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。

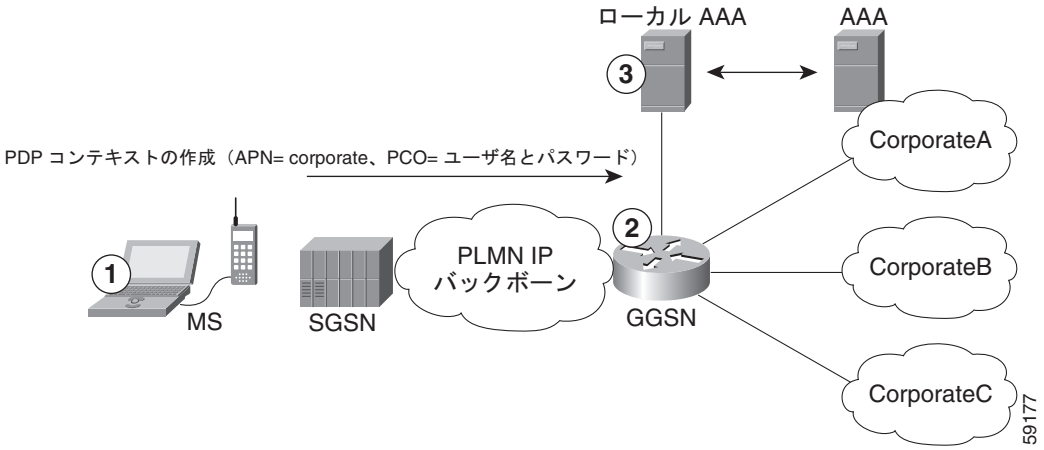
- Call Detail Record（CDR; 呼詳細レコード）にはドメイン情報が含まれません。仮想 APN の場合、Username アトリビュートからドメイン情報が削除されるためです。デフォルトでは、CDR および仮想 APN に対する認証要求には、その仮想 APN に関連付けられた実 APN 名が使用されます。ただし、**gprs charging cdr-option** コマンドに **apn virtual** キーワード オプションを指定して、CDR で仮想 APN を送信するように GGSN を設定できます。
- Cisco IOS ソフトウェアでは仮想アクセス ポイントに他のアクセス 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
```

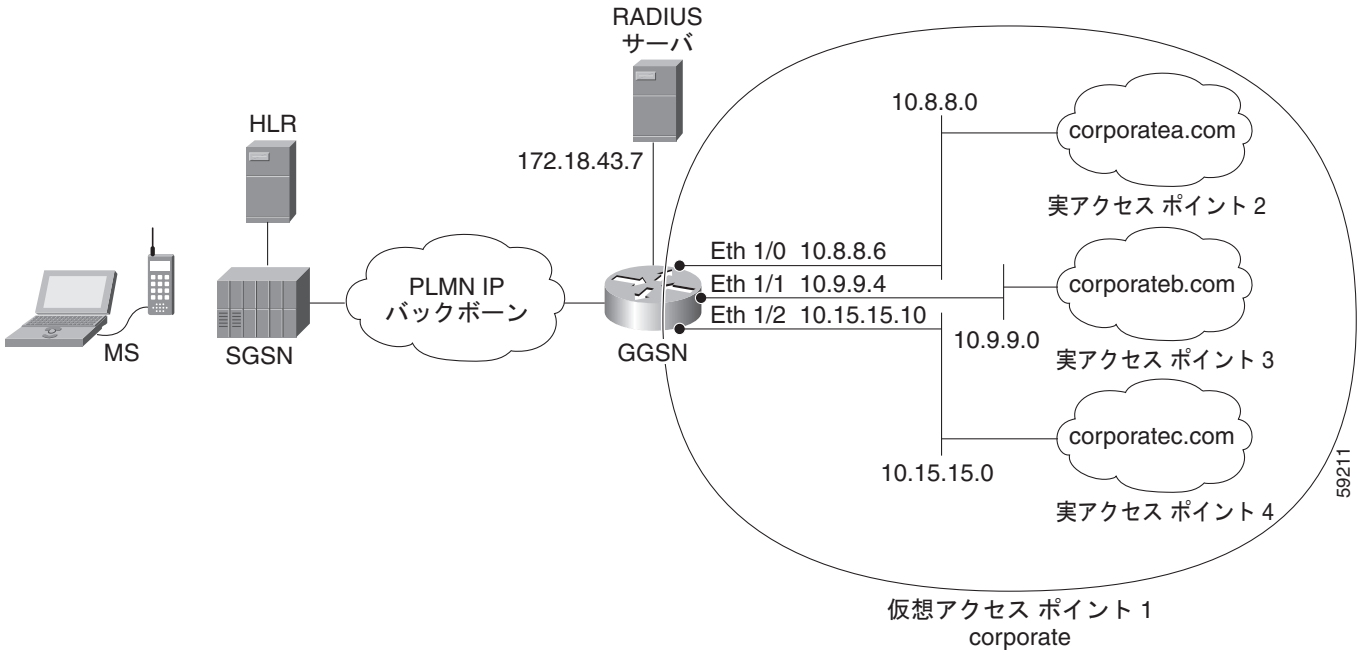
仮想 APN 設定の例

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
!
```