッピングし、DSCP 値を DiffServ PHB グループに割り当てるには、**class map** と **match ip dscp** の各コマンドを使用してクラス マップを設定する必要があります。クラス マップの設定の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』および『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。

（注） デフォルトでは、signalling クラスは CS5（101000）に割り当てられます。これは IP precedence 5 と同等です。

DSCP 値を DiffServ PHB グループに割り当てるには、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)# **gprs umts-qos map diffserv-phb** *diffserv-phb-group* [*dscp1*] [*dscp2*] [*dscp3*]	DSCP を DiffServ PHB グループに割り当てます。DiffServ PHB グループは次のとおりです。 • signalling • ef-class • af1-class • af2-class • af3-class • af4-class • best-effort DSCP は次のとおりです。 • dscp1：すべてのクラスで必要です。64 個の DSCP 値（0 ～ 63）から 1 つ指定します。この DSCP 値は廃棄優先順位 1 と対応します。 • dscp2：（AF クラスの場合は任意）64 個の DSCP 値（0 ～ 63）から 1 つ指定します。この DSCP 値は廃棄優先順位 2 と対応します。 • dscp3：（AF クラスの場合は任意）64 個の DSCP 値（0 ～ 63）から 1 つ指定します。この DSCP 値は廃棄優先順位 3 と対応します。

加入者データグラムでの DSCP の設定

デフォルトでは、加入者データグラム内の DSCP は、PDP コンテキストが作成されたときにトラフィック クラスに割り当てられた DSCP で再マーキングされます。

加入者データグラムが、DSCP を変更することなく GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）パスを介して転送されるように指定するには、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)# **gprs umts-qos dscp unmodified** [**up** | **down** | **all**]	加入者データグラムが、DSCP を変更することなく GTP パスを介して転送されるように指定します。

デフォルト値に戻すには、**no gprs umts-qos dscp unmodified** コマンドを発行します。

Cisco 7600 プラットフォームでの GGSN UMTS QoS 要件の設定

Cisco 7600 プラットフォームの Cisco Service and Application Module for IP（SAMI）上で実行されている GGSN の UMTS QoS を設定する場合、プラットフォームの各種コンポーネントでさまざまな QoS 機能が実行されます。表 10-3 は、Cisco 7600 プラットフォームのコンポーネントで実行される QoS 機能を示しています。

表 10-3　Cisco 7600 プラットフォームのコンポーネントでの QoS 機能

Cisco 7600 コンポーネント	UMTS QoS 機能
Catalyst ラインカード	分類、および入力/出力のスケジューリング
スーパーバイザ エンジン	分類および集約ポリシング
Cisco SAMI での Cisco IOS GGSN イメージ	分類、DSCP マーキング、および出力キューイング

GGSN で UMTS QoS を設定したあと、次の作業を完了する必要があります。

スーパーバイザ エンジン

（注）　次のリストは、GGSN で UMTS QoS のスーパーバイザ エンジンで完了しておく必要がある、必須作業の概要を示しています。これらの各作業の詳細については、『*Cisco 7600 Series Cisco IOS Software Configuration Guide*』を参照してください。

1. グローバル コンフィギュレーション モードで **mls qos** コマンドを使用して、マルチレイヤ スイッチング QoS をイネーブルにします。

```
Router# mls qos
```

2. スーパーバイザ エンジンで、Gi トラフィックの集約ポリシングを設定します。

（注）　複数の Gn インターフェイスと Gi インターフェイスを使用できますが、すべてのトラフィックが最終的に SAMI 上の単一の GE ポートに到達する必要があるため（2 つの GGSN に対して 1 つの GE）、SAMI へのトラフィックのレートを制限するために名前付き集約ポリサーを使用することを推奨します。また、不適合トラフィックはすべて廃棄することも推奨します。

次の例は、名前付き集約ポリサーの設定を示しています。名前付きポリサーは Gi インターフェイスに付加されます。

```
Access-list 101 permit ip any any dscp ef
Access-list 102 permit ip any any dscp af21
Access-list 103 permit ip any any dscp af31
Access-list 103 permit ip any any dscp af32
Access-list 103 permit ip any any dscp af33
Access-list 104 permit ip any any

Class-map match-all conversational
    Match access-group 101
Class-map match-all streaming
    Match access-group 102
Class-map match-all interactive
    Match access-group 103
```

```
Class-map match-all background
    Match access-group 104

Mls qos aggregate-policer AGGREGATE-CONV bit-rate1 normal-burst max-burst
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-STREAMING bit-rate1 normal-burst max-burst
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-INTERACTIVE bit-rate1 normal-burst max-burst
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-BACKGROUND bit-rate1 normal-burst max-burst
conform-action transmit exceed-action drop

Policy-map Gi-incoming
     Class conversational
         Police aggregate AGGREGATE-CONV
     Class streaming
         Police aggregate AGGREGATE-STREAMING
     Class interactive
         Police aggregate AGGREGATE-INTERACTIVE
     Class background
         Police aggregate AGGREGATE-BACKGROUND

Router(config-if)# service-policy input Gi-incoming
```

（注）　ポリシング統計情報をモニタリングするときは、次の **show** コマンドを使用できます。
- **show mls qos aggregate-policer** *name*
- **show policy-map interface** *interface*
- **show policy interface** *interface*

3. **msl qos trust dscp** インターフェイス コンフィギュレーション コマンドを使用して、入力ポートの信頼状態を trust-dscp モードに設定します。

```
Router(config)# interface FastEthernet2/1
Router(config-if)# mls qos trust dscp
```

4. 次の作業を実行して、出力ポート スケジューリングを設定します。

   a. Cisco SAMI で実行されている GGSN インスタンスで **show gprs umts-qos traffic class** 特権 EXEC コマンドを使用して、UMTS トラフィックのクラス/DSCP マッピングを取得します。

```
Router# ggsn show gprs umts-qos traffic-class
```

   b. **show mls qos maps** 特権 EXEC コマンドを使用して QoS マッピング情報を表示することにより、デフォルトの DSCP/CoS マッピングを取得します。

```
Router# show mls qos maps
```

   c. **show queuing interface** 特権 EXEC コマンドを使用して、インターフェイスのキューイング統計情報を表示することにより、デフォルトの CoS / キュー マッピングを取得します。

```
Router# show queuing interface interface
```

   d. ステップ A、B、および C で取得される情報を使用して、カスタマイズされた DSCP/CoS 出力マッピングが必要かどうかを判別します。必要な場合は、グローバル コンフィギュレーション モードで **mls qos map dscp-cos** コマンドを使用してマッピングを定義します。

```
Router(config)# mls qos map dscp-cos dscp to cos
```

DSCP/CoS マッピングをカスタマイズする場合は、次のことを確認します。

- conversational トラフィックと streaming トラフィックが出力キュー 4 に割り当てられていること

- interactive トラフィックと background トラフィックが、2 つの通常キューの間で同等に分散されること

- 異なるしきい値をキューで設定して Weighted Random Early Detection（WRED; 重み付けランダム早期検出）を活用できるように、interactive トラフィックが他の CoS 値にマッピングされていること

5. ラインカードで重み付けランダム早期検出（WRED）がサポートされている場合は、次の作業を実行して輻輳回避を設定します。

a. **wrr-queue random-detect max-threshold** インターフェイス コンフィギュレーション コマンドを使用して、WRED をイネーブルにし、指定したキューに対するしきい値の下限と上限を指定します（デフォルトを推奨します）。

```
Router(config-if)# wrr-queue random-detect max-threshold queue
percent-of-queue-size
```

b. **wrr-queue cos map** インターフェイス コンフィギュレーション コマンドを使用して、CoS 値を廃棄しきい値にマッピングします。このしきい値を超過すると、特定の CoS 値を持つフレームが廃棄されます。

```
wrr-queue cos-map queue-id threshold-id cos-1 ... cos-n
```

次の例では、CoS 値 3 および 4 は、送信キュー 1/ しきい値 2 および送信キュー 2/ しきい値 1 にそれぞれ割り当てられます。

```
Router(config-if)# wrr-queue cos-map 1 1 3
Router(config-if)# wrr-queue cos-map 1 2 4
```

c. **wrr-queue bandwidth** インターフェイス コンフィギュレーション コマンドを使用して、帯域幅を標準送信キュー 1（低プライオリティ）と標準送信キュー 2（高プライオリティ）に割り振ります。

```
Router(config-if)# wrr-queue bandwidth weight1 weight2 weight3
```

Cisco GGSN

1. 各 GGSN の UMTS トラフィック クラスに対して出力キューイング方法を設定します。

各 GGSN の UMTS トラフィック クラスごとにキューイング方法を設定できます。

次の設定例では、UMTS トラフィック クラスとクラス マップが定義されていると想定しています。

```
Interface GigabitEthernet0/0
    Bandwidth <max-bandwidth>
       Service-policy output sami-output

Policy-map sami-output
    Class conversational
        Priority percent 5
    Class streaming
        Priority percent15
    Class interactive
        Bandwidth 20
    Class background
        Bandwidth 20
    Class signaling
        Bandwidth 15
```

UMTS QoS 設定の確認

UMTS QoS 設定を確認するには、Cisco SAMI で実行されているスーパーバイザ エンジンおよび GGSN インスタンスで **show running-config** コマンドを使用して、次の例の UMTS QoS パラメータを確認します。

スーパーバイザ エンジン設定

```
Mls qos

Mls qos map dscp-cos 18 20 22 to 5
Mls qos map dscp-cos 26 to 4
Mls qos map dscp-cos 28,30 to 3


Access-list 101 permit ip any any dscp ef
Access-list 102 permit ip any any dscp af21
Access-list 103 permit ip any any dscp af31
Access-list 103 permit ip any any dscp af32
Access-list 103 permit ip any any dscp af33
Access-list 104 permit ip any any

Class-map match-all conversational
    Match access-group 101
Class-map match-all streaming
    Match access-group 102
Class-map match-all interactive
    Match access-group 103
Class-map match-all background
    Match access-group 104


Mls qos aggregate-policer AGGREGATE-CONV <bit rate1> <normal-burst> <max-burst>
Conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-STREAMING <bit rate2> <normal-burst> <max-burst>
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-INTERACTIVE <bit rate3> <normal-burst> <max-burst>
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-BACKGROUND <bit rate4> <normal-burst> <max-burst>
conform-action transmit exceed-action drop

Policy-map Gi-incoming
    Class conversational
        Police aggregate AGGREGATE-CONV
    Class streaming
        Police aggregate AGGREGATE-STREAMING
    Class interactive
        Police aggregate AGGREGATE-INTERACTIVE
    Class background
        Police aggregate AGGREGATE-BACKGROUND


Interface FastEthernet2/1
    Description “Gi interface”
    Mls qos trust dscp
    Wrr-queue cos-map 1 1 3
         Wrr-queue cos-map 1 2 4
         Wrr-queue bandwidth 50 40 10
    Service-policy input Gi-incoming

Interface FastEthernet2/2
    Description “Gn interface”
```

```
    Mls qos trust dscp
```

GGSN 設定

```
Gprs qos map umts

Class-map match-all conversational
    Match ip dscp 46
Class-map match-any interactive
    Match ip dscp 26
    Match ip dscp 28
    Match ip dscp 30
Class-map match-any streaming
    Match ip dscp 18
    Match ip dscp 20
    Match ip dscp 22
Class-map match-all signaling
    Match ip dscp 40
Class-map match-any background
    Description default class
    Match ip dscp 0

Policy-map sami-output
    Class conversational
        Priority percent 5
    Class streaming
        Priority percent 15
    Class interactive
        Bandwidth 20
    Class background
        Bandwidth 20
    Class signaling
        Bandwidth 15

interface Gigabitthernet 0/0
        bandwidth 250000
        service-policy output max-output
```

GGSN デフォルト QoS を要求された QoS として設定

GGSN で UMTS QoS マッピングを使用しない場合は、応答メッセージ内の GGSN のデフォルト QoS 値が、PDP コンテキストの作成要求で要求されたとおりに設定されるように、GGSN を設定できます。このコマンドを使用すると、要求された QoS が GGSN により引き下げられることを防止できます。

要求された QoS がデフォルトの QoS として設定されるように GGSN 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)# **gprs qos default-response requested**	（任意）GGSN が、応答メッセージ内のそのデフォルト QoS 値を、PDP コンテキストの作成要求で要求されたとおりに設定することを指定します。

（注）　**gprs qos default-response requested** コマンドが設定されておらず、GPRS 標準 QoS がイネーブルでない場合、GGSN ではそのデフォルト QoS クラスが best effort に設定されます。

GGSN でのコール アドミッション制御の設定

GGSN の Call Admission Control（CAC; コール アドミッション制御）機能を使用すると、リアルタイムのデータ トラフィック（音声やビデオなど）で必要なネットワーク リソースを確実に使用できます。CAC は Access Point Name（APN; アクセス ポイント ネーム）で適用され、最大 QoS 認可と帯域幅管理という 2 つの機能で構成されています。

次の項では、GGSN でこれらの機能を設定する方法について説明します。

（注）　GGSN の CAC を使用するには、グローバル コンフィギュレーション モードで **gprs qos map umts** コマンドを使用して UMTS QoS がイネーブルにされており、かつトラフィック クラス基準とトラフィック ポリシーが作成されている必要があります。

最大 QoS 認可の設定

CAC 最大 QoS 認可機能を使用すると、PDP コンテキストの作成によって要求された QoS が、APN 内で設定された最大 QoS を超えないようにできます。*CAC 最大 QoS ポリシー*を使用すると、ポリシー内で特定の QoS パラメータを定義し、そのポリシーを APN に付加できます。CAC 最大 QoS ポリシーにより、PDP の作成プロセスおよび変更プロセス中に PDP によって要求される QoS が制限されます。

（注）　CAC 最大 QoS ポリシーは複数の APN に付加できます。

CAC 最大 QoS ポリシーでは次のパラメータを定義できます。

- **アクティブな PDP コンテキストの最大数**：APN に対してアクティブな PDP コンテキストの最大数。APN でアクティブな PDP の合計数が、このパラメータを使用してポリシー内に設定した数を超過すると、GGSN は PDP コンテキストを拒否します。任意で、このしきい値に達したあとに、割り当て/保持プライオリティが 1 に設定されている PDP コンテキストだけを受け入れるように CAC を設定できます。
- **最大ビット レート**：APN のアップリンク方向とダウンリンク方向の両方で、各トラフィック クラスに対して許可できる Maximum Bit Rate（MBR; 最大ビット レート）の最高値。ポリシーに MBR を設定すると、CAC で MBR が最大 GBR よりも大きい値になります。MBR を設定しない場合、CAC は PDP コンテキストによって要求される任意の MBR を受け入れます。
- **保証ビット レート**：APN のアップリンク方向とダウンリンク方向の両方で、リアルタイム トラフィック（conversational および streaming）に対して受け入れ可能な Guaranteed Bit Rate（GBR; 保証ビット レート）の最高値。ポリシーで GBR を設定しない場合、CAC は PDP コンテキストによって要求される任意の GBR を受け入れます。
- **最高トラフィック クラス**：APN で受け入れ可能な最高トラフィック クラス。要求されたトラフィック クラスが、ポリシーで指定した最高トラフィック クラスよりも高い場合、PDP コンテキストは拒否されます。このパラメータが設定されていない場合は、任意のトラフィック クラスが受け入れられます。

GGSN では、PDP コンテキストの作成中にトラフィック クラスをダウングレードしません。ただし、PDP コンテキストの作成後に APN で設定した最高トラフィック クラスが変更され、かつ、この新しい最高トラフィック クラスよりも大きい値の新しいトラフィック クラスの要求を GGSN が受信した（PDP コンテキストの更新要求で）場合、GGSN では PDP コンテキストの変更中にトラフィック クラスをダウングレードします。この場合、GGSN は要求を新規の最高トラフィック クラスまでダウングレードします。

- **最大トラフィック処理プライオリティ**：APN で受け入れ可能な interactive トラフィック クラスの最大トラフィック処理プライオリティを指定します。このパラメータが指定されていない場合は、すべてのトラフィック処理プライオリティが受け入れられます。
- **最大遅延クラス**：APN で受け入れ可能な R97/R98 QoS の最大遅延クラスを定義します。
- **最大ピーク スループット クラス**：APN で受け入れ可能な R97/R98 QoS の最大ピーク スループット クラスを定義します。

CAC 最大 QoS ポリシーの設定

CAC 最大 QoS ポリシーを設定するには、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
ステップ 1	`Router(config)# gprs qos cac-policy` *policy-name*	CAC 最大 QoS ポリシーを作成または変更します。
ステップ 2	`Router(config-umts-cac-policy)# maximum pdp-context` *number* [**threshold** *number2*]	特定の APN に対して作成可能な PDP コンテキストの最大数を指定します。任意で、2 番めのしきい値を設定し、このしきい値に到達したあと、割り当て/保持プライオリティが 1 である PDP コンテキストだけを受け入れるように設定できます。
ステップ 3	`Router(config-umts-cac-policy)# maximum traffic-class` *traffic-class-name* [**priority** *value*]	APN で受け入れ可能な最高トラフィック クラスを指定します。有効な値は、conversational、streaming、interactive、または background です。 任意で、interactive トラフィック クラスの最高トラフィック処理プライオリティを指定できます。
ステップ 4	`Router(config-umts-cac-policy)# maximum peak-throughput` *value* [**reject**]	APN で受け入れ可能な R97/R98 QoS の最大ピーク スループットを定義します。有効な値は 1 ～ 9 です。 デフォルトでは、ピーク スループットが設定値よりも高い PDP コンテキストは、設定値までダウングレードされます。代わりに、任意で、**reject** キーワードを指定して、このような PDP コンテキストが拒否されるようにできます。
ステップ 5	`Router(config-umts-cac-policy)# maximum delay-class` *value* [**reject**]	APN で受け入れ可能な R97/R98 QoS の最大遅延クラスを指定します。 デフォルトでは、最大遅延クラスが設定値よりも高い PDP コンテキストは、設定値までダウングレードされます。代わりに、任意で、**reject** キーワードを指定して、このような PDP コンテキストが拒否されるようにできます。

	コマンド	目的
ステップ 6	`Router(config-umts-cac-policy)# mbr traffic-class` *traffic-class-name bitrate* {**uplink** | **downlink**} [**reject**]	両方向（アップリンクとダウンリンク）で、各トラフィック クラスに対して許可できる Maximum Bit Rate（MBR; 最大ビット レート）の最高値を指定します。有効な値は 1 ～ 256000 です。 任意で、**reject** キーワード オプションを使用して、MBR が設定値を超過したときに PDP コンテキストの作成要求が拒否されるように指定できます。
ステップ 7	`Router(config-umts-cac-policy)# gbr traffic-class` *traffic-class-name bitrate* {**uplink** | **downlink**} [**reject**]	APN でリアルタイム クラス（conversational および streaming）に対して、アップリンク方向とダウンリンク方向で許可できる保証ビット レート（GBR）の最高値を指定します。有効な値は 1 ～ 256000 です。 任意で、**reject** キーワード オプションを使用して、GBR が設定値を超過したときに PDP コンテキストの作成要求が拒否されるように指定できます。

CAC 最大 QoS ポリシー機能のイネーブルおよび APN へのポリシーの付加

CAC 最大 QoS ポリシー機能をイネーブルにし、ポリシーを APN に付加するには、アクセス ポイント 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-access-point)# cac-policy`	CAC 機能の最大 QoS ポリシー機能をイネーブルにし、ポリシーを APN に適用します。

帯域幅管理の設定

CAC 帯域幅管理機能を使用すると、PDP コンテキストのアクティベーションや変更プロセス中に、リアルタイム PDP コンテキストに十分な帯域幅を確保できます。

CAC 機能では、帯域幅をネゴシエーションおよび確保するために、ユーザ定義の帯域幅プールを使用します。これらのプールについて、各プールに割り当てる総帯域幅を定義し、次に、その帯域幅のパーセンテージを各トラフィック クラスに割り当てます。

次の例では、作成する帯域幅プール（プール A）に 100000 kbps を割り当てます。また、帯域幅 100000 kbps のパーセンテージを各トラフィック クラスに割り当てて、トラフィック クラスベースの帯域幅プールを 4 つ作成します。

```
gprs bandwidth-pool A
  bandwidth 100000
  traffic-class conversational percent 40
  traffic-class streaming percent 30
  traffic-class interactive percent 20
  traffic-class background percent 10
```

CAC 帯域幅プールの設定

（注）　CAC 帯域幅プールは、帯域幅をネゴシエーションおよび確保するために CAC によって使用されます。ただし、確保した帯域幅を保証するために、キューイングとスケジューリングを定義する Cisco IOS QoS サービス ポリシーを作成し、物理インターフェイスに付加する必要があります。

CAC 帯域幅プールを設定するには、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
ステップ 1	`Router(config)# gprs qos bandwidth-pool pool-name`	CAC 帯域幅プールを作成または変更します。
ステップ 2	`Router(config-gprs-bw-pool)# bandwidth value`	帯域幅プールの総帯域幅をキロビット/秒単位で指定します。有効な値は 1 ～ 4294967295 の数値です。
ステップ 3	`Router(config-gprs-bw-pool)# traffic-class traffic-class [percent] value`	帯域幅プールの帯域幅を特定のトラフィック クラスに割り当てます。この割り当ては、パーセンテージ（オプションの **percent** キーワードとともに使用する場合は 1 ～ 100%）、またはキロビット/秒単位の絶対値（0 ～ 4292967295）で指定します。すべてのトラフィック クラスで同じ単位（パーセンテージまたは絶対値）を使用する必要があります。

CAC 帯域幅管理機能のイネーブルおよび APN への帯域幅プールの適用

CAC 帯域幅管理機能をイネーブルにし、帯域幅プールを APN に適用するには、アクセス ポイント 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-access-point)# bandwidth pool {input | output} pool-name`	CAC 帯域幅管理機能をイネーブルにし、帯域幅プールを、APN のダウンリンク方向の入力（Gn）インターフェイス（**input** キーワード）、またはアップリンク方向の出力（Gi）インターフェイス（**output** キーワード）に適用します。

（注）　CAC 帯域幅プールは複数の APN に適用できます。

Per-PDP ポリシングの設定

Per-PDP ポリシング（セッションベースのポリシング）は、GGSN Traffic Conditioner（3G TS 23.107）の機能です。この機能を使用すると、特定の PDP コンテキストについて Gi インターフェイスで受信するトラフィックの最大レートを制限できます。

このポリシング機能により、PDP コンテキストに対して CAC ネゴシエーション データ レートが適用されます。輻輳が発生した場合に、不適合トラフィックを廃棄するか、または不適合トラフィックを優先廃棄としてマーキングするように GGSN を設定できます。

使用するポリシング パラメータは、PDP コンテキストによって異なります。詳細は次のとおりです。

- R99 QoS プロファイルを持つ GTPv1 PDP の場合、CAC ネゴシエーション QoS プロファイルの MBR パラメータと GBR パラメータが使用されます。非リアルタイム トラフィックの場合、MBR パラメータだけが使用されます。
- R98 QoS プロファイルを持つ GTPv1 PDP および GTPv0 PDP の場合、CAC ネゴシエーション QoS ポリシーのピーク スループット パラメータが使用されます。

制約事項

Per-PDP ポリシングを設定する場合は、次の点に注意してください。

- Per-PDP ポリシングは、IPv4 PDP コンテキストでだけサポートされています。
- GGSN で UMTS QoS マッピングがイネーブルである必要があります。
- Gi インターフェイスで Cisco Express Forwarding（CEF）がイネーブルである必要があります。
- Per-PDP ポリシングは、Gi インターフェイスのダウンリンク トラフィックでだけサポートされています。
- PDP コンテキストの初期パケットはポリシングされません。
- 階層ポリシングはサポートされていません。
- APN に付加されたポリシー マップでフローベースのポリシングが設定されている場合、**show policy-map apn** コマンドによって、ポリシング前に受信したパケットの総数が表示されますが、ポリシング カウンタは表示されません。
- APN に適用されるサービス ポリシーは変更できません。サービス ポリシーを変更するには、APN からサービス ポリシーを削除し、変更を加えてから再適用します。
- それぞれ **match flow pdp** が設定されており、異なる DiffServ コード ポイント（DSCP）を持つ複数のクラス マップは、この DSCP が信頼されている場合にだけ、ポリシー マップでサポートされます（GGSN で **gprs umts-qos dscp unmodified** グローバル コンフィギュレーション コマンドが設定されていません）。

Per-PDP ポリシング設定の作業リスト

GGSN で Per-PDP ポリシングを設定するには、次の作業を実行します。

- 「PDP フローを一致基準として設定したクラス マップの作成」（P.10-17）
- 「ポリシー マップの作成およびトラフィック ポリシングの設定」（P.10-17）
- 「APN へのポリシーの付加」（P.10-18）
- 「APN ポリシング統計情報のリセット」（P.10-19）

PDP フローを一致基準として設定したクラス マップの作成

クラス一致を作成し、PDP フローを一致基準として指定するには、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
ステップ 1	`Router(config)# class-map class-map-name`	一致するパケットに使用するクラス マップを作成します。
ステップ 2	`Router(config-cmap)# match flow pdp`	クラス マップで PDP フローを一致基準として指定します。
ステップ 3	`Router(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了します。

（注）　PDP フォロー分類のクラスを定義するときは、**match-any** オプションを指定しないでください。デフォルトは **match-all** です。

（注）　クラス マップで追加の一致基準を設定することもできます。DSCP および優先順位ベースの分類がサポートされています。

ポリシー マップの作成およびトラフィック ポリシングの設定

ポリシー マップを作成し、クラス マップを割り当てるには、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
ステップ 1	`Router(config)# policy map policy-map-name`	1 つ以上の APN に付加してサービス ポリシーを指定できるポリシー マップを作成または変更します。
ステップ 2	`Router(config-pmap)# class class-map-name`	作成または変更するポリシーを持つクラスの名前を指定します。

	コマンド	目的
ステップ 3	`Router(config-pmap)# police rate pdp [burst bytes] [peak-rate pdp [peak-burst bytes]] conform-action action exceed-action action [violate-action action]`	トラフィック ポリシングを設定し、不適合パケットに対する処理を設定します。 レート パラメータとピーク レート パラメータは個別のフローから取得されます。 （注）　**police** コマンドを設定するときは、バースト サイズを指定できますが、推奨しません。バースト値の設定が誤っている場合は、誤った動作が実行されます。 *action* 変数に使用できる値は、次のとおりです。 • **drop**：パケットを廃棄します。 • **set-dscp-transmit**：IP DiffServ コード ポイント（DSCP）値を設定し、新規の IP DSCP 値設定を持つパケットを送信します。 • **set-prec-transmit**：IP precedence を設定し、新規の IP precedence 値設定を持つパケットを送信します。 • **transmit**：パケットを送信します。パケットは変更されません。
ステップ 4	`Router(config-pmap)# exit`	ポリシー マップ コンフィギュレーション モードを終了します。

APN へのポリシーの付加

ポリシー マップを APN に付加するには、アクセス ポイント 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
ステップ 1	`Router(config-)# access-point index`	アクセス ポイント番号を指定し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-access-point)# service-policy input policy-map-name`	サービス ポリシーを APN に付加し、この APN の PDP フローに対するダウンリンク方向のサービス ポリシーとして使用します。
ステップ 3	`Router(config-access-point)# exit`	アクセス ポイント コンフィギュレーション モードを終了します。

APN ポリシング統計情報のリセット

show policy-map apn コマンドによって表示されるポリシング カウンタをリセットするには、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)# **clear gprs access-point statistics** *access-point-index*	特定のアクセス ポイントの統計情報カウンタをクリアします。

GGSN での QoS のモニタリングおよびメンテナンス

ここでは、GGSN で QoS の設定パラメータとステータスを表示するコマンドについて説明します。内容は次のとおりです。

- 「show コマンドの要約」（P.10-19）
- 「UMTS QoS のモニタリング」（P.10-20）

show コマンドの要約

ここでは、GGSN で GPRS および UMTS QoS をモニタリングするために使用できる **show** コマンドの要約を示します。すべてのコマンドで、GGSN のすべてのタイプの QoS 方式に関する情報が提供されるわけではありません。

次の特権 EXEC コマンドを使用して GGSN で QoS のモニタリングおよびメンテナンスを行います。

コマンド	目的
Router# **show gprs bandwidth-pool status** *pool-name*	設定した CAC 帯域幅プールとそのステータスのリストを表示します。
Router# **show gprs gtp pdp-context imsi** *hex-data*	International Mobile Subscriber Identity（IMSI）に基づいて PDP コンテキストを表示します。
Router# **show gprs gtp pdp-context tid** *hex-data*	トンネル ID に基づいて PDP コンテキストを表示します。
Router# **show gprs gtp pdp-context qos-umts-class** {**conversational** | **streaming** | **interactive** | **background**}	UMTS QoS トラフィック クラスに基づいて PDP コンテキストを表示します。UMTS QoS にだけ適用されます。
Router# **show gprs qos status**	GGSN の QoS 統計情報を表示します。
Router# **show gprs umts-qos map traffic-class**	UMTS QoS マッピング情報を表示します。
Router# **show gprs umts-qos police pdp tid** *tid*	PDP コンテキストのポリシング統計情報を表示します。
Router# **show gprs umts-qos profile pdp tid** *tid*	PDP コンテキストに対して要求およびネゴシエーションされた QoS 情報を表示します。

UMTS QoS のモニタリング

ここでは、GGSN で UMTS QoS の設定パラメータとステータスを表示するコマンドについて説明します。

内容は次のとおりです。

GGSN での UMTS QoS ステータスの表示

show gprs qos status コマンドを使用して、UMTS トラフィック クラスごとに現在アクティブな PDP コンテキストの数を表示できます。

次の例は、UMTS QoS conversational トラフィック クラスを使用している GGSN でアクティブな PDP コンテキスト 100 個、UMTS QoS streaming トラフィック クラスを持つアクティブな PDP コンテキスト 140 個、UMTS interactive トラフィック クラスを持つアクティブな PDP コンテキスト 1345 個、および UMTS QoS background トラフィック クラスを持つアクティブな PDP コンテキスト 2000 個を示しています。

次の例は、UMTS QoS の **show gprs qos status** コマンドの出力を示しています。

```
Router# show gprs qos status
GPRS QoS Status:
  type:UMTS
  conversational_pdp      100   streaming_pdp     150
  interactive_pdp         1345  background_pdp    2000
```

PDP コンテキストの UMTS QoS 情報の表示

特定の PDP コンテキストの UMTS QoS 情報を表示するには、**show gprs gtp pdp-context** コマンドを **tid** キーワードまたは **imsi** キーワードとともに使用します。次の例は、XX UMTS QoS トラフィック クラスでの PDP コンテキストに対する **show gprs gtp pdp-context tid** コマンドのサンプル出力を示しています。QoS 情報を表示している出力フィールドは太字で示されています。

```
Router# show gprs gtp pdp-context tid 111111111111111
TID              MS Addr         Source  SGSN Addr       APN
1111111111111111 10.0.0.1        Static  10.39.39.1      www.corporate.com

current time :Nov 12 2002 08:10:23
    user_name (IMSI):213000000000000    MS address:2.0.0.1
    MS International PSTN/ISDN Number (MSISDN):987
    sgsn_addr_signal:15.15.0.2          sgsn_addr_data:  15.15.0.3
    control teid local: 0x6309ABF4
    control teid remote:0x00000021
    data teid local:    0x6308AA38
    data teid remote:   0x00000022
    primary pdp:Y           nsapi:1
    signal_sequence: 1                  seq_tpdu_up:     0
    seq_tpdu_down:   0
    upstream_signal_flow:  0            upstream_data_flow:  0
    downstream_signal_flow:0            downstream_data_flow:0
    RAupdate_flow:         0
    pdp_create_time:  Nov 12 2002 08:10:09
    last_access_time: Nov 12 2002 08:10:09
    mnrgflag:         0                 tos mask map:68
    gtp pdp idle time:72
```

```
umts qos_req:091101690101011105010l
umts qos_neg:091101690101011105010l
QoS class:interactive
QoS for charging:       qos_req:000000      qos_neg:000000
rcv_pkt_count:    0             rcv_byte_count:  0
send_pkt_count:   0             send_byte_count: 0
cef_up_pkt:       0             cef_up_byte:     0
cef_down_pkt:     0             cef_down_byte:   0
cef_drop:         0
charging_id:        223415403
pdp reference count:2
primary dns:        0.0.0.0
secondary dns:      0.0.0.0
primary nbns:       0.0.0.0
secondary nbns:     0.0.0.0
ntwk_init_pdp:      0
```

設定例

ここには次の例があります。

- 「UMTS QoS の設定例」（P.10-21）
- 「CAC の設定例」（P.10-23）
- 「Per-PDP ポリシングの設定例」（P.10-24）

UMTS QoS の設定例

スーパーバイザ エンジン設定

```
Mls qos

Mls qos map dscp-cos 18 20 22 to 5
Mls qos map dscp-cos 26 to 4
Mls qos map dscp-cos 28,30 to 3


Access-list 101 permit ip any any dscp ef
Access-list 102 permit ip any any dscp af21
Access-list 103 permit ip any any dscp af31
Access-list 103 permit ip any any dscp af32
Access-list 103 permit ip any any dscp af33
Access-list 104 permit ip any any

Class-map match-all conversational
    Match access-group 101
Class-map match-all streaming
    Match access-group 102
Class-map match-all interactive
    Match access-group 103
Class-map match-all background
    Match access-group 104


Mls qos aggregate-policer AGGREGATE-CONV <bit rate1> <normal-burst> <max-burst>
Conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-STREAMING <bit rate2> <normal-burst> <max-burst>
conform-action transmit exceed-action drop
```

```
Mls qos aggregate-policer AGGREGATE-INTERACTIVE <bit rate3> <normal-burst> <max-burst>
conform-action transmit exceed-action drop
Mls qos aggregate-policer AGGREGATE-BACKGROUND <bit rate4> <normal-burst> <max-burst>
conform-action transmit exceed-action drop

Policy-map Gi-incoming
    Class conversational
        Police aggregate AGGREGATE-CONV
    Class streaming
        Police aggregate AGGREGATE-STREAMING
    Class interactive
        Police aggregate AGGREGATE-INTERACTIVE
    Class background
        Police aggregate AGGREGATE-BACKGROUND


Interface FastEthernet2/1
    Description "Gi interface"
    Mls qos trust dscp
    Wrr-queue cos-map 1 1 3
         Wrr-queue cos-map 1 2 4
         Wrr-queue bandwidth 50 40 10
    Service-policy input Gi-incoming

Interface FastEthernet2/2
    Description "Gn interface"
    Mls qos trust dscp
```

GGSN 設定

```
Gprs qos map umts

Class-map match-all conversational
    Match ip dscp 46
Class-map match-any interactive
    Match ip dscp 26
    Match ip dscp 28
    Match ip dscp 30
Class-map match-any streaming
    Match ip dscp 18
    Match ip dscp 20
    Match ip dscp 22
Class-map match-all signaling
    Match ip dscp 40
Class-map match-any background
    Description default class
    Match ip dscp 0

Policy-map sami-output
    Class conversational
        Priority percent 5
    Class streaming
        Priority percent 15
    Class interactive
        Bandwidth 20
    Class background
        Bandwidth 20
    Class signaling
        Bandwidth 15
```

```
interface Gigabitthernet 0/0
        bandwidth 250000
        service-policy output max-output
```

CAC の設定例

次に、Cisco 7600 シリーズ ルータの Cicso SAMI で実行されている GGSN に実装された CAC および QoS の設定例を示します。

```
!Enable UMTS QoS Mapping

gprs qos map umts

!Create CAC Maximum QoS authorization policy
gprs qos cac-policy abc_qos_policy1
  maximum pdp-context 1200 threshold 1000
  maximum traffic-class conversational
  mbr traffic-class conversational 100 uplink
  mbr traffic-class conversational 100 downlink
  mbr traffic-class streaming 100 uplink
  mbr traffic-class streaming 100 downlink
  mbr traffic-class interactive 120 uplink
  mbr traffic-class interactive 120 downlink
  mbr traffic-class background 120 uplink
  mbr traffic-class background 120 downlink
  gbr traffic-class conversational 64 uplink
  gbr traffic-class conversational 80 uplink
  gbr traffic-class streaming 80 downlink
  gbr traffic-class streaming 80 downlink

gprs qos cac-policy max_qos_policy2
  maximum pdp-context 1500
  maximum traffic-class interactive priority 1
  mbr traffic-class interactive 200
  mbr traffic-class background 150

! Create class-map to classify UMTS traffic class

class-map match-any conversational
  match ip dscp ef

class-map match-any streaming
  match ip dscp af21
  match ip dscp af22
  match ip dscp af23

class-map match-any interactive
  match ip dscp af31
  match ip dscp af32
  match ip dscp af33

class-map match-any background
  match ip dscp default

!Create traffic policy

policy-map ggsn1_traffic_policy
  class conversational
  priority percent 25

class streaming
```

```
  bandwidth percent 20

class interactive
  bandwidth percent 20
  random-detect dscp-based

 class background
  bandwidth percent 10
  random-detect dscp-based

! Create bandwidth pool

gprs qos bandwidth-pool ggsn1_bw_pool
  bandwidth 500000

  traffic-class streaming percent 20
  traffic-class interactive percent 20
  traffic-class background percent 10

! Set interface bandwidth

int gigabitEthernet 0/0
  bandwidth  500000
  service-policy output ggsn1_traffic_policy

!Attach bandwidth pool to the APN

gprs access-point-list gprs
 access-point 1
  access-point-name abc.com
  cac-policy abc_qos_policy1
  bandwidth-pool output ggsn1_bw_pool
  bandwidth-pool input ggsn1_bw_pool

 access-point 2
  access-point-name xyz.com
  cac-policy xyz_qos_policy1
  bandwidth-pool output ggsn1_bw_pool
  bandwidth-pool input ggsn1_bw_pool
```

Per-PDP ポリシングの設定例

次に、Per-PDP ポリシングの設定例を示します。

```
! Create a class for PDP flows
class-map class-pdp
  Match flow pdp

! Create a policy map and assign a class to the map
policy-map policy-gprs
  class class-pdp

! Configure traffic policing
  police rate pdp conform-action action exceed-action action violate-action action

! Attach a service policy to an APN
gprs access-point-list gprs
 access-point 1
  service-policy in policy-gprs
```

CHAPTER 11

GGSN でのセキュリティの設定

この章では、Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）でのセキュリティ機能の設定方法について説明します。Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）および Remote Authentication Dial-In User Service（RADIUS）についても説明します。

（注） Cisco 7600 シリーズ ルータ プラットフォーム上の IP Security（IPSec）は、IPSec Virtual Private Network（VPN; バーチャル プライベート ネットワーク）アクセラレーション サービス モジュール上で実行されます。Cisco Service and Application Module for IP（SAMI）上で稼動する GGSN での設定は必要ありません。

Cisco 7600 シリーズ ルータ プラットフォームでの IPSec の設定の詳細については、『*IPSEC VPN Acceleration Services Module Installation and Configuration Note*』を参照してください。

このマニュアルのセキュリティ設定手順および例（GGSN 固有の実装に関するものを除く）では、セキュリティ サービスを実装するために使用できる基本的なコマンドについて説明します。

Cisco IOS ソフトウェアでの AAA、RADIUS、および IPSec セキュリティ サービスの詳細については、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。Cisco 7600 プラットフォームでの IPSec セキュリティ サービスの詳細については、『*IPSec VPN Acceleration Services Module Installation and Configuration Note*』を参照してください。

この章に記載されている GGSN コマンドの詳細については、使用している Cisco GGSN リリースの『*Cisco GGSN Command Reference*』を参照してください。この章に記載されているその他のコマンドのマニュアルを参照するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

この章は、次の内容で構成されています。

- Cisco GGSN での合法的傍受サポートの実装（任意）
- 「設定例」（P.11-46）

GGSN でのセキュリティ サポートの概要

GGSN は、ルータ上で Cisco IOS ソフトウェアを介して使用できる同一レベルのセキュリティの多くをサポートしています。次のタイプのセキュリティがあります。

- 認証、認可、アカウンティング（AAA）ネットワーク セキュリティ サービスおよびサーバ グループ
- RADIUS セキュリティ サービス
- IP セキュリティ プロトコル（IPSec）

また、GGSN ソフトウェアでは、次のような追加セキュリティ機能を設定できます。

- アドレス確認
- トラフィック リダイレクション
- IP アクセス リスト

AAA および RADIUS サポートにより、GGSN およびその Access Point Name（APN; アクセス ポイント ネーム）へのモバイル ユーザによるアクセスを認証および認可するセキュリティ サービスが提供されます。IPSec サポートでは、GGSN とその関連ピア間のデータを保護できます。

AAA や IPSec サポートなどの場合は、GGSN コマンドを追加設定しなくても、GGSN は標準の Cisco IOS ソフトウェア設定によって動作します。

RADIUS サーバ設定の場合、GGSN では、ルータ上で AAA セキュリティをイネーブルにし、RADIUS サーバ通信をグローバルに確立する必要があります。そこから、新しい GGSN コンフィギュレーション コマンドを使用して、すべての GGSN アクセス ポイントに対して、またはアクセス ポイントごとに、RADIUS セキュリティを設定できます。

（注）　AAA、RADIUS、および IPSec セキュリティ サービス以外に、GGSN は APN へのアクセスをさらに制御するために、IP アクセス リストもサポートします。Cisco IOS GGSN ソフトウェアは、APN で IP アクセス リスト ルールを適用する新しい **ip-access-group** アクセス ポイント コンフィギュレーション コマンドを実装しています。

AAA サーバ グループ サポート

Cisco GGSN は、AAA サーバ グループを使用して APN での認証およびアカウンティングをサポートします。AAA サーバ グループを使用することには、次のような利点があります。

- さまざまな APN で、認証およびアカウンティング用のサーバ グループを選択的に実装できます。
- 同じ APN で、認証サービス用およびアカウンティング サービス用の異なるサーバ グループを設定できます。
- 特定の APN でイネーブルにする RADIUS サービス（AAA アカウンティングなど）を制御できます。

GGSN での GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）-Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）終端および GTP-PPP 再生成の場合、PPP が適切な AAA 機能を実行できるように透過的アクセス モードが使用されます。ただし、AAA サーバ グループを設定して、AAA サポート用の対応するサーバ グループを指定することもできます。

GGSN は、グローバル コンフィギュレーション レベルとアクセス ポイント コンフィギュレーション レベルの両方で AAA サーバ グループの実装をサポートします。グローバル コンフィギュレーション レベルで、ほとんどの APN にわたってサポートする設定を指定することによって、設定を最小限にすることができます。その後、アクセス ポイント コンフィギュレーション レベルで、特定の APN でサポートするサービスおよびサーバ グループを選択的に変更できます。したがって、AAA サーバのグローバル設定は APN コンフィギュレーション レベルで上書きできます。

GGSN のすべての APN に対して使用するデフォルトの AAA サーバ グループを設定するには、グローバル コンフィギュレーション モードで **gprs default aaa-group** コマンドを使用します。認証およびアカウンティング用に特定の APN で使用する異なる AAA サーバ グループを指定するには、**aaa-group** アクセス ポイント コンフィギュレーション コマンドを使用します。

APN で認証がイネーブルの場合、GGSN は最初に APN で認証サーバ グループを検索します。APN で認証サーバ グループが見つからない場合、GGSN はグローバルに設定された General Packet Radio Service（GPRS; グローバル パケット ラジオ サービス）/Universal Mobile Telecommunication System（UMTS）デフォルト認証サーバ グループを検索します。

APN でアカウンティングがイネーブルの場合、GGSN は次の順序で APN で、またはグローバルにアカウンティング サーバ グループを検索します。

- 最初に、APN でアカウンティング サーバ グループ（**aaa-group accounting** コマンドで設定）を検索します。
- 次に、グローバルな GPRS/UMTS デフォルト アカウンティング サーバ グループ（**gprs default aaa-group accounting** コマンドで設定）を検索します。
- 3 番めに、APN で認証サーバ グループ（**aaa-group authentication** コマンドで設定）を検索します。
- 最後に、グローバルな GPRS/UMTS デフォルト認証サーバ グループ（**gprs default aaa-group authentication** コマンドで設定）を検索します。

設定を完了するには、GGSN で次の設定要素も指定する必要があります。

- **radius-server host** コマンドを使用して、RADIUS サーバを設定します。
- グローバル コンフィギュレーション モードで **aaa group server** コマンドを使用し、グループ内の AAA サーバの IP アドレスを使用してサーバ グループを定義します。
- APN でサポートする AAA サービスのタイプ（アカウンティングおよび認証）をイネーブルにします。
  - GGSN は、非透過的 APN に対してデフォルトでアカウンティングをイネーブルにします。

    aaa-accounting disable コマンドを使用して、APN でアカウンティング サービスをディセーブルにすることができます。
  - **access-mode non-transparent** コマンドを設定して、APN レベルで認証をイネーブルにすることができます。認証をイネーブルにすると、GGSN は APN でアカウンティングを自動的にイネーブルにします。認証をイネーブルまたはディセーブルにするグローバル コンフィギュレーション コマンドはありません。
- グローバル コンフィギュレーション モードで **aaa accounting** および **aaa authentication** コマンドを使用して、AAA アカウンティングおよび認証を設定します。

（注）　AAA および RADIUS のグローバル コンフィギュレーション コマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

AAA セキュリティのグローバルな設定

認証、認可、アカウンティング（AAA）ネットワーク セキュリティ サービスは、GGSN 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。ここでは、シスコ ルータで AAA セキュリティを実装するために使用される基本的なコマンドについて説明します。

AAA をイネーブルにし、認証および認可を設定するには、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
ステップ 1	`Router(config)# aaa new-model`	AAA をグローバルにイネーブルにします。
ステップ 2	`Router(config)# aaa authentication ppp {default | list-name} method1 [method2...]`	ローカル認証方式リストを作成します。次のオプションがあります。 • **default**：ユーザがルータにログインしたときに、この引数のあとの認証方式が認証方式のデフォルト リストであることを指定します。 • *method*：PPP の有効な AAA 認証方式を指定します。たとえば、**group**（RADIUS）はグローバル RADIUS 認証をイネーブルにします。
ステップ 3	`Router(config)# aaa authorization {auth-proxy | network | exec | commands level | reverse-access} {default | list-name} [method1 [method2...]]`	特定の認可タイプの認可方式リストを作成し、認可をイネーブルにします。
ステップ 4	`Router(config)# aaa accounting {system default [vrf vrf-name] | network {default | none | start-stop | stop-only | wait-start} group group-name`	RADIUS を使用する場合、課金およびセキュリティのために、要求されたサービスの AAA アカウンティングをイネーブルにします。

AAA の設定の詳細については、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

RADIUS サーバ通信のグローバルな設定

ここでは、GGSN がユーザの認証および認可のために使用できるグローバルな RADIUS サーバ ホストの設定方法について説明します。GGSN グローバル コンフィギュレーション レベルで追加の RADIUS サーバ通信を設定できます。

RADIUS サーバ通信をルータでグローバルに設定するには、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
ステップ 1	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]`	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。次のオプションを使用できます。 • **auth-port**：認証要求の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）宛先ポートを指定します。 • **acct-port**：アカウンティング要求の UDP 宛先ポートを指定します。 • **timeout**：ルータが再送信の前に RADIUS サーバの応答を待機する間隔（範囲 1 ～ 1000 秒）を指定します。この設定によって、**radius-server timeout** コマンドのグローバル値が上書きされます。timeout 値を指定しない場合は、グローバル値が使用されます。 • **retransmit**：サーバが応答しないか応答が遅い場合に、RADIUS 要求がそのサーバに再送信される回数（範囲 1 ～ 100）を指定します。この設定によって、**radius-server retransmit** コマンドのグローバル値が上書きされます。 • **key**：ルータとこの RADIUS サーバ上で稼動する RADIUS デーモン間で使用される認証および暗号キーを指定します。この設定によって、**radius-server key** コマンドのグローバル値が上書きされます。
ステップ 2	`Router(config)# radius-server key string`	ルータとベンダー独自の RADIUS サーバ間で使用される共有秘密文字列を指定します。ルータおよび RADIUS サーバは、この文字列を使用してパスワードを暗号化し、応答を交換します。

RADIUS セキュリティの設定の詳細については、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。例については、「RADIUS サーバのグローバル設定例」（P.11-47）を参照してください。

（注）　**radius-server host** コマンドは複数回設定できますが、Cisco IOS ソフトウェアでは、同じ IP アドレスでサポートされる RADIUS サーバは 1 つだけです。

GGSN コンフィギュレーション レベルでの RADIUS サーバ通信の設定

GGSN のセキュリティ設定を完了するには、各アクセス ポイントに対して非透過的アクセスを設定する必要があります。GGSN グローバル コンフィギュレーション レベルでセキュリティを設定すると、すべてのアクセス ポイントまたは特定のアクセス ポイントに対して RADIUS サーバ通信を設定することもできます。

GGSN グローバル コンフィギュレーション レベルで RADIUS を設定するには、次の作業を実行します。

- 「非透過的アクセス モードの設定」（P.11-6）（必須）
- 「すべてのアクセス ポイントの AAA サーバ グループの指定」（P.11-7）（任意）
- 「特定のアクセス ポイントの AAA サーバ グループの指定」（P.11-7）（任意）
- 「アクセス ポイントでの AAA アカウンティング サービスの設定」（P.11-8）（任意）

非透過的アクセス モードの設定

GGSN で RADIUS 認証をサポートするには、非透過的アクセス用の GGSN アクセス ポイントを設定する必要があります。RADIUS サービスをサポートするすべてのアクセス ポイントに対して、非透過的アクセスを設定する必要があります。アクセス モードをグローバルに指定する方法はありません。

（注）　GGSN での GTP-PPP 終端および GTP-PPP 再生成の場合、PPP が適切な AAA 機能を実行できるように透過的アクセス モードが使用されます。ただし、AAA サーバ グループを設定して、AAA サポート用の対応するサーバ グループを指定することもできます。

GGSN アクセス ポイントの非透過的アクセスを設定するには、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
ステップ 1	`Router(config)# gprs access-point-list list-name`	アクセス ポイント リスト名を指定し、アクセス ポイント リスト コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-ap-list)# access-point access-point-index`	既存のアクセス ポイント定義に関連付けられた番号を指定し（または、新しいアクセス ポイントを作成し）、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-access-point)# access-mode non-transparent`	Public Data Network（PDN; 公衆データ網）へのアクセス ポイントで GGSN がユーザ認証を要求することを指定します。

GGSN アクセス ポイントの設定の詳細については、「GGSN でのアクセス ポイントの設定」（P.8-7）を参照してください。

すべてのアクセス ポイントの AAA サーバ グループの指定

RADIUS サーバ通信をグローバル レベルで設定したあと、すべての GGSN アクセス ポイントが使用するデフォルトの AAA サーバ グループを設定できます。

すべての GGSN アクセス ポイントのデフォルト AAA サーバ グループを指定するには、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)# gprs default aaa-group {authentication | accounting} server-group`	デフォルト AAA サーバ グループを指定し、GGSN のすべてのアクセス ポイントに対してサーバ グループによってサポートされる AAA サービスのタイプを割り当てます。各項目の意味は次のとおりです。 • **authentication**：選択したサーバ グループを、すべての APN での認証サービス用に割り当てます。 • **accounting**：選択したサーバ グループを、すべての APN でのアカウンティング サービス用に割り当てます。 • *server-group*：すべての APN で AAA サービスに使用する AAA サーバ グループの名前を指定します。 **（注）** 指定する AAA サーバ グループの名前は、**aaa group server** コマンドを使用して設定するサーバ グループに対応している必要があります。

特定のアクセス ポイントの AAA サーバ グループの指定

すべてのアクセス ポイントに対して設定されたデフォルト AAA サーバ グループを上書きするには、特定のアクセス ポイントに対して異なる AAA サーバ グループを指定します。または、デフォルト AAA サーバ グループを設定しない場合は、各アクセス ポイントで AAA サーバ グループを指定できます。

特定のアクセス ポイントの AAA サーバ グループを指定するには、アクセス ポイント 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-access-point)# aaa-group {authentication | accounting} server-group`	デフォルト AAA サーバ グループを指定し、GGSN の特定のアクセス ポイントに対してサーバ グループによってサポートされる AAA サービスのタイプを割り当てます。各項目の意味は次のとおりです。 • **authentication**：選択したサーバ グループを APN での認証サービスに割り当てます。 • **accounting**：選択したサーバ グループを APN でのアカウンティング サービスに割り当てます。 • *server-group*：APN で AAA サービスに使用する AAA サーバ グループの名前を指定します。 **（注）** 指定する AAA サーバ グループの名前は、**aaa group server** コマンドを使用して設定するサーバ グループに対応している必要があります。

アクセス ポイントでの AAA アカウンティング サービスの設定

Cisco GGSN には、透過的または非透過的アクセス ポイントのアカウンティング サービスをイネーブルまたはディセーブルにする、次のような異なるデフォルトがあります。

- **access-mode** コマンドを使用して非透過的アクセスの APN を設定する場合、GGSN は APN で認証を使用するアカウンティングを自動的にイネーブルにします。
- 透過的アクセス（デフォルトのアクセス モード）の APN を設定する場合、GGSN は APN でアカウンティングを自動的にディセーブルにします。

したがって、透過的アクセス APN を設定しており、その APN でアカウンティングを提供する場合は、APN で **aaa-accounting enable** コマンドを設定する必要があります。

ただし、アカウンティングを提供するには、GGSN で次のようなその他の設定要素を指定して、設定を完了する必要もあります。

- グローバル コンフィギュレーション モードで **aaa new-model** コマンドを使用して、AAA サービスをイネーブルにします。
- グローバル コンフィギュレーション モードで **aaa group server** コマンドを使用して、グループ内の RADIUS サーバの IP アドレスを使用してサーバ グループを定義します。
- 次の AAA サービスを設定します。
  - AAA 認証（グローバル コンフィギュレーション モードで **aaa authentication** コマンドを使用）
  - AAA 認可（グローバル コンフィギュレーション モードで **aaa authorization** コマンドを使用）
  - AAA アカウンティング（グローバル コンフィギュレーション モードで **aaa accounting** コマンドを使用）

- AAA サーバ グループで提供する必要があるサービスのタイプを割り当てます。サーバ グループでアカウンティング サービスだけをサポートする場合は、アカウンティングだけのためにサーバを設定する必要があります。**gprs default aaa-group** コマンドを使用して GGSN グローバル コンフィギュレーション レベルで、または **aaa-group** コマンドを使用して APN で、AAA サービスを AAA サーバ グループに割り当てることができます。
- **radius-server host** コマンドを使用して、RADIUS サーバを設定します。

（注）　AAA および RADIUS のグローバル コンフィギュレーション コマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

アカウンティングが不要な特定の APN で選択的にそのサービスをディセーブルにするには、**aaa-accounting disable** アクセス ポイント コンフィギュレーション コマンドを使用します。

このコマンドの **no** フォームはありません。

アクセス ポイントでのアカウンティング サービスのイネーブルおよびディセーブル

Cisco Systems GGSN には、透過的または非透過的アクセス ポイントのアカウンティング サービスをイネーブルまたはディセーブルにする、次のような異なるデフォルトがあります。

- **access-mode** コマンドを使用して非透過的アクセスの APN を設定する場合、GGSN は APN で認証を使用するアカウンティングを自動的にイネーブルにします。
- 透過的アクセス（デフォルトのアクセス モード）の APN を設定する場合、GGSN は APN でアカウンティングを自動的にディセーブルにします。

アカウンティングが不要な特定の APN で選択的にそのサービスをディセーブルにするには、**aaa-accounting disable** アクセス ポイント コンフィギュレーション コマンドを使用します。

アクセス ポイントでの中間アカウンティングの設定

aaa-accounting アクセス ポイント コンフィギュレーション コマンドを **interim** キーワード オプションを指定して使用すると、Interim-Update Accounting 要求を AAA サーバに送信するように GGSN を設定できます。

（注）　中間アカウンティングのサポートでは、APN に対してアカウンティング サービスがイネーブルであり、**aaa accounting update newinfo** グローバル コンフィギュレーション コマンドが設定されている必要があります。

アクセス ポイントでアカウンティング サービスを設定するには、アクセス ポイント 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-access-point)# aaa-accounting [enable | disable | interim {update | periodic minutes | periodic radius}]`	GGSN のアクセス ポイントでアカウンティング サービスを設定します。次のオプションがあります。 • **enable**：（任意）GGSN のアクセス ポイントでアカウンティング サービスをイネーブルにします。 • **disable**：（任意）GGSN のアクセス ポイントでアカウンティング サービスをディセーブルにします。 • **interim update**：（任意）ルーティング エリアの更新（Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）の変更となる）または QoS の変更が発生したときに、中間アカウンティング レコードをアカウンティング サーバに送信できます。 • **interim periodic** *minutes*：（任意）定期的な設定間隔で、中間定期アカウンティング レコードをアカウンティング サーバに送信できます。 • **interim periodic radius**：（任意）RADIUS によって送信された定期アカウンティング値（アトリビュート 85）を GGSN が受け入れることができます。

その他の RADIUS サービスの設定

ここでは、GGSN がユーザの認証および認可のために使用できる RADIUS セキュリティ サービスの設定方法について説明します。

ここでは、次の作業について説明します。

RADIUS サーバへのアクセス要求の RADIUS アトリビュートの設定

GGSN が RADIUS サーバへのアクセス要求で RADIUS アトリビュートを送信する方法を設定します。ここでは、次の作業について説明します。

チャレンジ ハンドシェーク認証プロトコル（CHAP）Challenge の設定

チャレンジ ハンドシェーク認証プロトコル（CHAP）Challenge を RADIUS サーバへのアクセス要求の Challenge Attribute フィールド（Authenticator フィールドではない）に常に含めることを指定するには、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)# gprs radius attribute chap-challenge`	CHAP Challenge が RADIUS 要求の Challenge Attribute に常に含まれることを指定します。

（注）　**gprs radius attribute chap-challenge** コマンドが設定されている場合、CHAP Challenge は RADIUS サーバへのアクセス要求の Challenge Attribute フィールドで常に送信されます。Authenticator フィールドではありません。このコマンドが設定されていない場合、CHAP Challenge は 16 バイトを超えないかぎり Authenticator フィールドで送信されます。超える場合は、アクセス要求の Challenge Attribute フィールドで送信されます。

モバイル ステーション ISDN（MSISDN）情報エレメント（IE）の設定

モバイル ステーション ISDN（MSISDN）情報エレメント（IE）の最初のバイトが RADIUS サーバへのアクセス要求に含まれることを指定するには、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)# gprs radius msisdn first-byte`	MSISDN IE の最初のバイトがアクセス要求に含まれることを指定します。

ネットワーク アクセス サーバ（NAS）-Identifier の設定

グローバル レベルまたは APN レベルで、ネットワーク アクセス サーバ（NAS）-Identifier（RADIUS アトリビュート 32）を RADIUS サーバへのアクセス要求で送信するように GGSN を設定できます。APN レベルの設定によって、グローバル レベルの設定が上書きされます。

NAS-Identifier をすべてのアクセス要求に含めるように指定するには、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)# radius-server attribute 32 include-in-access-req format` *format*	GGSN が RADIUS アトリビュート 32（NAS-Identifier）をアクセス要求で送信することを指定します。*format* はアトリビュート 32 で送信される文字列であり、IP アドレス（%i）、ホスト名（%h）、およびドメイン名（%d）が含まれます。

このグローバル設定をディセーブルにするには、グローバル コンフィギュレーション モードでこのコマンドの **no** フォームを使用します。

APN で NAS-Identifier をすべてのアクセス要求に含めるように指定するには、アクセス ポイント 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-access-point)# radius attribute nas-id` *format*	GGSN が APN で NAS-Identifier をアクセス要求で送信することを指定します。*format* はアトリビュート 32 で送信される文字列であり、IP アドレス（%i）、ホスト名（%h）、およびドメイン名（%d）が含まれます。

この APN 設定をディセーブルにするには、アクセス ポイント コンフィギュレーション モードでこのコマンドの **no** フォームを使用します。

Acct-Session-ID アトリビュートの課金 ID の設定

GGSN が APN で Acct-Session-ID（アトリビュート 44）の課金 ID をアカウンティング要求に含めることを指定するには、アクセス ポイント 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)# radius attribute acct-session-id charging-id`	Acct-Session-ID（アトリビュート 44）の課金 ID がアカウンティング要求に含まれることを指定します。

この APN 設定をディセーブルにするには、アクセス ポイント コンフィギュレーション モードでこのコマンドの **no** フォームを使用します。

User-Name アトリビュートの MSISDN の設定

GGSN が APN で User-Name アトリビュート（アトリビュート 1）の MSISDN をアクセス要求に含めることを指定するには、アクセス ポイント 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)# radius attribute user-name msisdn`	MSISDN がアクセス要求の User-Name（アトリビュート 1）フィールドに含まれることを指定します。

この APN 設定をディセーブルにするには、アクセス ポイント コンフィギュレーション モードでこのコマンドの **no** フォームを使用します。

RADIUS サーバへのアクセス要求でのベンダー固有アトリビュートの設定

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）の規格草案では、ベンダー固有アトリビュート（アトリビュート 26）を使用してベンダー固有の情報を RADIUS サーバに通信する方式が指定されています。Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）では、一般的な使用には適さない独自の拡張アトリビュートをベンダーがサポートできるようにすることで、通信に使用できる大規模な情報が構成されます。

表 11-1 に、アトリビュート 26 が設定されている場合に GGSN が RADIUS サーバへの認証およびアカウンティング要求で送信できる、Third Generation Partnership Project（3GPP; 第 3 世代パートナーシップ プロジェクト）VSA サブアトリビュートを示して説明します。

表 11-1　3GPP VSA サブアトリビュート

番号	ベンダー独自のアトリビュート	説明
1	3GPP-IMSI	ユーザの International Mobile Subscriber Identity（IMSI）番号。 このサブアトリビュートは、**radius attribute suppress imsi** コマンドを使用して抑制できます。
2	3GPP-Charging-Id	この PDP コンテキストの課金 ID。
3	3GPP-PDP-Type	PDP コンテキストのタイプ（IP、PPP など）。
4	3GPP-CG-Address	現在のアクティブな課金ゲートウェイの IP アドレス。現在のアクティブな課金ゲートウェイがない場合、GGSN は 0.0.0.0 を送信します。
5	3GPP-GPRS-QoS-Profile	ネゴシエーションされた QoS 値。 このサブアトリビュートは、**radius attribute suppress qos** コマンドを使用して抑制できます。

表 11-1　3GPP VSA サブアトリビュート （続き）

番号	ベンダー独自のアトリビュート	説明
6	3GPP-SGSN-Address	コントロール メッセージを処理するために GTP コントロール プレーンによって使用される SGSN の IP アドレス。このアドレスは、ユーザが接続される Public Land Mobile Network（PLMN; パブリック ランド モバイル ネットワーク）を識別するために使用される場合もあります。 このサブアトリビュートは、**radius attribute suppress sgsn-address** コマンドを使用して抑制できます。
7	3GPP-GGSN-Address	コンテキスト確立のために GTP コントロール プレーンによって使用される GGSN の IP アドレス。このアドレスは、GGSN CDR（G-CDR）で使用される GGSN IP アドレスと同じです。
8	3GPP-IMSI-MCC-MNC	ユーザの IMSI 番号から抽出された Mobile Country Code（MCC; モバイル国コード）および Mobile Network Code（MNC; モバイル ネットワーク コード）(IMSI に応じて最初の 5 桁または 6 桁)。 このサブアトリビュートでは、**gprs mcc mnc** グローバル コンフィギュレーション コマンドを使用して、GGSN が使用する MCC 値および MNC 値が設定されている必要があります。
9	3GPP-GGSN-MCC-MNC	GGSN が属すネットワークの MCC および MNC。 このサブアトリビュートでは、グローバル コンフィギュレーション モードで **gprs mcc mnc** コマンドを使用して、GGSN が使用する MCC 値および MNC 値が設定されている必要があります。
12	3GPP-Selection-Mode	PDP コンテキストの作成要求で受信される、この PDP コンテキストの選択モード。
18	3GPP-SGSN-MCC-MNC	Routing Area Identity（RAI）MCC-MNC 値の符号化。

RADIUS アトリビュート 26 で定義されているように VSA を送信および認識するように GGSN 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)#radius-server vsa send [accounting | authentication]`	（任意）GGSN が RADIUS IETF アトリビュート 26 で定義されているように VSA を送信および認識できます。

ベンダー固有アトリビュートの使用の設定の詳細については、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

RADIUS 認証のアトリビュートの抑制

RADIUS サーバへのアクセス要求で特定のアトリビュートを抑制するように GGSN を設定できます。次の項では、抑制できるアトリビュートとその方法について説明します。

この項は、次の内容で構成されています。

RADIUS 認証の MSISDN 番号の抑制

一部の国には、サービス プロバイダーが認証要求内のモバイル ステーションの MSISDN 番号を識別することを禁止するプライバシー法があります。**msisdn suppression** コマンドを使用して、GGSN が RADIUS サーバへの認証要求で MSISDN 番号の代わりに送信する値を指定します。値を設定しない場合、RADIUS サーバには値は送信されません。

msisdn suppression コマンドを使用するには、グローバルに、またはアクセス ポイントで RADIUS サーバを設定して、非透過的アクセス モードを指定する必要があります。

RADIUS サーバに送信されるアクセス要求で MSISDN 番号を GGSN が上書きまたは抑制するように指定するには、アクセス ポイント 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-access-point)# msisdn suppression [value]`	（任意）GGSN がアクセス要求で MSISDN 番号を事前設定値で上書きすることを指定します。

この APN 設定をディセーブルにするには、アクセス ポイント コンフィギュレーション モードでこのコマンドの **no** フォームを使用します。

RADIUS 認証の 3GPP-IMSI VSA サブアトリビュートの抑制

GGSN が RADIUS サーバへの認証およびアカウンティング要求で第 3 世代パートナーシップ プロジェクト（3GPP）ベンダー固有アトリビュート（VSA）3GPP-International Mobile Subscriber Identity（3GPP-IMSI）番号を抑制するように設定するには、**radius attribute suppress imsi** アクセス ポイント コンフィギュレーション コマンドを使用します。

RADIUS サーバへの認証およびアカウンティング要求で 3GPP VSA 3GPP-IMSI 番号を抑制するように GGSN を設定するには、アクセス ポイント 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-access-point)# radius attribute suppress imsi`	（任意）RADIUS サーバへの認証およびアカウンティング要求で 3GPP-IMSI 番号を抑制するように GGSN を設定します。

この APN 設定をディセーブルにするには、アクセス ポイント コンフィギュレーション モードでこのコマンドの **no** フォームを使用します。

RADIUS 認証の 3GPP-GPRS-QoS Profile VSA サブアトリビュートの抑制

RADIUS サーバへの認証およびアカウンティング要求で 3GPP-GPRS-Qos Profile を抑制するように GGSN を設定するには、**radius attribute suppress qos** アクセス ポイント コンフィギュレーション コマンドを使用します。

RADIUS サーバへの認証およびアカウンティング要求で 3GPP-GPRS-Qos Profile を抑制するように GGSN を設定するには、アクセス ポイント 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-access-point)# radius attribute suppress qos`	（任意）GGSN が RADIUS サーバへの認証およびアカウンティング要求で 3GPP-GPRS-Qos Profile を抑制することを指定します。

RADIUS 認証の 3GPP-GPRS-SGSN-Address VSA サブアトリビュートの抑制

RADIUS サーバへの認証およびアカウンティング要求で 3GPP-GPRS-SGSN-Address を抑制するように GGSN を設定するには、**radius attribute suppress sgsn-address** アクセス ポイント コンフィギュレーション コマンドを使用します。

GGSN が RADIUS サーバへの認証およびアカウンティング要求で 3GPP-GPRS-SGSN-Address を抑制することを指定するには、アクセス ポイント 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-access-point)# radius attribute suppress sgsn-address`	（任意）GGSN が要求で 3GPP-GPRS-SGSN-Address を抑制することを指定します。

RADIUS サーバからのドメイン ネーム システム（DNS）および NetBIOS アドレス情報の取得

RADIUS サーバからドメイン ネーム システム（DNS）アドレスおよび Network Basic Input/Output System（NetBIOS）アドレス情報を取得するには、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て、RADIUS アトリビュート 26 で定義されているように VSA を送信および認識するように GGSN を設定します。

コマンド	目的
`Router(config)# radius-server vsa send [accounting | authentication]`	（任意）GGSN が RADIUS IETF アトリビュート 26 で定義されているように VSA を送信および認識できます。

（注）　DNS および NetBIOS アドレス情報が Mobile Station（MS; モバイル ステーション）に送信されるには、**ip-address-pool radius-client** コマンドを使用して、RADIUS サーバによって提供される IP アドレス プールを使用するダイナミック アドレス割り当て方法がアクセス ポイントに対して設定されている必要があります。アクセス ポイントの設定の詳細については、「GGSN でのアクセス ポイントの設定」（P.8-7）を参照してください。

RADIUS パケット オブ ディスコネクトの設定

RADIUS Packet of Disconnect（PoD; パケット オブ ディスコネクト）機能は、セッションの確立後にユーザ セッションを終了するための方法です。PoD は RADIUS Disconnect-Req パケットであり、RADIUS access-accept パケットがセッションを受け入れたあと、認証エージェント サーバでユーザを切断する場合に使用するためのものです。たとえば、前払い課金の場合、この機能の一般的な使用法では、前払いユーザのクォータ分が終了したときに前払い課金サーバによって PoD が送信されます。

PoD を受信すると、GGSN は次の処理を実行します。

- PoD 内にあるアトリビュート情報によって、PoD が生成された PDP コンテキストを識別します。VSA サブアトリビュート 3GPP-IMSI および 3GPP-NSAPI によって、PDP コンテキストは一意に識別されます。また、これらのサブアトリビュートが PoD 内にあることによって、PoD が GPRS ユーザ セッション用であることも識別されます。
- PDP コンテキストの削除要求を SGSN に送信します。
- ACK 切断要求または NAK 切断要求を PoD を生成したデバイスに送信します。GGSN は、ユーザ セッションを終了できるときに ACK 切断要求を送信し、ユーザ セッションを終了できないときに NAK 切断要求を送信します。ACK/NAK 切断要求は、アトリビュートを含まない RADIUS パケットです。

（注）　PoD 機能を GGSN で正しく機能させるには、IMSI アトリビュートが **radius attribute suppress imsi** コマンドによって抑制されていないことを確認してください。

GGSN で PoD サポート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)# aaa pod server [port port-number] [auth-type {any| all| session-key}] server-key [encryption-type] string`	特定のセッション アトリビュートが存在するときに、インバウンド ユーザ セッションを切断できます。 • **port** *port-number*：（任意）PoD 要求のネットワーク アクセス サーバのユーザ データグラム プロトコル（UDP）ポート。デフォルト値は 1700 です。 これは、GGSN が PoD 要求を受信するポートです。 • **auth-type**：（任意）セッションの切断に必要な認可のタイプ。 – **any**：PoD パケットで送信されるすべてのアトリビュートに一致するセッションが切断されます。PoD パケットには、4 つの主要アトリビュート（user-name、framed-IP-address、session-ID、および session-key）のうちの 1 つ以上を含めることができます。 – **all**：4 つの主要アトリビュートのすべてに一致するセッションだけが切断されます。**all** がデフォルトです。 – **session-key**：一致する session-key アトリビュートを持つセッションが切断されます。その他のアトリビュートはすべて無視されます。 （注） GGSN で PoD を設定する場合、**auth-type** キーワード オプションは設定しないことを推奨します。 • **server-key**：共有秘密文字列を設定します。 • *encryption-type*：（任意）直後のテキストが暗号化されるかどうか、および暗号化される場合は使用される暗号化タイプを定義する 1 桁の数字。定義されている暗号化タイプは、0（直後のテキストは暗号化されない）および 7（テキストはシスコが定義した暗号化アルゴリズムを使用して暗号化される）です。 • *string*：ネットワーク アクセス サーバとクライアント ワークステーション間で共有される共有秘密文字列。この共有秘密文字列は、双方のシステムで同じものである必要があります。

GGSN での RADIUS 応答の待機の設定

gtp response-message wait-accounting コマンドを使用して、GGSN が PDP コンテキストの作成要求を SGSN に送信する前に、RADIUS アカウンティング サーバからの RADIUS アカウンティング応答を待機するように設定します。

gtp response-message wait-accounting コマンドが設定されており、GGSN が RADIUS アカウンティング サーバから応答を受信しない場合、GGSN は PDP コンテキスト要求を拒否します。

ブロードキャスト アカウンティングが使用された場合（アカウンティング要求は複数の RADIUS サーバに送信される）、1 台の RADIUS サーバがアカウンティング応答で応答すると、GGSN は PDP コンテキストの作成要求を送信し、他の RADIUS サーバの応答を待機しません。

GGSN は、グローバル コンフィギュレーション レベルとアクセス ポイント コンフィギュレーション レベルの両方で、RADIUS 応答メッセージ待機の設定をサポートします。グローバル コンフィギュレーション レベルで、ほとんどの APN にわたってサポートする設定を指定することによって、設定を最小限にすることができます。その後、アクセス ポイント コンフィギュレーション レベルで、特定の APN でサポートする動作を選択的に変更できます。したがって、APN コンフィギュレーション レベルで、RADIUS 応答メッセージ待機のグローバル設定を上書きできます。

すべての APN のデフォルト動作として RADIUS アカウンティング応答を待機するように GGSN 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 **gprs gtp response-message wait-accounting** コマンドを使用します。特定の APN についてこの動作をディセーブルにするには、**no gtp response-message wait-accounting** アクセス ポイント コンフィギュレーション コマンドを使用します。

APN で RADIUS 応答メッセージ待機がイネーブルかディセーブルかを確認するには、**show gprs access-point** コマンドを使用して、wait_accounting 出力フィールドで報告される値を確認します。

RADIUS アカウンティング応答を待機するように GGSN をグローバルに設定するには、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)# gprs gtp response-message wait-accounting`	すべてのアクセス ポイントで受信される PDP コンテキストの作成要求について、GGSN が PDP コンテキストの作成要求を SGSN に送信する前に、RADIUS アカウンティング応答を待機するように設定します。

特定のアクセス ポイントについて RADIUS アカウンティング応答を待機するように GGSN を設定するには、アクセス ポイント 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-access-point)# gtp response-message wait-accounting`	特定のアクセス ポイントで受信される PDP コンテキストの作成要求について、GGSN が PDP コンテキストの作成要求を SGSN に送信する前に、RADIUS アカウンティング応答を待機するように設定します。

VPN ルーティングおよび転送（VRF）を使用した RADIUS サーバへのアクセスの設定

Cisco IOS GGSN ソフトウェアでは、VRF を使用した RADIUS サーバへのアクセスがサポートされています。この Cisco IOS ソフトウェア機能は *Per VRF AAA* と呼ばれ、この機能を使用して、Internet Service Provider（ISP; インターネット サービス プロバイダー）は VRF に基づいて AAA サービスを区分できます。これにより、GGSN は、RADIUS プロキシを経由しなくても、カスタマー バーチャル プライベート ネットワーク（VPN）に関連付けられたカスタマー RADIUS サーバと直接通信できます。したがって、お客様が必要とする柔軟性を提供するためにプロキシ AAA が必要なくなるため、ISP は VPN の提供をより効率的に拡張できます。

この設定をサポートするには、AAA が VRF 認識である必要があります。ISP は、同じ運用パラメータ（AAA サーバ グループ、方式リスト、システム アカウンティング、プロトコル固有のパラメータなど）の複数のインスタンスを定義し、パラメータを VRF パーティションに固定する必要があります。

（注）　VRF は Cisco 7600 Supervisor II および MSFC2 ではサポートされません。したがって、Supervisor II を使用する場合は、カプセル化された VRF トラフィックを GGSN から RADIUS サーバへの Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネル経由で、Supervisor を通過してトンネリングする必要があります。GRE トンネルの設定の詳細については、「トンネルを使用した RADIUS サーバへのアクセスの設定」（P.11-25）を参照してください。

Cisco 7600 Sup720 では VRF はサポートされます。

方式リストなどの AAA 設定が一意に複数回定義された場合、IP アドレスおよびポート番号に基づく AAA サーバの指定によって、VRF 間でプライベート アドレスの重複が発生する場合があります。AAA 方式リストの VRF への固定は、次のソースの 1 つ以上から実現できます。

- 仮想テンプレート：汎用インターフェイス設定として使用されます。
- サービス プロバイダー AAA サーバ：ドメイン名または Dialed Number Identification Service（DNIS; 着信番号識別サービス）に基づいて、リモート ユーザを特定の VPN に関連付けるために使用されます。このサーバによって、VPN 固有の設定がバーチャル アクセス インターフェイスに提供されます。カスタマー AAA サーバの IP アドレスおよびポート番号などです。
- カスタマー VPN AAA サーバ：リモート ユーザを認証し、ユーザ固有の設定をバーチャル アクセス インターフェイスに提供するために使用されます。

（注）　グローバルな AAA アカウンティング設定および一部の AAA プロトコル固有のパラメータは、仮想テンプレート設定では論理的にグループ化できません。

Per VRF 機能を設定する場合は、次の点に注意してください。

- VRF 間でプライベート アドレスが重複する可能性を防ぐには、サーバ グループ内で使用される単一のグローバル プールに AAA サーバを定義します。
- サーバは IP アドレスおよびポート番号で一意に識別できなくなります。
- 「プライベート」サーバ（すべてのサーバを含むデフォルト サーバ グループ内のプライベート アドレスを持つサーバ）をサーバ グループ内に定義し、他のグループからは非表示にしておくことができます。サーバ グループ内のサーバのリストには、グローバル設定でのホストの参照およびプライベート サーバの定義が含まれています。

（注）　プライベート サーバのパラメータが指定されていない場合は、グローバル設定が使用されます。グローバル設定が指定されていない場合は、デフォルト値が使用されます。

- すべてのサーバ運用パラメータは、ホストごと、サーバ グループごと、またはグローバルに設定できます。ホストごとの設定は、サーバ グループごとの設定よりも優先されます。サーバ グループごとの設定は、グローバルな設定よりも優先されます。

（注）　VRF を使用した RADIUS サーバへのアクセスの設定の詳細については、「*Per VRF AAA*」フィーチャ モジュールを参照してください。

ここでは、VRF を使用したプライベート RADIUS サーバへのアクセスの設定および確立について説明します。グローバルな RADIUS サービスの場合は、グローバルに配置されたサーバを設定してあることを確認してください。

VRF を使用した RADIUS サーバへのアクセスを設定するには、次の作業を実行します。

- 「AAA のグローバルなイネーブル」（P.11-21）（必須）
- 「VRF 認識プライベート RADIUS サーバ グループの設定」（P.11-22）（必須）
- 「指定した方式リストを使用した認証、認可、アカウンティングの設定」（P.11-22）（必須）
- 「VRF ルーティング テーブルの設定」（P.11-23）（必須）
- 「インターフェイスでの VRF の設定」（P.11-23）（必須）
- 「プライベート RADIUS サーバへのアクセスのためのアクセス ポイントでの VRF の設定」（P.11-24）（必須）
- 「VRF を使用した RADIUS サーバへのルートの設定」（P.11-27）（任意）

AAA のグローバルなイネーブル

AAA が GGSN でグローバルにイネーブルにされていない場合、VRF 経由でのプライベート RADIUS サーバへのアクセスを設定する前にイネーブルにする必要があります。

AAA をグローバルに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
ステップ 1	`Router(config)# aaa new-model`	AAA をグローバルにイネーブルにします。

VRF 認識プライベート RADIUS サーバ グループの設定

プライベート サーバの運用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
ステップ 1	`Router(config)# aaa group server radius group-name`	異なる RADIUS サーバ ホストを別々のリストおよび別々の方式にグループ化します。 • *group-name*：サーバのグループを指定するために使用される文字列。
ステップ 2	`Router(config-sg-radius)# server-private ip-address auth-port port_num acct-port port_num key string`	グループ サーバのプライベート RADIUS サーバの IP アドレスを設定します。 • *ip-address* : プライベート RADIUS サーバ ホストの IP アドレスを指定します。 • **auth-port** *port_num*：認証専用のポートを指定します。 • **acct-port** *port_num*：アカウンティング専用のポートを指定します。 • *string*：（任意）ルータと RADIUS サーバ間のすべての RADIUS 通信用の認証および暗号キーを指定します。 （注）　プライベート サーバのパラメータが指定されていない場合は、グローバル設定が使用されます。グローバル設定が指定されていない場合は、デフォルト値が使用されます。
ステップ 3	`Router(config-sg-radius)# ip vrf forwarding vrf-name`	AAA RADIUS サーバ グループの VRF 参照を設定します。 • *vrf-name* : VRF に割り当てられる名前。

指定した方式リストを使用した認証、認可、アカウンティングの設定

指定した方式リストを使用して AAA を設定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

ステップ 1	`Router(config)# aaa authentication ppp {default | list-name} method1 [method2...]`	ローカル認証方式リストを作成します。次のオプションがあります。 • **default**：ユーザがルータにログインしたときに、この引数のあとの認証方式が認証方式のデフォルト リストであることを指定します。 • *method* : PPP の有効な AAA 認証方式を指定します。たとえば、**group RADIUS** はグローバル RADIUS 認証をイネーブルにします。

ステップ 2	`Router(config)# aaa authorization {auth-proxy | network | exec | commands level | reverse-access} {default | list-name} [method1 [method2...]]`	特定の認可タイプの認可方式リストを作成し、認可をイネーブルにします。
ステップ 3	`Router(config)# aaa accounting {system default [vrf vrf-name] | network {default | none | start-stop | stop-only | wait-start} group group-name`	RADIUS を使用する場合、課金およびセキュリティのために、要求されたサービスの AAA アカウンティングをイネーブルにします。

VRF ルーティング テーブルの設定

プライベート RADIUS サーバへのアクセスのために GGSN で VRF ルーティング テーブルを設定するには、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
ステップ 1	`Router(config)# ip vrf vrf-name`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-vrf)# rd route-distinguisher`	VRF のルーティング テーブルおよび転送テーブルを作成し、VPN のデフォルトのルート識別子を指定します。

インターフェイスでの VRF の設定

プライベート RADIUS サーバにアクセスするには、サーバへのインターフェイスで VRF を設定する必要があります。

Cisco 7600 シリーズ ルータ プラットフォームでは、このインターフェイスはスーパーバイザ エンジンに設定されたレイヤ 3 ルーテッド Gi VLAN への論理インターフェイスとなります（ここに IEEE 802.1Q カプセル化が設定されます）。

スーパーバイザ エンジン上の必要な VLAN の詳細については、「プラットフォームの前提条件」（P.2-2）を参照してください。

インターフェイスの設定の詳細については、『*Cisco IOS Interface Configuration Guide*』および『*Cisco IOS Interface Command Reference*』を参照してください。

802.1Q カプセル化サブインターフェイスの設定

スーパーバイザ エンジン上の関連付けられた VLAN に対する IEEE 802.1Q カプセル化をサポートするサブインターフェイスを設定するには、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
ステップ 1	`Router(config)# interface gigabitethernet slot/port.subinterface-number`	IEEE 802.1Q が使用されるサブインターフェイスを指定します。
ステップ 2	`Router(config-if)# encapsulation dot1q vlanid`	カプセル化形式を IEEE 802.1Q（dot1q）と定義し、VLAN 識別子を指定します。
ステップ 3	`Router(config-if)# ip address ip-address mask`	インターフェイスのプライマリ IP アドレスを設定します。

プライベート RADIUS サーバへのアクセスのためのアクセス ポイントでの VRF の設定

前提条件の設定作業を完了したあと、トンネルを使用して、またはトンネルを使用しないで RADIUS サーバへのアクセスを設定できます。

次の項では、RADIUS サーバへのアクセスを設定するために使用できるさまざまな方法について説明します。

- トンネルを使用しない RADIUS サーバへのアクセスの設定
- トンネルを使用した RADIUS サーバへのアクセスの設定

トンネルを使用しない RADIUS サーバへのアクセスの設定

トンネルを使用しない RADIUS サーバへのアクセスを設定するには、**vrf** アクセス ポイント コンフィギュレーション コマンドを設定する必要があります。

（注）　GPRS アクセス ポイント リストで RADIUS サーバへのアクセスを設定するには、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
ステップ 1	`Router(config)# gprs access-point-list list-name`	新しいアクセス ポイント リストの名前を指定するか、既存のアクセス ポイント リストの名前を参照し、アクセス ポイント リスト コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-ap-list)# access-point access-point-index`	新しいアクセス ポイント定義のインデックス番号を指定するか、既存のアクセス ポイント定義を参照し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-access-point)# access-point-name apn-name`	定義されたアクセス ポイントでユーザが GGSN からアクセスできる PDN のネットワーク（またはドメイン）名を指定します。 （注）　*apn-name* は、MS、Home Location Register（HLR; ホーム ロケーション レジスタ）、および DNS サーバでプロビジョニングされる APN に一致する必要があります。
ステップ 4	`Router(config-access-point)# aaa-group authentication server-group`	デフォルト AAA サーバ グループを指定し、GGSN の特定のアクセス ポイントに対してサーバ グループによってサポートされる AAA サービスのタイプを割り当てます。各項目の意味は次のとおりです。 • **authentication**：選択したサーバ グループを APN での認証サービスに割り当てます。 • *server-group*：APN で AAA サービスに使用する AAA サーバ グループの名前を指定します。 （注）　指定する AAA サーバ グループの名前は、**aaa group server** コマンドを使用して設定するサーバ グループに対応している必要があります。

	コマンド	目的
ステップ 5	`Router(config-access-point)# access-mode non-transparent`	GGSN が認証用のプロキシとして機能することを指定します。
ステップ 6	`Router(config-access-point)# ip-address-pool radius-client`	RADIUS サーバが現在のアクセス ポイントの IP アドレス プールを提供することを指定します。 （注）　ダイナミック アドレス割り当て方法を使用している場合は、適切な IP アドレス プール ソースに従ってこのコマンドを設定する必要があります。
ステップ 7	`Router(config-access-point)# vrf vrf-name`	GGSN アクセス ポイントで VPN ルーティングおよび転送を設定し、アクセス ポイントを特定の VRF インスタンスに関連付けます。 （注）　*vrf-name* 引数は、「指定した方式リストを使用した認証、認可、アカウンティングの設定」（P.11-22）で **ip vrf** コマンドを使用して設定した VRF の名前と一致している必要があります。
ステップ 8	`Router(config-access-point)# exit`	アクセス ポイント コンフィギュレーション モードを終了します。

トンネルを使用した RADIUS サーバへのアクセスの設定

RADIUS サーバへのインターフェイスが 1 つだけであり、そこから 1 台以上のプライベート RADIUS サーバにアクセスする必要がある場合、IP トンネルを設定してそれらのプライベート サーバにアクセスできます。

トンネルを使用した RADIUS サーバへのアクセスを設定するには、次の作業を実行します。

- プライベート RADIUS サーバ アクセス ポイントの設定（必須）
- IP トンネルの設定（必須）

プライベート RADIUS サーバ アクセス ポイントの設定

GPRS アクセス ポイント リストでプライベート RADIUS サーバへのアクセスを設定するには、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
ステップ 1	`Router(config)# gprs access-point-list list-name`	新しいアクセス ポイント リストの名前を指定するか、既存のアクセス ポイント リストの名前を参照し、アクセス ポイント リスト コンフィギュレーション モードを開始します。
ステップ 2	`Router(config-ap-list)# access-point access-point-index`	新しいアクセス ポイント定義のインデックス番号を指定するか、既存のアクセス ポイント定義を参照し、アクセス ポイント コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	`Router(config-access-point)# access-point name apn-name`	アクセス ポイント ネットワーク ID を指定します。これには、インターネット ドメイン名が広く使用されています。 （注）　*apn-name* は、モバイル ステーション（MS）、ホーム ロケーション レジスタ（HLR）、および DNS サーバでプロビジョニングされる APN に一致する必要があります。
ステップ 4	`Router(config-access-point)# access-mode {transparent | non-transparent}`	（任意）アクセス ポイントで GGSN がユーザ認証を要求するかどうかを指定します。使用できるオプションは次のとおりです。 • **transparent**：このアクセス ポイントに対しては、セキュリティ認証および認可のいずれも GGSN によって要求されません。これはデフォルト値です。 • **non-transparent**：GGSN は、認証を実施するプロキシとして機能します。
ステップ 5	`Router(config-access-point)# access-type real`	GGSN の外部ネットワークへのインターフェイスに対応する APN タイプを指定します。デフォルト値は実です。
ステップ 6	`Router(config-access-point)# ip-address-pool {dhcp-proxy-client | radius-client | local pool-name | disable}`	（任意）IP アドレス プールを使用するダイナミック アドレス割り当て方法を現在のアクセス ポイントのために指定します。使用できるオプションは次のとおりです。 • **dhcp-proxy-client**：Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト コンフィギュレーション プロトコル）サーバが IP アドレス プールを提供します。 • **radius-client**：RADIUS サーバが IP アドレス プールを提供します。 • **local**：ローカル プールが IP アドレスを提供することを指定します。このオプションでは、**aggregate** アクセス ポイント コンフィギュレーション コマンドを使用してアドレス範囲が設定され、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用してローカル プールが設定される必要があります。 • **disable**：ダイナミック アドレス割り当てをオフにします。 （注）　ダイナミック アドレス割り当て方法を使用している場合は、適切な IP アドレス プール ソースに従ってこのコマンドを設定する必要があります。

	コマンド	目的
ステップ 7	`Router(config-access-point)# vrf vrf-name`	GGSN アクセス ポイントで VPN ルーティングおよび転送を設定し、アクセス ポイントを特定の VRF インスタンスに関連付けます。
ステップ 8	`Router(config-access-point)# exit`	アクセス ポイント コンフィギュレーション モードを終了します。

IP トンネルの設定

トンネルを設定する場合は、ループバック インターフェイスを実インターフェイスではなく、トンネル エンドポイントとして使用することを推奨します。これは、ループバック インターフェイスが常に稼動しているためです。

プライベート ネットワークへの IP トンネルを設定するには、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
ステップ 1	`Router(config)# interface tunnel number`	論理トンネル インターフェイス番号を設定します。
ステップ 2	`Router(config-if)# ip vrf forwarding vrf-name`	VRF インスタンスをインターフェイスに関連付けます。
ステップ 3	`Router(config-if)# ip address ip-address mask [secondary]`	トンネル インターフェイスの IP アドレスを指定します。 **（注）** この IP アドレスは、GGSN に関する他の設定では使用されません。
ステップ 4	`Router(config-if)# tunnel source {ip-address | type number}`	RADIUS サーバへのインターフェイスまたはループバック インターフェイスの IP アドレス（またはインターフェイス タイプおよびポートまたはカード番号）を指定します。
ステップ 5	`Router(config-if)# tunnel destination {hostname | ip-address}`	このトンネルからアクセスできるプライベート ネットワークの IP アドレス（またはホスト名）を指定します。

VRF を使用した RADIUS サーバへのルートの設定

VRF インスタンスと RADIUS サーバ間にルートが存在するようにします。VRF から RADIUS サーバに対して **ping** コマンドを使用して、接続性を検証できます。ルートを設定するには、スタティック ルートまたはルーティング プロトコルを使用できます。

VRF を使用したスタティック ルートの設定

VRF を使用してスタティック ル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
Router(config)# **ip route vrf** *vrf-name prefix mask* [*next-hop-address*] [*interface* {*interface-number*}] [**global**] [*distance*] [**permanent**] [**tag** *tag*]	スタティック IP ルートを設定します。 • *vrf-name*：スタティック ルート用の VPN ルーティングおよび転送（VRF）インスタンスの名前を指定します。 • *prefix*：宛先の IP ルート プレフィクスを指定します。 • *mask*：宛先のプレフィクス マスクを指定します。 • *next-hop-address*：宛先ネットワークに到達するために使用できるネクストホップの IP アドレスを指定します。 • *interface interface-number*：宛先ネットワークに到達するために使用できるネットワーク インターフェイスのタイプとインターフェイス番号を指定します。 • **global**：指定のネクストホップ アドレスが VRF ルーティング テーブル以外のテーブルにあることを指定します。 • *distance*：ルートの管理ディスタンスを指定します。 • **permanent**：インターフェイスがシャットダウンした場合でも、ルートを削除しないことを指定します。 • **tag** *tag*：ルート マップ経由で再配布を制御するための「一致」値として使用できるタグ値を指定します。

VRF を使用したスタティック ルートの検証

設定したスタティック VRF ルートを確認するには、次の例に示すように **show ip route vrf** 特権 EXEC コマンドを使用します。

```
GGSN# show ip route vrf vpn1 static

      172.16.0.0/16 is subnetted, 1 subnets
C       172.16.0.1 is directly connected, Ethernet5/1
C       10.100.0.3/8 is directly connected, Virtual-Access5
```

VRF を使用した OSPF ルートの設定

VRF を使用して Open Shortest Path First（OSPF）ル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
`Router(config)# router ospf process-id [vrf vrf-name]`	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。 • *process-id* : OSPF ルーティング プロセスのために内部で使用する識別パラメータを指定します。*process-id* はローカルで割り当てられ、任意の正の整数を指定できます。OSPF ルーティング プロセスごとに一意の値を割り当てます。 • **vrf** *vrf-name* : VPN ルーティングおよび転送インスタンスの名前を指定します。

GGSN Gn インターフェイスの保護

アドレス確認およびモバイル間トラフィック リダイレクション機能により、ネットワークへの不正アクセスやネットワーク ダウンタイムにつながる攻撃に対するセキュリティが、GGSN モバイル インターフェイスに追加されます。これらの機能を設定するには、次の作業が必要です。

- 「アドレス確認の設定」（P.11-29）
- 「モバイル間トラフィック リダイレクションの設定」（P.11-30）
- 「すべてのトラフィックのリダイレクト」（P.11-31）

アドレス確認の設定

security verify source（IPv4 アドレス確認）および **ipv6 security verify source**（IPv6 アドレス確認）アクセス ポイント コンフィギュレーション コマンドを使用して、MS に以前に割り当てられたアドレスに対して、アップストリーム Transport Protocol Data Unit（TPDU; 転送プロトコル データ ユニット）の送信元 IP アドレスを確認するように GGSN を設定します。

security verify source または **ipv6 security verify source** コマンドが APN で設定されると、GTP が TPDU を受け入れて転送する前に、GGSN はその送信元アドレスを確認します。アドレスが MS に以前に割り当てられたものと異なることを判別すると、GGSN は TPDU を廃棄し、PDP コンテキストおよび APN で不正なパケットと見なします。**security verify source** および **ipv6 security verify source** アクセス ポイント コンフィギュレーション コマンドの設定によって、GGSN は偽のユーザ ID から保護されます。

security verify destination アクセス ポイント コンフィギュレーション コマンド（IPv4 アドレス確認だけ）を使用して、GGSN で、**gprs plmn ip address** コマンドを使用して指定された PLMN アドレスのグローバル リストに対して、アップストリーム TPDU の宛先アドレスを確認します。GGSN は、TPDU の宛先アドレスがアドレス リストの範囲内にあることを判別すると、TPDU を廃棄します。TPDU にリストの範囲外の宛先アドレスが含まれていることを判別すると、TPDU を最終宛先に転送します。

（注）　**security verify destination** コマンドは、VRF または IPv6 アドレス確認を使用する APN には適用されません。また、宛先アドレスの確認は、GTP-PPP 再生成または Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）を含む GTP-PPP には適用されません。

アクセス ポイントで IPv4 アドレス確認を設定するには、アクセス ポイント 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-access-point)# security verify {source | destination}`	（任意）GGSN が Gn インターフェイスから受信した TPDU の送信元アドレスまたは宛先アドレスを確認することを指定します。

（注）　IPv4 宛先アドレスと送信元アドレスの両方の確認を APN で設定できます。

アクセス ポイントで IPv6 送信元アドレス確認を設定するには、アクセス ポイント 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-access-point)# ipv6 security verify source`	（任意）MS に以前に割り当てられたアドレスに対して、アップストリーム TPDU の IPv6 送信元アドレスを確認するように GGSN を設定します。アクセス ポイント コンフィギュレーション モードで **ipv6 security verify source** コマンドを使用します。

モバイル間トラフィック リダイレクションの設定

モバイル間トラフィックは、Gn インターフェイスを介して開始および終了されます。したがって、ネットワーク側の Gi インターフェイスを介さずに GGSN によって切り替えられます。このため、GGSN のネットワーク側に配置されたファイアウォールでは、このレベルのトラフィックを確認できません。

redirect intermobile ip アクセス ポイント コマンドを使用して、確認のために、モバイル間トラフィックを外部デバイス（外部ファイアウォールなど）にリダイレクトします。

コマンド	目的
`Router(config-access-point)# redirect intermobile ip` *ip address*	（任意）すべての IPv4 モバイル間トラフィックを外部デバイスにリダイレクトするように GGSN を設定します。
`Router(config-access-point)# ipv6 redirect intermobile` *ipv6-address*	（任意）すべての IPv6 モバイル間トラフィックを外部 IPv6 デバイスにリダイレクトするように GGSN を設定します。

（注）　Cisco 7600 シリーズ インターネット ルータ プラットフォームでのモバイル間リダイレクション機能では、スーパーバイザ エンジンおよび Cisco SAMI からの着信 VLAN インターフェイスで Policy Based Routing（PBR; ポリシー ベース ルーティング）が設定され、**set ip next-hop** コマンドを使用して基準に一致したパケットをルーティングするネクストホップが設定されている必要があります。

（注）　TPDU が同じ APN で終了しないかぎり、入力 APN ではモバイル間トラフィックのリダイレクションは発生しません。また、入力 APN から PDN の L2TP Network Server（LNS; L2TP ネットワーク サーバ）へ L2TP によってトンネリングされる TPDU のリダイレクションも発生しません。

すべてのトラフィックのリダイレクト

すべてのトラフィックのリダイレクト機能を使用すると、次のことを実行できます。

- 同じ GGSN 上のモバイル ステーション（MS）に宛先アドレスが属するかどうかに関係なく、すべてのパケットを指定された宛先にリダイレクトします。モバイル間リダイレクト機能を使用してトラフィックをリダイレクトする場合、同じ GGSN 上でアクティブな MS に宛先アドレスが属するパケットだけをリダイレクトできます。送信 MS の PDP コンテキストが作成される GGSN 内に受信 MS の PDP コンテキストがない場合、パケットは廃棄されます。
- 集約ルートが設定されている場合、すべてのトラフィックを特定の宛先にリダイレクトします。

すべてのトラフィックを特定の IP アドレスにリダイレクトするには、アクセス ポイント コンフィギュレーション モードで次のコマンドを発行します。

コマンド	目的
`Router(config-access-point)# redirect all ip ip address`	（任意）すべての IPv4 トラフィックを外部デバイスにリダイレクトするように GGSN を設定します。
`Router(config-access-point)# ipv6 redirect allintermobile ipv6-address`	（任意）すべての IPv6 トラフィックを外部 IPv6 デバイスにリダイレクトするように GGSN を設定します。

GGSN Gn インターフェイスでの GRX トラフィックの分離

Cisco GGSN は、Gn および Gp インターフェイスで SGSN からのトラフィックを受信します。Gn トラフィックは同じ PLMN 内の SGSN から、Gp トラフィックは異なる PLMN 内の SGSN から、GPRS Roaming Exchange（GRX）経由で GGSN に到達します。

プライバシーおよびセキュリティを確保するために、Cisco GGSN は、GRX トラフィックを分離して別々のルーティング テーブルの一部とすることができるように、Gn インターフェイス上でバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスをサポートします。

Gn VRF を設定する場合は、次の点に注意してください。

- VRF ごとに GTP 仮想テンプレートを設定する必要があります。
- デフォルト GTP 仮想テンプレート（Virtual-Template 1）は設定が必須であり、**service gprs ggsn** が設定されているかぎり設定解除しません。
- デフォルト GTP 仮想テンプレート（Virtual-Template 1）には、**ip address** または **ip unnumbered** コマンドを使用して有効な IP アドレスが関連付けられている必要があります。

- GTP カプセル化を使用する 2 つの仮想テンプレートを同じ VRF で使用することはできません。
- 課金元インターフェイスが設定されていないかぎり、GTP 仮想テンプレートに関連付けられたすべてのループバック インターフェイスに対して同じ IP アドレスを使用して、PDP コンテキストの Call Detail Record（CDR; 呼詳細レコード）に同じ GGSN アドレスが含まれるようにする必要があります。
- すべての仮想テンプレートを同じアクセス ポイント リスト名で設定する必要があります。

Gn VRF 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
ステップ 1	`Router(config)# interface virtual-template number`	仮想テンプレート インターフェイスを作成します。*number* によって、仮想テンプレート インターフェイスが識別されます。このコマンドにより、インターフェイス コンフィギュレーション モードになります。
ステップ 2	`Router(config-if)# description description`	インターフェイスの説明。
ステップ 3	`Router(config-if)# ip vrf forwarding vrf-name`	VRF インスタンスをインターフェイスに関連付けます。
ステップ 4	`Router(config-if)# ip unnumber loopback number`	以前に定義されたループバック IP アドレスを仮想テンプレート インターフェイスに割り当てます。
ステップ 5	`Router(config-if)# encapsulation gtp`	仮想テンプレート インターフェイスで送信されるパケットのカプセル化タイプとして GTP を指定します。
ステップ 6	`Router(config-if)# gprs access-point-list list-name`	新しいアクセス ポイント リストの名前を指定するか、既存のアクセス ポイント リストの名前を参照し、アクセス ポイント リスト コンフィギュレーション モードを開始します。

Gn VRF 設定を削除するには、グローバル コンフィギュレーション モードで **interface virtual-template** コマンドの **no** フォームを使用し、Gn VRF 仮想テンプレート インターフェイスの番号を指定します。

ブロードキャスト アカウンティングと待機アカウンティングの同時設定

Cisco GGSN リリース 8.0 以降、ブロードキャスト アカウンティングと待機アカウンティングを同時に使用するように設定できます。待機アカウンティング機能は APN レベルで設定され、ブロードキャスト アカウンティングは AAA 方式レベルで指定されます。

ブロードキャスト アカウンティングでは、開始、停止、および中間アカウンティング レコードが、方式リストに設定されたすべてのサーバ グループに送信されます。サーバ グループ内では、アカウンティング レコードは最初のアクティブなサーバに送信されます。そのアクティブなサーバに到達できない場合、アカウンティング レコードはグループ内の次のサーバに送信されます。

また、方式リスト内の 1 つ以上のサーバ グループを「必須」として設定できます。これは、そのサーバ グループのサーバがアカウンティング開始メッセージに応答する必要があることを意味します。APN レベルの待機アカウンティングでは、アカウンティング応答がすべての必須サーバ グループから受信されてから、PDP コンテキストが確立されます。

ブロードキャスト アカウンティングと待機アカウンティングを同時に使用することの利点は、次のとおりです。

- アカウンティング レコードは複数のサーバに送信され、エントリが行われると、ユーザは別のサービスを使用して起動できます。
- 冗長性のために、レコードは複数の AAA サーバに送信されます。
- PDP コンテキストは有効なアカウンティング開始レコードがすべての必須のサーバで受信された場合にだけ確立され、情報の損失を防ぎます。
- 方式リスト内の最大 10 個のサーバ グループにブロードキャスト レコードを送信できます。

ブロードキャスト アカウンティングと待機アカウンティングを同時に設定する場合は、次の点に注意してください。

- 方式リストの設定では、**mandatory** キーワードはブロードキャスト アカウンティングが設定されている場合にだけ使用できます。
- 待機アカウンティングが必要ない場合、すべてのサーバ グループへのブロードキャスト アカウンティングは、必須グループを定義しないで使用できます。
- ブロードキャスト アカウンティングを設定するときに必須サーバ グループを指定しないと、待機アカウンティングは Cisco GGSN リリース 7.0 以前のリリースの場合と同様に機能します。
- 待機アカウンティングは PPP PDP コンテキストには適用されません。
- PDP は、すべての必須サーバからアカウンティング応答が受信された場合にだけ作成されます。
- 定期的なタイマーは、アカウンティング応答（PDP 作成）が受信されたときに開始されます。

（注） 複数のサーバ グループを必須サーバ グループとして方式リストで定義できます。

ブロードキャスト アカウンティングおよび待機アカウンティングを GGSN で設定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# aaa accounting network` *methodlist-name*	RADIUS を使用する場合、課金およびセキュリティのために、要求されたサービスの認証、認可、アカウンティング（AAA）アカウンティングをイネーブルにします。
ステップ 2	`Router(cfg-acct-mlist)# action-type {start-stop | stop-only | none}`	アカウンティング レコードで実行されるアクションのタイプ。使用可能な値は次のとおりです。 • **start-stop**：プロセスの開始時にアカウンティング「開始」通知、プロセスの終了時にアカウンティング「停止」通知を送信します。 • **stop-only**：要求されたユーザ プロセスの終了時にアカウンティング「停止」通知を送信します。 • **none**：この回線またはインターフェイスでアカウンティング サービスをディセーブルにします。

	コマンド	目的
ステップ 3	Router(cfg-acct-mlist)# **broadcast**	（任意）複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバにアカウンティング レコードを同時に送信します。最初のサーバが使用不可の場合は、そのグループ内で定義されているバックアップ サーバを使用してフェールオーバーが発生します。
ステップ 4	Router(cfg-acct-mlist)# **group** {*server-group*} [**mandatory**]	サーバ グループを指定します。任意で、mandatory を指定して、このサーバ グループを必須として定義します。サーバ グループが必須の場合、そのサーバ グループのサーバがアカウンティング開始メッセージに応答する必要があります。 **（注）** 方式リスト内の最大 10 個のサーバ グループを定義できます。
ステップ 5	Router(cfg-acct-mlist)# **exit**	アカウンティング方式リスト モードを終了します。
ステップ 6	Router(config)# **gprs access-point-list** *list_name*	GGSN 上の公衆データ網（PDN）アクセス ポイントを定義するために使用するアクセス ポイント リストを設定します。
ステップ 7	Router(config-ap-list)#**access-point** *access-point-index*	アクセス ポイント番号を指定し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 8	Router(config-access-point)#**aaa-group accounting** *method-list name*	アカウンティング サーバ グループを指定します。
ステップ 9	Router(config-access-point)# **gtp-response-message wait-accounting**	APN が PDP コンテキストの作成要求を SGSN に送信する前に、RADIUS アカウンティング応答を待機するように設定します。

定期アカウンティング タイマー

Cisco IOS ソフトウェアでは、AAA セッションの定期アカウンティング レコードの送信をイネーブルにするグローバル AAA コンフィギュレーション コマンドがサポートされています。ただし、GGSN は、PDP コンテキストの定期アカウンティング レコードの送信に、この設定を使用しません。

Cisco GGSN リリース 8.0 以降、定期アカウンティング タイマーの間隔値は、次のいずれかを使用して取得されます。

- APN レベルで設定された定期タイマー
- GGSN グローバル コンフィギュレーション レベルで設定された定期タイマー
- access-accept メッセージ内の accounting-interim 間隔アトリビュート

これらの設定が存在する場合、適用可能な PDP コンテキストに対して設定された間隔で、「中間」タイプのアカウンティング レコードが送信されます。次の優先順位が適用されます。

- APN レベルの設定
- GGSN のグローバル設定
- アトリビュート 85（access-accept メッセージ内）

（注）　値が access-accept メッセージのアトリビュート 85 によって取得された場合、GGSN は最小値および最大値が GGSN で設定された範囲内にあることを確認し、範囲外の場合はアトリビュートは無視されます。また、APN でアカウンティングがイネーブルではない場合、アトリビュート 85 は無視されます。

GGSN が Interim Update Accounting（IAU）レコードを送信する場合、定期タイマーは次の定期アカウンティング レコードが定期間隔の終了後に送信されるようにリセットされ、IAU レコードが送信されたインスタンスから開始されます。

両方のタイプのレコードには同じ情報が含まれているため、この処理によって RADIUS アカウンティング トラフィックは制限されます。ただし、フェールオーバー後は、送信されるレコードは元の START レコードと調整されます。

注意　GGSN で **aaa accounting update periodic** コマンドが設定されており、GGSN レベルの定期アカウンティングが設定されていない場合、アカウンティング開始メッセージが AAA サーバに送信されたあとに GGSN は中間アカウンティング レコードを送信します。これにより GGSN に悪影響を及ぼす可能性があるため、**aaa accounting update periodic** コマンドは設定しないでください。

GGSN で定期アカウンティング タイマーを設定する場合は、次の点に注意してください。

- タイマーは PPP 再生成、IPv4、および IPv6 PDP に対してサポートされています。タイマーは PPP PDP には適用されません。
- PDP の送信/受信バイト カウントは、フェールオーバー時に 0 にリセットされます。
- タイマー間隔を正確に保つために、冗長システムのクロックは NTP などのメカニズムと同期化されている必要があります。
- 冗長設定での定期アカウンティングでは、スイッチオーバーの前後で間隔は維持されます。
- タイマーは PDP 作成が成功した場合にだけ開始されます。たとえば、待機アカウンティングでは、正常なアカウンティング応答が受信されたあとです。

デフォルトの GGSN 定期アカウンティング タイマーの設定

すべての APN に対してデフォルトの定期アカウンティング値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)# gprs default aaa-accounting interim periodic` *minutes*	GGSN でデフォルトの定期アカウンティング タイマーを設定します。有効な値は 15 ～ 71582 です。デフォルトでは、定期アカウンティング タイマーはグローバルに設定されません。

APN レベルの定期アカウンティング タイマーの設定

APN で定期アカウンティング タイマーを設定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	目的
ステップ 1	`Router(config)# gprs access-point-list list_name`	アクセス ポイント リストを設定します。
ステップ 2	`Router(config-ap-list)#access-point access-point-index`	アクセス ポイント番号を指定し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-access-point)#aaa-accounting interim periodic minutes`	APN で定期アカウンティング タイマーを設定します。有効な値は 15 ～ 71582 です。デフォルトでは、定期アカウンティング タイマーは APN レベルで設定されません。
ステップ 4	`Router(config-access-point)#aaa-accounting interim periodic radius`	RADIUS によって送信された定期アカウンティング値（アトリビュート 85）を APN が受け入れることができます。

（注） AAA グローバル設定値（**aaa accounting update periodic** *minutes*）は常に無視されます。また、APN アカウンティングがイネーブルでないかぎり、設定方法にかかわらず定期アカウンティングは有効ではありません。

Cisco GGSN での合法的傍受サポートの実装

ここでは、合法的傍受について説明します。次の項目について説明します。

注意 この項は、合法的傍受の実装の法的義務に対応するものではありません。サービス プロバイダーには、そのネットワークが、適用される合法的傍受の法令および規制に適合することを保証する責任があります。法的な助言を求め、果たすべき義務を明確にすることを推奨します。

合法的傍受の概要

合法的傍受は、裁判所または行政機関による命令を根拠として、Law Enforcement Agency（LEA; 司法当局）が個人（ターゲット）に対して電子監視を実施できるようにするプロセスです。合法的傍受プロセスを容易にするために、特定の法律および規制によって、Service Provider（SP; サービス プロバイダー）およびインターネット サービス プロバイダー（ISP）に対して、認可された電子監視を明示的にサポートするようにネットワークを実装することが定められています。

監視は、音声、データ、およびマルチサービス ネットワークによる従来のテレコミュニケーションおよびインターネット サービスに対する傍受を使用して実行されます。LEA は、ターゲットのサービス プロバイダーに傍受を要求します。サービス プロバイダーには、その個人が送受信するデータ通信を傍受する責任があります。サービス プロバイダーは、ターゲットの IP アドレスまたはセッションを使用して、ターゲットのトラフィック（データ通信）を処理しているエッジ ルータを判別します。次に、サービス プロバイダーは、ターゲットのトラフィックがルータを通過するときにそれを傍受し、傍受したトラフィックのコピーをターゲットに気付かれずに LEA に送信します。

合法的傍受機能は、米国内のサービス プロバイダーによる合法的傍受のサポート方法を定めた Communications Assistance for Law Enforcement Act（CALEA）をサポートしています。現在、合法的傍受は次の規格によって定義されています。

- Telephone Industry Association（TIA）仕様 J-STD-025
- Packet Cable Electronic Surveillance Specification（PKT-SP-ESP-101-991229）

シスコの合法的傍受ソリューションの詳細については、シスコの代理店にご連絡ください。

Cisco GGSN での合法的傍受のサポートには、次の利点があります。

- 複数の LEA が相互に知られることなく同じターゲットに対して合法的傍受を実行できます。
- GGSN での加入者サービスには影響しません。
- 入力と出力の両方向の傍受をサポートします。
- レイヤ 3 およびレイヤ 2 トラフィックの傍受をサポートします。
- ターゲットに気付かれません。ネットワーク管理者も通話者もパケットがコピーされていることや通話が傍受されていることに気付きません。
- ***Simple Network Management Protocol Version 3（SNMPv3; 簡易ネットワーク管理プロトコル バージョン 3）および View-based Access Control Model（SNMP-VACM-MIB）や User-based Security Model（SNMP-USM-MIB）などのセキュリティ機能を使用して、合法的傍受情報およびコンポーネントへのアクセスを制限します。***
- 合法的傍受に関する情報を、最高特権を持つユーザ以外のユーザから秘匿します。管理者は、特権ユーザが法的傍受情報にアクセスできるアクセス権を設定する必要があります。
- 傍受を実行するための 2 つの保護されたインターフェイスがあります。1 つは傍受の設定用、もう 1 つは傍受したトラフィックの LEA への送信用です。

合法的傍受に使用されるネットワーク コンポーネント

合法的傍受には、次のネットワーク コンポーネントが使用されます。

- **メディエーション デバイス**：メディエーション デバイス（サードパーティ ベンダーから提供される）は、合法的傍受処理のほとんどを処理します。メディエーション デバイスは次の処理を行います。
  - 合法的傍受の設定およびプロビジョニングに使用されるインターフェイスを提供します。
  - 他のネットワーク デバイスに対して、合法的傍受を設定および実行する要求を生成します。

- 傍受したトラフィックを LEA が要求する形式（国によって異なる）に変換し、傍受したトラフィックのコピーをターゲットに気付かれずに LEA に送信します。

（注）　複数の LEA が同じターゲットに対して傍受を実行している場合、メディエーション デバイスは LEA ごとに傍受したトラフィックのコピーを作成する必要があります。メディエーション デバイスには、障害のために中断された合法的傍受を再開する役割もあります。

- **傍受アクセス ポイント**：Intercept Access Point（IAP; 傍受アクセス ポイント）は、合法的傍受に情報を提供するデバイスです。次の 2 つのタイプの IAP があります。
  - Identification（ID）IAP：傍受のための Intercept-Related Information（IRI; 傍受関連情報）（ターゲットのユーザ名、システム IP アドレスなど）を提供する認証、認可、アカウンティング（AAA）サーバなどのデバイス。IRI は、ターゲットのトラフィックが通過するコンテンツ IAP（ルータ）をサービス プロバイダーが判別する場合に有用です。
  - コンテンツ IAP：ターゲットのトラフィックが通過する Cisco 7600 シリーズ ルータなどのデバイス。コンテンツ IAP は次の処理を行います。

    - 司法命令で指定された期間、ターゲットが送受信するトラフィックを傍受します。傍受が気付かれないように、ルータは宛先へのトラフィックの転送を継続します。

    - 傍受したトラフィックのコピーを作成し、ユーザ データグラム プロトコル（UDP）パケットにカプセル化し、ターゲットに気付かれずにメディエーション デバイスにパケットを転送します。

（注）　コンテンツ IAP は、傍受したトラフィックの単一のコピーをメディエーション デバイスに送信します。複数の LEA が同じターゲットに対して傍受を実行している場合、メディエーション デバイスは LEA ごとに傍受したトラフィックのコピーを作成する必要があります。

- **収集機能**：収集機能は、サービス プロバイダーが傍受したトラフィックを格納および処理するプログラムです。このプログラムは、LEA にある機器で実行されます。

合法的傍受処理

監視を実行する司法命令または令状を取得したあと、LEA はターゲットのサービス プロバイダーに監視を要求します。サービス プロバイダーの担当者は、メディエーション デバイスで実行される管理機能を使用して合法的傍受を設定し、ターゲットの電子トラフィックを（司法命令で定義された）特定の期間モニタリングします。

傍受を設定したあとは、ユーザの介入は必要ありません。管理機能が他のネットワーク デバイスと通信し、合法的傍受を設定および実行します。合法的傍受では、次の一連のイベントが発生します。

1. 管理機能は、ID IAP と通信して傍受関連情報（IRI）（ターゲットのユーザ名、システムの IP アドレスなど）を取得し、ターゲットのトラフィックが通過するコンテンツ IAP（ルータ）を判別します。
2. ターゲットのトラフィックを処理するルータを特定したあと、管理機能は SNMPv3 の get および set 要求をルータの Management Information Base（MIB; 管理情報ベース）に送信し、合法的傍受を設定および有効化します。GGSN の合法的傍受 MIB には、CISCO-TAP2-MIB および CISCO-MOBILITY-TAP-MIB があります。

3. 合法的傍受中に、ルータは次の処理を行います。
   a. 着信および発信トラフィックを調べ、合法的傍受要求の指定と一致するトラフィックを傍受します。
   b. 傍受したトラフィックのコピーを作成し、ターゲットが疑いを持たないように元のトラフィックを宛先に転送します。
   c. 傍受したトラフィックを UDP パケットにカプセル化し、そのパケットをターゲットに気付かれずにメディエーション デバイスに転送します。

   （注）　ターゲットのトラフィックの傍受および複製のプロセスによって、トラフィック ストリームに検出可能な遅延が発生することはありません。

4. メディエーション デバイスは、傍受したトラフィックを必要な形式に変換し、LEA で実行される収集機能に送信します。傍受したトラフィックはここに格納されて処理されます。

   （注）　司法命令で許可されていないトラフィックをルータが傍受した場合、メディエーション デバイスは余分なトラフィックをフィルタで除外し、司法命令で許可されたトラフィックだけを LEA に送信します。

5. 合法的傍受の期間が終了すると、ルータはターゲットのトラフィックの傍受を停止します。

合法的傍受 MIB

合法的傍受を実行するために、GGSN は次の MIB を使用します。

- **CISCO-TAP2-MIB**：CISCO-TAP2-MIB には、ルータでの合法的傍受を制御する SNMP 管理オブジェクトが含まれています。メディエーション デバイスはこの MIB を使用して、トラフィックがルータを通過するターゲットに対して合法的傍受を設定および実行します。この MIB は、合法的傍受をサポートするシスコのソフトウェア イメージにバンドルされています。

  CISCO-TAP2-MIB には、ルータで実行される合法的傍受に情報を提供する複数のテーブルが含まれています。

  - cTap2MediationTable：ルータで現在、合法的傍受を実行している各メディエーション デバイスに関する情報が含まれています。各テーブル エントリは、ルータがメディエーション デバイスと通信するために使用する情報（デバイスのアドレス、傍受したトラフィックを送信するインターフェイス、傍受したトラフィックを送信するプロトコルなど）を提供します。
  - cTap2StreamTable：傍受するトラフィックを特定するために使用する情報が含まれています。各テーブル エントリには、合法的傍受のターゲットに関連するトラフィック ストリームを特定するために使用するフィルタへのポインタが含まれています。フィルタに一致するトラフィックが傍受およびコピーされて、対応するメディエーション デバイス アプリケーション（cTap2MediationContentId）に送信されます。
  - テーブルには、傍受されたパケット数のカウント、および傍受する必要があったが傍受されずに廃棄されたパケットのカウントも含まれています。
  - cTap2DebugTable：合法的傍受のエラーをトラブルシューティングするためのデバッグ情報が含まれています。

  CISCO-TAP2-MIB には、合法的傍受イベントの複数の SNMP 通知も含まれています。MIB オブジェクトの詳細については、MIB 自体を参照してください。

（メディエーション デバイスで実行される）管理機能によって、SNMPv3 の **set** および **get** 要求がルータの CISCO-TAP2-MIB に対して発行され、合法的傍受が設定および開始されます。このために、管理機能によって次の処理が実行されます。

a. cTap2MediationTable のエントリを作成し、ルータが傍受を実行するメディエーション デバイスと通信する方法を定義します。

（注） cTap2MediationNewIndex オブジェクトによって、メディエーション テーブル エントリの一意のインデックスが提供されます。

b. cTap2StreamTable にエントリを作成し、傍受するトラフィック ストリームを特定します。

c. cmTapStreamTable にエントリを作成し、cmTapStreamStatus を active (1) に設定します。

d. cTap2StreamInterceptEnable を true(1) に設定し、傍受を開始します。ルータは、傍受期間（cTap2MediationTimeout）が終了するまでストリーム内のトラフィックを傍受します。

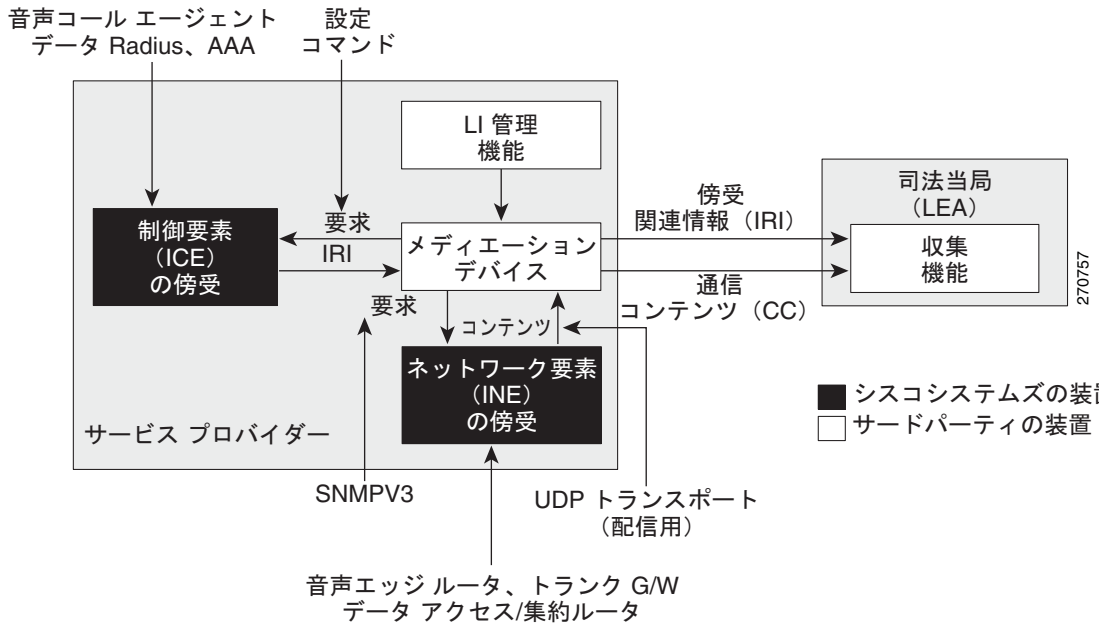
- **CISCO-MOBILITY-TAP-MIB**：CISCO-MOBILITY-TAP-MIB には、モビリティ ゲートウェイ トラフィックで傍受を設定および実行するための SNMP 管理オブジェクトが含まれています。

  CISCO-MOBILITY-TAP-MIB には、傍受するデータ ストリームがリストされた cmtapStreamTable（モビリティ ストリーム テーブル）が含まれています。複数の傍受で同じデータ ストリームが必要になる場合があります。このテーブルには基本的にパケット選択のオプションがあり、その一部だけを使用できます。たとえば、ある加入者が送受信するトラフィックのすべてを傍受する必要がある場合、エントリのリストは、SubscriberID と、傍受するストリームに対応する SubscriberIDType をリストして設定されます（詳細については、CISCO-MOBILITY-TAP-MIB を参照してください）。

合法的傍受トポロジ

次の図は、音声とデータの両方の傍受の合法的傍受トポロジにおける傍受アクセス ポイントおよびインターフェイスを示しています（図 1）。

図 11-1　合法的傍受トポロジ



合法的傍受サポートの設定

ここでは、次の情報について説明します。

前提条件

合法的傍受のサポートを設定するには、次の前提条件を満たす必要があります。

- 最高アクセス レベル（レベル 15）で GGSN にログインしている必要があります。レベル 15 のアクセス権でログインするには、**enable** コマンドを入力し、ルータに対して定義された最高レベルのパスワードを指定します。
- コマンドはグローバル コンフィギュレーション モードで発行する必要があります。グローバル コンフィギュレーション モードを開始するには、**config** を入力します。
- （任意）GGSN がメディエーション デバイスとの通信に使用するインターフェイスについて、ループバック インターフェイスを使用すると役立つ場合があります。
- メディエーション デバイスはプロビジョニングされている必要があります。詳細については、ご使用のメディエーション デバイスに関するベンダーのマニュアルを参照してください。シスコが推奨するメディエーション デバイス機器サプライヤのリストについては、http://www.cisco.com/wwl/regaffairs/lawful_intercept/index.html を参照してください。

セキュリティの考慮事項

合法的傍受サポートについて GGSN を設定する場合は、セキュリティに関する次の問題を考慮してください。

- 合法的傍受の SNMP 通知は、メディエーション デバイス上のユーザ データグラム プロトコル（UDP）ポート 161 に送信する必要があります。ポート 162（簡易ネットワーク管理プロトコル（SNMP）のデフォルト）ではありません。手順については、「Cisco GGSN による合法的傍受の SNMP 通知送信の設定」（P.11-45）を参照してください。
- 合法的傍受 MIB にアクセスできるユーザは、メディエーション デバイス、およびルータでの合法的傍受について知る必要があるシステム管理者だけにします。また、これらのユーザには、合法的傍受 MIB にアクセスするための authPriv または authNoPriv アクセス権が必要です。NoAuthNoPriv アクセス権を持つユーザは、合法的傍受 MIB にアクセスできません。
- デフォルトの SNMP ビューでは次の MIB は除外されています。

  CISCO-TAP2-MIB
  CISCO-MOBILITY-TAP-MIB

設定ガイドラインおよび制限事項

ここでは、合法的傍受の一般的な制限事項と設定ガイドライン、Cisco GGSN 固有のガイドライン、および加入者ごとのガイドラインについて説明します。

- GGSN のパフォーマンスを維持するために、合法的傍受はアクティブ セッションの 0.2% 以下に制限されます。たとえば、GGSN が 4000 セッションを処理している場合、それらのセッションのうち 8 つのセッションを傍受できます。
- **一般的な設定ガイドライン**：GGSN がメディエーション デバイスと通信して合法的傍受を実行するには、次の設定要件を満たしている必要があります。
  - GGSN とメディエーション デバイスの両方のドメイン名が、ドメイン ネーム システム（DNS）に登録されている必要があります。
  - DNS で、ルータの IP アドレスは、通常はルータ上の FastEthernet0/0/0 インターフェイスのアドレスです。
  - メディエーション デバイスに Access Function（AF）および Access Function Provisioning Interface（AFPI）が必要です。
  - メディエーション デバイスを、CISCO-TAP2-MIB ビューにアクセスできる SNMP ユーザ グループに追加する必要があります。グループに追加するユーザとして、メディエーション デバイスのユーザ名を指定します。
  - メディエーション デバイスを CISCO-TAP2-MIB ユーザとして追加するときに、必要に応じてメディエーション デバイスの認可パスワードを指定できます。パスワードの長さは、最低 8 文字である必要があります。
- **MIB ガイドライン**：次の Cisco MIB が合法的傍受処理に使用されます。これらの MIB を合法的傍受 MIB の SNMP ビューに含めて、メディエーション デバイスがルータを通過するトラフィックに対する傍受を設定および実行できるようにします。
  - CISCO-TAP2-MIB：両方のタイプの合法的傍受（通常およびブロードバンド）に必要です。
  - CISCO-MOBILITY-TAP-MIB：モビリティ ゲートウェイ トラフィックに対する傍受に必要です。
- **Cisco GGSN の設定ガイドラインおよび制限事項**：次に、Cisco GGSN での通常の合法的傍受の設定ガイドラインを示します。
  - 合法的傍受では、パケット転送レートに影響を与えずに 6000 パケット / 秒（pps）のレートでトラフィックを傍受できます。この傍受レートには、アクティブな傍受がすべて含まれており、パケットの長さは 150 ～ 200 バイトと想定されています。合法的傍受はプロセッサに負荷がかかるため、傍受レートが 6000 pps を超えると、パケット転送率はわずかに低下します。
  - 合法的傍受は、レイヤ 2 インターフェイスではサポートされません。ただし、合法的傍受では、VLAN インターフェイスがレイヤ 3 インターフェイスで、トラフィックが VLAN インターフェイスによってルーティングされる場合は、レイヤ 2 インターフェイスで実行される VLAN 上のトラフィックを傍受できます。
  - ハードウェア レート制限の対象のパケットは、合法的傍受で次のように処理されます。
  - レート リミッタによって廃棄されるパケットは、傍受または処理されません。
  - レート リミッタを通過するパケットは、傍受および処理されます。

- 複数の司法当局（LEA）が 1 つのメディエーション デバイスを使用しており、それぞれが同じターゲットに対して傍受を実行している場合、ルータは 1 つのパケットをメディエーション デバイスに送信します。各 LEA 用にパケットを複製するのは、メディエーション デバイスの役割です。
- GGSN での合法的傍受は、CISCO-MOBILITY-MIB で記述されている加入者 IMSI 値に基づきます。

合法的傍受 MIB へのアクセス

機密に関係するため、シスコの合法的傍受 MIB は合法的傍受機能をサポートするソフトウェア イメージだけで使用できます。これらの MIB には、Network Management Software MIBs Support ページ（http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からはアクセスできません。

合法的傍受 MIB へのアクセスの制限

合法的傍受 MIB へのアクセスは、メディエーション デバイスおよび合法的傍受について知る必要があるユーザだけに許可する必要があります。これらの MIB へのアクセスを制限するには、次の作業を実行する必要があります。

1. シスコの合法的傍受 MIB を含むビューを作成します。
2. このビューへの読み取りおよび書き込みアクセス権を持つ SNMP ユーザ グループを作成します。このユーザ グループに割り当てられたユーザだけが、MIB の情報にアクセスできます。
3. シスコの合法的傍受ユーザ グループにユーザを追加して、MIB および合法的傍受に関する情報にアクセスできるユーザを定義します。このグループのユーザとして、メディエーション デバイスを追加してください。追加しないと、ルータで合法的傍受を実行できません。

（注） シスコの合法的傍受 MIB ビューへのアクセスは、メディエーション デバイス、およびルータでの合法的傍受について知る必要があるシステム管理者だけに制限する必要があります。MIB にアクセスするには、ルータ上でレベル 15 のアクセス権がユーザに必要です。

SNMPv3 の設定

次の手順を実行するには、GGSN で SNMPv3 が設定されている必要があります。SNMPv3 の設定方法および次の項で説明するコマンドの詳細については、次のシスコのマニュアルを参照してください。

- 『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Part 3: System Management」の「Configuring SNMP Support」。次の URL で入手できます。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.htm
- 『*Cisco IOS Configuration Fundamentals and Network Management Command Reference*』。次の URL で入手できます。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun_r/cfr_1g11.htm

合法的傍受 MIB の制限付き SNMP ビューの作成

シスコの合法的傍受 MIB を含む SNMP ビューを作成し、ユーザを割り当てるには、グローバル コンフィギュレーション モードでレベル 15 のアクセス権を使用して、Command Line Interface（CLI; コマンドライン インターフェイス）で次の手順を実行します。コマンドの例については、「設定例」（P.11-45）を参照してください。

（注）　次の手順のコマンド構文には、各作業の実行に必要なキーワードだけが示されています。コマンド構文の詳細については、前の項（「SNMPv3 の設定」）に記載されているマニュアルを参照してください。

ステップ 1　GGSN で SNMPv3 が設定されていることを確認します。手順については、「SNMPv3 の設定」（P.11-43）に記載されているマニュアルを参照してください。

ステップ 2　CISCO-TAP2-MIB を含む SNMP ビューを作成します（*view_name* は、MIB 用に作成するビューの名前です）。この MIB は、通常とブロードバンドの両方の合法的傍受に必要です。

```
Router(config)# snmp-server view view_name ciscoTap2MIB included
```

ステップ 3　次の MIB を SNMP ビューに追加して、モビリティ ゲートウェイ ストリームに対する傍受のサポートを設定します（*view_name* は、ステップ 2 で作成したビューの名前です）。

```
Router(config)# snmp-server view view_name ciscoMobilityTapMIB included
```

ステップ 4　合法的傍受 MIB ビューにアクセスできる SNMP ユーザ グループ（*groupname*）を作成し、ビューに対するこのグループのアクセス権を定義します。

```
Router(config)# snmp-server group groupname v3 auth read view_name write view_name
notify notify-view
```

ステップ 5　作成したユーザ グループにユーザを追加します（*username* はユーザ、*groupname* はユーザ グループ、*auth_password* は認証パスワード）。

```
Router(config)# snmp-server user username groupname v3 auth md5 auth_password
```

（注）　ユーザを追加する場合、**priv** および **auth** キーワード オプションはどちらも有効なオプションです。

（注）　SNMP ユーザ グループにメディエーション デバイスを追加してください。追加しないと、ルータで合法的傍受を実行できません。合法的傍受 MIB ビューへのアクセスは、メディエーション デバイス、およびルータでの合法的傍受について知る必要があるシステム管理者だけに制限する必要があります。

ステップ 6　ユーザが接続を許可されるホストを指定します。

```
Router(config)# snmp-server host ip-address version 3 auth user-name
```

ステップ 7　エンジン ID を指定します。

```
Router(config)# snmp-server engineID local engine-ID
```

これで、メディエーション デバイスは合法的傍受 MIB にアクセスして、SNMP の **set** および **get** 要求を発行し、ルータ上で合法的傍受を設定および実行できるようになります。

SNMP 通知をメディエーション デバイスに送信するためのルータの設定方法については、「Cisco GGSN による合法的傍受の SNMP 通知送信の設定」（P.11-45）を参照してください。

設定例

次のコマンドは、メディエーション デバイスが合法的傍受 MIB にアクセスできるようにする方法の例です。

```
Router(config)# snmp-server view tapV ciscoTap2MIB included
Router(config)# snmp-server view tapV ciscoMobilityTapMIB included
Router(config)# snmp-server group tapGrp v3 auth read tapV write tapV notify tapV
Router(config)# snmp-server user ss8user tapGrp v3 auth md5 ss8passwd
Router(config)# snmp-server host 172.10.10.1 version 3 auth ss8usr
Router(config)# snmp-server engineID local 0123467891
```

1. 適切な合法的傍受 MIB（CISCO-TAP2-MIB および CISCO-MOBILITY-TAP-MIB）を含むビュー（tapV）を作成します。
2. tapV ビューの MIB への読み取り、書き込み、および通知アクセス権を持つユーザ グループ（tapGrp）を作成します。
3. メディエーション デバイス（ss8user）をユーザ グループに追加し、パスワード（ss8passwd）を使用して MD5 認証を指定します。
4. （任意）管理用に 24 文字の SNMP エンジン ID（123400000000000000000000 など）をルータに割り当てます。エンジン ID を指定しない場合は、自動的に生成されます。上記の例の最後の行に示されているように、エンジン ID の後ろのゼロは省略できます。

（注） エンジン ID を変更すると、SNMP ユーザ パスワードおよびコミュニティ ストリングに影響します。

Cisco GGSN による合法的傍受の SNMP 通知送信の設定

SNMP では、合法的傍受イベントの通知が自動的に生成されます（表 11-2 を参照）。これは、cTap2MediationNotificationEnable オブジェクトのデフォルト値が true(1) であるためです。

メディエーション デバイスに合法的傍受通知を送信するように GGSN を設定するには、グローバル コンフィギュレーション モードでレベル 15 のアクセス権を使用して、次のコマンドを発行します（*MD-ip-address* はメディエーション デバイスの IP アドレス、*community-string* は通知要求とともに送信するパスワードに似たコミュニティ ストリング）。

```
Router(config)# snmp-server host MD-ip-address community-string udp-port 161 snmp
```

- 合法的傍受では、**udp-port** は 161 である必要があります。162（SNMP のデフォルト）ではありません。

表 11-2 は、合法的傍受イベント用に生成される SNMP 通知を示しています。

表 11-2　合法的傍受イベントの SNMP 通知

通知	説明
cTap2MIBActive	ルータは、CISCO-TAP2-MIB に設定されたトラフィック ストリームのパケットを傍受する準備ができています。
cTap2MediationTimedOut	合法的傍受が終了しました（cTap2MediationTimeout の期限切れのためなど）。
cTap2MediationDebug	cTap2MediationTable のエントリに関するイベントのデバッグ情報。
cTap2StreamDebug	cTap2StreamTable のエントリに関するイベントのデバッグ情報。
cTap2Switchover	冗長でアクティブな Route Processor（RP; ルートプロセッサ）がスタンバイ モードになります。スタンバイはアクティブな RP です。

SNMP 通知のディセーブル

次の手順で、GGSN での SNMP 通知をディセーブルにすることができます。

- すべての SNMP 通知をディセーブルにするには、**no snmp-server enable traps** コマンドを発行します。
- 合法的傍受通知をディセーブルにするには、SNMPv3 を使用して CISCO-TAP2-MIB オブジェクト cTap2MediationNotificationEnable を false(2) に設定します。合法的傍受通知を SNMPv3 で再度イネーブルにするには、このオブジェクトを true(1) にリセットします。

設定例

ここでは、GGSN でのセキュリティに関する次の設定例を示します。

- 「AAA のセキュリティ設定例」（P.11-47）
- 「RADIUS サーバのグローバル設定例」（P.11-47）
- 「RADIUS サーバ グループの設定例」（P.11-47）
- 「RADIUS 応答メッセージの設定例」（P.11-49）
- 「アドレス確認およびモバイル間トラフィック リダイレクションの例」（P.11-50）
- 「定期アカウンティング タイマーの例」（P.11-53）

AAA のセキュリティ設定例

次の例は、ルータで AAA セキュリティをグローバルにイネーブルにする方法、およびグローバルな RADIUS 認証および認可を指定する方法を示しています。

```
! Enables AAA globally
aaa new-model
!
! Creates a local authentication list for use on
! serial interfaces running PPP using RADIUS
!
aaa authentication ppp abc group abc
!
! Enables authorization and creates an authorization
! method list for all network-related service requests
! and enables authorization using a RADIUS server
!
aaa authorization network network abc group abc
```

AAA の設定の詳細については、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

RADIUS サーバのグローバル設定例

次の例は、ルータで RADIUS サーバ通信をグローバルに設定する方法を示しています。

```
! Specifies a global RADIUS server host at IP address 10.100.0.2
! Port 1645 is destination port for authentication requests
! Port 1646 is the destination port for accounting requests
! Specifies the key "abc" for this radius host only
!
radius-server host 10.100.0.2 auth-port 1645 acct-port 1646 key abc
!
! Sets the authentication and encryption key to mykey for all
! RADIUS communications between the router and the RADIUS daemon
!
radius-server key mykey
```

（注）　**radius-server host** コマンドは複数回設定できますが、Cisco IOS ソフトウェアでは、同じ IP アドレスでサポートされる RADIUS サーバは 1 つだけです。

RADIUS セキュリティの設定の詳細については、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

RADIUS サーバ グループの設定例

次の設定例は、**aaa group server** コマンドで示されているように、GGSN 上に 4 つの AAA サーバ グループ abc、abc1、abc2、および abc3 を定義しています。

gprs default aaa-group コマンドを使用して、これらのサーバ グループのうちの 2 つがデフォルト サーバ グループとしてグローバルに定義されています。abc2 が認証用、abc3 がアカウンティング用です。

認証がイネーブルにされた access-point 1 では、デフォルトのグローバル認証サーバ グループ abc2 は上書きされ、サーバ グループ abc が APN で認証サービスを提供するように指定されています。このアクセス ポイントではアカウンティング サービスは明示的には設定されていませんが、認証がイネーブルであるため、自動的にイネーブルになります。グローバルに定義されたアカウンティング サーバ グループが定義されているため、サーバ abc3 がアカウンティング サービスに使用されます。

aaa-accounting enable コマンドを使用してアカウンティングがイネーブルにされた access-point 4 では、デフォルトのアカウンティング サーバ グループ abc3 は上書きされ、サーバ グループ abc1 が APN でアカウンティング サービスを提供するように指定されています。

access-point 5 は、透過的アクセス モード用に設定されているため、AAA サービスをサポートしていません。

```
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server groups
!
aaa group server radius abc
 server 10.2.3.4 auth-port 1645 acct-port 1646
 server 10.6.7.8 auth-port 1645 acct-port 1646
aaa group server radius abc1
 server 10.10.0.1 auth-port 1645 acct-port 1646
aaa group server radius abc2
 server 10.2.3.4 auth-port 1645 acct-port 1646
 server 10.10.0.1 auth-port 1645 acct-port 1646
aaa group server abc3
 server 10.6.7.8 auth-port 1645 acct-port 1646
 server 10.10.0.1 auth-port 1645 acct-port 1646
!
! Configures AAA authentication
! and authorization
!
aaa authentication ppp abc group abc
aaa authentication ppp abc2 group abc2
aaa authorization network abc group abc
aaa accounting network abc start-stop group abc
aaa accounting network abc1 start-stop group abc1
aaa accounting network abc2 start-stop group abc2
aaa accounting network abc3 start-stop group abc3
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
!
! Specifies a RADIUS server group
! for use by the GGSN to authenticate
! mobile users at this access point
!
  aaa-group authentication abc
!
 access-point 4
  access-point-name www.pdn2.com
!
! Enables AAA accounting services
!
  aaa-accounting enable
!
! Specifies a RADIUS server group
! for use by the GGSN for accounting
! services at this access point
```

```
  aaa-group accounting abc1
!
 access-point 5
  access-point-name www.pdn3.com
!
! Configures default AAA server
! groups for the GGSN for authentication
! and accounting services
!
gprs default aaa-group authentication abc2
gprs default aaa-group accounting abc3
!
! Configures global RADIUS server hosts
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.10.0.1 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

（注）　**radius-server host** コマンドは複数回設定できますが、Cisco IOS ソフトウェアでは、同じ IP アドレスでサポートされる RADIUS サーバは 1 つだけです。

RADIUS 応答メッセージの設定例

次の例では、GGSN が PDP コンテキストの作成要求を SGSN に送信する前に、RADIUS サーバからの RADIUS アカウンティング応答を待機するようにグローバルに設定されています。GGSN は、access-point 1 を除くすべてのアクセス ポイントで受信された PDP コンテキスト要求の応答を待機します。RADIUS 応答メッセージ待機は、access-point 1 では **no gtp response-message wait-accounting** コマンドを使用して上書きされています。

```
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius abc
 server 10.2.3.4 auth-port 1645 acct-port 1646
 server 10.6.7.8 auth-port 1645 acct-port 1646
!
! Configures AAA authentication
! and authorization
!
aaa authentication ppp abc group abc
aaa authorization network abc group abc
aaa accounting network abc start-stop group abc
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication abc
!
```

```
! Disables waiting for RADIUS response
! message at APN 1
!
  no gtp response-message wait-accounting
  exit
access-point 2
 access-mode non-transparent
 access-point-name www.pdn2.com
 aaa-group authentication abc
!
! Enables waiting for RADIUS response
! messages across all APNs (except APN 1)
!
gprs gtp response-message wait-accounting
!
! Configures global RADIUS server hosts
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

アドレス確認およびモバイル間トラフィック リダイレクションの例

次の例は、IPv4 アドレス確認をイネーブルにし、IPv4 モバイル間トラフィックが外部デバイスにリダイレクトされるように指定する方法を示しています。

GGSN 設定

```
service gprs ggsn
!
hostname t7600-7-2
!
ip cef
!
ip vrf vpn4
 description abc_vrf
 rd 104:4
!
!
interface Loopback2
 description USED FOR DHCP2 - range IN dup prot range
 ip address 111.72.0.2 255.255.255.255
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.2
 description Ga/Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 103
 ip vrf forwarding vpn4
```

```
 ip address 10.1.3.72 255.255.255.0
 no cdp enable
!
interface GigabitEthernet0/0.95
 description CNR and CAR
 encapsulation dot1Q 95
 ip address 10.2.25.72 255.255.255.0
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
! In case the ms is on another SAMI GGSN
ip route vrf vpn4 0.0.0.0 0.0.0.0 10.1.3.1
!
gprs access-point-list gprs
  access-point 7
   access-point-name ms_redirect.com
   ip-address-pool dhcp-proxy-client
   aggregate auto
   dhcp-server 10.2.25.90
   dhcp-gateway-address 111.72.0.2
   vrf vpn4
   ! In case the ms is on this GGSN.
   redirect intermobile ip 10.1.3.1
   !
```

スーパーバイザ エンジン設定

```
hostname 7600-a

interface FastEthernet9/15
 description OUT to Firewall
 no ip address
 duplex half
 switchport
 switchport access vlan 162
!
interface FastEthernet9/16
 description In from Firewall
 no ip address
 switchport
 switchport access vlan 163
!
interface Vlan103
 description Vlan to GGSN redirect to FW
 ip address 10.1.3.1 255.255.255.0
 ip policy route-map REDIRECT-TO-FIREWALL
!
interface Vlan162
 ip address 162.1.1.1 255.255.255.0
!
interface Vlan163
 ip address 163.1.1.1 255.255.255.0
!
ip route 111.72.0.0 255.255.0.0 10.1.3.72
ip route 111.73.0.0 255.255.0.0 10.1.3.73
ip route 111.74.0.0 255.255.0.0 10.1.3.74
ip route 111.75.0.0 255.255.0.0 10.1.3.75
ip route 111.76.0.0 255.255.0.0 10.1.3.76
!
access-list 102 permit ip any any
```

```
!
route-map REDIRECT-TO-FIREWALL permit 10
 match ip address 102
 set ip next-hop 162.1.1.11
```

VRF を使用したプライベート RADIUS サーバへのアクセスの設定例

次の例は、VRF を使用したプライベート RADIUS サーバへのアクセスの設定例を示しています。

GGSN 設定

```
aaa new-model
!

aaa group server radius vrf_aware_radius
 server-private 99.100.0.2 auth-port 1645 acct-port 1646 key cisco
 ip vrf
!
aaa authentication ppp vrf_aware_radius group vrf_aware_radius
aaa authorization network default local group radius
aaa authorization network vrf_aware_radius group vrf_aware_radius
aaa accounting network vrf_aware_radius start-stop group vrf_aware_radius
aaa session-id common

!
ip vrf vpn2
 rd 101:1
!
interface Loopback1
 ip address 150.1.1.72 255.255.0.0
!
interface Tunnel2
 ip vrf forwarding vpn2
 ip address 80.80.72.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 167.2.1.12
!
ip local pool vpn2_pool 100.72.0.1 100.72.255.255 group vpn2
ip route vrf vpn2 0.0.0.0 0.0.0.0 Tunnel2
!
gprs access-point-list gprs
  access-point 1
   access-point-name apn.vrf2.com
   access-mode non-transparent
   aaa-group authentication vrf_aware_radius
   aaa-group accounting vrf_aware_radius
   ip-address-pool local vpn2_pool
   aggregate 100.72.0.0 255.255.0.0
   vrf vpn2
   !
```

スーパーバイザ エンジン設定

```
...
!
interface FastEthernet9/5
 switchport
 switchport access vlan 167
!

interface Vlan167
 ip address 167.1.1.1 255.255.0.0
```

```
!
ip route 150.1.1.72 255.255.255.255 10.1.1.72
ip route 167.2.0.0 255.255.0.0 167.1.1.12
!
...
```

定期アカウンティング タイマーの例

次の例は、APN レベルで、およびグローバルに設定された定期アカウンティング タイマーを示しています。

```
gprs default aaa-accounting interim periodic 60
!
gprs access-point-list APLIST
  access-point 100
   access-point-name peracct.com
   access-mode non-transparent
   aaa-accounting interim update
   aaa-accounting interim periodic 15
   aaa-group authentication radaccess
   aaa-group accounting default
   ip-address-pool radius-client
   gtp response-message wait-accounting
!
```

CHAPTER 12

GGSN でのダイナミック アドレッシングの設定

この章では、Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）でダイナミック IP アドレッシングを設定する方法について説明します。

（注） この章に記載されている作業は、IPv4 Packet Data Protocol（PDP; パケット データ プロトコル）のコンテキストにだけ適用されます。IPv6 アドレッシングの情報については、第 4 章「GGSN での IPv6 PDP サポートの設定」を参照してください。

この章に記載されている GGSN コマンドの詳細については、使用している Cisco GGSN リリースの『*Cisco GGSN Command Reference*』を参照してください。この章に記載されているその他のコマンドのマニュアルを参照するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

この章は、次の内容で構成されています。

GGSN でのダイナミック IP アドレッシングの概要

GGSN を設定して、Public Data Network（PDN; 公衆データ網）にアクセスする必要があるモバイル ステーション ユーザに IP アドレスを割り当てる方法には、次の 3 つの方法があります。Dynamic Host Configuration Protocol（DHCP）割り当て、Remote Authentication Dial-In User Service（RADIUS）割り当て、および Access Point Name（APN; アクセス ポイント ネーム）で設定されるかまたはダウンロードされるローカル IP アドレス プール割り当ての 3 つです。

ダイアミック IP アドレッシングの方法は、グローバルか、またはアクセス ポイント コンフィギュレーション レベルで設定できます。

ネットワークで使用されている IP アドレス割り当てのタイプをサポートするには、次の設定ガイドラインが満たされていることを確認してください。

- DHCP IP アドレス割り当て
  - ループバック インターフェイスと同じサブネットに対して、割り当て対象のアドレスの範囲を設定してください。
  - RADIUS サーバのユーザ用の IP アドレスを設定しないでください。
  - PPP 仮想テンプレート インターフェイスで、**peer default ip address dhcp** コマンドを指定します。
  - GGSN で、**aaa authorization network** *method_list* **none** コマンドを指定します。
- RADIUS IP アドレス割り当て
  - 完全な username@domain フォーマットを使用して、RADIUS サーバにユーザを設定します。
  - PPP 仮想テンプレート インターフェイスで、**no peer default ip address** コマンドを指定します。
  - GGSN での RADIUS サービスの設定については、このマニュアルの「GGSN でのセキュリティの設定」を参照してください。
- ローカル プール IP アドレス割り当て
  - **ip local pool** コマンドを使用してローカル プールを設定してください。
  - GGSN で、**aaa authorization network** *method_list* **none** コマンドを指定します。
  - **peer default ip address pool** *pool-name* コマンドを指定します。

（注） Cisco 7600 プラットフォームでは、DHCP サーバ方式または RADIUS サーバ方式を使用してダイナミック アドレス割り当てを行うには、DHCP サーバまたは RADIUS サーバが、スーパーバイザ エンジンからルーティング可能なレイヤ 3 である必要があります。

GGSN での DHCP の設定

Cisco IOS ソフトウェア内でローカル DHCP サービスを使用したり、Cisco Network Registrar（CNR）などの外部 DHCP サーバを使用するように GGSN を設定したりできます。Cisco IOS ソフトウェアでの内部 DHCP サービスの設定については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』を参照してください。

DHCP サーバは次の 2 つの方法で指定できます。

- グローバル コンフィギュレーション レベルで **gprs default dhcp-server** コマンドを使用
- アクセス ポイント コンフィギュレーション レベルで **dhcp-server** コマンドを使用

GGSN で DHCP サポートを設定するには、**gprs default ip-address-pool** グローバル コンフィギュレーション コマンドまたは **ip-address-pool** アクセス ポイント コンフィギュレーション コマンドを **dhcp-proxy-client** キーワード オプションとともに設定する必要があります。

アクセス ポイントを DHCP プロキシ クライアント サービス用に設定したあと、**dhcp-server** アクセス ポイント コンフィギュレーション コマンドを使用して、DHCP サーバを指定します。

DHCP サーバの IP アドレスを指定するには、*ip-address* 引数を使用します。プライマリ DHCP サーバが使用できない場合に使用するバックアップ DHCP サーバの IP アドレスを指定するには、任意で 2 番めの *ip-address* 引数を指定できます。バックアップ DHCP サーバを指定しない場合、バックアップ DHCP サーバは使用できません。

dhcp-server コマンドを使用してアクセス ポイント レベルで DHCP サーバを指定する場合、アクセス ポイントで指定されたサーバ アドレスによって、グローバル レベルで指定されたアドレスが上書きされます。アクセス ポイント レベルで DHCP サーバを指定しない場合は、グローバル レベルで指定されたアドレスが使用されます。

このため、アクセス ポイントごとに別々の DHCP サーバを使用する必要がある場合は、グローバル アドレス設定と、1 つまたは複数のローカル アクセス ポイント レベル設定を指定できます。

DHCP サーバ自体が GGSN で Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）インターフェイスのアドレス スペース内に配置されている場合は、**vrf** キーワードを使用します。DHCP サーバが VRF アドレス スペース内に配置されている場合は、**dhcp-gateway-address** に対応するループバック インターフェイスも VRF アドレス スペース内に設定する必要があります。

ここでは、次の情報について説明します。

DHCP サーバ通信のグローバルな設定

ここでは、モバイル ユーザに IP アドレスを割り当てるために GGSN で使用できるグローバル DHCP サーバ ホストの設定方法について説明します。GGSN グローバル コンフィギュレーション レベルで追加の DHCP サーバ通信を設定できます。

ルータ上または Cisco IOS ソフトウェアのインスタンス上で DHCP サーバ通信をグローバルに設定するには、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
ステップ 1	`Router(config)# ip address-pool {dhcp-proxy-client | local}`	IP アドレス プールのメカニズムを指定します。 • **dhcp-proxy-client**：サード パーティ DHCP サーバと、ルータまたは IOS インスタンスに接続しているピアとの間のプロキシ クライアントとして、ルータまたは Cisco IOS ソフトウェアのインスタンスを指定します。 • **local**：「default」という名前のローカル アドレス プールを指定します。 （注）　**ip address-pool** コマンドにデフォルトのオプションはありません。**local** キーワードを使用してローカル アドレス プールを設定する場合、ステップ 4 およびステップ 5 の任意のコマンドも設定できます。
ステップ 2	`Router(config)# ip dhcp-server {ip-address | name}`	DHCP サーバの IP アドレスまたは名前を指定します。

	コマンド	目的
ステップ 3	`Router(config)# ip dhcp excluded address low-address [high-address]`	（任意）DHCP サーバで DHCP クライアントに割り当ててはならない IP アドレスを指定します。 • *low-address*：除外されるアドレス範囲の最初の IP アドレスを指定します。このアドレスは、通常、DHCP サーバ自体のアドレスです。 • *high-address*：（任意）除外されるアドレス範囲の最後の IP アドレスを指定します。
ステップ 4	`Router(config)# ip dhcp pool name`	（任意：**ip address-pool local** コマンドだけがサポートされています。） DHCP アドレス プールを設定し、DHCP プール コンフィギュレーション モードを開始します。*name* には、シンボリック ストリング（「engineering」など）または整数（0 など）を指定できます。
ステップ 5	`Router(config-dhcp)# network network-number [mask | /prefix-length]`	（任意：**ip address-pool local** コマンドだけがサポートされています。） DHCP アドレス プールのサブネットのネットワーク数およびマスクを指定します。 プレフィクス長には、アドレス プレフィクスのビット数を指定します。プレフィクスを使用してクライアントのネットワーク マスクを指定することもできます。プレフィクス長には、先頭にスラッシュ（/）を挿入する必要があります。

グローバル DHCP サービスの設定については、『*Cisco IOS IP Configuration Guide*』、『*Cisco IOS IP Command References*』、および『*Cisco IOS Dial Technologies Command Reference*』を参照してください。

GGSN グローバル コンフィギュレーション レベルでの DHCP の設定

GGSN での DHCP 設定を完了するには、GGSN グローバル コンフィギュレーション レベルで DHCP を設定します。GGSN コンフィギュレーション レベルで DHCP を設定すると、すべてのアクセス ポイントまたは特定のアクセス ポイントに対して DHCP サーバ通信を設定できます。

GGSN コンフィギュレーション レベルで DHCP を設定するには、次の作業を実行します。

- 「ループバック インターフェイスの設定」（P.12-5）（必須）
- 「すべてのアクセス ポイントに対する DHCP サーバの指定」（P.12-5）（任意）
- 「特定のアクセス ポイントの DHCP サーバの指定」（P.12-6）（任意）

ループバック インターフェイスの設定

アクセス ポイントで DHCP サービス用に DHCP ゲートウェイ アドレスを設定する場合や、DHCP 用に GGSN のアクセス ポイント全体で一意であるスーパーネットをサポートする場合は、一意のネットワークごとにループバック インターフェイスを設定する必要があります。

ループバック インターフェイスは、常に稼動しているインターフェイスをエミュレートするソフトウェア専用インターフェイスであり、すべてのプラットフォームでサポートされている仮想インターフェイスです。インターフェイス数は、作成または設定するループバック インターフェイスの数です。作成できるループバック インターフェイスの数に制限はありません。

GGSN でループバック インターフェイスを設定するには、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
ステップ 1	`Router(config)# interface loopback` *interface-number*	GGSN でループバック インターフェイスを定義します。*interface-number* によって、ループバック インターフェイスが識別されます。
ステップ 2	`Router(config-if)# ip address` *ip-address mask* [**secondary**]	インターフェイスの IP アドレスを指定します。 • *ip-address*：インターフェイスの IP アドレスをドット付き 10 進表記で指定します。 • *mask*：サブネット マスクをドット付き 10 進表記で指定します。 • **secondary**：セカンダリ IP アドレスとしてアドレスを設定することを指定します。このキーワードを省略すると、設定したアドレスがプライマリ IP アドレスになります。 （注）　*ip-address* は、アクセス ポイントの DHCP ゲートウェイ アドレスの IP アドレスに対応しています。マスクは、**dhcp-gateway-address** の値に正確に一致するように 255.255.255.255 にする必要があります。

すべてのアクセス ポイントに対する DHCP サーバの指定

DHCP アドレス割り当てを処理する場合、GGSN では、最初に DHCP サーバがアクセス ポイント コンフィギュレーション レベルで指定されているかどうかがチェックされます。サーバが指定されている場合、GGSN では、アクセス ポイントで指定されている DHCP サーバが使用されます。アクセス ポイント コンフィギュレーション レベルで DHCP サーバが指定されていない場合は、デフォルトの GGSN DHCP サーバが使用されます。

すべての GGSN アクセス ポイントに対して DHCP サーバを指定するには、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
ステップ 1	`Router(config)# gprs default ip-address-pool {dhcp-proxy-client | radius-client | disable}`	GGSN の IP アドレス プールを使用して、ダイナミック アドレス割り当て方法を指定します。 • **dhcp-proxy-client** : GGSN で、Mobile Station（MS; モバイル ステーション）用の IP アドレスを DHCP サーバからダイナミックに取得するように指定します。DHCP サービスをイネーブルにするには、このキーワードを使用します。 • **radius-client** : GGSN で、MS 用の IP アドレスを RADIUS サーバからダイナミックに取得するように指定します • **disable** : GGSN によるダイナミック アドレス割り当てをディセーブルにします。 このコマンドにデフォルト オプションはありません。
ステップ 2	`Router(config)# gprs default dhcp-server {ip-address | name} [{ip-address | name}]`	GGSN の IP アドレスの取得元となるプライマリ（およびバックアップ）DHCP サーバで、モバイル ユーザに対してリースが行われるように指定します。 • *ip-address* : DHCP サーバの IP アドレスを指定します。2 番め（任意）の *ip-address* 引数には、バックアップ DHCP サーバの IP アドレスを指定します。 • *name* : DHCP サーバのホスト名を指定します。2 番め（任意）の *name* 引数には、バックアップ DHCP サーバのホスト名を指定します。

特定のアクセス ポイントの DHCP サーバの指定

すべてのアクセス ポイントに対して設定されたデフォルトの DHCP サーバを上書きするには、特定のアクセス ポイントに別の DHCP サーバを指定します。デフォルトの GGSN DHCP サーバを設定しないように選択した場合は、アクセス ポイントごとに DHCP サーバを指定できます。

特定のアクセス ポイントに対して DHCP サーバを指定するには、アクセス ポイント 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
ステップ 1	`Router(config-access-point)# ip-address-pool {dhcp-proxy-client | radius-client | local pool-name | disable}`	（任意）IP アドレス プールを使用するダイナミック アドレス割り当て方法を現在のアクセス ポイントのために指定します。使用できるオプションは次のとおりです。 • **dhcp-proxy-client**：DHCP サーバが IP アドレス プールを提供します。 • **radius-client**：RADIUS サーバが IP アドレス プールを提供します。 • **local**：ローカル プールが IP アドレスを提供することを指定します。このオプションを機能させるには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用して、ローカル プールを設定する必要があります。 • **disable**：ダイナミック アドレス割り当てをオフにします。 **（注）** ダイナミック アドレス割り当て方法を使用している場合は、適切な IP アドレス プール ソースに従ってこのコマンドを設定する必要があります。
ステップ 2	`Router(config-access-point)# dhcp-server {ip-address} [ip-address] [vrf]`	GGSN で IP アドレスを取得するために特定のアクセス ポイントで使用されるプライマリ（およびバックアップ）DHCP サーバで、モバイル ユーザが PDN にアクセスできるようにリースが行われるよう指定します。 • *ip-address*：DHCP サーバの IP アドレスを指定します。2 番め（任意）の *ip-address* 引数には、バックアップ DHCP サーバの IP アドレスを指定します。 • **vrf**：DHCP サーバによって、APN に関連付けられた VPN ルーティングおよび転送（VRF）テーブルが使用されます。
ステップ 3	`Router(config-access-point)# dhcp-gateway-address ip-address`	特定の PDN アクセス ポイントに接続する MS ユーザの DHCP 要求に対して、DHCP サーバからアドレスが返されるサブネットを指定します。 **（注）** DHCP ゲートウェイ アドレスと同じ IP アドレスで、対応するループバック インターフェイスを設定する必要があります。

ローカル DHCP サーバの設定

（注）　Cisco 7600 プラットフォームでローカル DHCP サーバを使用することは推奨していません。

ほとんどのネットワークで外部 DHCP サーバ（Cisco Network Registrar（CNR）によって使用可能な DHCP サーバなど）が使用されていますが、GGSN では、内部 DHCP サービスも設定できます。GGSN でローカル DHCP サービスを使用する場合、内部 DHCP 応答時間を向上させるために、いくつかのコマンドを設定する必要があります。

GGSN でローカル DHCP サービスを最適化するには、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
ステップ 1	`Router(config)# ip dhcp ping packets 0`	ping 操作の一部として、Cisco IOS DHCP サーバからプール アドレスに 0 個のパケットが送信されるように指定します。
ステップ 2	`Router(config)# ip dhcp ping timeout 100`	Cisco IOS DHCP サーバでアドレス プールからの ping 応答に対して 100 ミリ秒間待機するように指定します。

設定例

次の例は、グローバル コンフィギュレーション モードで **ip vrf** コマンドを使用した vpn3（トンネリングなし）の VRF 設定を示しています。**ip vrf** コマンドによって VRF ルーティング テーブルと CEF ルーティング テーブルの両方が確立されるため、すべてのインターフェイスで CEF スイッチングをイネーブルにするために、**ip cef** もグローバル コンフィギュレーション レベルで設定されることに注意してください。

次に示すその他の設定要素でも、vpn3 という名前の同一の VRF を関連付ける必要があります。

- FastEthernet0/0 は、**ip vrf forwarding** インターフェイス コンフィギュレーション コマンドを使用して、Gi インターフェイスとして設定されます。
- アクセス ポイント 2 では、**vrf** コマンド アクセス ポイント コンフィギュレーション コマンドを使用して、VRF が実装されます。

アクセス ポイント 2 の DHCP サーバも VRF をサポートするように設定されています。アクセス ポイント 1 は同じ DHCP サーバを使用していますが、VRF アドレス スペースをサポートしていないことに注意してください。アクセス ポイント 1 の IP アドレスは、グローバル ルーティング テーブルに適用されます。

```
aaa new-model
!
aaa group server radius abc
 server 10.2.3.4
 server 10.6.7.8
!
aaa authentication ppp abc group abc
aaa authorization network abc group abc
aaa accounting network abc start-stop group abc
!
ip cef
!
ip vrf vpn3
```

```
 rd 300:3
!
interface Loopback1
 ip address 10.30.30.30 255.255.255.255
!
interface Loopback2
 ip vrf forwarding vpn3
 ip address 10.27.27.27 255.255.255.255
!
interface FastEthernet0/0
 ip vrf forwarding vpn3
 ip address 10.50.0.1 255.255.0.0
 duplex half
!
interface FastEthernet1/0
 ip address 10.70.0.1 255.255.0.0
 duplex half
!
interface loopback 1
 ip address 10.8.0.1 255.255.255.0
!
interface Virtual-Template1
 ip unnumber loopback 1
 encapsulation gtp
 gprs access-point-list gprs
!
ip route 10.10.0.1 255.255.255.255 Virtual-Template1
ip route vrf vpn3 10.100.0.5 255.255.255.0 fa0/0 10.50.0.2
ip route 10.200.0.5 255.255.255.0 fa1/0 10.70.0.2
!
no ip http server
!
gprs access-point-list gprs
 access-point 1
  access-point-name gprs.pdn.com
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.200.0.5
  dhcp-gateway-address 10.30.30.30
  network-request-activation
  exit
  !
 access-point 2
  access-point-name gprs.pdn2.com
  access-mode non-transparent
  ip-address-pool dhcp-proxy-client
  dhcp-server 10.100.0.5 10.100.0.6 vrf
  dhcp-gateway-address 10.27.27.27
  aaa-group authentication abc
  vrf vpn3
  exit
!
gprs default ip-address-pool dhcp-proxy-client
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

GGSN でのローカル プールによる MS アドレッシングの設定

PDP コンテキストの数が増えると、ローカルに設定されたアドレス プールによる IP アドレスの割り当てによって、PDP コンテキストのアクティベーション レートが増加します。アドレスがローカル プールを使用して MS に割り当てられるかどうかは、アクセス ポイント コンフィギュレーション レベルで指定されます。IP アドレスのローカル プールは、**ip local pool** コンフィギュレーション コマンドを使用して GGSN で設定されている必要があります。

ホールドバック タイマー

IP ローカル プールのホールドバック タイマー機能（**recycle delay** キーワード オプション）を使用すると、新しく解放された IP アドレスが再割り当て可能になるまでに保持される特定の時間を設定できます。この機能により、PDP セッションの削除後に新しく解放された IP アドレスは、IP とユーザの関連付けがシステムのすべてのバックエンド コンポーネントから削除されてから、別の PDP コンテキストに再割り当てされるようになります。IP アドレスが即座に新しい PDP コンテキストに再割り当てされると、バックエンド システムで新しいユーザが誤って前のユーザの記録に関連付けられるおそれがあります。これにより、新しいユーザの課金情報やサービスへのアクセス情報が誤って前のユーザに関連付けられることになります。

ホールドバック機能は、プール要素のデータ構造に追加された新しいタイムスタンプ フィールドをサポートすることによって提供されます。アドレスが再割り当て可能になっている場合に、特定のアドレスを割り当てる要求が出されると、現在の時刻と要素のタイムスタンプ フィールドが照合されます。数値が recycle delay に設定された秒数以上である場合は、アドレスが再割り当てされます。

最初のフリー アドレスをフリー キューから割り当てる要求が出されると、現在のタイムスタンプと要素に格納されたタイムスタンプの差が計算されます。数値が recycle delay の設定値以上である場合は、アドレスが割り当てられます。数値が recycle delay の設定値を下回っている場合、その要求に対するアドレス割り当ては実行されません（フリー キューは First-In First-Out（FIFO）キューです。このため、他のすべての要素には、最初の要素より大きな recycle delay 値が指定されます）。

IP アドレスが一定期間保持されることによって、アドレス割り当てがブロックされると、ブロックされたアドレス割り当てのカウント（ローカル プールで保持されます）は増加します。

（注）　ホールドバック タイマー機能では、IPv6 ローカル プールはサポートされていません。

ローカル IP アドレス プールを設定するには、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
ステップ 1	`Router(config)#ip local pool {default | pool-name low-ip-address [high-ip-address]} [recycle delay seconds]`	リモート ピアがポイントツーポイント インターフェイスに接続するときに使用される IP アドレスのローカル プールを設定します。 • **default**：他のプールが指定されていない場合は、デフォルトのローカル アドレス プールが使用されます。 • *pool-name*：特定のローカル アドレス プールの名前。 • *low-ip-address*：プール内で最小の IP アドレス。 • *high-ip-address*：（任意）プール内で最大の IP アドレス。この値を省略すると、low-ip-address IP アドレス引数がローカル プールに組み込まれます。 • **recycle delay** *seconds*：（任意）アドレスが再割り当て可能になるまでの保持時間（秒）。

ローカル プールをアクセス ポイントに割り当てるには、アクセス ポイント 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
ステップ 1	`Router(config-access-point)# ip-address-pool local pool-name`	（任意）ローカル プールによって IP アドレスが提供されるように指定します。

（注）　アクセス ポイントで VRF を使用すると、同じ IP アドレス プール（オーバーラッピング アドレス）を使用する APN を設定できます。

アクセス ポイントから VRF 経由で VPN アクセスを設定する方法については、「VRF を使用した VPN アクセスの設定の作業リスト」（P.8-13）を参照してください。

ローカル プールの設定を確認するには、特権 EXEC モードで **show ip local** [*pool name*] コマンドを使用します。

```
Router#show ip local pool
Pool    Begin       End         Free    In use  Blocked
poola   10.8.8.1    10.8.8.5    5       0       0

Router #show ip local pool poolA
Pool    Begin       End         Free    In use  Blocked
poola   10.8.8.1    10.8.8.5    5       0       0

Available addresses:
10.8.8.1
10.8.8.2
10.8.8.3
10.8.8.4
```

```
10.8.8.5

Inuse addresses:
None

Held addresses: Time Remaining
None
```

設定例

次に、APN で設定されたローカル アドレス プールの設定例を示します。

```
!
ip local pool local_pool1 128.1.0.1 128.1.255.254
!
access-point 1
access-point-name gprs.pdn.com
ip-address-pool local local_pool1
aggregate 128.1.0.0/16
exit
```

RADIUS による MS アドレッシングの設定

RADIUS サーバによるダイナミック IP アドレッシングは、アクセス ポイント コンフィギュレーション レベルで **ip-address-pool** アクセス ポイント コンフィギュレーション コマンドを使用して設定されます。

ip-address-pool アクセス ポイント コンフィギュレーション コマンドの詳細については、「追加の実アクセス ポイント オプションの設定」（P.8-20）を参照してください。RADIUS の設定の詳細については、『*Cisco IOS Security Configuration Guide*』を参照してください。

IP オーバーラッピング アドレス プールの設定

IP オーバーラッピング アドレス プール機能を使用すると、ダイナミック IP アドレス割り当ての柔軟性が向上します。この機能を使用すると、オーバーラッピング IP アドレス プール グループを設定して、異なるアドレス スペースを作成し、異なるアドレス スペースで同じ IP アドレスを同時に使用できます。

IP オーバーラッピング アドレス プールによって、ダイナミック IP アドレス割り当てをより柔軟に実行できます。この機能を使用すると、オーバーラッピング IP アドレス プール グループを設定して、異なるアドレス スペースを作成し、異なるアドレス スペースで同じ IP アドレスを同時に使用できます。

Cisco IOS リリース 12.3(2)XB 以降では、複数の IP アドレス スペースをサポートし、かつ、プール グループ内で非オーバーラッピング IP アドレス プールの検証を可能にする IP アドレス グループの概念が、GGSN でサポートされています。プール名は GGSN 内で一意である必要があります。プール名を関連付けることができるのは 1 つのグループだけであるため、プール名には暗黙グループ識別子が含まれています。明示グループ名なしのプールは、ベース システム グループのメンバーと見なされ、元の IP プール実装と同じ方法で処理されます。

新しいプール機能によって既存の設定が影響を受けることはありません。「グループ」の概念は、既存の **ip local pool** コマンドの拡張です。グループのメンバーとして指定されていないプールの処理は、既存の実装から変更されていません。

ローカル IP アドレス プール グループを設定し、グループが存在することを確認するには、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
ステップ 1	Router(config)#**ip local pool** {**default** | *pool-name* *low-ip-address* [*high-ip-address*]} **例：** GGSN(config)# ip local pool testpool 10.2.2.1 10.2.2.10 group testgroup cache-size 10000	リモート ピアがポイントツーポイント インターフェイスに接続するときに使用される IP アドレスのローカル プールを設定します。 • **default**：他のプールが指定されていない場合に使用される、デフォルトのローカル アドレス プールとなります。 • *pool-name*：特定のローカル アドレス プールの名前。 • *low-ip-address*：プール内で最小の IP アドレス。 • *high-ip-address*：（任意）プール内で最大の IP アドレス。この値を省略すると、low-ip-address IP アドレス引数がローカル プールに組み込まれます。
ステップ 2	Router(config)# **show ip local pool** [*poolname* | [**group** *group-name*]] **例：** GGSN(config)# **show ip local pool group testgroup testpool**	定義済みの IP アドレス プールすべての統計情報を表示します。

設定例

次に、IP オーバーラッピング アドレス プールの設定例を示します。

- 「グローバル デフォルトとしてのローカル アドレス プールの定義」（P.12-13）
- 「複数範囲の IP アドレスの単一プールへの設定例」（P.12-13）
- 「Cisco 7600 プラットフォーム、スーパーバイザ II / MSFC2 での GGSN の IP オーバーラッピング アドレス プールの設定例」（P.12-14）

グローバル デフォルトとしてのローカル アドレス プールの定義

次の例は、ローカル プールをグローバル デフォルト メカニズムとして定義する方法を示しています。

```
ip address-pool local ip local pool default 192.169.15.15 192.68.15.16
```

複数範囲の IP アドレスの単一プールへの設定例

次の例は、2 つの範囲の IP アドレスを 1 つの IP アドレス プールに設定する方法を示しています。

```
ip local pool default 192.169.10.10 192.169.10.20
ip local pool default 192.169.50.25 192.169.50.50
```

Cisco 7600 プラットフォーム、スーパーバイザ II / MSFC2 での GGSN の IP オーバーラッピング アドレス プールの設定例

次の例は、Cisco 7600 プラットフォームでの IP オーバーラッピング アドレス プールの設定方法を示しています。

次の例は、2 つの VPN（vpn1 および vpn2）と、それに関連した GRE トンネル設定（Tunnel1 および Tunnel2）の設定の一部も示しています。

GGSN 上：

```
service gprs ggsn
!
hostname 7600-7-2
!
ip cef
!
ip vrf vpn1
 description GRE Tunnel 1
 rd 100:1
!
ip vrf vpn2
 description GRE Tunnel 3
 rd 101:1
!
interface Loopback1
 ip address 150.1.1.72 255.255.0.0
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface Tunnel1
 description VRF-GRE to PDN 7500(13) Fa0/1
 ip vrf forwarding vpn1
 ip address 50.50.52.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 165.2.1.13
!
interface Tunnel2
 description VRF-GRE to PDN PDN x(12) Fa3/0
 ip vrf forwarding vpn2
 ip address 80.80.82.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 167.2.1.12
!
interface GigabitEthernet0/0.1
 description Gi
 encapsulation dot1Q 100
 ip address 10.1.2.72 255.255.255.0
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
router ospf 10
 network 10.1.2.0 0.0.0.255 area 10
 network 150.1.0.0 0.0.255.255 area 10
!
ip local pool vpn1_pool 100.2.0.1 100.2.255.255 group vpn1
ip local pool vpn2_pool 100.2.0.1 100.2.255.255 group vpn2
```

```
ip route vrf vpn1 0.0.0.0 255.255.255.0 Tunnel1
ip route vrf vpn2 0.0.0.0 255.255.255.0 Tunnel2

gprs access-point-list gprs
  access-point 1
   access-point-name apn.vrf1.com
   access-mode non-transparent
   aaa-group authentication ipdbfms
   ip-address-pool local vpn1_pool
   vrf vpn1
   !
  access-point 2
   access-point-name apn.vrf2.com
   access-mode non-transparent
   aaa-group authentication ipdbfms
   ip-address-pool local vpn2_pool
   vrf vpn2
   !
```

スーパーバイザ / MSFC2 での関連した設定：

```
interface FastEthernet9/5
 no ip address
 switchport
 switchport access vlan 167
 no cdp enable
!
interface FastEthernet9/10
 no ip address
 switchport
 switchport access vlan 165
 no cdp enable
!
interface Vlan165
 ip address 165.1.1.1 255.255.0.0
!
interface Vlan167
 ip address 167.1.1.1 255.255.0.0
!
! provides route to tunnel endpoints on GGSNs
router ospf 10
 network 10.1.2.0 0.0.0.255 area 10
!
! routes to tunnel endpoints on PDN
!
ip route 165.2.0.0 255.255.0.0 165.1.1.13
ip route 167.2.0.0 255.255.0.0 167.1.1.12
```

APN の NBNS および DNS アドレスの設定

APN で、プライマリおよびセカンダリの NetBIOS Name Service（NBNS）、および Domain Name System（DNS; ドメイン ネーム システム）を設定できます。この機能は、これらのアドレスを取得するメカニズムがないアドレス割り当てスキームにとって有益です。また、RADIUS ベースの割り当てスキームの場合、オペレータはユーザ プロファイルごとに NBNS および DNS を設定する必要がありません。

NBNS アドレスおよび DNS アドレスの取得元として、DHCP サーバ、RADIUS サーバ、およびローカル APN 設定の 3 つを挙げることができます。アドレスの選択基準は、APN で設定された IP アドレス割り当てスキームによって異なります。設定ごとの DNS アドレスおよび NBNS アドレスの選択基準は次のとおりです。

1. DHCP ベースの IP アドレス割り当てスキーム（ローカルおよび外部）: DHCP サーバから返される NBNS アドレスが MS に送信されます。DHCP サーバが NBNS アドレスを返さない場合は、ローカル APN 設定が使用されます。
2. RADIUS ベースの IP アドレス割り当てスキーム : RADIUS サーバから（Access-Accept 応答で）返される NBNS アドレスが使用されます。RADIUS サーバが NBNS アドレスを返さない場合は、ローカル APN 設定が使用されます。
3. ローカル IP アドレス プール ベースの IP アドレス割り当てスキーム : ローカル APN 設定が使用されます。
4. スタティック IP アドレス : ローカル APN 設定が使用されます。

（注）　MS によって PCO IE で DNS アドレスが要求されている場合だけ、PDP の作成応答で NBNS アドレスおよび DNS アドレスが GGSN から送信されます。

プライマリ（およびバックアップ）NBNS が PDP の作成応答で送信されるように指定するには、**nbns primary** アクセス ポイント コンフィギュレーション コマンドを使用します。アクセス ポイント設定から NBNS 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。

nbnsprimary *ip-address* [**secondary** *ip-address*]

プライマリ（およびバックアップ）DNS がアクセス ポイントから PDP の作成応答で送信されるように指定するには、**dns primary** アクセス ポイント コンフィギュレーション コマンドを使用します。アクセス ポイント設定から DNS 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。

dnsprimary *ip-address* [**secondary** *ip-address*]

CHAPTER 13

GGSN でのロード バランシングの設定

この章では、Cisco IOS ソフトウェアの Server Load Balancing（SLB; サーバ ロード バランシング）機能を使用して、ロード バランシング機能をサポートするように Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）を設定する方法について説明します。GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）ロード バランシングによって、General Packet Radio Service（GPRS; グローバル パケット ラジオ サービス）/Universal Mobile Telecommunication System（UMTS）ネットワークで複数の Cisco GGSN またはシスコ以外の GGSN を使用する場合の信頼性と可用性が向上します。

この章に記載されている GGSN コマンドの詳細については、使用している Cisco GGSN リリースの『*Cisco GGSN Command Reference*』を参照してください。この章に記載されている他の Cisco IOS SLB コマンドの詳細については、「*IOS Server Load Balancing*」フィーチャ モジュールを参照してください。

この章に記載されているその他のコマンドのマニュアルを参照するには、コマンド リファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

この章は、次の内容で構成されています。

GTP ロード バランシングの概要

ここでは、Cisco IOS SLB 機能と GGSN での GTP ロード バランシング サポートの概要を示します。次の内容で構成されています。

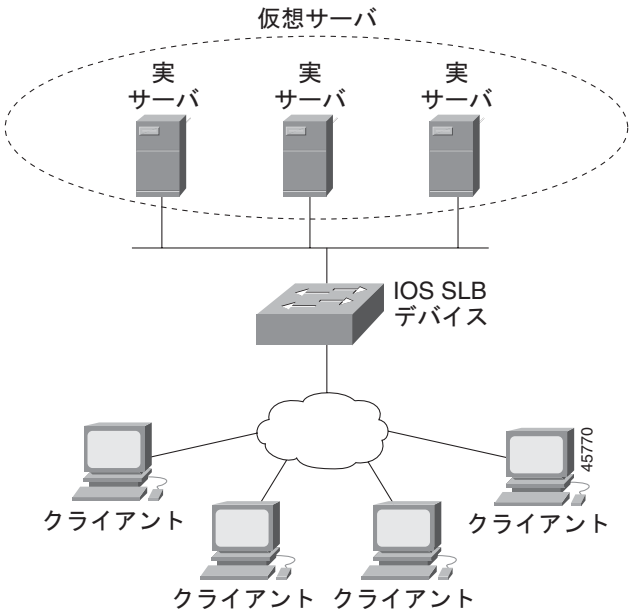
Cisco IOS SLB の概要

Cisco SLB 機能は、IP サーバのロード バランシングを備えた IOS ベースのソリューションです。Cisco IOS SLB 機能を使用すると、ネットワーク サーバ クラスタ内の*実サーバのグループを表す仮想サーバ*を定義できます（*サーバ ファーム*と呼ばれます）。この環境では、クライアントは仮想サーバの IP アドレスに接続します。クライアントが仮想サーバへの接続を開始すると、Cisco IOS SLB 機能によって、設定されている*ロード バランシング アルゴリズム*に基づいて、接続用の実サーバが選択されます。

また、Cisco IOS SLB 機能には、*ファイアウォールのグループ*間でフローを分散する、ファイアウォールのロード バランシングも備えられています（*ファイアウォール ファーム*と呼ばれます）。

図 13-1 に、単純な Cisco IOS SLB ネットワークの論理構成図を示します。

図 13-1　　IOS SLB の論理構成図



GTP ロード バランシングの概要

Cisco IOS SLB によって、GGSN GTP ロード バランシングと GGSN の高度な信頼性および可用性がもたらされます。GGSN GTP ロード バランシングでは、Cisco IOS SLB 機能で使用可能なサーバ ロード バランシング機能全体のサブセットがサポートされています。したがって、グローバル パケット ラジオ サービス /Universal Mobile Telecommunication System（GPRS/UMTS）環境に、すべての範囲の Cisco IOS SLB 機能が適用されるわけではありません。サポートされない機能の詳細については、「GTP SLB の制約事項」（P.13-7）を参照してください。

GTP ロード バランシングを設定する場合、GGSN プールが Cisco IOS SLB でサーバ ファームとして設定されます。これらの GGSN 全体で、GTP セッションをロード バランシングします。GGSN ファーム全体で GTP セッションをロード バランシングするために、Cisco IOS SLB で仮想サーバ インスタンスが設定されます。この仮想サーバは、Cisco IOS SLB で設定したサーバ ファームに関連付けられます。

GTP ロード バランシングを設定する場合、次の点に注意してください。

- GTP ロード バランシングは、スーパーバイザ エンジン上の Cisco IOS SLB 機能を使用することによってサポートされます。
- スーパーバイザ エンジン上の IOS SLB では、GGSN の仮想 IP アドレスに送信された Packet Data Protocol（PDP; パケット データ プロトコル）コンテキストの作成要求だけが処理されます。PDP コンテキストの作成要求が受信されると、その時点での負荷に基づいて実 GGSN が選択されます。PDP コンテキストが確立されたあと、PDP コンテキストに対応する後続のトランザクションすべてが、その GGSN と対応する Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）との間で直接発生し、スーパーバイザ エンジン上の Cisco IOS SLB がバイパスされます。
- 上記以外に、次の点に注意してください。
  - 複数の仮想サーバがサポートされている。
  - ロード バランシングされた実サーバは Cisco 7600 シャーシ搭載のサーバまたはシャーシの外側に設置されたサーバの可能性がある。
  - 各仮想サーバには、SGSN から到達可能な固有のパブリック IP アドレスがある必要がある。
  - 各仮想サーバは 1 つまたは複数の Access Point Name（APN; アクセス ポイント ネーム）に対応付けできる。
  - SGSN が APN を GGSN の IP アドレスに解決する場合に使用する Domain Name Server（DNS; ドメイン ネーム サーバ）サーバは、GGSN の仮想 IP アドレスを使用する必要がある。

サポートされる GTP ロード バランシング タイプ

Cisco IOS SLB では、次の 2 つのタイプの GTP ロード バランシングがサポートされています。

- 「GTP 原因コード検査を使用しない GTP ロード バランシング」（P.13-3）
- 「GTP 原因コード検査を使用する GTP ロード バランシング」（P.13-3）

GTP 原因コード検査を使用しない GTP ロード バランシング

Cisco GGSN では、イネーブルにされた GTP 原因コード検査を*使用しない* GTP ロード バランシングが推奨されます。次の特性があります。

- dispatched モードまたは directed server Network Address Translation（NAT; ネットワーク アドレス変換）モードで動作できますが、directed client NAT モードでは動作できません。dispatched モードでは、GGSN は Cisco IOS SLB デバイスに隣接するレイヤ 2 である必要があります。
- ステートフル バックアップをサポートしていません。
- 重み付けラウンドロビン ロード バランシング アルゴリズムを使用して、仮想 GGSN の IP アドレス宛てのトンネル作成メッセージを実 GGSN のいずれかに配信します。このアルゴリズムの詳細については、「重み付けラウンドロビン」（P.13-5）を参照してください。
- GTPv1 のセカンダリ PDP コンテキストに対応するには Dynamic Feedback Protocol（DFP）が必要です。

GTP 原因コード検査を使用する GTP ロード バランシング

イネーブルにされた GTP 原因コード検査を*使用する* GTP ロード バランシングによって、Cisco IOS SLB は、サーバ ファームとの間で送受信されるすべての PDP コンテキスト シグナリング フローをモニタリングできます。これにより、Cisco IOS SLB では、GTP 障害原因コードをモニタリングし、Cisco GGSN およびシスコ以外の GGSN の両方においてシステムレベルの問題を検出できます。

表 13-1 に、PDP コンテキストの作成応答の原因コードとそれに対応する Cisco IOS SLB の処理のリストを示します。

表 13-1　PDP 作成応答の原因コードとそれに対応する Cisco IOS SLB の処理

原因コード	Cisco IOS SLB の処理
Request Accepted	セッションを確立する。
No Resource Available	現在の実サーバを破棄し、セッションを再割り当てして応答を廃棄する。
All dynamic addresses are occupied	現在の実サーバを破棄し、セッションを再割り当てして応答を廃棄する。
No memory is available	現在の実サーバを破棄し、セッションを再割り当てして応答を廃棄する。
System Failure	現在の実サーバを破棄し、セッションを再割り当てして応答を廃棄する。
Missing or Unknown APN	応答を転送する。
Unknown PDP Address or PDP type	応答を転送する。
User Authentication Failed	応答を転送する。
Semantic error in TFT operation	応答を転送する。
Syntactic error in TFT operation	応答を転送する。
Semantic error in packet filter	応答を転送する。
Syntactic error in packet filter	応答を転送する。
Mandatory IE incorrect	応答を転送する。
Mandatory IE missing	応答を転送する。
Optional IE incorrect	応答を転送する。
Invalid message format	応答を転送する。
Version not supported	応答を転送する。
PDP context without TFT already activated	現在の実サーバを破棄し、セッションを再割り当てして応答を廃棄する。

イネーブルにされた GTP 原因コード検査を*使用する* GTP ロード バランシングには、次の特性があります。

- directed server NAT モードで動作している必要があります。
- ある特定の International Mobile Subscriber ID（IMSI）からの PDP コンテキストの作成を同じ GGSN に割り当てるか、GTP APN 認識ロード バランシングが設定されている場合は同じサーバ ファームに割り当てます。
- ステートフル バックアップをサポートしています。
- GGSN または APN それぞれについて、開いている PDP コンテキストの数を追跡します。これにより、サーバ ファームは GTP ロード バランシングに重み付け最小接続（**leastconns**）アルゴリズムを使用できるようになります。このアルゴリズムの詳細については、「重み付け最小接続」（P.13-5）を参照してください。
- Cisco IOS SLB は、要求元 IMSI のキャリア コードが指定の値に一致しない場合、仮想 GGSN へのアクセスを拒否できます。
- Cisco IOS SLB は、DFP なしでもセカンダリ PDP コンテキストをサポートできます。

GTP ロード バランシングでサポートされる Cisco IOS SLB アルゴリズム

GTP ロード バランシングでは、次の 2 つの Cisco IOS SLB アルゴリズムがサポートされています。

- 「重み付けラウンドロビン」（P.13-5）
- 「重み付け最小接続」（P.13-5）

重み付けラウンドロビン

重み付けラウンドロビン アルゴリズムは、仮想サーバへの新しい接続に使用する実サーバを、サーキュラ方式でサーバ ファームから選択するように指定します。各実サーバに重み *n* が割り当てられます。n は、仮想サーバに関連付けられている他の実サーバと比較した、その実サーバによる接続処理容量を示しています。つまり、新しい接続は、*n* 回までは指定の実サーバに割り当てられ、そのあとはサーバ ファーム内の次の実サーバが選択されます。

たとえば、*n* = 3 の ServerA、*n* = 1 の ServerB、および *n* = 2 の ServerC の 3 つの実サーバで構成されるサーバ ファームがあるとします。仮想サーバへの最初の 3 回の接続は ServerA に割り当てられ、4 番めの接続は ServerB に割り当てられ、5 番めと 6 番めの接続は ServerC に割り当てられます。

（注） サーバ ファームのすべてのサーバに *n* = 1 の重みを割り当てると、Cisco IOS SLB デバイスは単純なラウンドロビン アルゴリズムを使用するように設定されます。

イネーブルにされた GTP 原因コード検査を*使用しない* GTP ロード バランシングには、重み付けラウンドロビン アルゴリズムが必要です。重み付け最小接続を使用するサーバ ファームは、イネーブルにされた GTP 原因コード検査を使用しない GTP ロード バランシングを備えた仮想サーバにバインドできますが、この仮想サーバを **INSERVICE** にはできません。INSERVICE にしようとすると、Cisco IOS SLB によってエラー メッセージが発行されます。

重み付け最小接続

GTP 原因コード検査がイネーブルにされている場合、GTP ロード バランシングでは、Cisco IOS SLB の重み付け最小接続アルゴリズムがサポートされます。

重み付け最小接続アルゴリズムは、仮想サーバへの新しい接続用に、サーバ ファームからアクティブな接続が最も少ない実サーバが次の実サーバとして選択されるよう指定します。このアルゴリズムの場合も、各実サーバに重みが割り当てられます。重みが割り当てられている場合、各サーバでのアクティブな接続数と各サーバの相対容量に基づいて、接続数が最も少ないサーバが判別されます。指定の実サーバの容量は、そのサーバの割り当て済み重みを、この仮想サーバに関連付けられているすべての実サーバの割り当て済み重みの合計で割って算出されます（つまり、$n_1/(n_1+n_2+n_3...)$ となります）。

たとえば、*n* = 3 の ServerA、*n* = 1 の ServerB、および *n* = 2 の ServerC の 3 つの実サーバで構成されるサーバ ファームがあるとします。ServerA の計算済み容量 3/(3+1+2)（つまり、仮想サーバ上のすべてのアクティブな接続の 2 分の 1）、ServerB の計算済み容量はすべてのアクティブな接続の 6 分の 1、ServerC の場合はすべてのアクティブな接続の 3 分の 1 になります。任意の時点で、仮想サーバへの次の接続は、アクティブな接続の数が計算済み容量を最も下回る実サーバに割り当てられます。

（注）　重み *n* = 1 をサーバ ファームのすべてのサーバに割り当てると、Cisco IOS SLB デバイスは、単純な最小接続アルゴリズムを使用するように設定されます。

イネーブルにされた GTP 原因コード検査を*使用しない* GTP ロード バランシングでは、重み付け最小接続アルゴリズムはサポートされて*いません*。

GTP 原因コード検査を*使用する* GTP ロード バランシングでは、重み付け最小接続アルゴリズムがサポートされて*います*。

Cisco IOS SLB の Dynamic Feedback Protocol

GTP ロード バランシングでは、Cisco IOS SLB は、PDP コンテキストが確立されたことは検出しますが、PDP コンテキストがクリアされたことは検出しません。したがって、Cisco IOS SLB は、各 GGSN の開いている PDP コンテキストの数を判別できません。GPRS/UMTS ロード バランシングの重みを動的に計算するには、Cisco IOS SLB DFP を使用します。

Cisco IOS SLB DFP サポートによって、ロード バランシング環境の *DFP マネージャ*は、*DFP エージェント*との TCP 接続を開始できます。接続を開始したあと、DFP エージェントは 1 つまたは複数の実ホスト サーバからステータス情報を収集し、情報を相対的な重みに変換して、その重みを DFP マネージャに報告します。DFP マネージャは、実サーバをロード バランシングするときに重みを計算に入れます。ユーザ定義の間隔での報告以外に、DFP エージェントでは、実サーバのステータスに突然変更が生じた場合に早期報告を送信します。

DFP によって計算された重みによって、**weight (server farm)** コマンドを使用して定義したスタティックな重みが上書きされます。ネットワークから DFP が削除されると、重みは Cisco IOS SLB によってスタティックな重みに戻されます。

Cisco IOS SLB は、DFP マネージャまたは別の DFP マネージャ（DistributedDirector など）の DFP エージェント、あるいは同時にその両方として定義できます。このような設定では、Cisco IOS SLB は DistributedDirector に定期的な報告を送信し、DistributedDirector はその情報を使用して、新しい接続要求に最適なサーバ ファームを選択します。次に、Cisco IOS SLB は同じ情報を使用して、選択されたサーバ ファームから最適な実サーバを選択します。

また、DFP では、さまざまなクライアント サブシステム（Cisco IOS SLB、GPRS/UMTS など）からの複数の DFP エージェントの同時使用をサポートしています。

GTP ロード バランシングでは、Cisco IOS SLB を DFP マネージャとして定義し、サーバ ファームの各 GGSN に DFP エージェントを定義すると、その DFP エージェントは GGSN の重みを報告できます。DFP エージェントは、CPU 使用率、プロセッサ メモリ、および各 GGSN に対して開始できる PDP コンテキストの最大数に基づいて各 GGSN の重みを計算します。

各 GGSN の重みは、主に、許可されている PDP コンテキストの最大数に対する GGSN 上の既存の PDP コンテキストの比率に基づいています。

デフォルトでは、CPU 使用率およびメモリ使用率は、使用率が 85% を超えてからでないと DFP の重み計算に組み込まれません。**gprs dfp** グローバル コンフィギュレーション コマンドに **cpu-load** および **mem-load** キーワード オプションを追加して使用すると、CPU とメモリの負荷を重み計算に組み込む使用率のパーセンテージをカスタマイズできます。

（注）　許可されている PDP コンテキストの最大数は GGSN の最大負荷と見なされるため、**gprs maximum-pdp-context-allowed** コマンドで値を設定する場合は注意が必要です（デフォルトは 10,000 個の PDP コンテキスト）。

GTP IMSI スティッキ データベース サポート

Cisco IOS SLB は、指定の International Mobile Subscriber ID（IMSI）に対して GGSN、または GTP APN 認識ロード バランシングが設定されている場合は APN を選択し、同じ IMSI からの後続のパケット データ プロトコル（PDP）の作成要求すべてを、選択した GGSN または APN に転送できます。

この機能をイネーブルにするために、Cisco IOS SLB では、そのセッション データベース以外に、各 IMSI を対応する実サーバにマッピングする GTP IMSI スティッキ データベースを使用します。

Cisco IOS SLB では、指定の IMSI に対する最初の PDP コンテキストの作成要求を処理するときにスティッキ データベース オブジェクトを作成します。Cisco IOS SLB では、実サーバからスティック オブジェクトを削除するように指示する通知を受信したときにスティッキ オブジェクトを削除します。または、スティッキ オブジェクトが非アクティブであるため、そのスティッキ オブジェクトを削除します。IMSI に属している最後の PDP が削除されると、GGSN はスティッキ オブジェクトを削除するよう Cisco IOS SLB に通知します。

スティッキ データベース サポートおよび GTP APN 認識ロード バランシング

スティッキ IMSI 機能によって、同じ APN に対する同じユーザからのセッションが別の GGSN に割り当てられなくなります。APN（APN 認識ロード バランシング）に基づいたサーバ ファームが選択されていると、スティッキ IMSI 機能によって、IMSI を発行できるようになる前に、スティッキ エントリが APN に基づいた同じサーバ ファームに対するものであることが保証されます。新しい PDP コンテキストの作成要求が別の APN に対するものの場合、GTP SLB ではスティッキ エントリが作成されているサーバ ファームとは別のサーバ ファームを選択することになりますが、このサーバ ファームの方が実サーバよりも重要視されます。これは、実サーバが別のサーバ ファームに属している場合、そのサーバ ファームでは APN がサポートされない可能性があるためです。

GTP APN 認識ロード バランシング

Cisco IOS ソフトウェア リリース 12.2(18) SRB 以降がスーパーバイザ エンジン上にインストールされている場合は、*GTP APN 認識*ロード バランシングを設定できます。

GTP APN 認識機能を使用すると、APN のセットを Cisco IOS SLB のサーバ ファームにマッピングできます。APN の異なるセットをそれぞれサポートする複数のサーバ ファームを作成できます。PDP コンテキストの作成要求は APN 全体に均等に分散されます。

GTP APN 認識ロード バランシングの設定の詳細については、「GTP APN 認識ロード バランシングの設定」（P.13-16）を参照してください。

GTP SLB の制約事項

GTP ロード バランシングを設定する場合は、次の制約事項が適用されます。

- イネーブルにされた GTP 原因コード検査を使用しない GTP ロード バランシングの場合：
  - dispatched モードまたは directed server NAT モードのいずれかでだけ動作します。
  - ネットワークにより開始された PDP コンテキストの要求はロード バランシングできません。
  - 次の Cisco IOS SLB 機能はサポートされていません。
    - ID のバインド
    - クライアント割り当てのロード バランシング
    - スロースタート

- ステートフル バックアップ（Cisco 7600 プラットフォームではサポートされない）
- 重み付け最小接続ロード バランシング アルゴリズム

- イネーブルにされた GTP 原因コード検査を*使用する* GTP ロード バランシングの場合：
  - directed server NAT モードでだけ動作します。
  - ネットワークにより開始された PDP コンテキストの要求はロード バランシングできません。
  - SGSN または GGSN のいずれかでそのピアをエコーする必要があります。
  - インバウンド トラフィックおよびアウトバウンド トラフィックは、Cisco IOS SLB 経由でルーティングされる必要があります。
  - 次の Cisco IOS SLB 機能はサポートされていません。
    - ID のバインド
    - クライアント割り当てのロード バランシング
    - スロースタート
    - スティッキ接続

GTP ロード バランシングの設定

この項は、次の内容で構成されています。

GTP ロード バランシング設定の作業リスト

ここでは、GTP ロード バランシングの設定で実行する作業のリストを示します。詳細な設定情報は、このマニュアルや他のマニュアルで示される参照先の項に掲載されています。ここでは、必須の作業または任意の作業であるかが示されています。

1. Cisco IOS SLB で、次の作業を実行します。
   a. 「サーバ ファームおよび実サーバの設定」（P.13-10）（必須）
   b. 「仮想サーバの設定」（P.13-12）（必須）
   c. 「GSN アイドル タイマーの設定」（P.13-15）（GTP 原因コード検査がイネーブルにされている場合は任意）
   d. 「DFP サポートの設定」（P.13-15）（任意。ただし推奨）
   e. 「GTP APN 認識ロード バランシングの設定」（P.13-16）（任意）
2. GGSN で、次の作業を実行します。
   a. 「GTP SLB のループバック インターフェイスの設定」（P.13-20）（必須）
   b. 「GGSN での DFP サポートの設定」（P.13-21）（任意。ただし推奨）
   c. 「GGSN から Cisco IOS SLB へのメッセージングの設定」（P.13-23）（任意）

3. 関連付けられている各サービング GPRS サポート ノード（SGSN）に、各 GGSN をルーティングします（必須）。

   ルートはスタティックとダイナミックのいずれにもできますが、GGSN が SGSN に到達できる必要があります。詳細については、「SGSN へのルートの設定」（P.8-4）を参照してください。

4. SGSN で、関連付けられている各 GGSN 上の仮想テンプレート、および GGSN ロード バランシング仮想サーバに、各 SGSN をルーティングします（必須）。

設定ガイドライン

Cisco IOS SLB および GGSN によって共有されているネットワークを設定する場合は、次の考慮事項に注意してください。

- レイヤ 2 情報が正しくかつ明白となるように、スタティック ルート（**ip route** コマンドを使用）および実サーバの IP アドレス（**real** コマンドを使用）を指定します。
- SGSN から仮想サーバへのスタティック ルートを設定します。
- 次のいずれかの方法を使用して、サブネットを慎重に選択します。
  - 仮想テンプレート アドレスのサブネットがオーバーラップしないようにする。
  - 実サーバ上のインターフェイスへではなく、実サーバへのネクストホップ アドレスを指定する。
- Cisco IOS SLB では、次の 2 つのタイプの GTP ロード バランシングがサポートされています。
  - 「GTP 原因コード検査を使用しない GTP ロード バランシング」（P.13-3）
  - 「GTP 原因コード検査を使用する GTP ロード バランシング」（P.13-3）
- Cisco IOS SLB では、GTP v0 および GTP v1 の両方がサポートされています。GTP サポートによって Cisco IOS SLB を「GTP 認識」にし、Cisco IOS SLB でレイヤ 5 まで把握できるように拡張できます。
- Cisco 7600 プラットフォームでは、次のことが適用されます。
  - 複数の GTP 仮想サーバがサポートされている。
  - ロード バランシングされた実サーバは Cisco 7600 シャーシ搭載のサーバまたはシャーシの外側に設置されたサーバの可能性がある。
  - 各 GTP 仮想サーバには、SGSN から到達可能な固有のパブリック IP アドレスがある必要がある。
  - 各仮想サーバは 1 つまたは複数の APN に対応付けできる。
  - SGSN が APN を GGSN の IP アドレスに解決する場合に使用する DNS サーバは、GTP の仮想 IP アドレスを使用する必要がある。
- GTP APN 認識ロード バランシングを設定する場合、次の点に注意してください。
  - スーパーバイザ エンジン上に Cisco IOS ソフトウェア リリース 12.2(18) SRB 以降、GGSN 上に Cisco GGSN リリース 7.0、Cisco IOS リリース 12.4(9)XG 以降が必要です。
  - イネーブルにされた GTP 原因コード検査を使用する GTP ロード バランシングはサポートされていません。
  - 特定の IOS SLB GTP マップの場合は、最大で 100 個の **apn** コマンドを設定できますが、APN マップはパフォーマンスに影響を与える可能性があるため、vserver につき 10 個を超える APN マップを設定しないことを推奨します。

- プライマリとバックアップの仮想サーバのマッピング ルールが同じである必要があります。
- 1 つの実サーバは、複数のサーバ ファームには設定できません。

GTP ロード バランシング用の Cisco IOS SLB の設定

GTP ロード バランシングを設定するには、Cisco IOS SLB で次の作業を実行する必要があります。

- 「サーバ ファームおよび実サーバの設定」（P.13-10）（必須）
- 「仮想サーバの設定」（P.13-12）（必須）
- 「GSN アイドル タイマーの設定」（P.13-15）（任意）
- 「DFP サポートの設定」（P.13-15）（任意。ただし推奨）
- 「GTP APN 認識ロード バランシングの設定」（P.13-16）（任意）
- 「Cisco IOS SLB 設定の確認」（P.13-19）（任意）

サーバ ファームおよび実サーバの設定

GTP ロード バランシング用に Cisco IOS SLB でサーバ ファームおよび実サーバを設定する場合は、次のガイドラインに従って正しく設定するようにしてください。

- GTP 原因コード検査がイネーブルにされていない場合は、**predictor** コマンドのデフォルト設定（重み付けラウンドロビン アルゴリズム）を受け入れます。

  GTP 原因コード検査がイネーブルにされている場合は、重み付けラウンドロビン アルゴリズム（**roundrobin**）または重み付け最小接続アルゴリズム（**leastconns**）のいずれかを指定できます。
- **real** コマンドを使用して、GGSN 機能を実行している実サーバの IP アドレス（Cisco GGSN の場合は仮想テンプレート アドレス）を指定します。
- **reassign** コマンドを使用して、SGSN の N3-REQUESTS カウンタ値よりも小さい再割り当てしきい値を指定します。

Cisco IOS SLB サーバ ファームを設定するには、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
ステップ 1	`Router-SLB(config)# ip slb serverfarm` *serverfarm-name* `Router(config-slb-sfarm)#`	Cisco IOS SLB 設定にサーバ ファーム定義を追加し、サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 2	`Router-SLB(config-slb-sfarm)# predictor [roundrobin | leastconns]`	実サーバの選択方法を決定する場合に使用するアルゴリズムを指定します。 **（注）** イネーブルにされた GTP 原因コード検査を*使用しない* GTP ロード バランシングでは、デフォルト設定（重み付けラウンドロビン アルゴリズム）を受け入れる必要があります。 各アルゴリズムの詳細については、次の項を参照してください。 • 「重み付けラウンドロビン」（P.13-5） • 「重み付け最小接続」（P.13-5）

	コマンド	目的
ステップ 3	`Router-SLB(config-slb-sfarm)# nat server`	（GTP 原因コード検査がイネーブルにされている場合は必須、イネーブルにされた原因コード検査を*使用しない* GTP ロード バランシングの場合は任意）サーバ ファームで、NAT サーバ アドレス変換モードを設定します。
ステップ 4	`Router-SLB(config-slb-sfarm)# real` *ip-address* [*port*]	GGSN の仮想テンプレート インターフェイスの IP アドレスを使用して、実 GGSN をサーバ ファームのメンバーとして指定し、実サーバ コンフィギュレーション モードを開始します。
ステップ 5	`Router-SLB(config-slb-real)# faildetect numconns` *number-conns* [**numclients** *number-clients*]	（任意）実サーバの失敗を構成する、接続の連続失敗回数と、任意で固有のクライアント接続の失敗回数を指定します。
ステップ 6	`Router-SLB(config-slb-real)# maxconns` *number-conns*	（任意）実サーバで一度に許可されるアクティブな接続の最大数を指定します。 **（注）** イネーブルにされた原因コード検査を*使用しない* GTP ロード バランシングでは、セッションが **ip gtp request** コマンドで指定した期間よりも長く継続することがないため、このコマンドによる影響は最小限に抑えられます。
ステップ 7	`Router-SLB(config-slb-real)# reassign` *threshold*	（任意）連続した受信応答されない同期、または PDP コンテキストの作成要求のしきい値を指定します。このしきい値を超えると、別の実サーバへの接続が試行されます。
ステップ 8	`Router-SLB(config-slb-real)# retry` *retry-value*	（任意）サーバ障害の検出と障害の発生したサーバへの次の接続試行との間に待機する間隔を秒単位で指定します。
ステップ 9	`Router-SLB(config-slb-real)# weight` *weighting-value*	（任意）サーバ ファームの他のサーバと比較した、実サーバの作業負荷容量を指定します。 **（注）** DFP を使用する場合、**weight (server farm)** コマンドを使用して定義するスタティックな重みは、DFP によって計算される重みで上書きされます。ネットワークから DFP が削除されると、重みは Cisco IOS SLB によってスタティックな重みに戻されます。
ステップ 10	`Router-SLB(config-slb-real)# inservice`	Cisco IOS SLB で使用できるように実サーバをイネーブルにします。

仮想サーバの設定

GTP ロード バランシング用に Cisco IOS SLB で仮想サーバを設定する場合、次のガイドラインに従って正しく設定するようにしてください。

- SGSN から仮想サーバへのスタティック ルートを設定します。
- 仮想 GGSN の IP アドレスを仮想サーバとして指定し、**udp** キーワード オプションを使用します。
- GTP v1 セッションをロード バランシングするには、GGSN および SGSN が European Telecommunications Standards Institute（ETSI; 欧州電気通信標準化機構）標準に準拠している場合はポート番号 **2123** を指定し、全ポート仮想サーバ（すべてのポート宛てのフローを受け入れる仮想サーバ）を設定するにはポート番号 **0** または **any** を指定します。
- GTP v0 セッションをロード バランシングするには、GGSN および SGSN が European Telecommunications Standards Institute（ETSI）標準に準拠している場合はポート番号 **3386** を指定し、全ポート仮想サーバを設定するにはポート番号 **0** または **any** を指定します。
- GTP 原因コード検査を*使用しない* GTP ロード バランシングをイネーブルにするには、**service gtp** キーワード オプションを指定します。
- GTP 原因コード検査を*使用する* GTP ロード バランシングをイネーブルにするには、**service gtp-inspect** キーワード オプションを指定します。

  イネーブルにされた GTP 原因コード検査を*使用しない* GTP ロード バランシングでは、**idle** コマンドを使用して GTP アイドル タイマーを設定するときに、SGSN での PDP コンテキストの要求間で許可されている最大間隔よりも大きい GTP アイドル タイマーを指定します。

Cisco IOS SLB 仮想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
ステップ 1	`Router-SLB(config)# ip slb vserver virtual_server-name`	仮想サーバを識別し、仮想サーバ コンフィギュレーション モードを開始します。

ステップ 2	`Router-SLB(config-slb-vserver)# virtual ip-addr [netmask [group]] {esp | gre | protocol}`
	
	または
	
	`Router(config-slb-vserver)# virtual ip-addr [netmask [group]] {tcp | udp} [port | any] [service service]`
		仮想サーバの IP アドレス、接続タイプ、任意の TCP または UDP ポート番号、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）Internet Security Association and Key Management Protocol（ISAKMP）または Wireless Session Protocol（WSP）の設定、およびサービス カップリングを指定します。
		
		（注） GTP ロード バランシングの場合：
		
		– 仮想 GGSN の IP アドレスを仮想サーバとして指定し、**udp** キーワード オプションを指定します。
		
		– GTP v1 セッションをロード バランシングするには、GGSN および SGSN が European Telecommunications Standards Institute（ETSI; 欧州電気通信標準化機構）標準に準拠している場合はポート番号 **2123** を指定し、全ポート仮想サーバ（すべてのポート宛てのフローを受け入れる仮想サーバ）を設定するにはポート番号 **0** または **any** を指定します。
		
		– GTP v0 セッションをロード バランシングするには、GGSN および SGSN が ETSI 標準に準拠している場合はポート番号 **3386** を指定し、全ポート仮想サーバを設定するにはポート番号 **0** または **any** を指定します。
		
		– GTP 原因コード検査を*使用しない* GTP ロード バランシングをイネーブルにするには、**service gtp** キーワード オプションを指定します。
		
		– GTP 原因コード検査を*使用する* GTP ロード バランシングをイネーブルにするには、**service gtp-inspect** キーワード オプションを指定します。

	コマンド	目的
ステップ 3	Router-SLB(config-slb-vserver)# **serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**map** *map-id* **priority** *priority*]	実サーバ ファームを仮想サーバに関連付けます。 • **backup**：（任意）バックアップ サーバ ファームを設定します。 • **backup** *backup-farm* [**sticky**]：（任意）バックアップ サーバ ファームを設定し、任意で、バックアップ サーバ ファームのスティッキ接続を使用するように指定します。 • **map** *map-id* **priority** *priority*：（任意）GTP APN 認識ロード バランシング用に IOS SLB プロトコル マップをサーバ ファームに関連付け、このマップのプライオリティを定義します。マップはプライオリティを基準にして検索されます。数値が小さいほど、プライオリティが高くなります。 **（注）** **map** キーワード オプションを指定して設定されている場合、複数のインスタンスの **serverfarm** コマンドを使用できます。デフォルトのサーバ ファーム（**map** キーワード オプションなし）は、単一のインスタンスに制限されています。 **（注）** マップの設定を変更するには、仮想サーバをアウト オブ サービスにする必要があります。 **（注）** 各マップのプライマリ サーバ ファームとバックアップ サーバ ファームの NAT モードは一致している必要があります。
ステップ 4	Router-SLB(config-slb-vserver)# **idle** [**gtp request**] *duration*	（任意）Cisco IOS SLB がパケット アクティビティのないときに接続コンテキストを維持する最小時間を指定します。 **gtp request** キーワード オプションなしで指定された **idle** コマンドによって、イネーブルにされた原因コード検査を*使用しない*GTP ロード バランシングの GTP アイドル タイマーが制御されます。**idle gtp request** コマンドによって、イネーブルにされた原因コード検査を*使用しない*GTP ロード バランシングと、イネーブルにされた原因コード検査を*使用する*GTP ロード バランシングの両方の GTP アイドル タイマーが制御されます。推奨される設定は **idle gtp request** です。 **（注）** イネーブルにされた GTP 原因コードを*使用しない*GTP ロード バランシングでは、SGSN での PDP コンテキストの要求間で許可されている最大間隔よりも大きい GTP アイドル タイマーを指定します。
ステップ 5	Router-SLB(config-slb-vserver)# **inservice**	Cisco IOS SLB で使用できるよう仮想サーバをイネーブルにします。

	コマンド	目的
ステップ 6	`Router-SLB(config-slb-vserver)# client {ip-address network-mask [exclude] | gtp carrier-code [code]}`	（任意）仮想サーバを使用できるクライアントを指定します。 （注）　GTP ロード バランシングでは、**gtp carrier-code** オプションだけがサポートされます（GTP 原因コード検査がイネーブルにされている場合にだけ）。
ステップ 7	`Router-SLB(config-slb-vserver)# replicate casa listen-ip remote-ip port [interval] [password [0 | 7] password timeout]`	（任意）Cisco IOS SLB 決定テーブルのバックアップ スイッチへのステートフル バックアップを設定します。 （注）　イネーブルにされた GTP 原因コード検査を*使用しない* GTP ロード バランシングでは、このコマンドはサポートされていません。

GSN アイドル タイマーの設定

GTP 原因コード検査がイネーブルにされている場合は、Cisco IOS SLB がアイドルの GGSN または SGSN との間のセッションを維持する時間を設定できます。

GSN アイドル タイマーを設定するには、Cisco IOS SLB で、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-SLB(config)# ip slb timers gtp gsn duration`	Cisco IOS SLB がアイドルの GGSN または SGSN との間のセッションを維持する時間を変更します。

DFP サポートの設定

Cisco IOS SLB は、DFP マネージャまたは別の DFP マネージャ（DistributedDirector など）の DFP エージェント、あるいは同時にその両方として定義できます。ネットワーク設定によっては、Cisco IOS SLB を DFP マネージャとして設定するためのコマンドと Cisco IOS SLB を DFP エージェントとして設定するコマンドを、同じデバイスまたは異なるデバイス上で入力することがあります。

Cisco IOS SLB を DFP マネージャとして設定し、Cisco IOS SLB が接続を開始できる DFP エージェントを識別するには、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	説明
ステップ 1	`Router-SLB(config)# ip slb dfp [password [0|7] password [timeout]]`	DFP を設定し、任意のパスワードを指定して、DFP コンフィギュレーション モードを開始します。
ステップ 2	`Router-SLB(config-slb-dfp)# agent ip_address port-number [timeout [retry_count [retry_interval]]]`	Cisco IOS SLB の接続先となる DFP エージェントを識別します。

GTP APN 認識ロード バランシングの設定

GTP APN 認識ロード バランシングによって、APN 全体をロード バランシングできます。

GTP APN 認識ロード バランシングを実装する場合は、IOS SLB で作成された Cisco IOS SLB GTP マップに APN のセットが定義されている必要があります。次に、IOS SLB GTP マップを、IOS SLB の仮想テンプレートの下にあるサーバ ファームに関連付ける必要があります。

GTP APN 認識ロード バランシングを設定するには、次の項の作業を実行します。

- 「GTP APN 認識ロード バランシング用の Cisco IOS SLB GTP マップの設定」（P.13-16）
- 「仮想サーバのサーバ ファームへの IOS SLB GTP マップの関連付け」（P.13-17）

前提条件および制約事項

GTP APN 認識ロード バランシングを設定する場合、次の点に注意してください。

- スーパーバイザ エンジン上に Cisco IOS ソフトウェア リリース 12.2(18) SRB 以降、GGSN 上に Cisco GGSN リリース 7.0、Cisco IOS リリース 12.4(9)XG 以降が必要です。
- イネーブルにされた GTP 原因コード検査を使用する GTP ロード バランシングはサポートされていません。
- 特定の IOS SLB GTP マップの場合は、最大で 100 個の **apn** コマンドを設定できますが、APN マップはパフォーマンスに影響を与える可能性があるため、vserver につき 10 個を超える APN マップを設定しないことを推奨します。
- プライマリとバックアップの仮想サーバのマッピング ルールが同じである必要があります。
- 1 つの実サーバは、複数のサーバ ファームには設定できません。

GTP APN 認識ロード バランシング用の Cisco IOS SLB GTP マップの設定

APN 認識ロード バランシングをイネーブルにするには、特定の APN をグループ化する IOS SLB GTP マップが設定されている必要があります。

APN 全体でのロード バランシング用の IOS SLB GTP マップを設定するには、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
ステップ 1	`Router-SLB(config)# ip slb map map-id protocol`	IOS SLB プロトコル マップを設定し、SLB マップ コンフィギュレーション モードを開始します。 • *map-id* : IOS SLB プロトコル マップ ID。有効な範囲は 1 ～ 255 です。マップ ID はすべてのサービス タイプ全体でグローバルに固有である必要があります。 • *protocol* : マップに関連付けられているプロトコル。vserver サービス タイプに一致する必要があります。 – **gtp** : グローバル パケット ラジオ サービス（GPRS）ロード バランシングの場合、IOS SLB GPRS トンネリング プロトコル（GTP）マップを設定し、SLB GTP マップ コンフィギュレーション モードを開始します。 – **radius** : Remote Authentication Dial-In User Service（RADIUS）ロード バランシングの場合、IOS SLB RADIUS マップを設定し、SLB RADIUS マップ コンフィギュレーション モードを開始します。 （注）　このリリースでは、GTP マップがサポートされています。
ステップ 2	`Router-SLB(config-slb-map)# apn string`	グローバル パケット ラジオ サービス（GPRS）ロード バランシングのアクセス ポイント ネーム（APN）に一致させる ASCII 正規表現を設定します。 （注）　特定の IOS SLB GTP マップの場合は、最大で 100 個の **apn** コマンドを設定できますが、APN マップはパフォーマンスに影響を与える可能性があるため、vserver につき 10 個を超える APN マップを設定しないことを推奨します。

仮想サーバのサーバ ファームへの IOS SLB GTP マップの関連付け

IOS SLB GTP マップを作成したあと、仮想サーバの設定時にその GTP マップをサーバ ファームに関連付ける必要があります。

（注）　マップの設定を変更するには、仮想サーバをアウト オブ サービスにする必要があります。各マップのプライマリ サーバ ファームとバックアップ サーバ ファームの NAT モードは一致している必要があります。

サーバ ファームを仮想サーバに関連付けるときに IOS SLB GTP マップを指定するには、IOS SLB で、仮想サーバ 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-SLB(config-slb-vserver)# serverfarm` *primary-farm* [**backup** *backup-farm* [**sticky**]] [**map** *map-id*] **priority** *priority*]	実サーバ ファームを仮想サーバに関連付けます。 • **backup**：（任意）バックアップ サーバ ファームを設定します。 • **backup** *backup-farm* [**sticky**]：（任意）バックアップ サーバ ファームを設定し、任意で、バックアップ サーバ ファームのスティッキ接続を使用するように指定します。 • **map** *map-id* **priority** *priority*：（任意）GTP APN 認識ロード バランシング用に IOS SLB プロトコル マップをサーバ ファームに関連付け、このマップのプライオリティを定義します。マップはプライオリティを基準にして検索されます。数値が小さいほど、プライオリティが高くなります。 **（注）** **map** キーワード オプションを指定して設定されている場合、複数のインスタンスの **serverfarm** コマンドを使用できます。デフォルトのサーバ ファーム（**map** キーワード オプションなし）は、単一のインスタンスに制限されています。 **（注）** マップの設定を変更するには、仮想サーバをアウトオブ サービスにする必要があります。 **（注）** 各マップのプライマリ サーバ ファームとバックアップ サーバ ファームの NAT モードは一致している必要があります。

GTP APN 認識ロード バランシングの設定例

IOS SLB からの次の設定例は、IOS SLB GTP マップ設定と、仮想テンプレートの下のマップ / サーバ ファーム アソシエーションを示します。

```
!
/* server-farm configurations */
ip slb serverfarm farm1
 real 10.0.0.1
  inservice
 real 10.0.0.2
  inservice
ip slb serverfarm farm4
 real 10.0.0.7
  inservice
 real 10.0.0.8
  inservice
ip slb serverfarm farm5
 real 10.0.0.9
  inservice
 real 10.0.0.10
  inservice
!
```

```
/* GTP maps for GTP APN-aware SLB */
ip slb map 1 gtp
  apn www.*.edu
ip slb map 4 gtp
  apn abc.company1.com
  apn xyz.company2.com
ip slb map 5 gtp
  apn company3.com
!
/* associate the GTP map with server farm under virtual server */
ip slb vserver GGSN_SERVER
  virtual 10.10.10.10 udp 0 service gtp
  serverfarm farm1 map 1 priority 3
  serverfarm farm2 backup farm4 map 1 priority 2
  serverfarm farm4 map 4 priority 5
  serverfarm farm5 map 5 priority 4
  serverfarm farm6
```

Cisco IOS SLB 設定の確認

ここでは、Cisco IOS SLB 設定を確認する方法について説明します。内容は次のとおりです。

- 「仮想サーバの確認」（P.13-19）
- 「サーバ ファームの確認」（P.13-19）
- 「Cisco IOS SLB の接続の確認」（P.13-20）

仮想サーバの確認

次の **show ip slb vserver** コマンドによって、仮想サーバ PUBLIC_HTTP と RESTRICTED_HTTP の設定が確認されます。

```
Router-SLB# show ip slb vserver

slb vserver      prot  virtual               state         conns
-------------------------------------------------------------------
PUBLIC_HTTP      TCP   10.0.0.1:80           OPERATIONAL     0
RESTRICTED_HTTP  TCP   10.0.0.2:80           OPERATIONAL     0
IOSSLB#
```

サーバ ファームの確認

次の **show ip slb reals** コマンドによって、サーバ ファーム PUBLIC と RESTRICTED のステータス、関連付けられている実サーバ、およびそのステータスが表示されます。

```
Router-SLB# show ip slb real

real                    farm name        weight   state          conns
-------------------------------------------------------------------------
10.1.1.1                 PUBLIC           8       OPERATIONAL      0
10.1.1.2                 PUBLIC           8       OPERATIONAL      0
10.1.1.3                 PUBLIC           8       OPERATIONAL      0
10.1.1.20                RESTRICTED       8       OPERATIONAL      0
10.1.1.21                RESTRICTED       8       OPERATIONAL      0
IOSSLB#
```

次の **show ip slb serverfarm** コマンドによって、サーバ ファーム PUBLIC と RESTRICTED の設定およびステータスが表示されます。

```
Router-SLB# show ip slb serverfarm

server farm      predictor    nat   reals   bind id
--------------------------------------------------
PUBLIC           ROUNDROBIN   none  3       0
RESTRICTED       ROUNDROBIN   none  2       0
IOSSLB#
```

Cisco IOS SLB の接続の確認

Cisco IOS SLB 機能がインストールされ、正しく動作しているかどうかを確認するには、Cisco IOS SLB スイッチから実サーバに対して PING を実行し、次にクライアントから仮想サーバに対して PING を実行します。

次の **show ip slb stats** コマンドによって、Cisco IOS SLB ネットワーク ステータスに関する詳細が表示されます。

```
Router-SLB# show ip slb stats
Pkts via normal switching:    0
Pkts via special switching:   0
Pkts via slb routing:         0
Pkts Dropped:                 0
Connections Created:          0
Connections Established:      0
Connections Destroyed:        0
Connections Reassigned:       0
Zombie Count:                 0
Connections Reused:           0
Connection Flowcache Purges:  0
Failed Connection Allocs:     0
Failed Real Assignments:      0
RADIUS framed-ip Sticky Count:0
RADIUS username Sticky Count: 0
```

Cisco IOS SLB のネットワークおよび接続を確認する場合に使用される他のコマンドについては、「Cisco IOS SLB 機能のモニタリングおよびメンテナンス」（P.13-26）を参照してください。

GTP ロード バランシング用の GGSN の設定

GGSN で GTP ロード バランシングを設定するには、次の項の作業を実行します。

- 「GTP SLB のループバック インターフェイスの設定」（P.13-20）（イネーブルにされた GTP 原因コード検査を使用しない dispatched モードを使用している場合は必須）
- 「GGSN での DFP サポートの設定」（P.13-21）（任意。ただし推奨）

GTP SLB のループバック インターフェイスの設定

GTP ロード バランシングをイネーブルにするには、ファーム内の各 GGSN 上の Cisco IOS SLB で、ループバック インターフェイスに仮想サーバと同じ IP アドレスが設定されている必要があります。

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	説明
ステップ 1	`Router-GGSN(config)# interface loopback number`	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、常に稼動している仮想インターフェイスです。
ステップ 2	`Router-GGSN(config-if)# ip address ip-address mask`	ループバック インターフェイスに IP アドレスを割り当てます。

GGSN での DFP サポートの設定

GTP SLB の DFP サポートを設定するには、次の作業を実行する必要があります。

- 「DFP エージェントとしての GGSN の設定」（P.13-21）
- 「GGSN の DFP 重みの設定」（P.13-22）
- 「GGSN の PDP コンテキストの最大数の設定」（P.13-22）

DFP エージェントとしての GGSN の設定

DFP エージェントの設定の詳細については、「*DFP Agent Subsystem*」フィーチャ モジュールを参照してください。

DFP マネージャ（この場合は Cisco IOS SLB）が DFP エージェントへの接続に使用するポート番号を定義するには、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示されている順序で使用します。

	コマンド	説明
ステップ 1	`Router-GGSN(config)# ip dfp agent gprs`	DFP エージェント サブシステムを識別し、DFP エージェント コンフィギュレーション モードを開始します。
ステップ 2	`Router-GGSN(config-dfp)# interval seconds`	（任意）DFP エージェントの重み再計算間隔を設定します。
ステップ 3	`Router-GGSN(config-dfp)# password [0|7] password [timeout]`	（任意）Message-Digest Algorithm 5（MD5）認証用の DFP エージェントのパスワードを設定します。
ステップ 4	`Router-GGSN(config-dfp)# port port-number`	DFP マネージャが DFP エージェントへの接続に使用するポート番号を定義します。
ステップ 5	`Router-GGSN(config-dfp)# inservice`	DFP マネージャと通信できるよう DFP エージェントをイネーブルにします。DFP エージェントは、次の両方の条件が満たされるまで非アクティブです。 • DFP エージェントが inservice (DFP agent) コマンドを使用してイネーブルにされている。 • クライアント サブシステムによって DFP エージェントの状態がアクティブに変更されている。

GGSN の DFP 重みの設定

DFP を GTP ロード バランシングで使用する場合、DFP エージェントとして機能する各 GGSN には、DFP マネージャに送信できる最大の重みがあります。GGSN ごとに、デフォルトの最大の重み（85%）を受け入れるか、または最大の重みに別の値を指定できます。また、**cpu-load** および **mem-load** キーワード オプションを使用して、CPU とメモリの負荷を重み計算に組み込む使用率のパーセンテージを設定することもできます。

GGSN の最大の重みを指定するには、GGSN で、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-GGSN(config)# **gprs dfp** {**max-weight** *max-weight* | **min-cpu-load** *min-cpu-load* | **mem-load** *min-mem-load*}	DFP エージェントとして機能している GGSN の DFP 重みパラメータを指定します。 • **max-weight**：DFP エージェントとして機能する GGSN から DFP マネージャに送信される最大の重みを指定します。有効な範囲は 1 ～ 100 です。デフォルトは 8 です。 • **min-cpu-load**：CPU の負荷が DFP の重み計算に組み込まれる最小のパーセンテージを指定します。有効な範囲は 10 ～ 75% です。 • **mem-load**：メモリの負荷が DFP の重み計算に組み込まれる最小のパーセンテージを指定します。有効な範囲は 10 ～ 75% です。

GGSN の PDP コンテキストの最大数の設定

DFP を GTP ロード バランシングで使用する場合、**gprs maximum-pdp-context-allowed** コマンドを使用して、GGSN ごとの PDP コンテキストの最大数を指定する必要があります。PDP コンテキスト数のデフォルト値である 10,000 は使用*しないようにしてください*。デフォルト値の 10,000 を含め、値を大幅に小さくすると、GPRS/UMTS ロード バランシング環境のキャパシティに影響する可能性があります。

（注） DFP では、PPP PDP を IP PDP と比較します。1 つの PPP PDP は 8 つの IPv4 PDP と等価です。1 つの IPv6 PDP は、4 つの IPv4 PDP としてカウントされます。したがって、DFP を使用する場合は、設定された PDP コンテキストの最大数が GGSN の重みに影響を与えることに注意してください。他のパラメータがすべて同じままの場合は、PDP コンテキストの最大数が小さいほど、重みが小さくなります。

GGSN の PDP コンテキストの最大数を設定するには、GGSN で、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-GGSN(config)# **gprs maximum-pdp-context-allowed** [*pdp-contexts*]	GGSN で有効にできる PDP コンテキスト（モバイル セッション）の最大数を指定します。

GGSN から Cisco IOS SLB へのメッセージングの設定

GGSN-IOS SLB メッセージング機能を使用すると、Cisco IOS SLB によって転送されるセッションに影響を与える特定の条件が存在する場合に、Cisco IOS SLB に通知するように GGSN を設定できます。また、この通知によって、この条件に応答する方法が Cisco IOS SLB に指示されます。

gprs slb notify コマンドを使用して設定できる GGSN-IOS SLB 通知には、Call Admission Control（CAC; コール アドミッション制御）障害通知と削除通知（GTP IMSI のスティッキ データベース サポートの場合）の 2 つのタイプがあります。次の項では、それぞれのタイプを設定する方法について説明します。

- 「GGSN-IOS SLB メッセージング CAC 障害通知のサポートの設定」（P.13-23）
- 「GGSN-IOS SLB メッセージング削除通知のサポート（GTP IMSI スティッキ データベース サポート）の設定」（P.13-25）

GGSN-IOS SLB メッセージング CAC 障害通知のサポートの設定

GGSN は、UMTS QoS CAC 障害が原因で PDP コンテキストの作成要求が拒否された場合に Cisco IOS SLB に通知するよう設定できます。

GGSN によって送信される CAC 障害通知には、次の Information Elements（IE; 情報エレメント）が含まれます。

- タイプ：通知タイプ（再割り当て）。
- セッション ID：通知が属しているセッションを識別する、Cisco IOS SLB でのセッション キー。
- 作成応答：障害が発生したときに GGSN が SGSN に送信する作成応答。セッションを再割り当てできる代替の GGSN がない場合、または再割り当て試行の最大回数を超えている場合、Cisco IOS SLB ではこの情報を SGSN にリレーします。

CAC 障害通知のサポートを設定する方法は、Cisco IOS SLB が dispatched モードまたは directed server NAT モードのいずれで動作しているかによって異なります。それぞれの手順の詳細については、次の項を参照してください。

- 「Cisco IOS SLB が dispatched モードの場合の CAC 障害通知サポートの設定」（P.13-23）
- 「Cisco IOS SLB が directed server NAT モードのときの CAC 障害通知サポートの設定」（P.13-24）

Cisco IOS SLB が dispatched モードの場合の CAC 障害通知サポートの設定

Cisco IOS SLB が dispatched モードで機能している場合、PDP コンテキストの作成要求を GGSN に転送した仮想サーバが GGSN に対して既知であるため、GGSN では、CAC 障害通知を直接そのサーバに送信できます。

Cisco IOS SLB が dispatched モードのときに Cisco IOS SLB に CAC 障害通知を送信するよう GGSN 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	説明
ステップ 1	`Router-GGSN(config)# gprs slb mode dispatched`	GGSN-IOS SLB メッセージングの Cisco IOS SLB 動作モードとして dispatched を定義します。 **（注）**　デフォルトは dispatched モードです。
ステップ 2	`Router-GGSN(config)# gprs slb notify cac-failure`	UMTS QoS CAC 障害が原因で PDP コンテキストの作成要求が拒否された場合に Cisco IOS SLB に通知できるよう GGSN をイネーブルにします。

Cisco IOS SLB で CAC 障害通知サポートをイネーブルにするには、仮想サーバ モードで次のコマンドを使用します。

コマンド	目的
`Router-SLB(config-slb-vserver)# gtp notification cac` *count*	GGSN-IOS SLB メッセージングの CAC 障害通知のサポートをイネーブルにし、拒否された PDP コンテキストの作成要求を新しい実 GGSN に再割り当てできる最大回数を設定します。デフォルトは 2 です（セッションごとに、初期送信を含め実 GGSN が 3 回選択されます）。

Cisco IOS SLB が directed server NAT モードのときの CAC 障害通知サポートの設定

Cisco IOS SLB が directed server NAT モードで機能している場合、仮想サーバは GGSN に対して既知ではありません。したがって、Cisco IOS SLB に CAC 障害通知を送信するよう GGSN を設定すること以外に、グローバル コンフィギュレーション モードで **gprs slb vserver** コマンドを使用して GGSN で仮想サーバのリストを定義し、グローバル コンフィギュレーション モードで **gprs slb mode** コマンドを使用して Cisco IOS SLB の動作モードを定義する必要があります。

（注） Cisco IOS SLB が directed server NAT モードで機能しているときに、Cisco IOS SLB の動作モードと仮想サーバが GGSN で定義されていない場合は、**gprs slb notify cac-failure** および **gtp notification cac** コマンドが設定されていても、CAC 障害通知のサポートはイネーブルにされません。

Cisco IOS SLB が directed server NAT モードのときに Cisco IOS SLB に CAC 障害通知を送信できるよう GGSN 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	説明
ステップ 1	`Router-GGSN(config)# gprs slb mode directed`	GGSN-IOS SLB メッセージングの Cisco IOS SLB 動作モードとして directed server NAT を定義します。 **（注）** デフォルトは dispatched モードです。
ステップ 2	`Router-GGSN(config)# gprs slb notify cac-failure`	UMTS QoS CAC 障害が原因で PDP コンテキストの作成要求が拒否された場合に Cisco IOS SLB に通知できるよう GGSN をイネーブルにします。
ステップ 3	`Router-GGSN(config)# gprs slb vserver` *ip_address* [**next-hop ip** *ip-address* [**vrf** *name*]]	**gprs slb notify** コマンドを使用して定義した条件が発生したときに、GGSN が Cisco IOS SLB 仮想サーバに通知するよう設定します。 任意で、仮想サーバに到達するために使用できるネクストホップの IP アドレスも設定し、VPN ルーティング/転送インスタンスを指定します。

Cisco IOS SLB で CAC 障害通知サポートをイネーブルにするには、仮想サーバ モードで次のコマンドを使用します。

コマンド	目的
`Router-SLB(config-slb-vserver)# gtp notification cac` *count*	GGSN-IOS SLB メッセージングの CAC 障害通知のサポートをイネーブルにし、拒否された PDP コンテキストの作成要求を新しい実 GGSN に再割り当てできる最大回数を設定します。デフォルトは 2 です（セッションごとに、初期送信を含め実 GGSN が 3 回選択されます）。

GGSN-IOS SLB メッセージング削除通知のサポート（GTP IMSI スティッキ データベース サポート）の設定

GGSN および Cisco IOS SLB で削除通知のサポートが設定されている場合、加入者からの最初の PDP コンテキストの作成要求が受信されると、Cisco IOS SLB にスティッキ データベース エントリが作成されます。GGSN でその IMSI の最後の PDP コンテキストが削除されると、GGSN では、データベースからスティッキ エントリを削除するよう Cisco IOS SLB に指示する削除通知を送信します。

（注）　このように設定するには、**service gtp** キーワードを指定して **virtual** 仮想サーバ コンフィギュレーション コマンドを設定する必要があります。

（注）　複数の vserver で **sticky gtp imsi** コマンドが設定されている場合は、グループ番号を設定することによって、同じ Mobile Station（MS; モバイル ステーション）が異なる vserver 経由で接続するときにスティッキ オブジェクトを共有できるようになります。スティッキ グループ番号が同じすべての vserver によって、ユーザのスティッキ IMSI エントリが共有されます。

GGSN で IMSI の最後の PDP コンテキストが削除されたときに、削除通知を Cisco IOS SLB に送信するよう GGSN を設定するには、グローバル コンフィギュレーション モードで次の作業を実行します。

	コマンド	説明
ステップ 1	`Router-GGSN(config)# gprs slb mode {dispatched | directed}`	GGSN-IOS SLB メッセージングの Cisco IOS SLB 動作モードを定義します。デフォルトは dispatched モードです。
ステップ 2	`Router-GGSN(config)# gprs slb notify session-deletion`	IMSI に関連付けられている最後の PDP コンテキストが削除されたときに、削除通知メッセージを Cisco IOS SLB に送信するよう GGSN を設定します。
ステップ 3	`Router-GGSN(config)# gprs slb vservers` *ip_address* `[next-hop ip` *ip-address* `[vrf` *name*`]]`	**gprs slb notify** コマンドを使用して定義した条件が発生したときに、GGSN が Cisco IOS SLB 仮想サーバに通知するよう設定します。 任意で、仮想サーバに到達するために使用できるネクストホップの IP アドレスも設定し、VPN ルーティング/転送インスタンスを指定します。

Cisco IOS SLB で GTP IMSI スティッキ データベース サポートを設定するには、仮想サーバ コンフィギュレーション モードで次の作業を実行します。

コマンド	目的
Router-SLB(config-slb-vserver)# **sticky gtp imsi** [**group** *number*]	特定の IMSI に関する以前の作成要求すべてを処理したのと同じ実サーバへの GTP PDP コンテキストの作成要求をロード バランシングできるように、Cisco IOS SLB をイネーブルにします。

Cisco IOS SLB 機能のモニタリングおよびメンテナンス

GGSN に関する GTP SLB 情報をクリア、取得、および表示するには、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-GGSN# **clear gprs slb statistics**	Cisco IOS SLB 統計情報をクリアします。
Router-GGSN# **show gprs slb detail**	動作モード、GGSN-IOS SLB メッセージングの仮想サーバ アドレス、SLB 通知、統計情報など、Cisco IOS SLB 関連のすべての情報を表示します。
Router-GGSN# **show gprs slb mode**	Cisco IOS SLB の動作モードを表示します。
Router-GGSN# **show gprs slb statistics**	Cisco IOS SLB 統計情報を表示します。
Router-GGSN# **show gprs slb vservers**	GGSN-IOS SLB メッセージングの定義済み Cisco IOS SLB 仮想サーバのリストを表示します。

Cisco IOS SLB での GTP SLB に関する情報を取得および表示するには、Cisco IOS SLB で、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-SLB# **show ip slb conns** [**vserver** *virtual_server-name* | **client** *ip-address* | **firewall** *firewallfarm-name*] [**detail**]	Cisco IOS SLB によって処理されるすべての接続を表示するか、または任意で、特定の仮想サーバかクライアントに関連付けられた接続だけを表示します。
Router-SLB# **show ip slb dfp** [**agent** *agent_ip_address port-number* | **manager** *manager_ip_address* | **detail** | **weights**]	DFP および DFP エージェントに関する情報、および実サーバに割り当てられている重みに関する情報を表示します。
Router-SLB# **show ip slb gtp** {**gsn** [*gsn-ip-address*] | **nsapi** [*nsapi-key*] [**detail**]	原因コード検査を使用する GTP ロード バランシングがイネーブルにされている場合の Cisco IOS SLB GTP 情報を表示します。
Router-SLB# **show ip slb map** [*id*]	Cisco IOS SLB プロトコル マップに関する情報を表示します。
Router-SLB# **show ip slb reals** [**sfarm** *server-farm*] [**detail**]	Cisco IOS SLB に定義されている実サーバに関する情報を表示します。
Router-SLB# **show ip slb replicate**	Cisco IOS SLB 複製設定に関する情報を表示します。

コマンド	目的
Router-SLB# **show ip slb serverfarms** [**name** *serverfarm-name*] [**detail**]	Cisco IOS SLB に定義されているサーバ ファームに関する情報を表示します。
Router-SLB **show ip slb sessions** [**gtp** | **gtp-inspect** | **radius**] [**vserver** *virtual-server*] [**client** *ip-addr netmask*] [**detail**]	Cisco IOS SLB によって処理されるセッションに関する情報を表示します。 **（注）** 原因コード検査を*使用する* GTP ロード バランシングでは、1 つのセッションは **idle gtp request** コマンドを使用して指定した仮想サーバの GTP アイドル タイマーの期間よりも長く継続することはありません。
Router=SLB# **show ip slb stats**	Cisco IOS SLB 統計情報を表示します。
Router-SLB# **show ip slb sticky gtp imsi** [**id** *imsi*]	Cisco IOS SLB GTP IMSI スティッキ データベースに関連付けられている Cisco IOS SLB スティッキ データベースのエントリだけを表示し、ユーザがプライマリ PDP として使用したすべての Network Service Access Point Identifiers（NSAPI; ネットワーク サービス アクセス ポイント ID）を表示します。 任意で、指定した IMSI に関連付けられているスティッキ データベース エントリだけを表示します。
Router-SLB# **show ip slb vserver** [**name** *virtual_server*] [**redirect**] [**detail**]	Cisco IOS SLB に定義されている仮想サーバに関する情報を表示します。

設定例

ここでは、GGSN Cisco IOS SLB の例を示します。この項に記載されている GGSN コマンドの詳細については、『*Cisco GGSN Release Command Reference*』を参照してください。この項に記載されている Cisco IOS SLB コマンドの詳細については、「*IOS Server Load Balancing*」フィーチャ モジュール ドキュメントを参照してください。

ここでは、Cisco 7600 プラットフォーム上の GTP ロード バランシングおよび NAT が設定された Cisco IOS SLB の例を示します。

- 「Cisco IOS SLB の設定例」（P.13-27）
- 「GGSN1 の設定例」（P.13-29）

Cisco IOS SLB の設定例

```
hostname 7600-a
!
ip slb probe PINGPROBE ping
 interval 3
 faildetect 3
!
ip slb serverfarm SAMI1
 nat server
 probe PINGPROBE
!
 real 9.9.9.72
  reassign 4
  faildetect numconns 255 numclients 8
```

```
  inservice
!
 real 9.9.9.73
  reassign 4
  faildetect numconns 255 numclients 8
  inservice
!
 real 9.9.9.74
  reassign 4
  faildetect numconns 255 numclients 8
  inservice
!
 real 9.9.9.75
  reassign 4
  faildetect numconns 255 numclients 8
  inservice
!
 real 9.9.9.76
  reassign 4
  faildetect numconns 255 numclients 8
  inservice
!
ip slb vserver V0-GGSN
 virtual 10.10.10.10 udp 3386 service gtp
 serverfarm SAMI1
 idle gtp request 100
 inservice
!
ip slb vserver V1-GGSN
 virtual 10.10.10.10 udp 2123 service gtp
 serverfarm SAMI1
 idle gtp request 100
 inservice
!
ip slb dfp password ciscodfp 0
 agent 9.9.9.72 1111 30 0 10
 agent 9.9.9.73 1111 30 0 10
 agent 9.9.9.74 1111 30 0 10
 agent 9.9.9.75 1111 30 0 10
 agent 9.9.9.76 1111 30 0 10
!
interface FastEthernet9/36
 description TO SGSN
 no ip address
 switchport
 switchport access vlan 302
!
interface Vlan101
 description Vlan to GGSN for GN
 ip address 10.1.1.1 255.255.255.0
!
interface Vlan302
 ip address 40.0.2.1 255.255.255.0
!
router ospf 300
 log-adjacency-changes
 summary-address 9.9.9.0 255.255.255.0
 redistribute static subnets route-map GGSN-routes
 network 40.0.2.0 0.0.0.255 area 300
 network 40.0.3.0 0.0.0.255 area 300
!
ip route 9.9.9.72 255.255.255.255 10.1.1.72
ip route 9.9.9.73 255.255.255.255 10.1.1.73
ip route 9.9.9.74 255.255.255.255 10.1.1.74
```

```
ip route 9.9.9.75 255.255.255.255 10.1.1.75
ip route 9.9.9.76 255.255.255.255 10.1.1.76
!
access-list 1 permit 9.9.9.0 0.0.0.255
!
route-map GGSN-routes permit 10
 match ip address 1
!
!
```

GGSN1 の設定例

```
!
ip dfp agent gprs
 port 1111
 password ciscodfp 0
 inservice
!
interface Loopback100
 description GPRS GTP V-TEMPLATE IP ADDRESS
 ip address 9.9.9.72 255.255.255.0
!
interface GigabitEthernet0/0.2
 description Gn Interface
 encapsulation dot1Q 101
 ip address 10.1.1.72 255.255.255.0
 no cdp enable
!
interface Virtual-Template1
 description GTP v-access
 ip unnumbered Loopback100
 encapsulation gtp
 gprs access-point-list gprs
!
! route to SGSNs
ip route 40.1.2.1 255.255.255.255 10.1.1.1
ip route 40.2.2.1 255.255.255.255 10.1.1.1
```

APPENDIX A

モニタリング通知

この付録では、General Packet Radio Service（GPRS; グローバル パケット ラジオ サービス）または Universal Mobile Telecommunication System（UMTS）に関連する問題を管理するために、Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）通知をイネーブルおよびモニタリングする方法について説明します。SNMP では、管理対象デバイス上のイベントを報告するために、通知を使用します。通知とは、さまざまなイベントに関するトラップまたはインフォームのことです。

（注）この付録では、GGSN SNMP 通知のイネーブルおよびモニタリングについてだけ説明します。その他のタイプの SNMP 通知は、シスコ ルータ上でイネーブルにできます。イネーブルにできる SNMP 通知のタイプの詳細については、『*Cisco IOS Configuration Fundamentals, Release 12.4*』のマニュアルを参照してください。

また、ご使用のシスコ ルータで使用できる通知のリストを表示するには、**snmp-server enable traps ?** コマンドを入力します。

この付録は、次の内容で構成されています。

SNMP の概要

簡易ネットワーク管理プロトコル（SNMP）は、アプリケーション レイヤ プロトコルであり、ネットワーク内のデバイスをモニタリングおよび管理するための、標準化されたフレームワークと共通の言語を提供します。

SNMP フレームワークには、次の 3 つの部分があります。

- SNMP マネージャ：SNMP を使用して、ネットワーク ホストのアクティビティを制御およびモニタリングするために使用されるシステム。最も一般的な管理システムは Network Management System（NMS; ネットワーク管理システム）と呼ばれています。NMS という用語は、ネットワーク管理に使用する専用デバイスを意味する場合と、ネットワーク管理デバイス上で使用するアプリケーションを意味する場合があります。SNMP は、さまざまなネットワーク管理アプリケーションで使用できます。簡単なコマンドライン アプリケーションから機能が豊富なグラフィカル ユーザ インターフェイス（CiscoWorks2000 製品ラインなど）まで、このような機能は多岐にわたっています。

- SNMP エージェント：管理対象デバイス内のソフトウェア コンポーネントであり、デバイスのデータを維持し、必要に応じて、管理システムにそのデータを報告します。エージェントおよび Management Information Base（MIB; 管理情報ベース）はルーティング デバイス（ルータ、アクセス サーバ、またはスイッチ）上に常駐します。管理対象デバイス上で SNMP エージェントをイネーブルにする場合は、マネージャとエージェントの間の関係を定義する必要があります（「SNMP サポートのイネーブル」（P.A-9）を参照）。
- 管理情報ベース（MIB）：ネットワーク管理情報の集合であり、階層型に構成されます。

SNMP では、大量のコマンドのセットを定義する代わりに、すべての操作を get-request、get-next-request、および set-request の形式で処理します。たとえば、SNMP マネージャでは、SNMP エージェントからの値を取得したり、その SNMP エージェントに値を設定したりできます。

MIB の説明

管理情報ベース（MIB）はネットワーク管理情報の集合であり、階層型に構成されます。MIB は、オブジェクト ID によって識別される、管理対象オブジェクトの集合で構成されます。MIB には、SNMP などのネットワーク管理プロトコルを使用してアクセスします。管理対象オブジェクト（MIB オブジェクトまたはオブジェクトと呼ばれる場合もあります）は、ルータなどの管理対象デバイスが持つ、数多くの特性の 1 つです。管理対象オブジェクトは、1 つまたは複数のオブジェクト インスタンスで構成されます。本質的に、オブジェクト インスタンスは変数です。シスコが実装した SNMP では、RFC 1213 に記述されている、MIB II 変数の定義が使用されています。

MIB には、次の 2 つのタイプの管理対象オブジェクトを含めることができます。

- スカラ オブジェクト：単一のオブジェクト インスタンス（IF-MIB の ifNumber、BGP4-MIB の bgpVersion など）を定義します。
- カラム オブジェクト：行が含まれないか、または複数行が含まれ、かつ各行に 1 つまたは複数のスカラ オブジェクトが含まれる場合がある、MIB テーブルを定義します。たとえば、IF-MIB の ifTable ではインターフェイスを定義します。

システム MIB 変数には、SNMP を経由して次のようにアクセスできます。

- MIB 変数へのアクセス：NMS からの要求に応じて、SNMP エージェントによって機能が開始されます。エージェントでは、要求された MIB 変数の値を取得し、その値を使用して NMS に応答します。
- MIB 変数の設定：NMS からのメッセージに応じて、SNMP エージェントによって機能が開始されます。SNMP エージェントでは、MIB 変数の値を NMS によって要求された値に変更します。

SNMP 通知

次のような重要なシステム イベントが発生したとき、SNMP エージェントによってマネージャに通知される場合があります。

- インターフェイスまたはカードが実行を開始または停止した場合
- 温度がしきい値を超過した場合
- 認証が失敗した場合

エージェントによってアラーム条件が検出されると、エージェントによって次の処理が実行されます。

- その条件の時刻、タイプ、および重大度に関する情報のロギング
- 通知メッセージの生成と指定された IP ホストへの送信

SNMP 通知は次のいずれかとして送信されます。

- トラップ：SNMP マネージャからの受信確認応答を必要としない、信頼性の低いメッセージ。
- インフォーム：SNMP マネージャが応答を発行するまでメモリに保存される、信頼性の高いメッセージ。インフォームでは、トラップより多くのシステム リソースを使用します。

（注）　多くのコマンドでは、コマンド構文においてトラップという用語を使用します。コマンドにおいて、トラップまたはインフォームのいずれかを選択するオプションがある場合を除き、トラップというキーワードはトラップとインフォームのいずれか、または両方を意味します。**snmp-server host** コマンドを使用すると、SNMP 通知をトラップまたはインフォームのいずれとして送信するかを指定できます。

エージェントは、アラーム条件を検出すると、この条件の時刻、タイプおよび重大度に関する情報をロギングし、通知メッセージを生成して、次に、指定された IP ホストに送信します。

SNMP 通知は、*トラップ*または*インフォーム*のいずれかとして送信できます。GGSN でトラップをイネーブルにする方法については、「SNMP サポートのイネーブル」（P.A-9）を参照してください。GGSN トラップの詳細については、「GGSN 通知」（P.A-11）を参照してください。

シスコが実装した SNMP では、RFC 1215 に記述されている、SNMP トラップの定義が使用されています。

SNMP のバージョン

Cisco IOS ソフトウェアでは、次のバージョンの SNMP がサポートされています。

- SNMPv1：簡易ネットワーク管理プロトコル。RFC 1157 で定義されたインターネット標準です。コミュニティ ストリングに基づいてセキュリティを実現します。
- SNMPv2c：コミュニティ ストリングに基づく、SNMPv2 用の管理フレームワークです。SNMPv2c は、SNMPv2p（SNMPv2 クラシック）のプロトコル オペレーションおよびデータ型を更新したものであり、コミュニティベースのセキュリティ モデルである SNMPv1 を使用します。
- SNMPv3：SNMP バージョン 3。SNMPv3 では、次のセキュリティ機能を使用して、デバイスへの安全なアクセスを実現します。
  - メッセージ整合性：パケットが中継中に改ざんされていないことを確認します。
  - 認証：メッセージが有効な発信元からのものであることを判断します。
  - 暗号化：パケットのコンテンツをスクランブルして、不正な発信元によって認識されないようにします。

SNMPv1 および SNMPv2c

SNMPv1 と SNMPv2c の両方において、コミュニティベース形式のセキュリティが使用されます。エージェント MIB にアクセスできるマネージャのコミュニティが、IP アドレス アクセス コントロール リストおよびパスワードによって定義されます。

SNMPv2c サポートには、バルク取得メカニズム、および管理ステーションに対するより詳細なエラー メッセージ報告が含まれています。バルク取得メカニズムによって、テーブルおよび大量の情報を取得することがサポートされます。この処理によって、必要となるラウンドトリップ送信数が最小化されます。SNMPv2c ではエラー処理のサポートが改善されました。たとえば、異なる種類のエラー条件が区別されるように、エラー コードが拡張されました。SNMPv1 では、これらの条件は単一のエラー コードを使用して報告されていました。現在は、エラー戻りコードによってエラー タイプが報告されるようになりました。また、次の 3 種類の例外も報告されます。

- no such object exceptions（オブジェクト例外が見つかりません）
- no such instance exceptions（インスタンス例外が見つかりません）
- end of MIB view exceptions（MIB ビューの終わり例外）

SNMPv3

SNMPv3 には、次のセキュリティ モデルおよびセキュリティ レベルがあります。

- セキュリティ モデル：ユーザおよびユーザが属するグループに対して設定される認証方法です。
- セキュリティ レベル：セキュリティ モデル内で許可されるセキュリティのレベル。

セキュリティ モデルとセキュリティ レベルの組み合せによって、SNMP パケットを処理するときに適用されるセキュリティ メカニズムが決定されます。

SNMP セキュリティ モデルおよびセキュリティ レベル

表 A-1 に、異なるバージョンの SNMP によって実現されるセキュリティ モデルおよびセキュリティ レベルを示します。

表 A-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	説明
v1	noAuthNoPriv	コミュニティ ストリング	なし	認証にコミュニティ ストリングの照合を使用。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	認証にコミュニティ ストリングの照合を使用。
v3	noAuthNoPriv	ユーザ名	なし	認証にユーザ名の照合を使用。
v3	authNoPriv	MD5 または SHA	なし	HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供。
v3	authPriv	MD5 または SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供。CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化も提供します。

管理ステーションでサポートされている SNMP のバージョンが使用されるように、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できます。このため、1 つの管理ステーションとは SNMPv1 プロトコルを使用して通信し、1 つの管理ステーションとは SNMPv2c プロトコルを使用して通信し、もう 1 つの管理ステーションとは SMNPv3 を使用して通信することがサポートされるように、Cisco IOS ソフトウェアを設定できます。

コメント要求

MIB モジュールは、SNMP MIB モジュール言語を使用して記述され、一般的に、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）に対して提出される、Request For Comments（RFC; コメント要求）文書内で定義されています。RFC は、インターネット学会、およびインターネット コミュニティ全体での検討を要求することを目的に、個人またはグループによって作成されます。草案は、RFC ステータスが付与される前に、インターネット ドラフト（I-D）文書として公開されます。また、推奨される水準に達した RFC は、Standard（STD; 標準）文書というラベルも付けられます。詳細については、インターネット学会および IETF の Web サイト（http://www.isoc.org および http://www.ietf.org）を参照してください。

シスコでは、シスコのシステム専用の MIB 拡張を提供しています。シスコのエンタープライズ MIB は、このマニュアルで特に明記しないかぎり、該当の RFC に記述されているガイドラインに準拠しています。

オブジェクト ID

object identifier（OID; オブジェクト ID）によって、管理対象ネットワーク デバイス上の MIB オブジェクトが一意に識別されます。OID によって、MIB 階層内における MIB オブジェクトの位置が識別され、複数の管理対象デバイスのネットワーク内にある MIB オブジェクトにアクセスする方法が提供されます。

- 標準 RFC MIB OID は、Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）によって割り当てられます。
- エンタープライズ MIB OID は、Cisco Assigned Numbers Authority（CANA）によって割り当てられます。

OID 内の各番号は、MIB 階層のレベルに対応しています。たとえば、OID 1.3.6.1.4.1.9.9.xyz は、MIB 階層内で次の位置にある、*xyz*-MIB を表しています。カッコ内の数字は、MIB 階層内での対応を示すためにだけ含められています。実際に使用される OID は、数字の値だけで表現されます。

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoMgt(9).*nn*-MIB

IF-MIB の ifNumber などの管理対象オブジェクトは、オブジェクト名（iso.org.dod.internet.mgmt.enterprises.interfaces.ifNumber）または OID（1.3.6.1.2.1.2.1）によって、一意に識別できます。

MIB オブジェクトに割り当てられている OID のリストについては、次の URL を参照してください。

ftp://ftp.cisco.com/pub/mibs/oid/

関連情報および有益なリンク

次の URL にアクセスすると、シスコ MIB に関する一般的な情報を参照できます。このページのリンクを使用すると、MIB にアクセスしてダウンロードしたり、アプリケーション ノート、OID のリストなどの関連情報にアクセスしたりできます。

- http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

TAC に関する情報および FAQ

次の URL にアクセスすると、Cisco Technical Assistance Center（TAC）が開発した SNMP 情報を参照できます。

- http://www.cisco.com/warp/public/477/SNMP/index.html は、SNMP に関する Cisco TAC ページです。一般的な SNMP 情報へのリンク、および SNMP を使用してデータを収集するためのヒントが示されています。
- http://www.cisco.com/warp/public/477/SNMP/mibs_9226.shtml は、シスコ MIB に関する frequently asked questions（FAQ; よくある質問）のリストです。

SNMP 設定情報

次の URL にアクセスすると、SNMP の設定に関する情報を参照できます。

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fcmonitr.htm では、SNMP サポートの設定に関する一般的な情報を参照できます。この資料は、『*Cisco IOS Configuration Fundamentals Configuration Guide*』の一部です。
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_r/frprt3/frmonitr.htm では、SNMP コマンドに関する情報を参照できます。この資料は、『*Cisco IOS Configuration Fundamentals Command Reference*』の一部です。

MIB サポートの設定

この章では、シスコ ルータに SNMP および MIB サポートを設定する方法について説明します。次の内容で構成されています。

Cisco IOS のリリースに含まれている MIB の判別

使用している Cisco IOS リリースに、どの MIB が含まれているかを判別するには、次の手順を実行します。

ステップ 1　Feature Navigator のホームページ http://tools.cisco.com/ITDIT/MIBS/servlet/index にアクセスします。

ステップ 2　[Cisco IOS MIB Locator] をクリックしてアプリケーションを起動します。MIB Locator アプリケーションを使用すると、次の 3 通りの方法で MIB を検索できます。

a. リリース、プラットフォーム ファミリ、およびフィーチャ セットによる検索 : [MIB Locator] ページから

- ドロップダウン メニューをクリックし、目的の Cisco IOS ソフトウェア リリースを選択します。
- [Platform Family] メニューから、[7600-SAMI] を選択します。最初にプラットフォームを選択した場合は、選択したプラットフォームに該当するリリースおよびフィーチャ セットだけが表示されます。
- [Feature Set] メニューから、適切な GGSN リリースを選択します。

b. イメージ名による検索：[MIB Locator] ページから、[Search by Image Name] フィールドに使用する GGSN イメージ名を次のように（示されているイメージ名は一例です）入力し、[Submit] をクリックします。

```
c6svcsami-g8is-mz.124-15.XQ.bin
```

c. MIB 名による検索：[MIB Locator] ページから、[Search for MIB] メニューの MIB のリストで MIB を検索します。1 つを選択するか、または、複数選択する場合には、**Ctrl** キーを押した状態で [Submit] をクリックします。

（注）　選択したあとは、リンクを順に選択し、指示に従ってください。

MIB のダウンロードおよびコンパイル

次の項では、GGSN での MIB のダウンロードおよびコンパイル方法に関する情報を示します。

MIB の処理に関する考慮事項

MIB を使用する場合は、次のことについて留意してください。

データ型定義の不一致

- データ型定義が一致しない場合、コンパイラ エラーまたは警告メッセージが発生する場合があります。シスコ MIB のデータ型定義では不一致でなくても、標準 RFC MIB では不一致となる場合があります。次に例を示します。

```
MIB A defines: SomeDatatype ::= INTEGER(0..100)
MIB B defines: SomeDatatype ::= INTEGER(1..50)
```

この例は軽度のエラーであると判断され、警告メッセージが出力されますが、MIB は正常にロードされます。

次の例では、2 つの定義は本質的には同等であるものの、重大なエラーであると判断され、MIB は正常に解析されません。

```
MIB A defines: SomeDatatype ::= DisplayString
MIB B defines: SomeDatatype ::= OCTET STRING (SIZE(0..255))
```

使用している MIB コンパイラによってこれらのことがエラーとして扱われる場合、または警告メッセージを削除する場合は、定義が一致するように、この同じデータ型を定義する MIB のいずれかを編集します。

- 数多くの MIB が他の MIB から定義をインポートします。MIB をロードすることが管理アプリケーションによって要求され、かつ未定義のオブジェクトに関する問題が発生する場合は、次の MIB をこの順番に従ってロードできます。

  SNMPv2-SMI.my
  SNMPv2-TC.my
  SNMPv2-MIB.my

RFC1213-MIB.my
IF-MIB.my
CISCO-SMI.my
CISCO-PRODUCTS-MIB.my
CISCO-TC.my

- 詳細情報および SNMP のテクニカル ティップスを参照するには、[Locator] ページから [SNMP MIB Technical Tips] をクリックしてリンクを順に選択するか、または次の URL にアクセスしてください。

  http://www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Internetworking:SNMP&s=Implementation_and_Configuration#Samples_and_Tips

- MIB オブジェクトに割り当てられている SNMP オブジェクト ID（OID）のリストを参照するには、次の URL にアクセスして [SNMP Object Navigator] をクリックし、リンクを順に選択してください。

  http://tools.cisco.com/ITDIT/MIBS/servlet/index

（注） MIB Locator にアクセスするには、シスコ CCO 名およびパスワードが必要となります。

- シスコ MIB のダウンロードおよびコンパイル方法の詳細については、次の URL にアクセスしてください。

  http://www.cisco.com/warp/public/477/SNMP/mibcompilers.html

MIB のダウンロード

MIB がまだない場合に、MIB を使用するシステムにダウンロードするには、次の手順を実行します。

ステップ 1　前の項（「MIB の処理に関する考慮事項」）の考慮事項を確認します。

ステップ 2　次に示すシスコの URL のいずれかにアクセスします。ダウンロードする MIB がない場合は、もう一方の URL にアクセスします。いずれにもない場合は、ステップ 5 に示す URL のいずれかにアクセスします。

ftp://ftp.cisco.com/pub/mibs/v2
ftp://ftp.cisco.com/pub/mibs/v1

ステップ 3　MIB へのリンクをクリックすると、MIB がダウンロードされます。

ステップ 4　[File] > [Save]、または [File] > [Save As] を選択すると、システムに MIB が保存されます。

ステップ 5　業界標準の MIB は次の URL からダウンロードできます。

- http://www.ietf.org
- http://www.atmforum.com

MIB のコンパイル

シスコ ルータを SNMP ベースの管理アプリケーションと組み合せる場合は、そのプラットフォーム用に MIB をコンパイルすることも必要となります。たとえば、UNIX オペレーティング システムで HP OpenView を使用する場合は、HP OpenView ネットワーク管理システム（NMS）を使用して、プラットフォーム MIB をコンパイルする必要があります。詳しくは、NMS のマニュアルを参照してください。

SNMP サポートのイネーブル

SNMP がサポートされるようにシスコ ルータを設定する手順の概要は、次のとおりです。

SNMP コマンドの詳細については、次のシスコのマニュアルを参照してください。

- 『*Cisco IOS Release 12.3 Configuration Fundamentals Configuration Guide*』、「Monitoring the Router and Network」の項。次の URL で参照できます。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm

- 『*Cisco IOS Release 12.3 Configuration Fundamentals Command Reference*』、「Part 3: System Management Commands」の「Router and Network Configuration Commands」の項。次の URL で参照できます。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/index.htm

SNMP がサポートされるようにシスコ ルータを設定するには、次の手順を実行します。

ステップ 1　ルータの command line interface（CLI; コマンドライン インターフェイス）を使用して、基本的な SNMP 設定を設定します。これらの基本的なコンフィギュレーション コマンドは SNMPv2c の場合に発行します。SNMPv3 の場合は、SNMP ユーザおよびグループを設定する必要もあります（コマンドおよび設定の情報については、前述のマニュアルのリストを参照してください）。

a. SNMP read-only コミュニティおよびコミュニティを定義します。

```
Router (config)# snmp-server community Read_Only_Community_Name ro
Router (config)# snmp-server community Read_Write_Community_Name rw
```

b. SNMP ビューを定義します（異なる SNMP ユーザ グループからアクセスできるオブジェクトの範囲を制限するため）。

```
Router (config)# snmp-server view view_name oid-tree {included | excluded}
```

SNMP 通知のイネーブルおよびディセーブル

SNMP 通知をイネーブルおよびディセーブルにするには、次の項の作業を実行します。

- 「CLI を使用した GGSN 通知のイネーブルおよびディセーブル」（P.A-9）
- 「SNMP を使用した GGSN SNMP 通知のイネーブルおよびディセーブル」（P.A-11）
- 「SNMP を使用した GGSN SNMP 通知のイネーブルおよびディセーブル」（P.A-11）

CLI を使用した GGSN 通知のイネーブルおよびディセーブル

コマンドライン インターフェイス（CLI）を使用してシスコ ルータでの GGSN SNMP 通知（トラップおよびインフォーム）の送信をイネーブルにするには、次の手順を実行します。

ステップ 1　ルータで SNMP が設定されていることを確認します（「SNMP サポートのイネーブル」（P.A-9）を参照）。

ステップ 2　IP アドレスを使用して、シスコ ルータからトラップを受信するホストを識別します。

```
Router(config)#snmp-server host host-address version SNMP version community/user(V3)
udp-port <UDP port No>
```

ステップ 3　次のコマンドを使用して、シスコ ルータでの GGSN SNMP 通知をイネーブルにします（イネーブルにする通知のタイプごとに、個別のコマンドを入力します）。

```
Router(config)#snmp-server enable traps gprs [apn | charging | ggsn | ggsn-apn |
ggsn-general | ggsn-memory | ggsn-pdp | ggsn-service | gtp | csg | dcca]
```

上記で

- **apn**：access point name（APN; アクセス ポイント ネーム）通知をイネーブルにします。
- **charging**：課金通知をイネーブルにします。
- **ggsn**：GGSN グローバル通知をイネーブルにします。

（注）　フラッディングを防止するには、**snmp-server enable traps gprs ggsn** コマンドを設定すると、cGgsnGlobalErrorNotif、cGgsnAccessPointNameNotif、および cGgsnPacketDataProtocolNotif トラップ以外のすべての GGSN 関連のトラップがイネーブルになります。

- **ggsn-apn**：APN（cGgsnAccessPointNameNotif）固有の GGSN 通知をイネーブルにします。
- **ggsn-general**：GGSN 一般通知（cGgsnGlobalErrorNotif）をイネーブルにします。
- **ggsn-pdp**：Packet Data Protocol（PDP; パケット データ プロトコル）固有の GGSN 通知（cGgsnPacketDataProtocolNotif）をイネーブルにします。
- **ggsn-service**：GGSN サービス モード通知をイネーブルにします。
- **gtp**：GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）トラップをイネーブルにします。
- **csg**：GGSN CSG 固有の通知をイネーブルにします。
- **dcca**：GGSN Diameter Credit Control Application（DCCA）固有の通知をイネーブルにします。

（注）　キーワード オプションを指定しないで **snmp-server enable traps gprs** コマンドを発行すると、すべての GGSN SNMP 通知がイネーブルになります。

ステップ 4　シスコ ルータで GGSN SNMP 通知をディセーブルにするには、次のコマンドを入力します。

```
Router(config)# no snmp-server enable traps gprs
```

通知タイプのキーワード（gprs など）を省略すると、すべての通知がディセーブルになります。

（注）　**snmp-server enable traps gtp** コマンドは設定しないことを推奨します。これは、すべての関連する MIB が非推奨であるためです。

SNMP を使用した GGSN SNMP 通知のイネーブルおよびディセーブル

GGSN SNMP 通知は、次のオブジェクトを true（1）または false（2）に設定することによって、イネーブルおよびディセーブルにできます。

- cGgsnServiceNotifEnabled：GGSN サービス モード通知のイネーブルまたはディセーブル
- cGgsnMemoryNotifEnabled：メモリ関連の通知のイネーブルまたはディセーブル
- cGgsnGlobalErrorNotifEnabled：GGSN 一般通知のイネーブル
- cGgsnAccessPointNotifEnabled：cGgsnAccessPointNameNotif 通知のイネーブルまたはディセーブル
- cGgsnPdpNotifEnabled：cGgsnPacketDataProtocolNotif 通知のイネーブルまたはディセーブル
- cGgsnSACsgNotifEnabled：CSG 状態トラップのイネーブルまたはディセーブル
- cGgsnSADccaNotifEnabled：DCCA 関連の通知のイネーブルまたはディセーブル

GGSN 通知

この項では、GGSN MIB でサポートされ、GGSN によって生成される通知のリストおよび簡単な説明を示します。

この項では、次のタイプの通知のリストを示します。

- 「グローバル通知」（P.A-11）
- 「課金通知」（P.A-15）
- 「アクセス ポイント通知」（P.A-16）
- 「アラーム通知」（P.A-18）

グローバル通知

表 A-2 は、CISCO-GGSN-MIB でサポートされているグローバル通知のリストを示しています。これらの通知の送信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 **snmp-server enable traps gprs** コマンドを使用します。このとき、**ggsn**、**ggsn-apn**、**ggsn-memory**、**ggsn-pdp**、**ggsn-service**、**csg** および / または **dcca** キーワード オプションを指定します。

（注）　キーワード オプションごとに個別のコマンドを発行します。

（注）　cGgsnNotification（1.2.6.1.4.1.9.9.240.2.0.1）は非推奨です。

表 A-2　グローバル通知

通知および通知オブジェクト	注
cGgsnInServiceNotif（1.3.6.1.4.1.9.9.240.2.0.2）	GGSN が運用（inService）モードになったとき、送信されます。 GGSN を運用モードにするには、グローバル コンフィギュレーション モードで **gprs service-mode operational** コマンドを使用するか、または cGgsnServiceMode オブジェクトを inService(1) に設定します。 サービス モードは cGgsnServiceModeStatus によって識別されます。 この通知の生成をイネーブルにするには、cGgsnServiceNotifEnabled を true(1) に設定します。
cGgsnMaintenanceNotif（1.3.6.1.4.1.9.9.240.2.0.3）	GGSN がメンテナンス モードになったとき、送信されます。 GGSN をメンテナンス モードにするには、グローバル コンフィギュレーション モードで **gprs service-mode maintenance** コマンドを使用するか、または cGgsnServiceMode オブジェクトを maintenance(2) に設定します。 サービス モードは cGgsnServiceModeStatus によって識別されます。 この通知の生成をイネーブルにするには、cGgsnServiceNotifEnabled を true(1) に設定します。
cGgsnMemThresholdReachedNotif（1.3.6.1.4.1.9.9.240.2.0.4）	GGSN メモリしきい値に達したとき、送信されます。 メモリしきい値を設定するには、グローバル コンフィギュレーション モードで **gprs memory threshold** コマンドを使用するか、または cGgsnMemoryThreshold を設定します。 この通知の生成をイネーブルにするには、cGgsnMemoryNotifEnabled を true(1) に設定します。
cGgsnMemThresholdClearedNotif（1.3.6.1.4.1.9.9.240.2.0.5）	GGSN がメモリを保持し、設定されたしきい値を下回ったとき、送信されます。 メモリしきい値を設定するには、グローバル コンフィギュレーション モードで **gprs memory threshold** コマンドを使用するか、または cGgsnMemoryThreshold を設定します。 この通知の生成をイネーブルにするには、cGgsnMemoryNotifEnabled を true(1) に設定します。
cGgsnGlobalErrorNotif（1.3.6.1.4.1.9.9.240.2.0.8） cGgsnGlobalErrorTypes cGgsnHistNotifSeverity cGgsnHistNotifTimestamp cGgsnHistNotifGgsnIpAddrType cGgsnHistNotifGgsnIpAddr cGgsnHistNotifInfo	GGSN 関連のアラームが発生したとき、送信されます。 特定のタイプのアラームに関する追加情報がある場合は、その情報が追加の変数バインドとして、通知の末尾に付加されます。 この通知の生成をイネーブルにするには、cGgsnGlobalErrorNotifEnabled を true(1) に設定します。 **（注）** フラッディングを防止するために、リリース 5.1 以降では、GGSN の cGgsnNotification が cGgsnGlobalErrorNotif、cGgsnAccessPointNameNotif、および cGgsnPacketDataProtocolNotif に置き換えられています。 cGgsnGlobalErrorNotif アラームの詳細については、「cGgsnGlobalErrorNotif」（P.A-19）を参照してください。

表 A-2　グローバル通知 （続き）

通知および通知オブジェクト	注
cGgsnAccessPointNameNotif **（1.3.6.1.4.1.9.9.240.2.0.9）** cGgsnAccessPointErrorTypes cGgsnHistNotifSeverity cGgsnHistNotifTimestamp cGgsnHistNotifGgsnIpAddrType cGgsnHistNotifGgsnIpAddr cGgsnHistNotifInfo cGgsnNotifAccessPointName	APN 関連のアラームが発生したとき、送信されます。 特定のタイプのアラームに関する追加情報がある場合は、その情報が追加の変数バインドとして、通知の末尾に付加されます。 この通知の生成をイネーブルにするには、cGgsnAccessPointNotifEnabled を true(1) に設定します。 **（注）** フラッディングを防止するために、リリース 5.1 以降では、GGSN の cGgsnNotification が cGgsnGlobalErrorNotif、cGgsnAccessPointNameNotif、および cGgsnPacketDataProtocolNotif に置き換えられています。 cGgsnAccessPointNameNotif アラームの詳細については、「cGgsnAccessPointNameNotif」（P.A-19）を参照してください。
cGgsnPacketDataProtocolNotif **（1.3.6.1.4.1.9.9.240.2.0.10）** cGgsnPacketDataProtoErrorTypes cGgsnHistNotifSeverity cGgsnHistNotifTimestamp cGgsnHistNotifGgsnIpAddrType cGgsnHistNotifGgsnIpAddr cGgsnHistNotifInfo cGgsnNotifAccessPointName cGgsnNotifPdpMsisdn cGgsnNotifPdpImsi	ユーザ関連のアラームが発生したとき、送信されます。 特定のタイプのアラームに関する追加情報がある場合は、その情報が追加の変数バインドとして、通知の末尾に付加されます。 この通知の生成をイネーブルにするには、cGgsnPdpNotifEnabled を true(1) に設定します。 **（注）** フラッディングを防止するために、リリース 5.1 以降では、GGSN の cGgsnNotification が cGgsnGlobalErrorNotif、cGgsnAccessPointNameNotif、および cGgsnPacketDataProtocolNotif に置き換えられています。 cGgsnPacketDataProtocolNotif アラームの詳細については、「cGgsnPacketDataProtocolNotif」（P.A-22）を参照してください。

サービス認識課金通知

表 A-3 は、CISCO-GGSN-SERVICE-AWARE-MIB でサポートされている、サービス認識課金通知のリストを示しています。これらの通知の送信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 **snmp-server enable traps gprs** コマンドを使用します。このとき、**csg** および / または **dcca** キーワード オプションを指定します。

（注） キーワード オプションごとに個別のコマンドを発行します。

表 A-3　サービス認識課金通知

通知および通知オブジェクト	注
cGgsnSACsgStateUpNotif **(1.3.6.1.4.1.9.9.497.2.0.1)** cGgsnSANotifCsgRealAddressType, cGgsnSANotifCsgRealAddress, cGgsnSANotifCsgVirtualAddrType, cGgsnSANotifCsgVirtualAddress, cGgsnSANotifCsgPort	CSG へのリンクがアクティブになったとき、送信されます。 ポート番号が CSG グループで設定されていない場合、cGgsnSANotifCsgPort 情報ではデフォルト値が使用されます。 この通知の生成をイネーブルにするには、cGgsnSACsgNotifEnabled を true(1) に設定します。
cGgsnSACsgStateDownNotif **(1.3.6.1.4.1.9.9.497.2.0.2)** cGgsnSANotifCsgRealAddressType, cGgsnSANotifCsgRealAddress, cGgsnSANotifCsgVirtualAddrType, cGgsnSANotifCsgVirtualAddress, cGgsnSANotifCsgPort	CSG へのリンクがダウンしたとき、送信されます。 ポート番号が CSG グループで設定されていない場合、cGgsnSANotifCsgPort 情報ではデフォルト値が使用されます。 この通知の生成をイネーブルにするには、cGgsnSACsgNotifEnabled を true(1) に設定します。
cGgsnSADccaEndUsrServDeniedNotif **(1.3.6.1.4.1.9.9.497.2.0.3)** cGgsnNotifPdpImsi cGgsnNotifPdpMsisdn	サービス制限により、クレジット制御サーバがサービス要求を拒否したとき、送信されます。 この通知がカテゴリ レベルで受信されると、DCCA クライアントでは、その PDP のそのカテゴリに対する今後のすべてのユーザ トラフィックを廃棄します。 この通知の生成をイネーブルにするには、cGgsnSADccaNotifEnabled を true(1) に設定します。
cGgsnSADccaCreditLimReachedNotif **(1.3.6.1.4.1.9.9.497.2.0.4)** cGgsnNotifPdpImsi cGgsnNotifPdpMsisdn	クレジット制限に達したとき、送信されます。 エンド ユーザのアカウントでは、要求されたサービスを処理できなかったため、クレジット制御サーバがサービス リクエストを拒否します。クライアントは、CGgsnDccaEndUsrServDeniedNotif の場合と同様に動作します。 この通知の生成をイネーブルにするには、cGgsnSADccaNotifEnabled を true(1) に設定します。
cGgsnSADccaUserUnknownNotif **(1.3.6.1.4.1.9.9.497.2.0.5)** cGgsnNotifPdpImsi cGgsnNotifPdpMsisdn	指定されたエンド ユーザがクレジット コントロール サーバにとって未知である場合に送信されます。 このような固定的な障害が発生すると、クライアントはアイドル状態になります。クライアントでは、結果コードが CCA(Initial) または CCA(Update) のいずれにおいて受信されたかに応じて、PDP コンテキストを拒否または終了します。 この通知の生成をイネーブルにするには、cGgsnSADccaNotifEnabled を true(1) に設定します。

表 A-3　サービス認識課金通知 （続き）

通知および通知オブジェクト	注
cGgsnSADccaRatingFailedNotif (1.3.6.1.4.1.9.9.497.2.0.6) cGgsnNotifPdpImsi cGgsnNotifPdpMsisdn	レーティング入力が不十分であったか、Attribute Value Pair（AVP; アトリビュート値ペア）の組み合せが無効であったか、または AVP や AVP 値がレーティングで認識されないか、またはサポートされていないことによって、クレジット制御サーバがレーティングできなかったとき、送信されます。 この通知の生成をイネーブルにするには、cGgsnSADccaNotifEnabled を true(1) に設定します。
cGgsnSADccaAuthRejectedNotif (1.3.6.1.4.1.9.9.497.2.0.7) cGgsnNotifPdpImsi cGgsnNotifPdpMsisdn	クレジット制御サーバがエンド ユーザを認可できなかったとき、送信されます。 PDP コンテキストは削除され、そのカテゴリはブラックリストに含められます。 この通知の生成をイネーブルにするには、cGgsnSADccaNotifEnabled を true(1) に設定します。

課金通知

表 A-4 は、CISCO-GPRS-CHARGING-MIB でサポートされている、課金関連のトラップのリストを示しています。これらの通知の送信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 **snmp-server enable traps gprs charging** コマンドを使用します。

表 A-4　課金通知

通知および通知オブジェクト	注
cgprsCgAlarmNotif（1.3.6.1.4.1.9.9.192.2.0.1） cgprsCgAlarmHistType cgprsCgAlarmHistAddrType cgprsCgAlarmHistAddress cgprsCgAlarmHistSeverity cgprsCgAlarmHistInfo	管理対象システムで課金関連のアラームが検出されたとき、送信されます。 このアラームは、cgprsCgAlarmHistTable にエントリが追加されたあと、送信されます。 この通知の生成をイネーブルにするには、cgprsCgAlarmEnable を true(1) に設定します。 cgprsCgAlarmNotif アラームの詳細については、「CgprsCgAlarmNotif」（P.A-23）を参照してください。
cgprsCgGatewaySwitchoverNotif (1.3.6.1.4.1.9.9.192.2.0.2) cgprsCgActiveChgGatewayAddrType cgprsCgActiveChgGatewayAddress cgprsCgOldChgGatewayAddress	アクティブな課金ゲートウェイが切り替えられたとき、送信されます。 新しい課金ゲートウェイへのスイッチオーバーは、課金ゲートウェイのスイッチ タイマーに指定された値に基づいて発生します。 課金ゲートウェイのスイッチ タイマーを設定するには、グローバル コンフィギュレーション モードで **gprs charging server-switch-timer** コマンドを使用するか、または cgprsCgGroupSwitchOverTime を設定します。新しい課金ゲートウェイが選択される優先度を設定するには、グローバル コンフィギュレーション モードで **gprs charging switchover priority** コマンドを使用するか、または cgprsCgSwitchOverPriority を設定します。 この通知の生成をイネーブルにするには、cgprsCGAlarmEnable を true(1) に設定します。

表 A-4　課金通知 （続き）

通知および通知オブジェクト	注
cgprsCgInServiceModeNotif **（1.3.6.1.4.1.9.9.192.2.0.3）**	GGSN 課金機能が運用モードになったとき、送信されます。 GGSN の課金機能を運用モードにするには、グローバル コンフィギュレーション モードで **gprs charging service-mode** コマンドを使用するか、または cgprsCgServiceMode オブジェクトを operational(1) に設定します。 この通知の生成をイネーブルにするには、cgprsCGAlarmEnable を true(1) に設定します。
cgprsCgMaintenanceModeNotif **（1.3.6.1.4.1.9.9.192.2.0.4）**	GGSN 課金機能がメンテナンス モードになったとき、送信されます。 GGSN 課金機能をメンテナンス モードにするには、グローバル コンフィギュレーション モードで **gprs charging service-mode** コマンドを使用するか、または cgprsCgServiceMode オブジェクトを maintenance(2) に設定します。 この通知の生成をイネーブルにするには、cgprsCGAlarmEnable を true(1) に設定します。

アクセス ポイント通知

表 A-5 は、CISCO-GPRS-ACC-PT-MIB でサポートされている、アクセス ポイント関連の通知のリストを示しています。この通知の送信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 **snmp-server enable traps gprs apn** コマンドを使用します。

表 A-5　アクセス ポイント通知

通知および通知オブジェクト	注
cgprsAccPtCfgNotif（1.3.6.1.4.1.9.9.183.2.0.1） cgprsAccPtCfgNotifAccPtIndex cgprsAccPtCfgNotifReason	アクセス ポイント設定が発生したとき、送信されます。 この通知は、cgprsAccPtCfgNotifHistTable にエントリが追加されたあと、送信されます。 この通知の生成をイネーブルにするには、cgprsAccPtCfgNotifEnable を true(1) に設定します。 cgprsAccPtCfgNotif アラームの詳細については、「cgprsAccPtCfgNotif」（P.A-26）を参照してください。
cgprsAccPtSecSrcViolNotif **（1.3.6.1.4.1.9.9.183.2.0.2）** cgprsAccPtCfgNotifAccPtIndex cgprsAccPtMsAddrType cgprsAccPtMsAllocAddr cgprsAccPtMsNewAddr	セキュリティ違反が発生したとき、特に、GGSN によって、アップストリーム TPDU の送信元アドレスが以前に Mobile Station（MS; モバイル ステーション）に割り当てられたものと異なると判断された場合に、送信されます。 この通知の生成をイネーブルにするには、**security verify**（IPv4 PDP の場合）、または **ipv6 security verify source**（IPv6 PDP の場合）アクセス ポイント コンフィギュレーション コマンドを使用するか、cgprsAccPtVerifyUpStrTpduSrcAddr オブジェクトを true(1) に設定します。

表 A-5　アクセス ポイント通知 （続き）

通知および通知オブジェクト	注
cgprsAccPtSecDestViolNotif **（1.3.6.1.4.1.9.9.183.2.0.3）** cgprsAccPtCfgNotifAccPtIndex cgprsAccPtMsAddrType cgprsAccPtMsAllocAddr cgprsAccPtMsTpduDstAddr	セキュリティ違反が発生したとき、特に、アップストリーム TPDU の宛先アドレスが、ユーザ定義の Public LAN Mobile Network（PLMN; パブリック LAN モバイル ネットワーク）アドレスのグローバル リストの範囲内であると GGSN が判断した場合に、送信されます。 この通知の生成をイネーブルにするには、**security verify destination** アクセス ポイント コンフィギュレーション コマンドを使用するか、または cgprsAccPtVerifyUpStrTpduDstAddr オブジェクトを true(1) に設定します。
cgprsAccPtMaintenanceNotif **（1.3.6.1.4.1.9.9.183.2.0.4）** cgprsAccPtCfgNotifAccPtIndex	APN がメンテナンス モードになったとき、送信されます。 APN をメンテナンス モードにするには、**service-mode maintenance** アクセス ポイント コンフィギュレーション コマンドを使用するか、または cgprsAccPtOperationMode オブジェクトを maintenance(1) に設定します。 サービス モードは cGgsnServiceModeStatus によって識別されます。 この通知の生成をイネーブルにするには、cgprsAccPtMaintenanceNotif を true(1) に設定します。
cgprsAccPtInServiceNotif **（1.3.6.1.4.1.9.9.183.2.0.5）** cgprsAccPtCfgNotifAccPtIndex	APN が運用モードになったとき、送信されます。 APN を運用モードにするには、**service-mode operational** アクセス ポイント コンフィギュレーション コマンドを使用するか、または cgprsAccPtOperationMode を inService(0) に設定します。 サービス モードは cGgsnServiceModeStatus によって識別されます。 この通知の生成をイネーブルにするには、cgprsAccPtMaintenanceNotif を true(1) に設定します。

GTP 通知

表 A-6CISCO-GTP-MIB でサポートされている GTP 関連の通知のリストを示しています。この通知の送信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 **snmp-server enable traps gprs gtp** コマンドを使用します。

表 A-6　GTP 通知

通知および通知オブジェクト	注
cGtpPathFailedNotification **（1.3.6.1.4.1.9.9.188.2.0.1）** cGtpLastNoRespToEchoGSNIpAddrTyp cGtpLastNoRespToEchoGSNIpAddr	グローバル コンフィギュレーション モードで **gprs gtp n3-requests** コマンドを使用して設定された N3-requests カウンタの時間間隔において、GGSN ピア（Serving GPRS Support Node（SGSN; サービング GPRS サポート ノード）または課金ゲートウェイ）が GTP エコー要求メッセージへの応答に失敗したとき、送信されます。 この通知の生成をイネーブルにするには、cGtpNotifEnable を true(1) に設定します。

アラーム通知

通知は、重大度に応じて、アラームまたは情報イベントであると判断されます。重大度が critical、major、または minor である通知は、アラームに分類されます。アラームの重大度が報告対象外であっても、アラームのアラーム状態が変化した場合は、報告される必要があります。

情報イベントの状態の変化は必須ではありません。情報イベントは、修正処理が必要でない、通常と異なる条件が発生したことを示す警告です。情報イベントは報告されますが、一時的な状態です。問題解決のための修正処理は必要ありません。

表 A-7 は、重大度と必要な応答のリストを示しています。

表 A-7　通知の重大度

重大度	説明
Critical	重大な条件が存在します。処理が推奨される場合は、critical アラームをただちにクリアします。
Major	サービスの中断が発生しました。このアラームをただちにクリアします。
Minor	サービスの中断は発生しませんでしたが、できるだけ早くこのアラームをクリアします。
Informational	修正処理が必要でない、通常と異なる条件が発生したことを示す警告です。情報イベントは報告されますが、一時的な状態です。管理センターから問題解決のための修正処理は要求されません。

アラームにはトラップ タイプが関連付けられます。表 A-8 は、アラームと関連付けることができるトラップ タイプを示しています。

表 A-8　アラーム トラップ タイプ

トラップ タイプ	説明
1（cleared）	以前のアラーム条件がクリアされたことを示します。個々の状況について説明している他の箇所で、アラーム条件がクリアされることによって、通知またはこの値のアラーム重大度を含むその他のイベントが生成されることが特に記述されている場合を除き、必須ではありません。
2（indeterminate）	重大度を判別できないことを示します。
3（critical）	サービスに影響を及ぼす条件が発生し、ただちに処理することを要求される場合があります。
4（major）	サービスに影響を及ぼす条件が発生し、緊急の修正処理が要求される場合があります。
5（minor）	サービスに影響を及ぼさない条件が存在し、より重大な条件（安全性に影響を及ぼす問題など）が発生しないようにするために、修正処理を実行する必要があります。
6（warning）	重大な影響が発生する前に、潜在的な、または近い将来発生する可能性のあるサービスまたは安全性に影響を及ぼす条件が検出されました。
7（info）	アラーム条件は他の重大度定義のいずれにも該当しません。この条件には、重要であるものの、緊急性の低い通知または情報イベントが含まれる場合があります。

次の項では、次の通知でサポートされているアラームについて説明します。

- 「cGgsnGlobalErrorNotif」（P.A-19）
- 「cGgsnAccessPointNameNotif」（P.A-19）
- 「CgprsCgAlarmNotif」（P.A-23）
- 「cgprsAccPtCfgNotif」（P.A-26）

cGgsnGlobalErrorNotif

表 A-9 は、cGgsnGlobalErrorNotif 通知（CISCO-GGSN-MIB）でサポートされているアラームのリストを示しています。cGgsnGlobalErrorNotif 通知でサポートされているアラームはグローバル関連アラームです。

表 A-9　cGgsnGlobalErrorNotif Alarms

アラーム	説明
ggsnServiceUp	原因： GGSN サービスが開始されました。グローバル コンフィギュレーション モードで **service gprs** コマンドが発行されました。 **重大度およびトラップ タイプ：** 重大度は critical です。トラップ タイプは 3 です。 **推奨処置：** 情報イベントです。処理は必要ありません。
ggsnServiceDown	原因： GGSN サービスがダウンしました。グローバル コンフィギュレーション モードで **no gprs service** コマンドが発行されたか、またはシステム サービスが別の理由によってダウンしました。 **重大度およびトラップ タイプ：** 重大度は critical です。トラップ タイプは 3 です。 **推奨処置：** グローバル コンフィギュレーション モードで **service gprs** コマンドを発行することによって、ルータで GGSN サービスを再度開始します。問題が解決しない場合は、シスコ テクニカルサポート担当者にご連絡ください。このとき、エラー メッセージをご提示ください。
noDHCPServer	原因： DHCP サーバが設定されていません。このエラー通知は、DHCP サーバ設定の一部がないか、または誤っている場合に生成されます。 **重大度およびトラップ タイプ：** 重大度は major です。トラップ タイプは 4 です。 **推奨処置：** DHCP 設定のすべての要素が適切に設定されていることを確認します。

cGgsnAccessPointNameNotif

表 A-10 は、cGgsnAccessPointNameNotif 通知（CISCO-GGSN-MIB）でサポートされているアラームのリストを示しています。cGgsnAccessPointNameNotif 通知でサポートされているアラームは APN 関連アラームです。

表 A-10　cGgsnAccessPointNameNotif アラーム

アラーム	説明
noRadius	原因： Remote Authentication Dial-In User Service（RADIUS）サーバが設定されていません。このエラー通知は、RADIUS サーバ設定の一部がない場合に生成されます。 重大度およびトラップ タイプ： 重大度は major です。トラップ タイプは 4 です。 推奨処置： 1. RADIUS サーバが適切に設定されていること、およびこのサーバへの ping が成功することを確認します。 2. RADIUS サーバが適切に設定されていることを確認します。 （注）　シスコ テクニカルサポート担当者にご連絡ください。このとき、エラー メッセージ、および show running configuration コマンドを発行した結果をご提示ください。

表 A-10　cGgsnAccessPointNameNotif アラーム （続き）

アラーム	説明
ipAllocationFail	原因： 次の理由により、ダイナミック IP 割り当てが失敗しました。 1. DHCP サーバまたは RADIUS サーバに関する次のいずれかの問題が発生した可能性があります。 　a. DHCP サーバまたは RADIUS サーバの IP アドレスが GGSN で誤って設定されています。 　b. DHCP サーバまたは RADIUS サーバはアクセス可能ですが、IP アドレスを割り当てるための設定が誤っています。 　c. DHCP サーバまたは RADIUS サーバは適切に設定されていますが、アクセスできません。 2. ダイナミック IP 割り当てが APN 設定でディセーブルになっています。 3. 透過モードの RADIUS クライアントからの PAP または CHAP のユーザ名およびパスワード情報がありません。このため、この情報が PDP アクティベーション要求に含まれていません。 **重大度およびトラップ タイプ：** 重大度は major です。トラップ タイプは 4 です。 **推奨処置：** 1. DHCP サーバまたは RADIUS サーバの設定について、次のことを確認します。 　a. GGSN で設定されている DHCP サーバまたは RADIUS サーバの IP アドレスが有効であること 　b. DHCP サーバまたは RADIUS サーバでの IP アドレス割り当てが適切に設定されていること 　c. DHCP サーバまたは RADIUS サーバがアクセス可能であること（**ping** コマンドを使用） 2. APN において、DHCP プロキシ クライアントまたは RADIUS クライアントのいずれかとして、IP 割り当てプールを設定します。 3. 上記の処理のいずれによってもアラーム条件が解決しない場合は、シスコ テクニカルサポート担当者にご連絡ください。このとき、エラー メッセージをご提示ください。
apnUnreachable	原因： PDP コンテキストの作成要求で要求された APN が GGSN で設定されていないため、PDP アクティベーションが失敗しました。 **重大度およびトラップ タイプ：** 重大度は major です。トラップ タイプは 4 です。 **推奨処置：** 対応する APN の設定を確認します。設定が正しい場合は、シスコ テクニカルサポート担当者にご連絡ください。このとき、エラー メッセージ、および **show running-config** と **show gprs access-point all** コマンドの出力を保存したデータをご提示ください。

cGgsnPacketDataProtocolNotif

表 A-11 は、cGgsnPacketDataProtocolNotif 通知（CISCO-GGSN-MIB）でサポートされているアラームのリストを示しています。cGgsnPacketDataProtocolNotif 通知でサポートされているアラームは PDP 関連アラームです。

表 A-11　cGgsnPacketDataProtocolNotif アラーム

アラーム	説明
noResource	**原因：** 次のいずれかの理由により、GGSN サービスを継続するために使用できるリソースが不足しています。 • PDP コンテキストの最大数に達しました。 • PPP 再生成された PDP コンテキストの最大数に達しました。 **重大度およびトラップ タイプ：** 重大度は critical です。トラップ タイプは 3 です。 **推奨処置：** 可能な場合は、GGSN で処理できる PDP コンテキストの数を増やします。問題が解決しない場合は、シスコ テクニカルサポート担当者にご連絡ください。このとき、エラー メッセージをご提示ください。
authenticationFail	**原因：** 次のいずれかの理由により、PDP アクティベーションが失敗しました。 1. RADIUS サーバが設定されていないか、またはアクセス可能でないため、認証に使用できる RADIUS サーバがありません。 2. PDP コンテキストの作成要求で無効なユーザ名またはパスワードが使用されています。 3. 非透過モードの PDP コンテキストの作成要求に、PAP または CHAP 情報エレメントがありません。 4. PDP コンテキストの作成要求にユーザ名がありません。 5. APN にアクセスする IP アドレスが重複しています。 **重大度およびトラップ タイプ：** 重大度は warning です。トラップ タイプは 6 です。 **推奨処置：** RADIUS サーバが適切に設定されていること、および **ping** コマンドを使用してこのサーバにアクセスできることを確認します。これらが該当する場合は、シスコ テクニカルサポート担当者にご連絡ください。このとき、エラー メッセージ、および **show running-config** の出力を保存したデータをご提示ください。

表 A-11　cGgsnPacketDataProtocolNotif アラーム （続き）

アラーム	説明
ccrInitFail	原因： CCR(Initial) が Diameter サーバに送信され、CCA(Initial) 応答を受信する前に、Tx 時間が期限切れになりました。 重大度およびトラップ タイプ： 重大度は major です。トラップ タイプは 4 です。 推奨処置： PDP コンテキスト作成の処理は、credit control failure handling（CCFH; クレジット制御障害処理）設定によって決定されます。Diameter サーバ、および GGSN の DCCA Tx タイマーと CCFH の設定が、正しく設定されていることを確認します。
quotaPushFail	原因： クォータ プッシュが失敗しました。1）CSG と GGSN のクォータ サーバ プロセスの間のパスがダウンしているか、または 2）CSG が、クォータ プッシュ要求に対する否定的なクォータ プッシュ応答を送信した。 重大度およびトラップ タイプ： 重大度は major です。トラップ タイプは 4 です。 推奨処置： CSG 設定、GGSN のクォータ サーバ設定、および CSG とクォータ サーバの間のパス ステートを確認します。条件が解決しない場合は、シスコ テクニカルサポート担当者にご連絡ください。このとき、エラー メッセージをご提示ください。

CgprsCgAlarmNotif

表 A-12 は、CgprsCgAlarmNotif 通知（CISCO-GPRS-CHARGING-MIB）でサポートされているアラームのリストを示しています。CgprsCgAlarmNotif 通知でサポートされているアラームは、GGSN の課金機能に関連するアラームです。

表 A-12　CgprsCgAlarmNotif アラーム

アラーム	説明
cgprsCgAlarmCgDown	原因： 課金ゲートウェイが設定されていないか、または課金ゲートウェイ パスで nodealive 要求に対する応答がないことによって、課金ゲートウェイ（プライマリ、セカンダリ、およびターシャリ）がダウンしています。 重大度およびトラップ タイプ： 重大度は critical です。トラップ タイプは 3 です。 推奨処置： 課金ゲートウェイが存在し、正しい IP アドレスが割り当てられていることを確認します。このようになっている場合、課金ゲートウェイはダウンしています。
cgprsCgAlarmCgUp	原因： 課金ゲートウェイが活動化しています。 重大度およびトラップ タイプ： 重大度は critical です。トラップ タイプは 3 です。 推奨処置： 情報イベントです。処理は必要ありません。

表 A-12　CgprsCgAlarmNotif アラーム （続き）

アラーム	説明
cgprsCgAlarmTransFailure	**原因：** GGSN では、データ レコード転送要求に対する課金ゲートウェイからの応答の受信に繰り返し失敗しました。 **重大度およびトラップ タイプ：** 重大度は critical です。トラップ タイプは 3 です。 **推奨処置：** GGSN で課金ゲートウェイが適切に設定されていること、および課金機能がアクティブであることを確認します。
cgprsCgAlarmTransSuccess	**原因：** GGSN では、障害のあと、課金ゲートウェイにデータ レコード転送要求を正常に送信しました。 **重大度およびトラップ タイプ：** 重大度は critical です。トラップ タイプは 3 です。 **推奨処置：** 情報イベントです。処理は必要ありません。
cgprsCgAlarmCapacityFull	**原因：** GGSN バッファが一杯です。後続のパケットが廃棄される可能性があります。 **重大度およびトラップ タイプ：** 重大度は critical です。トラップ タイプは 3 です。 **推奨処置：** **gprs charging send-buffer** グローバル コンフィギュレーション コマンドに設定された値を確認し、可能な場合は、バッファに設定されたバイト数を大きくしてください。
cgprsCgAlarmCapacityFree	**原因：** GGSN call detail record（G-CDR; GGSN 呼詳細レコード）のバッファリング障害が発生したあと、GGSN では G-CDR をバッファリングできました。 **重大度およびトラップ タイプ：** 重大度は critical です。トラップ タイプは 3 です。 **推奨処置：** 情報イベントです。処理は必要ありません。
cgprsCgAlarmEchoFailure	**原因：** GGSN では、エコー要求に対する課金ゲートウェイからのエコー応答の受信に失敗しました。 **重大度およびトラップ タイプ：** 重大度は critical です。トラップ タイプは 3 です。 **推奨処置：** 課金ゲートウェイが GGSN で適切に設定されていることを確認します。条件が解決しない場合は、シスコ テクニカルサポート担当者にご連絡ください。このとき、エラーメッセージをご提示ください。

表 A-12　CgprsCgAlarmNotif アラーム （続き）

アラーム	説明
cgprsCgAlarmEchoRestored	**原因：** GGSN では、cgprsCgAlarmEchoFailure が送信されたあと、課金ゲートウェイからのエコー応答を受信しました。 **重大度およびトラップ タイプ：** 重大度は critical です。トラップ タイプは 3 です。 **推奨処置：** 情報イベントです。処理は必要ありません。
cgprsCgAlarmChargingDisabled	**原因：** GGSN で課金トランザクションがディセーブルになったことを示します。 **重大度およびトラップ タイプ：** 重大度は critical です。トラップ タイプは 3 です。 **推奨処置：** 情報イベントです。処理は必要ありません。
cgprsCgAlarmChargingEnabled	**原因：** GGSN で課金トランザクションがイネーブルになったことを示します。 **重大度およびトラップ タイプ：** 重大度は critical です。トラップ タイプは 3 です。 **推奨処置：** 情報イベントです。処理は必要ありません。
cgprsCgGatewaySwitchoverNotif	**原因：** アクティブな課金ゲートウェイが切り替えられたことを示します。 **推奨処置：** 情報イベントです。課金ゲートウェイのスイッチオーバーが発生した理由を判別します。
cgprsCgInServiceModeNotif	**原因：** GGSN 課金機能がメンテナンス モードからインサービス モードまたは運用モードになったことを示します。 **推奨処置：** 情報イベントです。処理は必要ありません。
cgprsCgMaintenanceModeNotif	**原因：** GGSN 課金機能がインサービス モードまたは運用モードからメンテナンス モードになったことを示します。 **推奨処置：** 情報イベントです。処理は必要ありません。

cgprsAccPtCfgNotif

表 A-13 は、cgprsAccPtCfgNotif 通知（CISCO-GPRS-ACC-PT-MIB）でサポートされているアラームのリストを示しています。

表 A-13　cgprsAccPtCfgNotif

アラーム	説明
cgprsAccPtCfgNotif	**原因：** アクセス ポイント コンフィギュレーションが作成、変更、または削除されました。 **重大度およびトラップ タイプ：** 適用されません。 **推奨処置：** 情報イベントです。処理は必要ありません。