



アドレス プールの設定

IP アドレス スペースの効率的な管理を目指しているサービス プロバイダーは、アドレス プールからリモート ユーザーにアドレスを効率的に割り当てたり、これらのプールを効果的に管理するためのアドレス割り当てメカニズムを実装する必要があります。この実装を行うには、利用率の低いアドレス プールや、アドレスが不足しているプールを取り扱うための戦略が必要です。アドレスが割り当てられたリモート ユーザーごとに、対応する **Virtual Routing and Forwarding (VRF)** インスタンス内で、各自へのルートを設定しなければなりません。単一の **Provider Edge (PE; プロバイダー エッジ)** ルータは数百個の VRF をサポートでき、プロバイダーのネットワークには数百または数千の PE ルータを収容できるため、設定はさらに複雑になります。すべての VRF 内、および単一 PE ルータ上のデフォルト ルーティング テーブル内のルートの総数は著しく増大することがあるため、経路集約のためのアドレス メカニズムが必要となります。

Cisco 10000 シリーズ ルータでは、IP アドレス スペースの管理を強化するために、次のアドレス プール機能をサポートしています。

- **ODAP マネージャ (p.10-5)** — アドレス プールのサイズを動的に変更し、効率的な経路集約を可能にするアドレス割り当てメカニズムを提供します。
- **オーバーラッピング IP アドレス プール (p.10-18)** — 複数の IP アドレス スペースの使用、および Cisco 10000 シリーズ ルータでサポートされる異なる **Virtual Private Network (VPN; バーチャルプライベート ネットワーク)** 間での IP アドレスの再利用が可能になります。

この章では、現在配備されているアドレス割り当てメカニズム (**On-demand Address Pool [ODAP] マネージャ機能**および**オーバーラッピング IP アドレス プール機能**) の利点および欠点について説明します。

- **アドレス割り当てメカニズム (p.10-2)**
- **ODAP マネージャ (p.10-5)**
- **オーバーラッピング IP アドレス プール (p.10-18)**

アドレス割り当てメカニズム

通常、サービス プロバイダーでは次のアドレス割り当てメカニズムを導入しています。

- ローカルアドレス プール (p.10-2)
- RADIUS ベース アドレス割り当て (p.10-2)
- DHCP ベース アドレス割り当て (p.10-3)

ここでは、これらのアドレス割り当てメカニズムの利点および欠点について説明します。

ローカル アドレス プール

ローカルアドレス プールは、PE ルータ上に静的に設定された IP アドレスのプールです。アドレス プールは、プール名で識別されます。Point-to-Point (PPP; ポイントツーポイント プロトコル) セッションが特定のプール内のアドレスを要求すると、プール マネージャはプール内の未使用のアドレスを割り当てます。PPP セッションがアドレスを戻すと、プール マネージャはアドレスを取得元のプールに戻します。

プールのグループは、共通のグループ ID で識別されます。Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) VPN ネットワーク アーキテクチャでは、各プール グループを使用して、特定の VPN に属するリモート ユーザにアドレスが割り当てられます。アドレス プールは公式に VRF に関連付けられていません。ただし、アドレス プールに関連付けられた各 VPN は、特定の VRF にも関連付けられるため、アドレス プールは VRF に非公式に関連付けられています。

オーバーラッピング アドレスの割り当て機能は、プライベート アドレスを使用する VPN カスタマーに大きな利点をもたらします。異なるグループ内の 2 つのアドレス プールにオーバーラッピング IP アドレスを格納することはできますが、同じグループ内の 2 つのアドレス プールにはオーバーラッピング アドレスを格納できません。

ローカル アドレス プールの利点

ローカルアドレス プールの主な利点は、ルートを効率的に集約できることです。

- 単一の PE ルータに設定されたルートの総数は、著しく増大することがあります。経路集約により、VRF およびデフォルト ルーティング テーブルのサイズが増大しないようにすることができます。
- 集約ルートは、アドレス プール内のすべてのサブネットに対応しています。
- 集約ルートは、アドレス プールに関連付けられた VRF で設定されます。

ローカル アドレス プールの欠点

ローカルアドレス プールの欠点は、静的に設定されているため、プールの利用率が低くなったり、アドレスが不足することがあることです。プロバイダーの Internet Service Provider (ISP; インターネット サービス プロバイダー) カスタマーはパブリック アドレス数が制限されているため、管理効率の悪いプールの影響を特に受けます。たとえば、同じ ISP 内で、ある PE ルータのローカル プール利用率が低いにもかかわらず、別の PE ルータのローカル プールを使い果たすことがあります。

RADIUS ベース アドレス割り当て

RADIUS は、ネットワークを不正なアクセスから保護する分散型クライアント / サーバ システムです。RADIUS は Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग) サービスを提供するだけでなく、ユーザ定義のスタティック ルートおよび RADIUS サーバ上の IP プール定義を使用して、IP アドレス割り当ても行います。

Cisco 10000 シリーズ ルータでは、RADIUS クライアントはルータ上で稼働し、中央の RADIUS サーバに対して、リモート ユーザのスタティック ルートまたは RADIUS IP プール定義内の IP アドレスを問い合わせます。通常、RADIUS サーバは、特定の PE ルータに関連付けられた VPN ごとに、別々のアドレス プール内のアドレスを割り当てます。これにより、サーバは同じ VPN 内のリモート ユーザ、および同じ PE ルータに接続しているリモート ユーザに対して、連続するアドレスを割り当てることができます。RADIUS サーバはリモート ユーザのドメイン名を使用して、VPN を識別します。

RADIUS ベース アドレス割り当ての利点

RADIUS は、リモート ユーザに IP アドレスを割り当てるための効率的なメカニズムです。

- RADIUS ベース アドレス割り当ての利点の 1 つは、サーバに設定された IP アドレス プールを効率的に管理できることです。RADIUS は必要に応じてプール サイズを動的に変更できるため、利用率の低いプールからアドレスを削除して、アドレスが不足しているプールに追加できます。
- RADIUS は経路集約、およびサーバに設定されたユーザ プロファイルをサポートすることにより、効率的なアドレスおよび AAA サービスを提供します。
- また、RADIUS はリモート ユーザのログインに固定 IP アドレスを付加することもできます。

RADIUS ベース アドレス割り当ての制限

アドレス指定メカニズムを決定するには、RADIUS ベース アドレス割り当ての制限および利点を評価する必要があります。RADIUS ベース アドレス割り当ての制限の一部を、次に示します。

- アドレス割り当てに RADIUS を使用すると、サーバの負荷が増大し、サーバのパフォーマンスが低下することがあります。
- リモート ユーザがログオンおよびログオフするときに、経路集約の効率が低下することがあります。これは、PE ルータが RADIUS サーバに対して集約できる連続する IP アドレス セットを維持することが困難になるためです。
- ユーザがログオンまたはログオフするたびに、Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) はアップデート情報を PE ルータに送信して、各ルータに設定された VRF をアップデートします。
- BGP が新しく設定されたルートをすべての PE ルータに伝播させる間、リモート ユーザの接続は制限されます。

DHCP ベース アドレス割り当て

Dynamic Host Configuration Protocol (DHCP) サーバを使用すると、リモート ユーザに IP アドレスが割り当てられるため、ユーザを個別に設定する作業が不要になります。また、DHCP は、ユーザ システムが接続先のインターネット ネットワーク上の情報を操作したり、交換する場合に必要なすべてのパラメータを提供することもできます。DHCP は、クライアント/サーバモデルに基づいています。クライアント ソフトウェアはユーザ システム上で稼働し、サーバ ソフトウェアは DHCP サーバ上で稼働します。

DHCP は、ネットワーク内のアドレスを分配および再利用するために自動で、信頼性が高く、安全な方法を提供するリース メカニズムを使用しています。アドレスを管理する必要はほとんどありません。システム管理者は、特定のネットワーク要求に合わせてリース ポリシーを調整できます。

リースは、*scope* という名前のアドレス プールにグループ化されます。スコープは、要求元ホストで利用可能な IP アドレス セットを定義します。リースは予約済み (ホストは常に同じ IP アドレスを受信)、またはダイナミック (ホストはスコープ内で次に利用可能な、未割り当てのリースを受信) のいずれかとなります。

DHCP ベース アドレス割り当ての利点

DHCP の最も重要な利点の 1 つは、ユーザ システムに IP アドレスを動的に設定して、割り当てられたアドレスにリースを関連付けることができることです。また、DHCP は複数のサーバにも対応します。冗長 DHCP サーバを設定して、1 つのサーバが要求元クライアントにリースを実行できない場合に、別のサーバに処理を引き継ぐことができます。既存の DHCP クライアントは、どのサーバが要求に応答しているかを認識しなくても、リースを維持したり、更新できます。

DHCP ベース アドレス割り当ての制限

DHCP ベース アドレス割り当てには、RADIUS ベース アドレス割り当ての場合と同様な経路集約の問題があります。リモート ユーザがログオンおよびログオフするときに、経路集約は効率が低下します。また、BGP が新しく設定されたルートを使用してすべての PE ルータをアップデートするときに、ユーザは接続が制限されます。

詳細については、「[RADIUS ベース アドレス割り当て](#)」(p.10-2) を参照してください。

ODAP マネージャ

On-demand Address Pool (ODAP) マネージャ機能は、IP アドレスを割り当てたり、管理するためのメカニズムです。

ODAP は中央サーバを使用して、カスタマーごとのアドレス ブロックを管理します。中央サーバには、DHCP サーバまたは RADIUS サーバを使用できます。ODAP が設定されたあと、中央サーバは、中央サーバからリースされているサブネットを 1 つまたは複数 ODAP に設定します。中央サーバは各アドレス プールをサブネットに分割し、要求時にこのサブネットを PE ルータに割り当てます。



(注)

Cisco Network Registrar (CNR; Cisco ネットワーク レジストラ) DHCP サーバおよび Cisco Access Registrar (CAR) RADIUS サーバは、ODAP をサポートしています。

カスタマー サイトは、プロバイダー ネットワーク内の PE ルータに接続されます。ODAP が設定されると、PE ルータのプール マネージャは中央サーバに対して、特定の ODAP の最初のサブネットを求める要求を開始します。その後、プール マネージャは ODAP の利用率を監視します。

プールの利用率が利用率上限しきい値 (利用率上限マーク) を超えると、プール マネージャは中央サーバ内の別のサブネットを要求し、そのサブネットを ODAP に追加します。同様に、プールの利用率が利用率下限しきい値 (利用率下限マーク) よりも低下すると、プール マネージャはリース元の中央サーバにサブネットを 1 つまたは複数戻します。ODAP に対してサブネットが追加または削除されるたびに、対応する VRF に、リースされたサブネットのサマライズ済みルートを追加または削除する必要があります。

ODAP マネージャ機能については、次の項目で説明します。

- [ODAP マネージャ機能の履歴 \(p.10-5\)](#)
- [PPP セッションのアドレス割り当て \(p.10-6\)](#)
- [サブネットの解放 \(p.10-6\)](#)
- [MPLS VPN の ODAP \(p.10-6\)](#)
- [ODAP マネージャの利点 \(p.10-7\)](#)
- [ODAP マネージャの要件 \(p.10-7\)](#)
- [ODAP マネージャの必須の設定作業 \(p.10-7\)](#)
- [ODAP マネージャの任意の設定作業 \(p.10-11\)](#)
- [ODAP の確認 \(p.10-13\)](#)
- [ODAP マネージャの設定例 \(p.10-15\)](#)
- [ODAP のモニタリングおよびメンテナンス \(p.10-16\)](#)

ODAP マネージャ機能の履歴

| Cisco IOS リリース | 説明 | 必要な PRE |
|----------------|--|---------|
| 12.2(15)BX | この機能が Cisco 10000 シリーズ ルータに導入されました。 | PRE2 |
| 12.3(7)XI1 | この機能が Cisco IOS Release 12.3(7)XI1 に統合されました。 | PRE2 |
| 12.2(28)SB | この機能が Cisco IOS Release 12.2(28)SB に統合されました。 | PRE2 |

PPP セッションのアドレス割り当て

PPP セッションのアドレスを個別に割り当てるために、プール マネージャは最初のリース済みサブネットから順番に、空きアドレスを検索します。最初のサブネット内に利用可能な空きアドレスがない場合、プール マネージャは 2 番目のリース済みサブネットを検索し、空きアドレスが見つかるまで同様な処理を続けます。このアドレス割り当て方式を使用すると、サブネットのリリースおよび経路集約を効率的に行うことができます。ただし、この方式は標準の DHCP アドレス選択ポリシーとは異なり、受信側インターフェイスの IP アドレスを考慮に入れません。ODAP マネージャ機能は、PPP 用の IP アドレス プーリング メカニズムを備えています。このメカニズムにより、DHCP サーバは、標準 DHCP アドレス要求と PPP クライアントに対するアドレス要求を区別できます。

サブネットの解放

プール マネージャは、最後のリース済みサブネットから順番に、サブネットを解放します。プール マネージャは解放可能なサブネット（現在リースされているアドレスがないサブネット）を検索します。解放可能なサブネットが検出されると、プール マネージャはそのサブネットを解放して、そのサブネットのサマライズ済みルートを削除します。複数の解放可能サブネットが存在する場合、プール マネージャは最近割り当てられたサブネットを解放します。解放可能なサブネットが検出されない場合、プール マネージャはアクションを実行しません。サブネットの解放によって利用率上限マークに達する場合、プール マネージャはサブネットを解放しません。瞬間的な利用率レベルに関係なく、プール マネージャは ODAP がディセーブルにならないかぎり、最初のリース済みサブネットを解放しません。

MPLS VPN の ODAP

ODAP マネージャ機能を使用すると、MPLS VPN 環境がサポートされます。この機能によりアドレスプールのサイズ変更が自動化されて、ネットワーク負荷および手動設定が軽減されます。

各 ODAP は、特定の MPLS VPN に対して設定および関連付けられます。各 VPN には VRF が 1 つまたは複数関連付けられます。VRF は、ルーティングテーブルと、特定のカスタマー VPN サイトに関連したその他の情報を保持します。ODAP は、「[ODAP マネージャ](#)」(p.10-5) に記載されている手順に従って利用されます。ただし、特定の VPN に関連付けられた VRF 内では、例外的にアドレス割り当てが発生します。

特定の VPN に属する PPP セッションにアドレスを割り当てることができるのは、その VPN に関連付けられた ODAP のみです。ODAP が設定されている PE ルータは、PPP セッションを終端し、リモートユーザを対応する MPLS VPN にマッピングします。



(注) ODAP の詳細については、「[ODAP マネージャ](#)」(p.10-5) を参照してください。MPLS VPN の設定の詳細については、「MPLS VPN に対するリモートアクセスの設定」、または『*Cisco IOS Switching Services Configuration Guide*』Release 12.2 を参照してください。

MPLS VPN の ODAP マネージャ機能については、次の項目で説明します。

ODAP マネージャの利点

ODAP マネージャ機能には、次の利点があります。

- IP アドレス プールのサイズ変更（必要に応じたプール サイズの増減）を動的に行います。
- アドレス割り当てを自動的に制御します。
- 簡単なモニタリング機能により、プール マネージャはアドレスの利用率を評価できます。
- サブネット単位またはインターフェイス単位でアドレスが割り当てられた MPLS VPN をサポートします（「MPLS VPN の ODAP」 [p.10-6] を参照）。
- 単純な VPN 設定により、プール マネージャは ODAP の設定時に、アドレス プール内の最初のサブネットを要求できます。

ODAP マネージャの要件

ODAP マネージャ機能には次の要件があります。

- ODAP に対して VRF を指定できること。この指定を行う場合は、最初に VRF を設定してから、ODAP に VRF を設定する必要があります。アドレス プールに VRF を設定しない場合、プールはグローバルアドレススペース内にあると想定されます。
- PPP セッションの VRF が、プールに設定された VRF と一致すること。一致させるには、**ip vrf forwarding** コマンドを使用して、バーチャル テンプレート インターフェイスを設定する必要があります。AAA を使用して PPP ユーザを許可する場合は、RADIUS サーバ内のユーザ プロファイル設定に VRF を追加できます。



(注)

AAA の設定についての詳細は、『Cisco IOS Security Configuration Guide』 Release 12.2 を参照してください。

ODAP マネージャの必須の設定作業

ODAP マネージャ機能を設定するには、次の必須の設定作業を行います。

- [グローバル デフォルト プーリング メカニズムとしての DHCP ODAP の定義 \(p.10-7\)](#)
- [ODAP としての DHCP プールの設定 \(p.10-8\)](#)
- [AAA クライアントの設定 \(p.10-9\)](#)
- [RADIUS の設定 \(p.10-10\)](#)

グローバル デフォルト プーリング メカニズムとしての DHCP ODAP の定義

ODAP をグローバル デフォルト メカニズムとして指定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

| コマンド | 目的 |
|--|---|
| Router(config)# ip address-pool dhcp-pool | MPLS VPN への PPP リモート アクセス セッションに対するグローバル デフォルト IP アドレス メカニズムとして、ODAP をイネーブルにします。ローカルに設定された VRF 対応 DHCP プールにより、IP アドレスが割り当てられます。 |



(注) DHCP サーバは、標準 DHCP アドレス要求と PPP クライアントに対するアドレス要求を区別できなければなりません。詳細については、「PPP セッションのアドレス割り当て」(p.10-6) を参照してください。

例 10-1 では、PPP クライアントからのアドレス要求を処理するメカニズムとして、ODAP をイネーブルにします。ローカルに設定された VRF 対応 DHCP プール `Green_pool` により、IP アドレスが提供されます。

例 10-1 グローバル デフォルト プーリング メカニズムとしての DHCP ODAP の定義

```
!
ip address-pool dhcp-pool
!
ip dhcp pool Green_pool
!
```

ODAP としての DHCP プールの設定

DHCP プールを ODAP として設定するには、グローバル コンフィギュレーション モードを開始して次のコマンドを入力します。

| | コマンド | 目的 |
|--------|---|---|
| ステップ 1 | Router(config)# ip dhcp pool name | Cisco IOS DHCP サーバに DHCP アドレス プールを設定して、DHCP プール設定モードを開始します。 |
| ステップ 2 | Router(config-dhcp)# vrf name | アドレス プールに VRF を関連付けます。 |
| ステップ 3 | Router(config-dhcp)# origin {dhcp aaa ipcp} [subnet size initial size [autogrow size]] | アドレス プールを ODAP として設定します。 |
| ステップ 4 | Router(config-dhcp)# utilizationmark low percentage-number | プール サイズの利用率下限マークを設定します。デフォルト値は 0% です。 |
| ステップ 5 | Router(config-dhcp)# utilization mark high percentage-number | プール サイズの利用率上限マークを設定します。デフォルト値は 100% です。 |

例 10-2 では、2 つの DHCP ODAP (`green_pool` および `red_pool`) を設定します。`green_pool` アドレス プールは `Green` VRF に、`red_pool` アドレス プールは `Red` VRF に関連付けられています。両方のプールは、外部 DHCP サーバからサブネットアドレスを取得します。

例 10-2 ODAP としての DHCP プールの設定

```

!
ip dhcp pool green_pool
  vrf Green
  utilization mark high 60
  utilization mark low 40
  origin dhcp subnet size initial /24 autogrow /24
!
ip dhcp pool red_pool
  vrf Red
  origin dhcp
!
ip vrf Green
  rd 200:1
  route-target export 200:1
  route-target import 200:1
!
ip vrf Red
  rd 300:1
  route-target export 300:1
  route-target import 300:1
ip address-pool dhcp-pool
!
interface Virtual-Template1
  ip vrf forwarding Green
  ip unnumbered Loopback1
  ppp authentication chap
!
interface Virtual-Template4
  ip vrf forwarding Red
  ip unnumbered Loopback2
  ppp authentication chap
!

```

AAA クライアントの設定

ODAP が RADIUS サーバからサブネットを取得できるようにするには、グローバル コンフィギュレーション モードで次のコマンドを入力します。これらのコマンドは、Cisco 10000 ルータに AAA クライアントを設定します。

| | コマンド | 目的 |
|--------|--|--|
| ステップ 1 | Router(config)# aaa new-model | AAA アクセス制御をイネーブルにします。 |
| ステップ 2 | Router(config)# aaa authorization configuration default group radius | RADIUS を使用して、AAA サーバからスタティック ルート設定情報をダウンロードします。 |
| ステップ 3 | Router(config)# aaa accounting network default start-stop radius または Router(config)# aaa accounting network default stop-only radius | RADIUS を使用するとき、課金またはセキュリティ用に、要求されたサービスの AAA アカウンティングをイネーブルにします。プロセスの開始時に、 <i>start</i> アカウンティング通知を送信します。 RADIUS を使用するとき、課金またはセキュリティ用に、要求されたサービスの AAA アカウンティングをイネーブルにします。要求されたユーザ プロセスの終了時に、 <i>stop</i> アカウンティング通知を送信します。 |
| ステップ 4 | Router(config)# aaa session-id common | コール内の各 AAA アカウンティング サービスで、同じセッション ID が使用されるようにします。 |

AAA の設定例については、「[RADIUS の設定](#)」(p.10-10) の例 10-3 を参照してください。

RADIUS の設定

Cisco10000 ルータに RADIUS を設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

| | コマンド | 目的 |
|--------|--|--|
| ステップ 1 | <code>Router(config)# ip radius source-interface subinterface-name</code> | すべての発信 RADIUS パケットに対して、Cisco 10000 ルータが指定インターフェイスの IP アドレスを使用するように設定します。 |
| ステップ 2 | <code>Router(config)# radius-server host ip-address auth-port port-number acct-port port-number</code> | RADIUS サーバホストを指定します。 |
| ステップ 3 | <code>Router(config)# radius server attribute 32 include-in-access-req</code> | アクセス要求またはアカウントング要求内で、RADIUS アトリビュート 32 (NAS-Identifier) を送信します。 |
| ステップ 4 | <code>Router(config)# radius server attribute 44 include-in-access-req</code> | アクセス要求またはアカウントング要求内で、RADIUS アトリビュート 44 (Acct-Session-Id) を送信します。 |
| ステップ 5 | <code>Router(config)# radius-server vsa send accounting</code> | Cisco 10000 ルータがネットワーク アクセス サーバ (NAS) として機能し、ベンダー固有のアカウントング属性を認識および使用するように設定します。 |
| ステップ 6 | <code>Router(config)# radius-server vsa send authentication</code> | ベンダー固有の認証アトリビュートを認識して使用するように、Cisco 10000 ルータ (NAS) を設定します。 |

例10-3 では、アドレス プール *Green*、および *Green* アドレス プールがサブネットを取得する RADIUS サーバを設定します。RADIUS サーバは、IP アドレス 172.16.1.1 に配置されています。

例 10-3 AAA および RADIUS の設定

```
!
aaa new-model
!
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius
aaa session-id common
!
ip subnet-zero
!
ip dhcp ping packets 0
!
ip dhcp pool Green
    vrf Green
    utilization mark high 50
    utilization mark low 30
    origin aaa subnet size initial /28 autogrow /28
!
ip vrf Green
    rd 300:1
    route-target export 300:1
    route-target import 300:1
!
interface Ethernet1/1
    ip address 172.16.1.12 255.255.255.0
    duplex half
!
interface Virtual-Template1
    ip vrf forwarding Green
    no ip address
!
ip radius source-interface Ethernet1/1
!
!IP address of the Radius server host
radius-server host 172.16.1.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 32 include-in-access-req
radius-server attribute 44 include-in-access-req
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

ODAP マネージャの任意の設定作業

ODAP マネージャ機能を設定するには、次の任意の設定作業のいずれかを行います。

- [インターフェイスでの ODAP の定義 \(p.10-11\)](#)
- [IPCP ネゴシエーションを介してサブネットを取得するための ODAP の設定 \(p.10-12\)](#)
- [ODAP のディセーブル化 \(p.10-13\)](#)

インターフェイスでの ODAP の定義

インターフェイスに ODAP マネージャ機能を設定するには、グローバル コンフィギュレーション モードを開始して次のコマンドを入力します。

| | コマンド | 目的 |
|--------|---|--|
| ステップ 1 | Router(config)# interface name | インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。 |
| ステップ 2 | Router(config-if)# peer default ip address dhcp-pool | ODAP 内の IP アドレスをインターフェイスに接続されたリモート ピアに戻すように指定します。このコマンドは、MPLS VPN へのリモート アクセス (PPP) セッションのみをサポートします。 |



(注) インターフェイスごとに ODAP メカニズムを設定した場合、ODAP はインターフェイスに設定されたグローバルデフォルトアドレス プール メカニズムよりも優先します。

IPCP ネゴシエーションを介してサブネットを取得するための ODAP の設定



(注) Customer Premise Equipment (CPE; 顧客宅内機器) に IP アドレス プールを割り当てた場合、プール マネージャは CPE 装置および DHCP プールに IP アドレスを割り当てます。ODAP 機能を使用するための条件は、次のとおりです。

- Cisco IOS CPE 装置には、サブネットを要求したり、使用するための機能が必要です。
- AAA を使用する RADIUS サーバには、サブネットを提供したり、フレーム化ルートを適切な VRF テーブルに挿入する機能が必要です。
- PE ルータには、IP Control Protocol (IPCP; IP コントロール プロトコル) を介したサブネットの提供を容易にするための機能が必要です。

ODAP にサブネット割り当てプロトコルとして IPCP 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を開始して次のコマンドを入力します。

| | コマンド | 目的 |
|--------|--|---|
| ステップ 1 | Router(config)# ip dhcp pool name | Cisco IOS DHCP サーバに DHCP アドレス プールを設定して、DHCP プール設定モードを開始します。 |
| ステップ 2 | Router(config-dhcp)# import all | Cisco IOS DHCP サーバ データベースにオプションのパラメータをインポートします。 |
| ステップ 3 | Router(config-dhcp)# origin ipcp | サブネット割り当てプロトコルとして IPCP を使用することにより、アドレス プールを ODAP として設定します。 |
| ステップ 4 | Router(config-dhcp)# exit | DHCP プール設定モードを終了します。 |
| ステップ 5 | Router(config)# interface type | インターフェイスを選択し、インターフェイス コンフィギュレーションモードを開始します。 |
| ステップ 6 | Router(Config-if)# ip address pool name | 指定されたプール内のインターフェイスの IP アドレスを自動設定するように指定します。 |



(注) プールは、IPCP からサブネットに設定されなければなりません。

ODAP のディセーブル化

DHCP プール内の ODAP をディセーブルにするには、グローバル コンフィギュレーション モードを開始して、次のコマンドを入力します。

| | コマンド | 目的 |
|--------|--|---|
| ステップ 1 | Router(config)# ip dhcp pool name | 指定された DHCP アドレス プールの DHCP プール設定モードを開始します。 |
| ステップ 2 | Router(config-if)# no origin {dhcp aaa ipcp} | ODAP をディセーブルにします。 |



(注) ODAP をディセーブルにすると、すべてのリース済みサブネットがリリースされます。アクティブな PPP セッションが、リリースされたサブネット内のアドレスを使用している場合、これらのセッションはリセットされます。リリースされたサブネット内のアドレスをリースしている DHCP クライアントは、これらのリースを更新できません。

例 10-4 では、オンデマンド DHCP プール *test_pool* をディセーブルにします。

例 10-4 ODAP のディセーブル化

```
!
ip dhcp pool test_pool
  import all
  no origin ipcp
!
```

ODAP の確認

ODAP 動作を確認するには、特権 EXEC モードで、次のコマンドを入力します。

| コマンド | 目的 |
|--------------------------------|---|
| Router# show ip dhcp pool | 利用率上限 / 下限マーク、サブネット サイズ、VRF 名、合計アドレス数、リース済みアドレスなど、設定されたすべてのプールに関する情報を表示します。 |
| Router# show ip dhcp pool name | 利用率上限 / 下限マーク、サブネット サイズ、VRF 名、合計アドレス数、リース済みアドレスなど、指定されたプールに関する情報を表示します。 |
| Router# show ip dhcp binding | IP アドレス、ハードウェア アドレス、リース期限、プールタイプなど、VRF に関連付けられたプールのバインディング情報を表示します。 |

例 10-5 では、**show ip dhcp pool** コマンドを使用して、2 つの DHCP プール (*Green* および *Global*) の情報を表示します。*Green* プール設定の各項目の意味は、次のとおりです。

- Autogrow — 利用率上限マークに達した場合、さらにサブネットを取得します。
- Subnet size — *Green* プールが要求できるサブネット サイズの初期値および増加値を指定します。これらの値は、**origin** コマンドを使用して設定します。
- VRF name — *Green* プールが *Green VRF* に関連付けられていることを示します。
- Total addresses — プール内の使用可能な全アドレスの個数です。
- Leased addresses — プールから作成されたバインディングの総数。

- **Pending event: subnet request** — プールに対するサブネット要求が待機中であることを示します。Leased addresses の値がプールの利用率上限マークを超えたために、サブネット要求がスケジューリングされています。
- **Current index** — 次にプールに割り当てられるサブネットアドレスを指定します。例 10-5 では、3 つのサブネットが現在追加されています。最初の 2 つのサブネットの Current index は 0.0.0.0 です。これは、各サブネット内の利用可能なアドレスがすべて使用されたことを示します。



(注) Green プールおよび Global プールには、同じサブネット 172.16.0.1 が割り当てられています。この割り当てが可能なのは、Green プールが Green VRF に関連付けられていて、Global プールがグローバルアドレススペース内に設定されているためです。

- **IP address range** — サブネットの使用可能なアドレス範囲を示します。
- **Leased addresses** — 各サブネットから作成されたバインディング数を個々に示します。

例 10-5 show ip dhcp pool コマンド

```
Router# show ip dhcp pool

Pool Green :
  Utilization mark (high/low)      : 50 / 30
  Subnet size (first/next)         : 24 / 24 (autogrow)
  VRF name                          : Green
  Total addresses                   : 18
  Leased addresses                  : 13
  Pending event                     : subnet request
  3 subnets are currently in the pool :
  Current index      IP address range      Leased addresses
  0.0.0.0            178.16.0.1 - 172.16.0.6    6
  0.0.0.0            172.16.0.9 - 172.16.0.14   6
  172.16.0.17        172.16.0.17 - 172.16.0.22  1

Pool Global :
  Utilization mark (high/low)      : 100 / 0
  Subnet size (first/next)         : 24 / 24 (autogrow)
  Total addresses                   : 6
  Leased addresses                  : 0
  Pending event                     : none
  1 subnet is currently in the pool :
  Current index      IP address range      Leased addresses
  172.16.0.1         172.16.0.1 - 172.16.0.6    0
```

例 10-6 では、**show ip dhcp binding** コマンドを使用して、Green プールのバインディングを表示します。この例の各項目の意味は、次のとおりです。

- **Type : On-demand** — PPP セッション用のアドレス バインディングが作成されることを示します。
- **Lease expiration : Infinite** — セッションが起動しているかぎり、バインディングが有効であることを示します。セッションの起動中にサブネットをリース元サーバに解放する必要がある場合、セッションは新規 IP アドレスを強制的に取得するようにリセットされます。
- **Hardware address** — オンデマンド エントリに対して PPP が検出したセッション ID を指定します。



(注) 例 10-6 では、グローバル プールのアドレスが割り当てられていないため、VRF に関連付けられたプールのバインディングが表示されません。

例 10-6 show ip dhcp binding コマンド

```
Router# show ip dhcp binding
Bindings from all pools not associated with VRF :
IP addressHardware addressLease expirationType

Bindings from VRF pool Green :
IP address      Hardware address      Lease expiration      Type
172.16.0.1      5674.312d.7465.7374. Infinite             On-demand
                  2d38.3930.39
172.16.0.2      5674.312d.7465.7374. Infinite             On-demand
                  2d38.3839.31
172.16.0.3      5674.312d.7465.7374. Infinite             On-demand
                  2d36.3432.34
172.16.0.4      5674.312d.7465.7374. Infinite             On-demand
                  2d38.3236.34
172.16.0.5      5674.312d.7465.7374. Infinite             On-demand
                  2d34.3331.37
172.16.0.6      5674.312d.7465.7374. Infinite             On-demand
                  2d37.3237.39
172.16.0.9      5674.312d.7465.7374. Infinite             On-demand
                  2d39.3732.36
172.16.0.10     5674.312d.7465.7374. Infinite             On-demand
                  2d31.3637
172.16.0.11     5674.312d.7465.7374. Infinite             On-demand
                  2d39.3137.36
172.16.0.12     5674.312d.7465.7374. Infinite             On-demand
                  2d37.3838.30
172.16.0.13     5674.312d.7465.7374. Infinite             On-demand
                  2d32.3339.37
172.16.0.14     5674.312d.7465.7374. Infinite             On-demand
                  2d31.3038.31
172.16.0.17     5674.312d.7465.7374. Infinite             On-demand
                  2d38.3832.38
172.16.0.18     5674.312d.7465.7374. Infinite             On-demand
                  2d32.3736.31
```

ODAP マネージャの設定例

ここでは、次の設定例を示します。

- [インターフェイスでの DHCP ODAP の設定 \(p.10-15\)](#)
- [IPCP ネゴシエーションを介してサブネットを取得するための ODAP の設定 \(p.10-16\)](#)

インターフェイスでの DHCP ODAP の設定

例 10-7 では、バーチャル テンプレート インターフェイス *Virtual-Template1* 上に ODAP を定義します。*Virtual-Template1* が適用されたインターフェイスに接続されているリモートピアは、ODAP 内の IP アドレスを取得します。

例 10-7 インターフェイスでの DHCP ODAP の定義

```
!
interface Virtual-Templat1
 ip vrf forwarding green
 ip unnumbered loopback1
 ppp authentication chap
 peer default ip address dhcp-pool
```


IPCP ネゴシエーションを介してサブネットを取得するための ODAP の設定

例 10-8 では、DHCP アドレス プール *my_pool* を作成し、IPCP を使用して ODAP をサブネット割り当てプロトコルとして設定し、アドレス プール *my_pool* 内の IP アドレスを自動的に取得するようにインターフェイス Ethernet0 を設定します。

例 10-8 IPCP ネゴシエーションを介してサブネットを取得するための ODAP のイネーブル化

```

!
ip dhcp pool my_pool
  import all
  origin ipcp
!
interface Ethernet0
  ip address pool my_pool
  ip verify unicast reverse-path
  shutdown
  hold-queue 32 in
!

```

ODAP のモニタリングおよびメンテナンス

ODAP を監視およびメンテナンスするには、特権 EXEC モードで次のコマンドを入力します。

| コマンド | 目的 |
|---|--|
| Router# <code>clear ip dhcp [pool name] binding {* address}</code> | DHCP サーバデータベースから、自動アドレス バインディングまたは特定のプールのオブジェクトを削除します。 |
| Router# <code>clear ip dhcp [pool name] conflict {* address}</code> | DHCP サーバデータベースから、特定のプールのアドレス競合を消去します。 |
| Router# <code>clear ip dhcp [pool name] subnet {* address}</code> | 特定のプールを指定しない場合は、指定された DHCP プールまたはすべての DHCP プール内の、現在リースされているすべてのサブネットを消去します。 |
| Router# <code>debug dhcp details</code> | ODAP のサブネット割り当ておよびサブネットの解放を監視します。 |
| Router# <code>debug ip dhcp server events</code> | 割り当てやデータベースアップデートなどの DHCP サーバイベントを報告します。 |
| Router# <code>show ip dhcp import</code> | DHCP サーバデータベースにインポートされたオプションのパラメータを表示します。 |
| Router# <code>show ip interface [type number]</code> | IP 用に設定されたインターフェイスの使用可能性に関するステータスを表示します。 |
| Router# <code>show ip dhcp pool name</code> | DHCP アドレス プール情報を表示します。このコマンドは、DHCP プールが着信 PPP セッションごとに IP アドレスを割り当てて、このアドレスに正しい VRF を関連付けたかどうかをチェックする場合に使用します。 |



ヒント

- デフォルトでは、プール マネージャが使用する Cisco IOS DHCP サーバは、アドレスを割り当てる前に、**ping** コマンドを使用してアドレスの可用性を確認します。デフォルトの DHCP ping 設定では、ICMP エコー応答を 2 秒間待機します。このデフォルト設定では、DHCP サーバは 2 秒ごとにアドレス要求を 1 つ処理します。送信される ping パケット数、および ping のタイムアウト タイマーを設定できます。アドレス割り当て時間を短縮するには、タイムアウト タイマー値または送信される ping パケット数を小さくします。



(注) アドレス割り当て時間を短縮すると、アドレス割り当てが改善されるますが、同時に、DHCP サーバが重複アドレスを検出する機能も使用できなくなります。

- 各 ODAP は、DHCP サーバまたは RADIUS サーバからサブネットを取得する処理を、最大 4 回試行します。この処理に失敗した場合は、プールに対して別のアドレス要求が行われたときに（たとえば、新規に起動された PPP セッションがアドレス要求を行ったときに）、サブネット要求が自動的に開始されます。アドレス割り当てサーバがプールにサブネットを割り当てなかった場合は、特権 EXEC モードで **clear ip dhcp pool name subnet *** コマンドを使用することにより、サブネット要求プロセスを強制的に再起動できます。

オーバーラッピング IP アドレス プール

オーバーラッピング IP アドレス プール機能によって、複数の IP アドレス スペースの使用、および Cisco 10000 ルータでサポートされる異なる VPN 間での IP アドレスの再利用が可能になります。複製された IP アドレスは、同じ IP アドレス スペースに存在することはできません。

与えられた IP アドレス スペースに、IP アドレスを一意に配置するために、複数のアドレス スペースが IP アドレス グループに割り当てられます。また、これによって IP アドレス グループ内の非オーバーラッピング IP アドレス プールの確認が可能になります。Cisco 10000 ルータ内では、一意のプール名を使用します。各プール名には暗黙のグループ識別子があり、1 つのグループだけに関連付けられていることを確認できます。

Cisco 10000 ルータは、明示的なグループ名を持たないプールをベース システム グループのメンバーとみなすので、その IP アドレスが単一の IP アドレス スペースに属するかのようにこれらのプールを処理します。単一の IP アドレス スペースのプールから与えられた IP アドレスを重複して割り当てることはできません。

オーバーラッピング IP アドレス プール機能は、既存の設定には影響しません。既存の実装から、グループのメンバーとして指定されていないプールの処理を変更することはできません。

オーバーラッピング IP アドレス プール機能は、次の配置モデルで利用できます。

- 管理型 L2TP (レイヤ 2 トンネル プロトコル) ネットワーク サーバ
- VRF インスタンスに対する PPP Terminated Aggregation (PTA)
- MPLS VPN に対する Remote Access (RA)

オーバーラッピング IP アドレス プール機能については、次の項目で説明します。

- [オーバーラッピング IP アドレス プール機能の履歴 \(p.10-18\)](#)
- [オーバーラッピング IP アドレス プールの制約事項 \(p.10-18\)](#)
- [オーバーラッピング IP アドレス プールの設定作業 \(p.10-18\)](#)
- [IP オーバーラッピング アドレス プールのローカル プール グループの確認 \(p.10-19\)](#)
- [オーバーラッピング IP アドレス プールの設定例 \(p.10-19\)](#)

オーバーラッピング IP アドレス プール機能の履歴

| Cisco IOS リリース | 説明 | 必要な PRE |
|----------------|--|---------|
| 12.2(4)BZ1 | この機能が Cisco 10000 シリーズ ルータに導入されました。 | PRE1 |
| 12.3(7)XI1 | この機能が Cisco IOS Release 12.3(7)XI1 に統合されました。 | PRE2 |
| 12.2(28)SB | この機能が Cisco IOS Release 12.2(28)SB に統合されました。 | PRE2 |

オーバーラッピング IP アドレス プールの制約事項

このソフトウェアではグループ単位ベースで、複製されたアドレスをチェックします。これは複製されたアドレスを持つ可能性のある複数のグループにおいて、プールを設定できることを意味します。この機能は、複数の IP アドレス スペースがサポートされる環境 (MPLS VPN など) でのみ使用してください。

オーバーラッピング IP アドレス プールの設定作業

IP オーバーラッピング アドレス プール機能を設定するために、ローカル プール グループを設定します ([「IP オーバーラッピング アドレス プールのローカル プール グループの設定」](#)を参照)。

IP オーバーラッピング アドレス プールのローカル プール グループの設定

ローカル プール 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入力します。

| コマンド | 目的 |
|---|--|
| Router(config)# ip local pool <i>pool-name</i> <i>start-IP</i> [end-IP] [group <i>group-name</i>] [cache-size <i>size</i>] | ローカル IP アドレス プールのグループを設定して、グループ名を与え、キャッシュ サイズを指定します。 |

IP オーバーラッピング アドレス プールのローカル プール グループの確認

プール グループが適切に設定されたことを確認するには、特権 EXEC モードで次のコマンドを入力して、プール グループ名に関する出力結果をチェックします。

| コマンド | 目的 |
|--|------------------------------------|
| Router# show ip local pool [<i>pool-name</i> [group <i>group-name</i>]] | 定義済み IP アドレス プールの統計情報を表示します。 |
| Router# show ip local pool | 設定されたすべてのプールの統計情報を表示します。 |
| Router# show ip local pool <i>pool-name</i> | 指定するプールの統計情報を表示します。 |
| Router# show ip local pool group | ベース システム グループ内のすべてのプールの統計情報を表示します。 |
| Router# show ip local pool group <i>group-name</i> | 指定されたグループのすべてのプールを表示します。 |

オーバーラッピング IP アドレス プールの設定例

ここでは、次の設定例を示します。

- [ジェネリック IP オーバーラッピング アドレス プールの例 \(p.10-19\)](#)
- [VPN および VRF の IP オーバーラッピング アドレス プールの例 \(p.10-20\)](#)

ジェネリック IP オーバーラッピング アドレス プールの例

次に、2 つのプール グループを設定する例を示します (ベース システム グループのプールを含む)。この例では、

- プール グループ **grp1** は、プール **p1_g1**、**p2_g1**、および **p3_g1** で構成されています。
- プール グループ **grp2** は、プール **p1_g2** および **p2_g2** で構成されています。
- プール **lp1** および **lp2** は、ベース システム グループのメンバーです。
- IP アドレス 10.1.1.1 は、**grp1**、**grp2**、およびベース システム グループをオーバーラップします。
- プール **lp1** および **lp2** で構成される名前のないベース システム グループにおいては、オーバーラッピング アドレスは発生しません。

```
ip local pool p1_g1 10.1.1.1 10.1.1.50 group grp1
ip local pool p2_g1 10.1.1.100 10.1.1.110 group grp1
ip local pool p1_g2 10.1.1.1 10.1.1.40 group grp2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3_g1 10.1.2.1 10.1.2.30 group grp1
ip local pool p2_g2 10.1.1.50 10.1.1.70 group grp2
ip local pool lp2 10.1.2.1 10.1.2.10
```



(注)

前述の例では、プール名をグループに容易に関連付けるプール名を示しています（独立型プール名するとき）。この関連付けは、操作上の便宜です。プールを定義するのに使用される名前と、グループ名の間に関連性は必要ありません。

VPN および VRF の IP オーバーラッピング アドレス プールの例

次に、VPN および VRF で使用する可能性がある一般的な IP アドレスの設定例を示します。この例では、プール名を VPN に関連付けるプール名を示しています（独立型プール名するとき）。この関連付けは、操作上の便宜です。プールを定義するのに使用される名前と、グループ名の間に関連性は必要ありません。この例では、

- プールグループ vpn1 は、プール p1_vpn1、p2_vpn1、および p3_vpn1 で構成されています。
- プールグループ vpn2 は、プール p1_vpn2 および p2_vpn2 で構成されています。
- プール lp1 および lp2 は、ベース システムのメンバーです。
- IP アドレス 10.1.1.1 は、vpn1、vpn2、およびベース システム グループをオーバーラップします。
- プール lp1 および lp2 で構成される名前のないベース システム グループにおいては、オーバーラッピング アドレスは発生しません。

```
ip local pool p1_vpn1 10.1.1.1 10.1.1.50 group vpn1
ip local pool p2_vpn1 10.1.1.100 10.1.1.110 group vpn1
ip local pool p1_vpn2 10.1.1.1 10.1.1.40 group vpn2
ip local pool lp1 10.1.1.1 10.1.1.10
ip local pool p3_vpn1 10.1.2.1 10.1.2.30 group vpn1
ip local pool p2_vpn2 10.1.1.50 10.1.1.70 group vpn2
ip local pool lp2 10.1.2.1 10.1.2.10
```