



CHAPTER 4

GGSN での IPv6 PDP サポートの設定

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

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

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

この章は、次の内容で構成されています。

- 「[GGSN での IPv6 PDP の概要](#)」(P.4-1)
- 「[GGSN での IPv6 PDP サポートの実装](#)」(P.4-5)
- 「[IPv6 のモニタリングおよびメンテナンス](#)」(P.4-13)
- 「[設定例](#)」(P.4-14)

GGSN での IPv6 PDP の概要

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

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

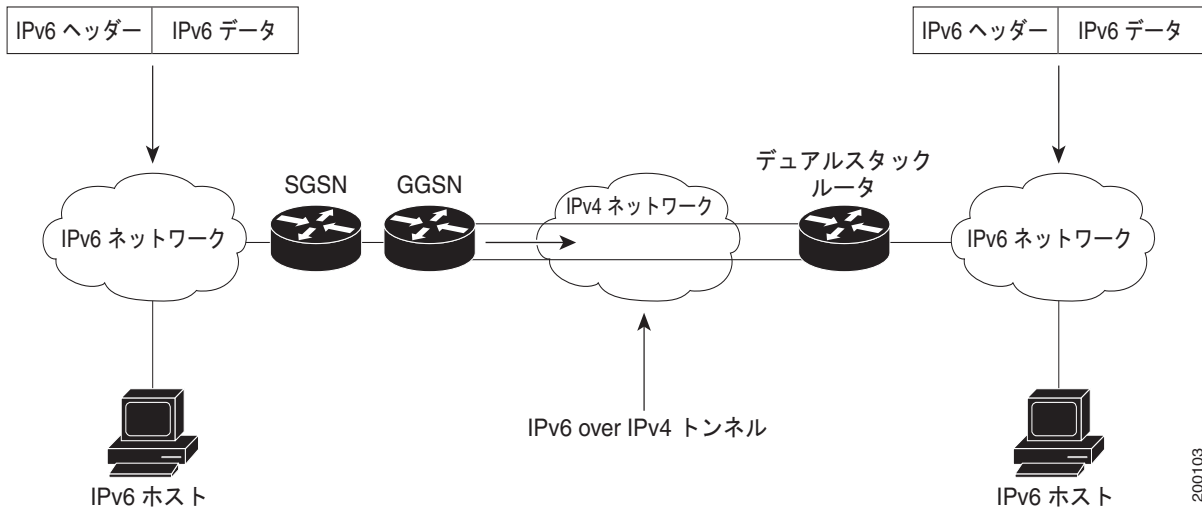


(注)

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

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

図 4-1 IPv6 over IPv4 トンネルの設定



IPv6 ステートレス自動設定

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

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

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

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

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

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

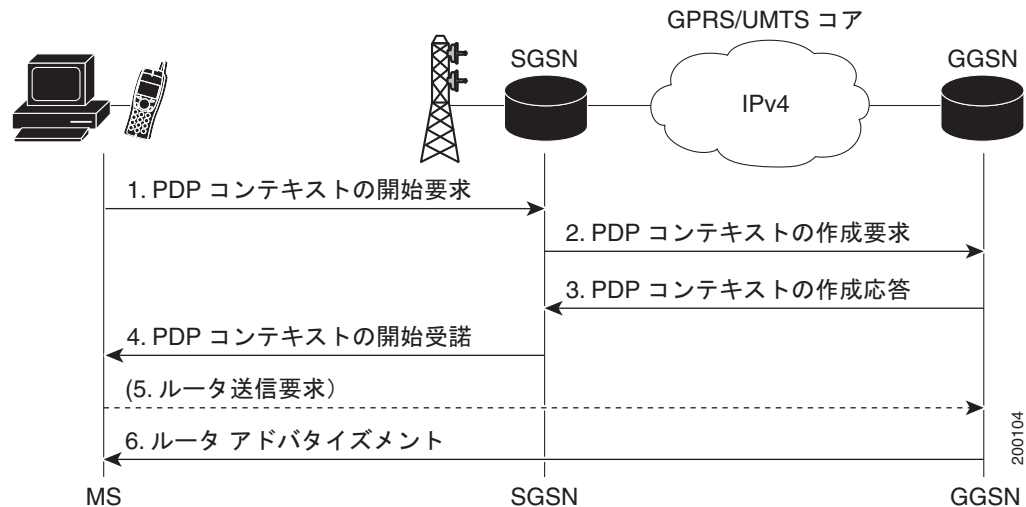


図 4-2 に示すコールフローの手順では、次のことが実行されます。

1. PDP コンテキストの開始要求：MS から SGSN に PDP コンテキストの開始要求が送信されます。
2. PDP コンテキストの作成要求：SGSN から GGSN に PDP コンテキストの作成要求が送信されます。
SGSN から PDP コンテキストの作成要求を受信すると、GGSN では、PDP コンテキストに割り当てられたプレフィクスと GGSN によって生成されたインターフェイス ID で構成される IPv6 アドレスが生成されます。
3. PDP コンテキストの作成応答：PDP コンテキストの作成応答で GGSN から SGSN にアドレスが返されます。
MS が GGSN へのリンク上で単独であると見なされるため、インターフェイス ID は PDP コンテキスト全体で一意である必要はありません。MS では、受信したアドレスからインターフェイス ID が抽出されて格納され、リンクローカルアドレスおよび完全な IPv6 アドレスを作成するために使用されます。
4. PDP コンテキストの開始受諾：SGSN から MS に PDP コンテキストの開始受諾が送信され、コンテキストが確立されます。
5. ルータ送信要求：MS から GGSN にルータ送信要求が送信される場合と、されない場合があります。
6. ルータ アドバタイズメント：GGSN から RA が定期的に送信されます。

RA では、GGSN から 64 ビットのプレフィクス（ステップ 3 で提供したものと同一プレフィクス）が送信されます。MS で RA が受信されると、ステップ 3 で受信したインターフェイス ID またはローカルで生成されたインターフェイス ID と、RA で提供されたプレフィクスを連結することによって、完全な IPv6 アドレスが作成されます。RA に複数のプレフィクスが含まれる場合、MS では 1 つめのプレフィクスだけが考慮され、残りは破棄されます。

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

サポートされる機能

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

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

制約事項

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

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

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



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

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

GGSN での IPv6 PDP サポートの実装

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

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

GGSN での IPv6 トラフィックの転送のイネーブル

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

手順の概要

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

手順の詳細

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

IPv6 ベース仮想テンプレート インターフェイスの設定

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

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

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



注意

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

手順の概要

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

手順の詳細

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

■ GGSN での IPv6 PDP サポートの実装

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

APN での IPv6 サポートのイネーブル

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

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

APN で IPv6 サポートをイネーブルにするには、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたは処理	目的
ステップ1	<code>enable</code> 例： Router> enable	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ2	<code>configure terminal</code> 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3	<code>access-point access-point-index</code> 例： Router(config)# access-point 2	アクセス ポイント番号を指定し、アクセス ポイント コンフィギュレーション モードを開始します。
ステップ4	<code>access-point-name apn-name</code> 例： Router(config-access-point)# access-point-name ipv6_apn1.com	定義されたアクセス ポイントでユーザが GGSN からアクセスできる PDN のネットワーク（またはドメイン）名を指定します。
ステップ5	<code>ipv6 [enable exclusive]</code> 例： Router(config-access-point) ipv6 enable	アクセス ポイントで IPv6 PDP コンテキストを許可するように設定します。 <ul style="list-style-type: none">• enable : APN で IPv4 と IPv6 両方の PDP コンテキストのサポートを設定します。• exclusive : APN で IPv6 PDP コンテキストだけのサポートを設定します。 デフォルトでは、IPv4 PDP コンテキストだけが APN でサポートされています。
ステップ6	<code>ipv6 dns primary ipv6-address [secondary ipv6-address]</code> 例： Router(config-access-point) ipv6 dns primary 2001:999::9	プライマリ（およびバックアップ）IPv6 DNS のアドレスが、要求された場合に IPv6 PDP コンテキストの作成応答で送信されるように指定します。
ステップ7	<code>ipv6 ipv6-address-pool {local pool-name radius-client}</code> 例： Router(config-access-point) ipv6 ipv6-address-pool local localv6	アクセス ポイントのダイナミック IPv6 プレフィクス割り当て方法を設定します。 (注) Cisco GGSN の今回のリリースでは、ローカルに設定されたプールによる IPv6 プレフィクス割り当てがサポートされています。
ステップ8	<code>ipv6 ipv6-access-group ACL-name [up down]</code> 例： Router(config-access-point) ipv6 ipv6-access-group ipv6filter down	Access Control List (ACL; アクセス コントロール リスト) 設定をアップリンクまたはダウンリンクのペイロード パケットに適用します。

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

ローカル IPv6 プレフィクス プールの設定

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

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

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

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

手順の概要

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

手順の詳細

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

コマンドまたは処理	目的
<p>ステップ3 <code>ipv6 local pool poolname prefix/prefix-length assigned-length [shared] [cache-size size]</code></p> <p>例 :</p> <pre>Router(config)# ipv6 local pool pool1 2001:0DB8::/48 64</pre> <pre>Router# show ipv6 local pool</pre> <pre>Pool Prefix Free In use</pre> <pre>pool1 2001:0DB8::/48 65516 20</pre>	<p>ローカル IPv6 プレフィクス プールを設定します。</p> <p>(注) 割り当てられた長さとして値 64 を設定する必要があります。GGSN で受け入れられるプレフィクスの最小の長さは /48 です。</p>
<p>ステップ4 <code>exit</code></p> <p>例 :</p> <pre>Router(config)# exit</pre>	<p>インターフェイス コンフィギュレーション モードを終了します。</p>

IPv6 アクセス コントロール リストの設定

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

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

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

手順の概要

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

手順の詳細

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

その他の IPv6 サポート オプションの設定

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

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

GGSN アクセス ポイントの IPv6 固有のその他のオプションを設定するには、アクセス ポイント コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
ステップ 1 Router(config-access-point)# ipv6 ipv6-access-group <i>ACL-name</i> [up down] 	(任意) アクセス コントロール リスト (ACL) 設定をアップリンクまたはダウンリンクのペイロード パケットに適用します。
ステップ 2 Router(config-access-point)# ipv6 redirect [all intermobile] <i>ipv6-address</i> 	(任意) GGSN で IPv6 トラフィックを外部 IPv6 デバイスにリダイレクトするように設定します。使用できるオプションは次のとおりです。 <ul style="list-style-type: none"> • 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。 • <i>ipv6-address</i>: IPv6 トラフィックのリダイレクト先となる IPv6 外部デバイスの IP アドレス。
ステップ 3 Router(config-access-point)# ipv6 security verify source 	(任意) GGSN で、アップストリーム Transport Protocol Data Unit (TPDU; 転送プロトコル データ ユニット) の IPv6 送信元アドレスを、以前に MS に割り当てられたアドレスと照合して検証できるようにします。

IPv6 のモニタリングおよびメンテナンス

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

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

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

設定例

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

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