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。

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。

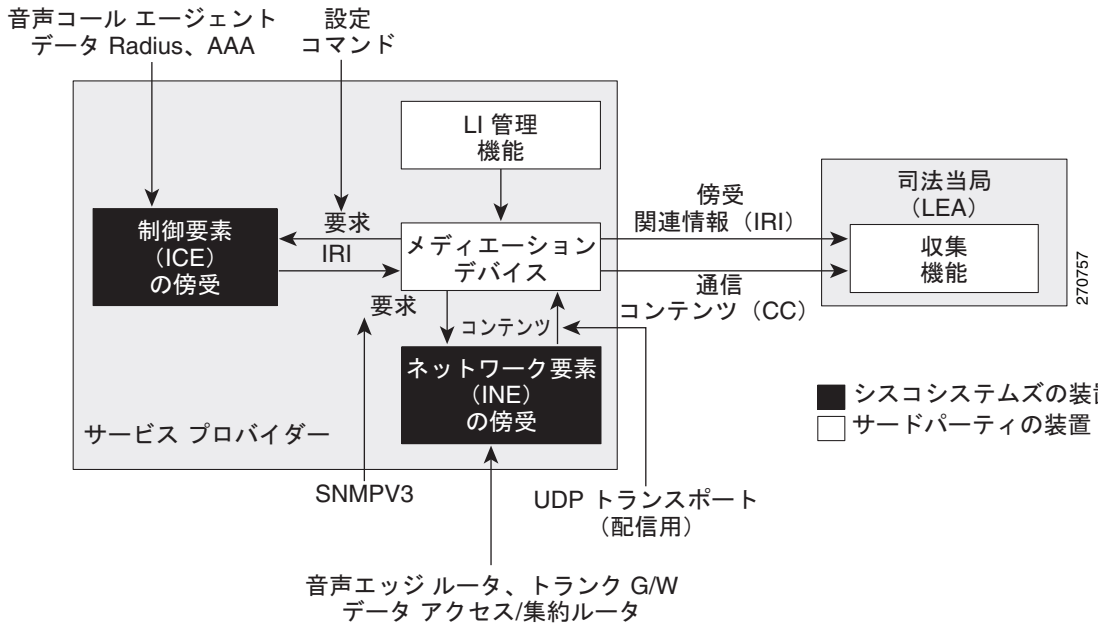
- **CISCO-MOBILITY-TAP-MIB**：CISCO-MOBILITY-TAP-MIB には、モビリティ ゲートウェイ トラフィックで傍受を設定および実行するための SNMP 管理オブジェクトが含まれています。

  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
!
```