



スコープ、プレフィックス、リンク、ネットワークの管理

動的ホスト構成プロトコル(DHCP)は、IP構成をデバイスに自動的に割り当てるための業界標準のプロトコルです。DHCPは、アドレスの割り当てにクライアント/サーバーモデルを使用します。管理者は、1つまたは複数のDHCPサーバーを設定し、IPアドレスの割り当てや、その他のTCP/IP指向の設定情報をデバイスに提供することができます。DHCPを使用すると、IPアドレスを各クライアントに手動で割り当てるという作業を省くことができます。DHCPプロトコルはRFC 2131で説明されています。プロトコルの概要については、[を参照してください](#) [ダイナミック ホスト コンフィギュレーションの概要](#)。

この章では、スコープ、プレフィックス、およびリンクを設定する方法について説明します。クライアントがアドレス割り当てにDHCPを使用できるようにするには、少なくとも1つのスコープ(動的アドレスプール)またはプレフィックスをサーバーに追加する必要があります。

- [スコープの管理 \(1 ページ\)](#)
- [DHCPv6 Addresses \(18 ページ\)](#)
- [プレフィックスとリンクの設定 \(25 ページ\)](#)
- [DHCP ネットワークの管理 \(33 ページ\)](#)

スコープの管理

この項では、DHCPサーバーのスコープを定義および設定する方法について説明します。スコープは、DHCPサーバーが管理するサブネット内の1つ以上の動的アドレス範囲で構成されます。DHCPサーバーがクライアントにリースを提供する前に、1つ以上のスコープを定義する必要があります。(リースの一覧表示とスコープのリース予約の定義の詳細については、[リースの管理](#))

関連項目

[スコープ テンプレートの作成と適用](#)

[スコープの作成 \(2 ページ\)](#)

- [サーバー上のスコープ数の取得 \(12 ページ\)](#)
- [複数のスコープの設定 \(3 ページ\)](#)
- [スコープの編集 \(10 ページ\)](#)
- [段階的な同期モード \(11 ページ\)](#)
- [スコープの埋め込みポリシーの設定 \(12 ページ\)](#)
- [ネットワーク上の複数サブネットの設定 \(13 ページ\)](#)
- [スコープの BOOTP の有効化と無効化 \(14 ページ\)](#)
- [スコープの DHCP の無効化 \(16 ページ\)](#)
- [スコープの非アクティブ化 \(17 ページ\)](#)
- [スコープを更新専用に設定 \(15 ページ\)](#)
- [スコープでの空きアドレス SNMP トラップの設定 \(15 ページ\)](#)
- [アドレスを再利用しない場合のスコープの削除 \(18 ページ\)](#)
- [アドレスを再利用しない場合のスコープの削除 \(18 ページ\)](#)

スコープの作成

スコープの作成は、ローカル クラスタ関数です。各スコープには、次の項目が必要です。

- [名前 (Name)]
- リース時間、猶予期間、およびオプションを定義するポリシー
- ネットワーク アドレスとサブネット マスク
- 範囲、またはアドレスの範囲

スコープはローカル クラスタでのみ構成できます。Web UI ページは、ローカルの基本モードと高度なモードで異なります。

ローカルの基本 Web UI

- ステップ 1** [デザイン]メニューからScopesサブメニューDHCPv4を選択し、[DHCP スコープの一覧/追加]ページを開きます。
- ステップ 2** 必要に応じて、Web UI の上部にある[設定]ドロップダウン リストから、スコープの VPN を選択します。
- ステップ 3** [スコープ] ウィンドウの [スコープの追加] アイコンをクリックし、スコープ名を入力して、サブネットの IP アドレスを入力し、ドロップダウン リストからマスク値を選択します。
- ステップ 4** 必要に応じて、ドロップダウン リストからスコープの構成済みサービス クラス (クライアント クラス) を選択します。
- ステップ 5** Add DHCP Scope をクリックします。
- ステップ 6** DHCP サーバーをリロードします。

- (注) スコープが Basic モードで作成されると、範囲とルーター アドレスが自動的に追加されます。これらのモードを変更する場合は、基本モードでは設定できないため、モードを [詳細設定] に変更する必要があります。

ローカルアドバンスド Web UI

- ステップ 1** [デザイン] メニューから Scopes サブメニュー DHCPv4 を選択し、[DHCP スコープの一覧/追加] ページを開きます。
- ステップ 2** 必要に応じて、Web UI の上部にある [設定] ドロップダウン リストから、スコープの VPN を選択します。
- ステップ 3** [スコープ] ウィンドウの [スコープの追加] アイコンをクリックするか、スコープ名を入力するか、または空白のままにして、スコープテンプレートのスコープ名式で定義されているスコープ [スコープテンプレートでの式の使用](#) 名式を使用します (ある場合は参照)。後者の場合は、スコープテンプレートを選択します。スコープには常にサブネットとマスクを入力する必要があります。
- ステップ 4** ドロップダウン リストからスコープのポリシーを選択します。ポリシーはデフォルトでデフォルトポリシーになります。
- ステップ 5** Add DHCP Scope をクリックします。
- ステップ 6** スコープ内のアドレスの範囲を追加します。範囲は、定義されたスコープの任意のサブセットにできますが、重複することはできません。ホスト番号だけを入力した場合、範囲はネットマスクを基準にします。ローカルホストまたはブロードキャストアドレス (通常は 0 と 255) を含む範囲を入力しないでください。範囲を追加し、Add Range をクリックします。
- ステップ 7** DHCP サーバーをリロードします。

ヒント スコープに関連付けられているリースと予約を表示するには、「」 [リースの管理](#) を参照してください。リースを検索するには、「」を [サーバー全体のリースの検索](#) 参照してください。

関連項目

[サーバー上のスコープ数の取得 \(12 ページ\)](#)

[複数のスコープの設定 \(3 ページ\)](#)

[スコープの編集 \(10 ページ\)](#)

[段階的な同期モード \(11 ページ\)](#)

複数のスコープの設定

同じネットワーク番号とサブネットマスクを使用して、(分離されたアドレス範囲を持つ) 複数のスコープを構成できます。既定では、DHCP サーバーは、同じサブネット上のすべてのスコープから使用可能なリースをプールし、リースを要求するクライアントにラウンドロビン方式でリースを提供します。ただし、各スコープに割り当て優先順位を設定することで、このラ

ラウンドロビン割り当てを[割り当て優先順位を使用した複数スコープの設定 \(4 ページ\)](#) 回避することもできます(「」を参照してください)。

単一サブネットのアドレスを複数のスコープに構成すると、より自然な方法でアドレスを管理しやすくなっています。スコープごとに実質的に無制限の数のリースを構成できますが、数千のリースを持つスコープがある場合は、それらを並べ替えるのに時間がかかることがあります。これは、リースを複数のスコープに分割する動機となります。

リースの種類に応じて、スコープ間でリースを分割できます。各スコープは個別の予約リストを持つことができるので、1つのオプションとリース時間のセットを持つポリシーを持つ1つのスコープに動的リースを配置し、別のスコープ内のすべての予約を別のスコープに置くことができます。複数のスコープの一部がローカルに接続されていない場合は、適切なヘルパーアドレスを使用してルーターを構成する必要があります (BOOTP リレーサポートを持つ) 必要があります。

関連項目

[ラウンドロビンアドレス割り当てのための複数スコープの設定 \(4 ページ\)](#)

[割り当て優先順位を使用した複数スコープの設定 \(4 ページ\)](#)

ラウンドロビンアドレス割り当てのための複数スコープの設定

既定では、DHCPサーバーはラウンドロビン方式で複数のスコープを検索します。このため、DHCPクライアント要求の種類によってスコープをセグメント化する必要があります。サブネット上でセカンダリスコープを使用して複数のスコープが使用できる場合、DHCPサーバーは、受信DHCPクライアント要求を満たすものを検索します。たとえば、サブネットに3つのスコープがあり、そのうちの1つだけが動的BOOTPをサポートする場合、予約のないBOOTP要求は、動的BOOTPをサポートする1つの要求によって自動的に処理されます。

また、DHCP要求を許可しないようにスコープを構成することもできます(既定では、スコープの許可です)。これらの機能を組み合わせて使用することで、すべてのDHCP要求が1つのスコープ(およびアドレス範囲)から満たされるようにサブネット上のアドレスを簡単に構成できます。このようにして、DHCPクライアントをサポートするアドレスプールへの影響を最小限に抑えながら、動的BOOTPをサポートできます。

割り当て優先順位を使用した複数スコープの設定

前項で説明したデフォルトのラウンドロビンの動作の代わりに範囲内で割り当ての優先順序を設定することができます。このようにして、配分プロセスをより詳細に制御できます。また、サブネット内から連続してアドレスを割り当て、DHCPサーバーのフェールオーバーを使用する場合にバックアップサーバーに割り当てられるアドレスのブロック[DHCP フェールオーバーの管理](#)を制御するように、DHCPサーバーを構成することもできます(を参照)。

通常のインストールでは、スコープの割り当て優先順位属性を使用して、すべてのスコープの割り当ての優先順位を設定します。インストールによっては、スコープで最初に使用可能な割り当て属性を有効にしたい場合もありますが、多くの場合は有効にしません。割り当て先使用可能を使用する場合はパフォーマンスが低下する可能性が小さいため、絶対に必要な場合にのみ使用してください。

次の制御が可能です。

- 最初にアドレスを割り当てる必要があるスコープ間の階層。
- 最も最近アクセスされたアドレスの既定の動作ではなく、スコープで最初に使用可能なアドレスを割り当てるかどうかを指定します。
- スコープのフェールオーバー構成で、連続するターゲットアドレスを割り当てる。
- 優先度アドレス割り当てサーバー全体。
- スコープの割り当て優先順位が等しい場合、サーバーが使用可能なアドレスの数が最も多いアドレスまたは最も多いアドレスからアドレスを割り当てる必要があるかどうか。

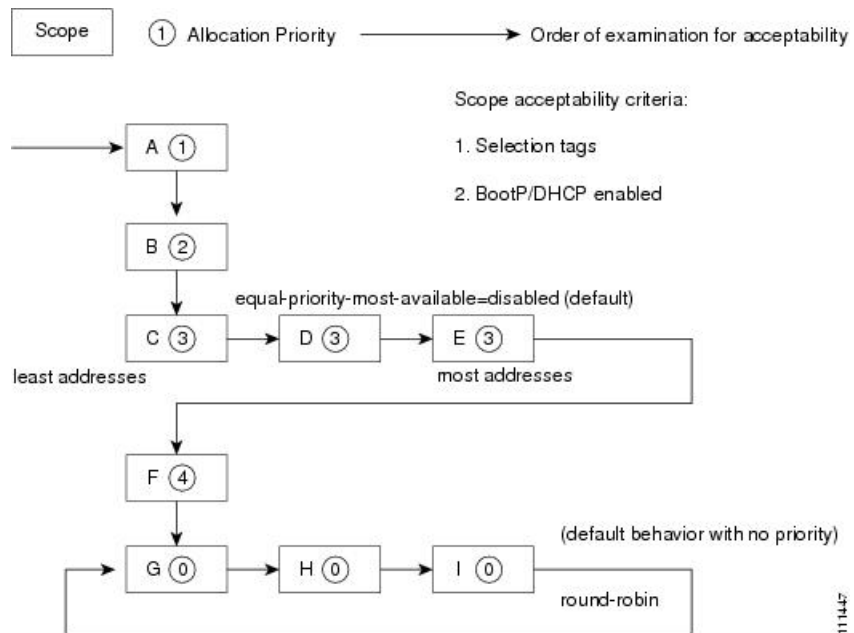
ネットワークに複数のスコープがある場合、DHCPは、既存のアドレスに関連付けられていない DHCP クライアントからの DHCPDISCOVER 要求を処理するとき、どのスコープから IP アドレスを割り当てるかを決定する必要があります。DHCPサーバーがこの割り当てを実行するために使用するアルゴリズムについては、次のセクションで説明します。

割り当て優先順位のアルゴリズム

DHCPサーバーは、ネットワーク内のスコープを1つずつ調べて、許容できるかどうかを判断します。受け入れ可能なスコープが見つかったら、DHCPDISCOVER 要求を満たすために IP アドレスを割り当てようとします。割り当て優先順位のスコープ属性は、割り当て優先順位がない場合、DHCPサーバーがラウンドロビン順序でスコープを調べるため、DHCPサーバーにネットワーク内のスコープを特定の順序で調べるように指示するために使用されます。

下の図は、9つのスコープを持つネットワークの例を示しています(これは珍しいことですが、割り当て優先順位を使用するいくつかの可能性を示しています)。

図 1: スコープ割り当て優先順位



これらのスコープのうち6つは割り当て優先順位で構成され、そのうちの3つは設定されませんでした。サーバーは、割り当て優先順位で構成された6個を、優先順位の最も低いものから

最も高い順に調べます。サーバーは、許容可能なスコープを検出すると、そこから IP アドレスを割り当てようとしています。サーバーが成功すると、このアドレスを使用して DHCPDISCOVER 要求の処理が終了します。そのスコープからアドレスを割り当てることができない場合は、スコープの調査を続行して別の受け入れ可能なスコープを探し、そこからアドレスを割り当てようとしています。

このプロセスは、同じ割り当て優先順位が構成されているスコープがない場合は簡単ですが、例のように複数のスコープが同じ 0 以外の割り当て優先順位を持つ場合、サーバーは等しいスコープの間で選択する方法を持っている必要があります。優先順位。既定の動作では、使用可能なアドレスが最も少ないスコープから始まり、優先順位が等しいスコープを調べます。これにより、別のスコープの他のアドレスを使用する前に、1 つのスコープ内のすべてのアドレスが使用されます。これは上の画像に示されている状況です。優先順位が最も高い DHCP サーバー属性を有効にすると、状況が逆転し、2 つのスコープの優先順位が等しい場合に、使用可能なアドレスが最も多いスコープが最初に調べられます。これにより、スコープの使用率が広がり、割り当て優先順位が等しいすべてのスコープにアドレスの使用が均等に分散されます。

優先順位が同じスコープの処理に別の機能があるため、この優先順位が最も高い方法を使用できます。同じ優先順位のスコープが 2 つある状況では、サーバーがアドレスを割り当てようとしている DHCPDISCOVER 要求にも制限 ID が設定されている場合 (オプション 82 の制限機能を使用しています。 [オプション 82 を使用したサブスクリバの制限](#)したがって、同じ制限 id を持つすべてのクライアントは、同じ優先順位のスコープ内の使用可能なアドレスの数や、優先順位が最も高いサーバー属性の設定に関係なく、同じスコープからアドレスを割り当てる傾向があります。

これを、最も利用可能な同等の状況に戻すために、最も利用可能な同等の優先度を構成し (かつ、いくつかの等しい優先順位スコープを持つ)、特定の制限 id を持つ最初の DHCP クライアントが、使用可能なアドレスが最も多いスコープからアドレスを取得します (同じ制限 id を持つクライアントが他に存在しないため)。その後、同じ制限 ID を持つ後続のクライアントはすべて同じスコープに入るようになります。この構成の結果、最初のクライアントは許容可能な同等の優先順位のスコープに均等に分散され、後続のクライアントは同じ制限 id を持つ既存のクライアントとクラスタ化されます。

同じネットワークに割り当て優先順位が構成されているスコープと、割り当て優先順位のないスコープが存在する場合、割り当て優先順位がゼロ以外のすべてのスコープが最初に受け入れ可能かどうかを調べます。その後、どのスコープも許容可能で、使用可能な IP アドレスも持っていない場合、割り当て優先順位のない残りのスコープはラウンドロビン方式で処理されます。このラウンドロビン検査は、現在の DHCPDISCOVER を送信する場合と同じ制限 ID を持つ既存の DHCP クライアントがある場合を除き、このネットワークで最後に調べたスコープを超える次のスコープで開始されます。この場合、ラウンドロビンスキャンは、既存のクライアント IP アドレスの取得元のスコープから開始されます。これにより、そのスコープが許容範囲であり、割り当て可能な IP アドレスがある場合、その制限 id を持つ後続のクライアントは、その制限 id を持つ最初のクライアントと同じスコープからアドレスを引き出します。

アドレス割り当て属性

アドレス割り当てに対応する属性を次の表に示します。

表 1: アドレスの割り当ての優先度の設定

属性	タイプ	説明
allocation-priority	スコープ (設定または設定解除)	<p>定義されている場合、すべてのスコープのアドレスが使い果たされるまで、優先順位の高い許容範囲からアドレス割り当てが行われるような順序付けをスコープに割り当てます。割り当て優先順位が 0 (事前設定値) の場合、スコープに割り当て優先順位がないことを意味します。優先度 1 が最も高い優先順位で、増加する数の優先順位が低くなります。スコープと割り当て優先度を混在させることもできます。この場合、優先度のあるスコープは、優先順位のないスコープよりも先に受け入れ可能なスコープを調べます。</p> <p>この属性を設定すると、DHCP サーバーの優先度-アドレス-割り当て属性の設定が上書きされます。ただし、割り当て優先順位が設定解除され、優先順位アドレス割り当てが有効になっている場合、スコープの割り当て優先順位はそのサブネット・アドレスになります。割り当て優先順位が設定解除され、優先順位アドレス割り当てが無効になっていると、スコープは既定のラウンドロビン方式で調べられます。</p>
割り当て先-使用可能	スコープ (有効または無効)	<p>有効にすると、このスコープから新しいアドレスのすべての割り当てが、最初に使用可能なアドレスから割り当てられます。無効にした場合 (プリセット値)、最近アクセスしたアドレスが使用されます。この属性を設定すると、DHCP サーバーの優先度-アドレス割り当て属性の設定が上書きされます。ただし、設定解除と優先順位アドレス割り当てが有効な場合、サーバーは最初に使用可能なアドレスを割り当てます。割り当て先使用可能な設定解除と優先順位アドレス割り当てが無効になっていると、スコープは既定のラウンドロビン方式で調べられます。</p>

スコープでのアドレスの割り当て

属性	タイプ	説明
フェールオーバーバックアップ-割り当て-境界	スコープ (設定または設定解除)	<p>最初に使用可能な割り当てが有効で、スコープがフェールオーバー構成にある場合、この値は、バックアップサーバーにアドレスを割り当てるポイントとして使用する IP アドレスです。この境界を下回るアドレスのみがバックアップサーバーに割り当てられます。この境界の下に使用可能なアドレスがない場合、その上のアドレスはバックアップ・サーバーに割り当てられます。実際の割り当てはこのアドレスから下がり、DHCP クライアントの通常の割り当てはスコープ内の最下位アドレスから上に働きます。</p> <p>この属性が設定されていないか、ゼロに設定されている場合、使用される境界は、範囲の範囲内の最初と最後のアドレスの間になります。この境界の下に使用可能なアドレスがない場合は、最初に使用可能なアドレスが使用されます。</p> <p>この設定を使用して、スコープ内でアドレスを割り当てる方法の図については、図 2: 割り当て先使用可能セットによるアドレス割り当てを参照してください。</p>
優先アドレス-割り当て	DHCP (有効または無効)	<p>DHCP サーバー全体の優先アドレス割り当てを有効にする方法を提供します。(ただし、スコープ割り当て優先順位の設定は、この設定を上書きします。優先順位アドレス割り当てが有効で、スコープ割り当て優先順位属性が設定されていない場合、スコープサブネットアドレスが割り当て優先順位に使用されます。スコープ割り当て先利用可能が設定解除されると、優先順位アドレス割り当てが有効と見なされます。もちろん、このアドレス割り当ての全体的な制御を実行する場合、各スコープの実際の優先順位は、そのサブネットアドレスにのみ依存します。</p>
同等の優先順位-最も利用可能	DHCP (有効または無効)	<p>既定では、0 以外の割り当て優先順位が同じ 2 つ以上のスコープが検出されると、使用可能な IP アドレスが最も少ないスコープが使用され、新しいクライアントのアドレスが割り当てられます(そのクライアントが制限リストに含まれていない場合)。優先順位が最も高い場合に使用可能なスコープが有効で、2 つ以上のスコープの割り当て優先順位がゼロ以外の場合、使用可能なアドレスが最も多いスコープが使用され、新しいクライアントのアドレスが割り当てられます(そのクライアントが制限リストにない場合)。いずれの場合も、クライアントが制限リストに含まれている場合、同じ優先順位のスコープの中で、同じリスト内の他のクライアントを含むクライアントが常に使用されます。</p>

スコープでのアドレスの割り当て

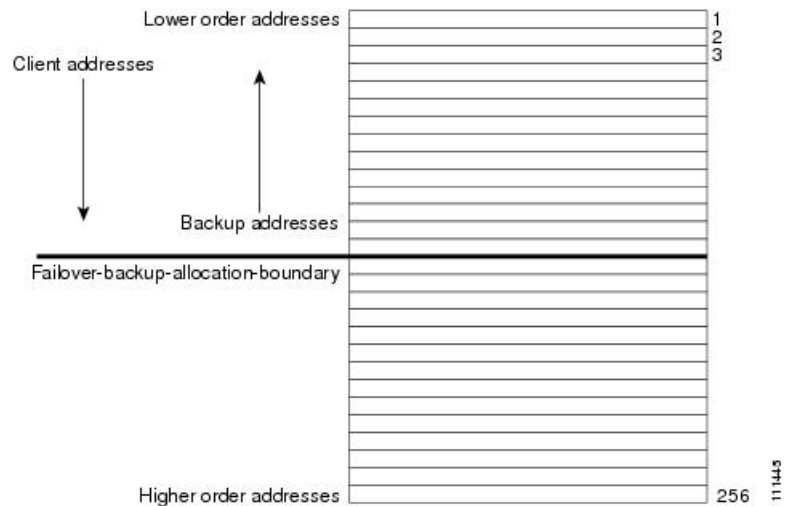
スコープ内から IP アドレスを割り当てようとする場合、DHCP サーバーの既定の動作では、使用可能なリースの一覧から、最も最近アクセスされたアドレスを最初に割り当てようとし、ただし、スコープ内のすべてのリースまたはすべてのリースのリスト表示、特定のリース

の要求 (nrcmd>リース addr)、リースの検索、リースの変更 (アクティブ化、非アクティブ化、または強制的に使用可能なリース) など、リースへのアクセスを必要とするすべての操作は、サーバーで利用可能なリースの一覧内のリースの順序に影響します。

リストの最後にリースする単一のリース場所で動作します。リースの一覧を作成すると、リースが数値順に配置され、最も低い番号のリースが使用可能なリストの最初に表示されます。リースクエリ要求など、サーバーがリースにアクセスする必要がある他の操作も、リースの順序に影響します。

したがって、一般的に、スコープ内のどの IP アドレスが特定の時点で割り当てられるかを予測する方法はありません。通常、これは難しい問題ではありませんが、より決定的な割り当て戦略が望まれる場合があります。完全に確定的なアドレス割り当て戦略を構成するには、スコープで最初に使用可能な割り当て属性を有効にします。これにより、最小の数値の使用可能なアドレスが DHCP クライアントに割り当てられます。したがって、最初のクライアントは最も低い範囲の最初のアドレスを取得し、2 番目のクライアントはその範囲の 2 番目のアドレスを取得します。これは下の画像に示されています。

図 2: 割り当て先使用可能セットによるアドレス割り当て



この決定論的割り当て方法にはわずかなパフォーマンスコストが発生しますが、使用すべきでないほどではなく、必要でない場合は使用しないように十分な場合もあります。スコープがフェールオーバー関係にある状況でこの決定論的な割り当て方法を使用する場合、バックアップサーバーに使用可能な IP アドレスを割り当てる方法がメインサーバーに表示されます。既定では、スコープ内の最下位アドレスと最上位アドレスの間にあるアドレスが、フェールオーバー-バックアップ-割り当て境界になります。バックアップサーバーで使用可能なアドレスは、この境界から下方向に割り当てられます(その方向で使用可能なアドレスがある場合)。この境界の下にアドレスが使用できない場合は、境界の上にある最初のアドレスがバックアップサーバーに使用されます。中間点とは異なるアドレス境界を設定する場合は、スコープのフェールオーバー-バックアップ-割り当て境界を構成できます。

必要以上に多くの IP アドレスを持つスコープを割り当てる場合は、決定的な割り当て戦略を使用し、割り当て先の使用可能な割り当てを構成します。アドレス空間を別のネットワークまたはサーバーに移動できるように、スコープ内の範囲を後で縮小することができます。非決定

的なアプローチでは、割り当てられたアドレスが範囲全体に散在し、スコープアドレスの半分を解放するようにDHCPクライアントを再構成するのは非常に困難です。ただし、割り当て先使用可能を構成すると、割り当てられたアドレスはスコープ範囲の低いクラスタに分類されます。その場合、そのアドレスを他の場所で使用できるように、必要ない範囲から範囲を削除する方が簡単でしょう。

スコープの編集



(注) スコープのサブネットに変更を加えることができるのは、現在のスコープ内、またはそれらのスコープのサブネットと同じ古いサブネットを持つ他のスコープに変更が適用される、変更と競合する予約または範囲がない場合のみです。

ローカルアドバンスド Web UI

ステップ1 [のスコープの作成 \(2 ページ\)](#) 説明に従って、スコープを作成します。

ステップ2 DHCP サーバーをリロードします。

ステップ3 [DHCPスコープの一覧/追加 (List/Add DHCP Scopes)] ページの [スコープ (Scopes)] ペインでスコープ名をクリックして、[DHCPスコープの編集 (Edit DHCP Scope)] ページを開きます(サーバーの再ロードが必要な場合は、ステータスメッセージが表示され、先に進む前に最初に再ロードする必要があります)。

ステップ4 必要に応じて、フィールドまたは属性を変更します。スコープの名前を変更することもできます。

ステップ5 スコープの埋め込みポリシーを [スコープの埋め込みポリシーの設定 \(12 ページ\)](#) 編集するには、「」を参照してください。スコープのリースを一覧表示するには、「」 [リースの表示](#) を参照してください。

ステップ6 Save をクリックします。

ステップ7 DHCP サーバーをリロードします。

CLI コマンド

スコープを作成したら、サーバー上のすべてのスコープのプロパティを調に入れ、使用(scopelist または scopelistnames scope listbrief、scope、scope get name show、name属性)を使用します。次のアクションを実行します。

- 属性をリセットするには、scope 名前 set属性=値[属性=値..] を使用します。たとえば、`scope name set name =new name` を使用して範囲の名前をリセットできます。
- 属性を有効または無効にするにはscope、nameenable属性またはscope name disable 属性を使用します。

構文とscope属性の説明については、/docs ディレクトリの CLIGuide.html ファイルのコマンドを参照してください。

関連項目

- [段階的な同期モード \(11 ページ\)](#)
- [スコープの埋め込みポリシーの設定 \(12 ページ\)](#)
- [ネットワーク上の複数サブネットの設定 \(13 ページ\)](#)
- [スコープの BOOTP の有効化と無効化 \(14 ページ\)](#)
- [スコープの DHCP の無効化 \(16 ページ\)](#)
- [スコープの非アクティブ化 \(17 ページ\)](#)
- [スコープを更新専用を設定 \(15 ページ\)](#)
- [スコープでの空きアドレス SNMP トラップの設定 \(15 ページ\)](#)
- [アドレスを再利用しない場合のスコープの削除 \(18 ページ\)](#)
- [アドレスを再利用しない場合のスコープの削除 \(18 ページ\)](#)

段階的な同期モード

スコープの新しいスコープまたは変更は、ステージングモードと同期モードの2つのモードのいずれかになります。

- **Staged:** 既存のスコープに対する新しいスコープまたは変更はデータベースに書き込まれますが、DHCP サーバーが再ロードされるまで DHCP サーバーに伝達されません。
- **Synchronous**—ほとんどの新しいスコープとスコープの変更(削除を含む)は、直ちに DHCP サーバーに伝播されます(リロードは不要)。スコープの変更の一覧が変更できるわけではありません。たとえば、スコープのプライマリ サブネットの変更は許可されません(変更を反映するには再ロードが必要です)。さらに、リロードせずに、スコープ属性の変更のみを反映できます。たとえば、名前付きポリシーを変更するには、DHCP サーバーの再ロードが必要です。

ステージングモードでスコープを追加または変更した後、dhcp 編集モードを同期モードに変更すると、同期モードでの最初の変更は、そのスコープに対するすべての保留中の変更を適用します(同期モードで行われた変更だけでなく)。

[ローカル基本 (Basic)] または [アドバンスド (Advanced)] Web UI

現在の dhcp 編集モードを表示したり、dhcp 編集モードを変更したりするには、Web UI の上部にある[設定]ドロップダウンリストをクリックして、を選択Session Settingsします。DHCP サーバーでスコープが最新の状態である場合、[同期されたスコープの総数]メッセージが [DHCP スコープの一覧/追加]ページ(詳細モード)に表示され、[スコープ名の状態: 同期済み]メッセージが [DHCP スコープの編集]ページ(両方のモード)に表示されます。スコープが最新でない場合は、[スコープ名の状態: 必要な再読み込み]メッセージが表示されます。

CLI コマンド

を `sessionget` 使用 `dhcp-edit-mode` して `dhcp` 編集モードを表示するか、`{sync sessionsetdhcp-edit-mode=}` を使用して DHCP 編集モードを設定する `|staged}`. DHCP サーバーと同期していないスコープを表示するには、`scope report-staged-edits` を使用します。次に例を示します。

```
nrcmd> scope report-staged-edits

100 Ok

example-scope: [reload-required]
```

サーバー上のスコープ数の取得

DHCP サーバーに関連付けられた作成されたスコープを表示できるため、Web UI でカウントを取得できます。

CLI コマンド

CLI を使用すると、`dhcp getScopeCount [vpn 名前all]`. VPN またはすべての VPN を指定できます。vpn 名前を省略すると、現在の VPN の数が返されます。フェールオーバー ペア名を指定すると、フェールオーバーペアのスコープとネットワークの合計が返されます。フェールオーバー ペア定義のマッチリストには明示的な VPN 設定が含まれているため、これらの数は現在の VPN だけに限定されません。

スコープを作成するには、`scope 名前 create アドレスマスク[テンプレート=テンプレート名][属性=値..]` を使用します。各スコープは、そのネットワークアドレスとマスクを識別する必要があります。スコープを作成すると、Cisco Prime Network レジストラーは、現在の仮想プライベート ネットワーク (VPN) `session set current-vpn` に配置されます。VPN は、スコープの作成時に設定した後は変更できません。

スコープのポリシーを設定するには、`scope name set policy` を使用します。

スコープに IP アドレスの範囲を追加するには、`scope 名前 addRange start end` を使用します。

スコープの埋め込みポリシーの設定

スコープを作成すると、Cisco Prime ネットワーク レジストラーは、そのスコープに組み込まれたポリシーを自動的に作成します。ただし、組み込みポリシーには、有効または追加するまで、関連付けられたプロパティや DHCP オプションはありません。埋め込みポリシーは、スコープのルーターを定義する場合などに役立ちます。説明 [ポリシーのタイプ](#) されているように、DHCP サーバーは、割り当てられた名前付きポリシーを参照する前に、スコープの埋め込みポリシーを参照します。



(注) スコープ ポリシーを削除すると、そのすべてのプロパティと属性が削除されます。

ローカルアドバンスド Web UI

-
- ステップ 1** [のスコープの作成 \(2 ページ\)](#) 説明に従って、スコープを作成します。
- ステップ 2** [DHCP スコープの一覧/追加] ページの [スコープ] ウィンドウでスコープの名前をクリックして、[DHCP スコープの編集] ページを開きます。
- ステップ 3** Create 新 New しい埋 Embedded め込みポリシーを作成するか、既存のポリシーが既に存在する場合は、[スコープの DHCP 埋め込みポリシーの編集] ページを開 Policy Edit Existing Embedded Policy きます。
- ステップ 4** このページのフィールド、オプション、および属性を変更します。必要に応じて、属性を設定解除します。
- ステップ 5** Save をクリックします。
-

CLI コマンド

最初にスコープを作成します。CLI では、`scope-policy` スコープ名を引数として `policy` 受け取ることを除いて、と同じ構文を使用します。次に、次の手順を実行します。

- スコープに対して既に設定されている埋め込みプロパティ値があるかどうかを `scope-policy` 判断し、`scope-nameshow` を使用します。
- 属性を有効または無効にする、`scope-policy` スコープ名 `enable` 属性または `scope-policy` スコープ名 `disable` 属性を使用する。
- 属性を設定および設定解除し、`scope-policy` スコープ名 `set` 属性=値 [属性=値..] および `scope-policy` スコープ名 `unset` 属性を使用します。
- [バンダーオプションの一覧、設定、および設定解除標準オプション定義セットの使用\(「」を参照\)](#)

ネットワーク上の複数サブネットの設定

Cisco Prime Network レジストラーは、同じネットワークセグメント上の複数の論理サブネットをサポートします。192.168.1.0/24 および 192.168.2.0/24 など、同じ物理ネットワーク上に複数の論理サブネットがある場合は、両方のプールからアドレスを提供するように構成できます。このようにアドレスをプールすることで、使用可能なリース数を増やすことができます。

2つの論理サブネットを結合するには、2つのスコープを作成し、1つをプライマリに、もう1つをセカンダリに選択します。セカンダリサブネットを構成すると、この物理ネットワーク上の新しいクライアントは、ラウンドロビンベースで1つまたは別のスコープからリースを取得します。

ローカルアドバンスド Web UI

-
- ステップ 1** セカンダリ スコープを作成 [スコープの作成 \(2 ページ\)](#) するスコープ (を参照) を作成します。

ステップ 2 [DHCPスコープの一覧/追加 (List/Add DHCP Scopes)] ページの [スコープ (Scopes)] ペインでスコープ名をクリックして、[DHCPスコープの編集 (Edit DHCP Scope)] ページを開きます。

ステップ 3 これをセカンダリ スコープにするには、[DHCP スコープの編集] ページの [プライマリ サブネット] 属性フィールドにプライマリ スコープのサブネットのネットワーク アドレスを入力します。

プライマリサブネットは、プライマリスコープのネットワークアドレスに直接対応するのが一般的です。たとえば、192.168.1.0/24 ネットワークで作成された `examplescope1` では、プライマリサブネット =192.168.1.0/24 を使用して `examplescope2` を関連付けます。(Cisco Prime Network レジストラーが、定義されたサブネットに関連するスコープがあることを検出した場合、マスクビット定義は無視され、一致しない場合に備えてプライマリスコープの定義を使用します)。ただし、プライマリサブネットは、スコープが関連付けられていないサブネットアドレスである場合があります。

ステップ 4 Save をクリックします。

ステップ 5 サーバーを再起動または再ロードします。

CLI コマンド

セカンダリ スコープをプライマリ スコープに割り当てる `scope` には、名前 `setprimary-subnet=値` を使用してから、サーバーを再ロードします。

セカンダリ スコープを削除するには、`scope name unset primary-subnet` を使用します。プライマリサブネット属性を設定する場合は、スラッシュ表記を使用して、ネットワークマスクのビット数を含めます。たとえば、ネットワーク 192.168.1.0 をマスク 255.255.255.0 で 192.168.1.0/24 として表します。マスクビットは重要です。これらを省略すると、/32 マスク (単一 IP アドレス) が使用されます。

スコープの BOOTP の有効化と無効化

BOOTstrap プロトコル (BOOTP) は、ディスクレスコンピュータをロードするために作成されました。その後、ホストがインターネットを使用できるように、必要なすべての TCP/IP 情報を取得できるようにするために使用されました。ホストは BOOTP を使用して、ネットワーク上で要求をブロードキャストしたり、BOOTP サーバーから必要なデータを取得したりします。BOOTP サーバーは、着信要求をリッスンし、そのネットワーク上の BOOTP クライアントの構成データベースから応答を生成します。BOOTP は DHCP とは異なり、リースまたはリース期限の概念はありません。BOOTP サーバーが割り当てるすべてのアドレスは永続的です。

Cisco プライム ネットワークレジストラー DHCP サーバーを BOOTP サーバーのように動作するように設定できます。さらに、BOOTP では通常静的アドレスの割り当てが必要ですが、アドレスを予約するか(静的割り当てを使用)、アドレスを動的に割り当てる(動的 BOOTP と呼ばれます)を選択することもできます。

BOOTP クライアントを移動または使用停止する必要がある場合は、リースの可用性を強制するだけで、リースを再利用できます。[リースを強制的に使用可能にする](#) を参照してください。

ローカルアドバンスド Web UI

[DHCP スコープの編集] ページの [BootP 設定] で、BOOTP の bootp 属性または動的ブート P の動的ブート属性を有効にします。デフォルトでは無効です。次に、Save をクリックします。

CLI コマンド

scope name enable bootp を使用して BOOTP を有効にし、scope name enable dynamic-bootp を使用して動的 BOOTP を有効にします。DHCP サーバーをリロードします(段階的な DHCP 編集モードの場合)。

スコープを更新専用を設定

既存のクライアントがリースを再取得することを許可するかどうかは制御できますが、新しいクライアントにリースを提供することはできません。更新のみのスコープでは、現在利用可能な IP アドレスを使用しているクライアントがリースを継続して使用することを許可する以外に、リースに関連付けられているクライアントは変更されません。

ローカルアドバンスド Web UI

[DHCP スコープの編集] ページの [その他の設定] で、更新専用属性を明示的に有効にします。次に、Save をクリックします。

CLI コマンド

scope名前enableをrenew-only使用して、スコープを更新専用を設定します。

スコープでの空きアドレス SNMP トラップの設定

SNMP トラップを設定して、トラップを有効にし、スコープの低しきい値と高しきい値を設定することで、予期しない空きアドレス イベントをキャプチャできます。スコープの代わりにネットワークと選択タグに基づいてトラップを設定することもできます。

しきい値を設定する場合は、下限値と高値の間の小さなオフセットを維持することをお勧めします。Cisco プライムネットワーク レジストラー 11.0 管理ガイドオフセットは、たとえば、20% の低い値と 25% の高い値(プリセット値)の 5% までです。

これらの属性のサーバーとスコープの値を設定する方法のバリエーションを次に示します。

- 少なくとも 1 人の受信者が構成されている限り、サーバーの設定に基づいて、各スコープをトラップして解放アドレスの値をリセットします。
- スコープ レベルでトラップを無効にするか、スコープごとに異なる割合を指定します。
- サーバー上でトラップをグローバルに無効にしますが、スコープごとに有効にします。
- ネットワーク レベルまたは選択タグ レベルでトラップを設定します。

ローカルアドバンスドおよびリージョン Web UI

- ステップ 1** トラップ構成を作成するには、[デプロイ] メニューのサブTrapsメニューのDHCP下で [リスト/トラップ構成の追加] ページを開きます。
- ステップ 2** [トラップの追加] アイコンをクリックし、トラップ設定の名前を入力scopeし、[モード] ドロップダウン リストから選択し、低しきい値と高しきい値を入力します(デフォルトでは、それぞれ20%と25%です)。Add AddrTrapConfig をクリックします。(必要に応じて、これらの値を編集するために戻ることができます。)
- ステップ 3** しきい値の設定を適用する作成されたスコープを編集します。[SNMP トラップ設定] の下の、フリーアドレス設定属性フィールドにトラップの名前を入力します。Save をクリックします。
- ステップ 4** リージョン Web UI では、レプリカ トラップ構成をプルし、トラップ構成をローカルクラスターにプッシュするには、[リスト/トラップ構成の追加] ページを使用します。トラップ構成を再利用することもできます。

CLI コマンド

トラップ addr-trap構成を追加するには、namecreateを使用します。しきい値を設定するには、addr-trap 名前 setの方法を使用します(または、トラップの作成時にしきい値の設定を含めます)。次に例を示します。

```
nrcmd> addr-trap trap-1 create
nrcmd> addr-trap trap-1 set low-threshold
nrcmd> addr-trap trap-1 set high-threshold
```

フリー・アドレス・トラップを設定するには、scope 名前 set free-address-config=トラップ名を使用します。次に例を示します。

```
nrcmd> scope scope-1 set free-address-config=trap-1
```

地域クラスターに接続すると、次のプル、プッシュ、および再利用のコマンドを使用できます。プッシュおよび再使用の場合は、クラスターのリストまたは「すべて」を指定できます。

- アドルトラップ<名前|すべて>プル<確認する |置き換える|正確な>クラスター名[-レポートのみ|-レポート]
- アドルトラップ<名前|すべて>プッシュ<確認する |置き換える|正確な>クラスターリスト[-レポートのみ|-レポート]
- 追加トラップ名再利用クラスターリスト[-レポートのみ|-レポート]

スコープの DHCP の無効化

BOOTPのためだけに使用する場合は、スコープのDHCPを無効にできます。[スコープのBOOTPの有効化と無効化 \(14 ページ\)](#) を参照してください。DHCP を無効にすることでスコープを

一時的に非アクティブにすることもできますが、BOOTP を有効にする場合は非アクティブ化が頻繁に使用されます。[スコープの非アクティブ化 \(17 ページ\)](#) を参照してください。

ローカルアドバンスド Web UI

[DHCP スコープの編集] ページの [BootP 設定] で dhcp 属性を無効Saveにし、bootp 属性を有効にして、をクリックします。

CLI コマンド

DHCPscopeを無効にするには、名前disabledhcpを使用します。また、BOOTP を有効にして、サーバーをリロードする必要があります (段階的な dhcp 編集モードの場合)。

スコープの非アクティブ化

スコープ内のすべてのリースを一時的に非アクティブ化する場合があります。これを行うには、スコープの BOOTP と DHCP の両方を無効にする必要があります。

ローカルアドバンスド Web UI

[DHCP スコープの編集] ページの [その他の設定] で、非アクティブ化属性を明示的に有効にします。次に、Save をクリックします。

CLI コマンド

スコープscopeのBOOTPとDHCPを無効にするには、名前enabled deactivatedを使用します。DHCPサーバーをリロードします(段階的なDHCP編集モードの場合)。

スコープの削除



注意 DHCP サーバーからスコープを削除するのは簡単ですが、注意が必要です。この操作を行うと、ネットワークの整合性が損なわれます。次のセクションで説明するように、アドレスを再利用するか、または使用しないかによって、サーバーからスコープを削除する方法はいくつかあります。

DHCP は、IETF によって定義されているように、特定の時間 (サーバー管理者によって定義される) クライアントにアドレスリースを提供します。その時間が経過するまで、クライアントはリースされたアドレスを自由に使用できます。サーバーは、リースを取り消して、クライアントがアドレスを使用するのを停止することはできません。したがって、DHCPサーバーからスコープを簡単に削除できますが、リースを取得したクライアントは、期限が切れるまで引き続き削除できます。これは、サーバーが更新の試行に応答しない場合でも、スコープが削除された場合に発生します。

削除したアドレスが何らかの方法で再利用されない場合、この方法では問題は発生しません。ただし、最後のリースの期限が切れる前に別のサーバーのアドレスが構成されている場合、2

つのクライアントが同じアドレスを使用する可能性があり、ネットワークが不安定になる可能性があります。

Cisco プライムネットワーク レジストラーは、削除されたスコープのリースを孤立したリースプールに移動します。スコープを作成する場合、孤立したリースは適切なスコープに関連付けられます。

アドレスを再利用しない場合のスコープの削除

アドレスを再利用しない場合は、スコープを削除できます。

[ローカル基本 (Basic)] または [アドバンスド (Advanced)] Web UI

スコープを再利用する予定がない場合は、[スコープの管理] ページまたは [DHCP スコープの一覧表示/追加] ページで、名前を選択した後、[スコープ] ウィンドウの[スコープの削除] アイコンをクリックし、削除を確認またはキャンセルします。

CLI コマンド

スコープ内のアドレスをすぐに再利用する予定がない場合は、`scope` 名前 `delete` を使用して削除してください。

アドレスを再利用しない場合のスコープの削除

削除するスコープのアドレスを再利用する場合は、次の 2 つの方法があります。

- **If you can afford to wait until all the leases in the scope expire—** : スコープをサーバーから削除し、ポリシーで設定された最も長いリース時間が期限切れになるまで待機します。これにより、そのスコープのアドレスを使用しているクライアントが存在しません。その後、アドレスを安全に再利用できます。
- **If you cannot afford to wait until all the leases in the scope expire** : スコープを削除しません。代わりに、非アクティブ化します。[スコープの非アクティブ化 \(17 ページ\)](#) を参照してください。削除されたスコープとは異なり、サーバーはすべてのクライアントの更新要求を拒否し、その多くが新しいリースを要求します。これにより、これらのクライアントは、削除されたスコープよりも非アクティブ化されたリースからより迅速に移動します。

Windows の `ipconfig` ユーティリティを使用して、クライアントがそのリースを解放/release し、再取得/renew し、非アクティブ化されたリースからすぐにそのリースを移動させることができます。このユーティリティはクライアントコンピュータからしか発行できないので、何千ものリースが使用されているスコープでは実用的ではありません。ただし、Windows 環境の最後の数個のクライアントをスコープ内の非アクティブ化リースから移動する場合に便利です。

DHCPv6 Addresses

Cisco Prime Network Registrar は、RFC 8415 に基づき 次の DHCP (DHCPv6) の IPv6 アドレスがサポートされています。

- **Stateless autoconfiguration** : DHCPv6 サーバーはアドレスを割り当てず、代わりに DNS サーバーデータなどの構成パラメータをクライアントに提供します。
- **Stateful autoconfiguration** : DHCPv6 サーバーは、非一時アドレスまたは一時アドレスを割り当て、クライアントに構成パラメータを提供します。
- **Prefix Delegation** : DHCPv6 サーバーはプレフィックスをクライアント (ルータ) に委任します。



(注) RFC 8415 は、以前の RFC である RFC 3315、RFC 3633、RFC 3736、RFC 4242、および RFC 7083 を組み込み、廃止しました。

DHCPv6 サービスは、次の機能を提供します。

- **アロケーショングループ**— 複数のプレフィックスを割り当ての観点から 1 つとして扱えるようにし、プレフィックスが使用される順序を制御できるようにします。
- **クライアント クラス化**: 既知のクライアントまたはパケット ベースの式に基づいて、クライアントを分類し、プレフィックスを選択できます。
- **DNS 更新**— DNS サーバーが (IPv4 経由で) DHCP アクティビティを更新します。
- **拡張機能- C/C++** および Tcl 拡張機能を使用して、DHCP サーバーの処理を拡張します。
- **フェールオーバー**: 要求しているクライアントにリースを提供できない場合に別のクライアントが引き継ぐように、DHCP フェールオーバー ペアを設定できます。
- **LDAP:LDAP** リポジトリ (Cisco Prime Network レジストラーの外部) でクライアント エントリ リックアップを許可し、クライアントがクライアント予約を指定する場合があります。
- **リースクエリ**-リースクエリのサポートを提供します。
- **リンクとプレフィックス**— ネットワーク トポロジを定義する DHCPv4 ネットワークおよびスコープに似ています。各リンクには、1 つ以上のプレフィックスを付けることができます。
- **ポリシーとオプション**: リンク、プレフィックス、クライアントに属性とオプションを割り当てることができます。
- **プレフィックスの安定性**: クライアントは、ある CMTS から別の CMTS に移動したり、アドレス空間内で移動したりした場合でも、位置を変更した場合に委任されたプレフィックスを保持できます。適切なインフラストラクチャサポート (CMTS、ルーター) を使用したプレフィックスの安定性により、別の委任されたプレフィックスを必要とせずに、サブスクリバを移動または移動できます。
- **SNMP トラップ**: プレフィックス内のリース数が一定の制限を超えた場合 (または一定の制限を下回った場合)、またはサーバーが重複アドレスを検出した場合など、イベントのトラップを生成します。
- **予約**— クライアントは、事前に決められたアドレスを受信できます。
- **統計収集およびロギング**-サーバー・アクティビティのモニターを提供します。
- **VPN サポート**— 複数のアドレス空間 (仮想プライベート ネットワーク) を提供します。

DHCPv6 サービスでは、サーバー・オペレーティング・システムが IPv6 をサポートし、システム上で IPv6 用に少なくとも 1 つのインターフェースを構成する必要があります。

IPv6 アドレス指定

IPv6 アドレスは 128 ビット長であり、コロンで区切られた 16 ビットの 16 進数のフィールドとして表現されます (:)。16 進数の A、B、C、D、E、および F は、大文字と小文字を区別しません。次に例を示します。

```
2001:db8:0000:0000:0000:0000:0000:0000
```

このアドレッシングに対するいくつかのショートカットは次のとおりです。

- フィールド内の先頭にある 0 は省略可能なため、09c0 は 9c0、そして 0000 は 0 と書き込むことができます。
- 連続した 0 (任意の数) のフィールドは、2つのコロン (::) で表すことができますが、アドレスで一度のみです。これは、二度以上使用すると、アドレスパーサーが 0 の各ブロックのサイズを識別できなくなるからです。これにより、アドレスの長さが減少します。たとえば、2001:db8:0000:0000:0000:0000:0000:0000 に書き込むことができます。

```
2001:db8::
```

リンク ローカルアドレスには、リンクに対して制限範囲があり、プレフィックス `fe 80::/10` を使用します。ループバックアドレスにはアドレス `::1` があります。マルチキャストアドレスには、`ff00::/8` のプレフィックスが付きます (IPv6 にはブロードキャストアドレスはありません)。

IPv6 の IPv4 に互換性のあるアドレスは、:: のプレフィックスが付く、IPv4 10 進数クアドアドレスです。たとえば、IPv4 アドレスを形式 `::c0a8:1e01::192.168.30.1` で解釈して記述できます。

リンクとプレフィックスの決定

DHCPv6 サーバーは、DHCPv6 メッセージを受信すると、要求の処理に使用するリンクおよびプレフィックスを決定します。サーバー:

1. 送信元アドレスを検索します。
 1. クライアントメッセージがリレーされた場合、サーバーは、クライアントに最も近い (作業している) Relay-Forward メッセージから始まる最初の 0 以外のリンクアドレスフィールドに送信元アドレスを設定します。サーバーが送信元アドレスを見つけた場合は、ステップ 2 に進みます。
 2. それ以外の場合、メッセージ・ソース・アドレスがリンク・ローカル・アドレスである場合、サーバーは、プレフィックスが存在するメッセージを受信したインターフェースの最初のアドレス (任意のアドレスの接頭部が見つかった場合は 0) にソース・アドレスを設定します。ステップ 2 に進みます。
 3. それ以外の場合、サーバーは送信元アドレスをメッセージ送信元アドレスに設定します。



注 この動作は、拡張機能によって変更するか、クライアント/クライアントクラスの環境への追加属性を使用して、IPv6アドレスまたはプレフィックス名のリンクアドレスオーバーライド属性値を追加することによって変更できます。表1を参照してください。

2. 送信元アドレスのプレフィックスを検索します。サーバーが送信元アドレスのプレフィックスを見つけられない場合、クライアントにサービスを提供できず、要求を破棄します。
3. プレフィックスのリンクを検索します。これは常に存在し、明示的に設定されたリンクか、プレフィックスアドレスに基づいて暗黙的に作成されたリンクのいずれかです。リンクはトポロジリンクである必要があります(プレフィックス安定性 (22 ページ) を参照してください)。

これで、サーバーはクライアントリンクを決定できるようになったので、クライアント要求を処理できます。クライアント要求がステートフルかプレフィックス委任か、選択基準などの要因によって、サーバーはクライアント要求にサービスを提供するリンクに1つ以上のプレフィックスを使用する場合があります。

これは、DHCPv4 と DHCPv6 の間の違いの1つの領域です。DHCPv4 では、サーバーはクライアント要求にサービスを提供するために、ネットワークからスコープの1つだけを選択します。DHCPv6 では、サーバーはリンクのすべてのプレフィックスを使用できます。したがって、サーバーがクライアントにアドレスを割り当てたり、リンクの複数のプレフィックスからプレフィックスを委任したりすることができます(選択基準やその他条件が適用されます)。リンクの作成と編集 (31 ページ) を参照してください。

アドレスの生成

IPv6アドレスは128ビットアドレスです(IPv4の場合は32ビットのアドレスと比較されます)。ほとんどの場合、DHCPv6サーバーは、これらのビットのうち64個のインターフェイス識別子(EUI-64)部分を割り当てます(RFC 4291を参照)。クライアントの64ビットインターフェイス識別子または乱数ジェネレーターを使用して、アドレスを生成できます。インターフェイス識別子は、ステートレス自動設定がクライアントにアドレスを割り当てる方法をエミュレートします。残念ながら、その使用に関するプライバシーの懸念があり、クライアントのプレフィックスごとに1つのアドレスに制限されています。

デフォルトでは、Cisco Prime Networkレジストラーは、RFC 4941で説明されているアルゴリズムと同様のアルゴリズムを使用してアドレスを生成し、ランダムなインターフェイス識別子を生成します。これらのランダムインターフェイス識別子は、ユニバーサル/ローカルビットの値がゼロで、EUI-64ベースの識別子と区別されます。サーバーは、ランダムに生成されたインターフェイス識別子を::0からスキップします。::ffにして、インフラストラクチャデバイス(ルーターなど)に識別子を使用できるようにします。各プレフィックスに対してinterface-identifier(使用可能な場合)を最初に割り当てるかどうかを設定できます(プレフィックスのallocation-algorithm属性のinterface-identifierフラグを使用)。(プレフィックスの作成と編集 (25 ページ) を参照)。インターフェイス識別子の使用を指定した場合、クライアントがア

ドレスを使用できない場合、またはクライアントがプレフィックスに複数のアドレスを要求する場合、サーバーはランダムに生成されたアドレスを使用する可能性があります。

サーバーは、プレフィックスが設定された範囲(または範囲がない場合はプレフィックスアドレス)に基づいてアドレスを生成します。範囲プレフィックス長が64より短い場合、サーバーは64ビットのみを提供し、アドレス・インターフェースIDフィールドに入れられます。プレフィックス長が64より長い場合、サーバーはアドレスの残りのビットだけを提供します。したがって、/96の範囲は、指定された範囲から96ビットを使用し、その後クライアントインターフェース識別子またはランダムに生成された値の32ビットを使用します。結果として得られるアドレスが使用できない場合(別のクライアントまたは同じクライアントにリースされているが、別のバインディング上にリースされている場合など)、サーバーは別のアドレスを生成しようとします。このプロセスは最大500回まで繰り返されます。

DHCPフェイルオーバーが構成されている場合、サーバー生成のアドレスは、メインアドレス上で常に奇数アドレスになり、バックアップ上のアドレスも偶数になります。



(注) DHCPサーバーは、ランダムに生成されたインターフェース識別子のみを::0からの値に対してテストします。結果のアドレスではなく::ffにします。したがって、ランダムに生成されたアドレスは、xxxx :xxxx :xxxx :xxxx ::0を使用する可能性があります。xxxx :xxxx :xxxx :xxxx :xxxx ::ffアドレスは、プレフィックスの長さが/64より長く、/64境界を超えるプレフィックスビットがすべてゼロである場合。



ヒント プレフィックスとプレフィックステンプレートに対して、追加のアドレス生成アルゴリズムから選択することもできます。「」を参照してください[プレフィックステンプレートの作成と編集](#)。

委任プレフィックスの生成

DHCPv6サーバーは、委任されたプレフィックスを生成するときに、最適な最初の適合アルゴリズムを使用します。サーバーは、構成または要求された長さの最初の使用可能なプレフィックスを使用します。

DHCPフェイルオーバーの場合、各サーバーは、使用可能な状態で委任されたプレフィックスリースのみを考慮します。サーバーがPARTNER-DOWN状態の場合、サーバーは、一定時間の制限が過ぎた後に、他の使用可能な状態または保留中の状態でリースを使用することもできます。

プレフィックス安定性

プレフィックスの安定性を使用すると、ネットワークトポロジの接頭辞の安定性に関係なくプレフィックスの委任を。新しいリンク属性の種類は、リンクの種類を指定します。

リンクには、次の3種類があります。

- トポロジカルルートポロジリンク上のクライアントは、接続されているネットワークセグメントに基づいてリースが割り当てられます。
- 場所に依存しない:このリンク タイプは、ケーブルラボ DOCSIS 3.0 の概念である CMTS プレフィックスの安定性をサポートするために導入されています。CMTS のグループ内(セントラル オフィスなど)内のサービス プロバイダのロード バランシングおよび再構成イベントをサポートします。ロケーションに依存しないリンクでCMTS間で移動されたサブスライバは、委任されたプレフィックスを保持できます。このリンクタイプは、単一のDHCPサーバー内での移動を可能にします。
- ユニバーサル:このリンク タイプは、加入者がネットワーク内の任意の場所で委任されたプレフィックスを保持できるように導入されます。このリンクの種類を使用するには、委任されたプレフィックスの管理割り当てと、クライアントまたはリース予約の使用が必要です。複数の DHCP サーバーに展開できます。



(注) プレフィックスの安定性の使用はルーティングに影響を与え、ルートをアドバタイズするためにリレー エージェント(つまり CMTS)からの適切なサポートが必要です。CMTS プレフィックスの安定性のために、これらは CMTS グループにローカライズされます。サービス プロバイダ ネットワーク全体でルートをアドバタイズする必要がある場合、ユニバーサルプレフィックスの安定性に対する影響は大きくなります。

CMTS プレフィックス安定性

ロケーションに依存しないリンクはCMTSプレフィックスの安定性のためのケーブルLabs DOCSIS 3.0の条件を実装します。すべてのプレフィックスが単一の DHCP サーバーによってサービスされる限り、CMTS プレフィックスの安定性は可能です。

特定の領域にCMTSプレフィックスの安定性を導入する場合は、次の手順を実行する必要があります。

- 既存のリンクを変更して、グループ内のすべてのリンクで同じリンク グループ名を指定します。各 CMTS(または CMTS バンドル)は個別のリンクを持っていますが、CMTS プレフィックスの安定性が望まれる領域内のこれらのリンクはすべて、同じリンクグループの一部にする必要があります。
- 場所に依存しないとしてフラグが設定され、このリンクグループの一部として作成された新しいリンクを作成します。この場所に依存しないリンクの下に1つ以上のプレフィックス委任プレフィックスを作成または移動します。
- 不要になった既存のリンクからプレフィックスの委任プレフィックスを削除します。ステートフルプレフィックス (dhcp タイプの dhcp) は削除しないでください。



(注) グループ内で使用できる場所に依存しないリンクは1つだけです。

クライアント要求を受信すると、サーバーは、最も長く一致するプレフィックスをチェックし、そのプレフィックスのリンクを使用して、リンクを検索します。ただし、このトポロジリンクがリンクグループの一部であり、そのグループにロケーションに依存しないリンクがある場合、場所に依存しないリンクのプレフィックスが最初にチェックされ、クライアントが要求する可能性のあるリースが確認されます。このロケーションに依存しないリンクからリースが利用できない場合にのみ、トポロジカルリンクが使用されます。これは、クライアントが要求したバインディングごとに使用されます。

リースメカニズム(リースまたはクライアント予約、最初の最適な状態、または生成/提供された拡張)は、CMTS グループにサービスを提供する単一サーバー内でのみリースが認識されるため、CMTS プレフィックスの安定性と共に使用できます。

ユニバーサルプレフィックス安定性

ユニバーサルプレフィックスの安定性を使用すると、接続先に関係なく、委任されたプレフィックスを保持できます。この機能を使用するには、デリゲートされたプレフィックスの予約を構成する必要があります。クライアントとリースの予約を使用できます。

クライアント予約では、DHCP サーバーが動的にアクセスする中央LDAP リポジトリで、委任されたプレフィックスを指定できます [クライアント予約の使用](#) (を参照)。リース予約は、CCM リージョナルサーバー上で一元管理され、ユニバーサルリンクを使用して各ローカル DHCP にプッシュされます。リース予約を使用する場合、予約の完全な一覧は各サーバーでレプリケートされるため、大規模な展開ではクライアントの予約を検討する必要があります。



(注) 特定の VPN アドレス空間にユニバーサルリンクを1つだけ持つことができます。

ユニバーサルリンクタイプでリンクが設定されている場合、クライアントにリースを割り当てようとする、そのリンクのプレフィックスが最初に考慮されます。リースが使用できない場合は、リンクグループ(存在する場合)のロケーション非依存リンクタイプのプレフィックスが使用されます。最後に、トポロジリンクのプレフィックスが使用されます。



(注) CMTS プレフィックスの安定性とユニバーサルプレフィックスの安定性の両方を同時に有効にできますが、加入者に適用されるのは1つだけです。

プレフィックス割り当てグループ

プレフィックスアロケーショングループを使用すると、クライアントに対して複数のリース割り当てが行われないように複数のプレフィックスを定義し、プレフィックスを使用するプレフィックス割を制御できます。この動作を指定するために、割り当てグループおよび割り当てグループの優先順位属性が導入されます。

同じ割り当てグループ名を持つリンク上のすべてのプレフィックスは、その割り当てグループに属します。割り当てグループ名のないプレフィックスは、独自の割り当てグループ内にあり

ます。バインディングごとに1つのリースが、同じアロケーショングループ内のすべてのプレフィックスに割り当てられます。

割り当てグループの優先順位設定は、使用するプレフィックスを制御します。数値が小さい場合は、優先順位が最も低い0(デフォルト)を除き、優先順位が高くなります。同じ優先順位のプレフィックスは、アクティブなリース数によって順序付けされ、カウント数が最も小さいプレフィックスが最も高い優先順位を持ちます。



(注) 割り振りグループ名は、リンクに固有のものです。異なるリンクで同じアロケーショングループ名を再利用できます。

クライアントがアロケーショングループプレフィックスから取得できるリースの数を制御するには、DHCPポリシーのバインディングごとの最大リース属性を設定します。たとえば、バインディングあたりの最大リース数を1に設定すると、クライアントはアロケーショングループプレフィックスからリースを1つだけ取得できます。さらに、同じ割り当てグループプレフィックスから複数のリースが既に割り当てられている場合、追加のリースは取り消されます(通常、最も古いリースは取り消されます)。

プレフィックスとリンクの設定

DHCPv6プレフィックスおよびリンクを直接設定することも、最初にプレフィックスまたはリンクテンプレートを作成することもできます。次のサブセクションを参照してください。

- [プレフィックステンプレートの作成と編集](#)
- [プレフィックスの作成と編集 \(25 ページ\)](#)
- [プレフィックスのアドレス使用率の表示](#)

プレフィックスの作成と編集

プレフィックスを直接作成できます(また、必要に応じて既存のテンプレートを適用[プレフィックステンプレートの作成と編集](#)することもできます)。設定できるプレフィックス属性は次のとおりです。

- **name** : このプレフィックスに名前を割り当てます。
- **vpn-id** : プレフィックスを含むVPN。
- **address** : IPv6アドレスの上位ビットを使用してインターフェイスが属しているプレフィックス(サブネット)。
- **leasequery-send-all** : プレフィックスについての説明。
- **dhcpタイプ** : プレフィックスのアドレス割り当てをDHCPが管理する方法を定義します。
 - **dhcp** (プリセット値) : ステートフルアドレス割り当てにプレフィックスを使用します。

- **stateless**—ステートレス オプションの設定にプレフィックスを使用します。
 - **プレフィックス-委任-プレフィックス**のプレフィックスを使用して、プレフィックスの委任します。
 - **infrastructure**—プレフィックスを使用して、プレフィックスにアドレス プールがない場合に、クライアントアドレスをリンクにマップします。
 - **親**—DHCPでプレフィックスを使用しない。ただし、子プレフィックスをグループ化するコンテナオブジェクトとして使用します。親プレフィックスは、Web UIのIPv6アドレス空間リストにのみ表示され、プレフィックスリストには表示されません。
- **owner** : プレフィックスの所有者。
 - **region** : プレフィックスのリージョン。
 - **reverse-zone-prefix-length** : ip6.arpa 更新の逆引きゾーンのプレフィックス長 (詳細については、[DNS 更新のための逆引きゾーンの決定](#)を参照してください) 。
 - **range** : サーバーがアドレス割り当てのプレフィックスを設定するために使用できるサブ範囲。使用されるプレフィックスは、**dhcp-type**属性に設定されている値によって異なります。設定されていない場合、プレフィックスアドレスが適用されます。この値は、割り当てに使用できるアドレスまたはプレフィックスの範囲を制限するために、プレフィックスアドレスより長いプレフィックスを指定できます。(詳細については、[リンクとプレフィックス](#)を参照してください) 。
 - **link** : プレフィックス (サブネット) に関連付けられたリンク。単一のリンク上にあるプレフィックスをグループ化するために使用されます。
 - **policy** : クライアントに返信するときに使用する共有ポリシー。
 - **selection-tags** : プレフィックスに関連付けられた選択タグのリスト。
 - **allocation-algorithms** : クライアントにリースする新しいアドレスやプレフィックスを選択する際にサーバーが使用する1つ以上のアルゴリズム。使用可能なアルゴリズムは次のとおりです。
 - **client-request** (プリセット値はoff) : クライアントが要求したリースをサーバーが使用するかどうかを制御します。
 - **reservation** (プリセット値はon) : クライアントで利用可能な予約をサーバーが使用するかどうかを制御します。
 - **extension** (プリセット値はオン) : クライアントに対してアドレスまたはプレフィックスを生成するために、**generate-lease** 拡張ポイントにアタッチした拡張機能をサーバーが呼び出すかどうかを制御します。DHCPv6 フェールオーバーでリースの生成拡張機能ポイントを使用する場合、サーバーは、拡張が返すアドレスまたはデリゲートされたプレフィックスを使用し、ランダムに生成されたアドレスと同様に、このアドレスまたはプレフィックスに対してハッシュを実行しません。拡張機能がアドレスまたはデリゲートされたプレフィックスを生成するアルゴリズムメソッドを使用している場合、拡張機能はフェールオーバーに対応する必要があります(拡張機能は、フェー

ルオーバー構成が有効になっているかどうか、およびフェールオーバーサーバーの役割を判断できます)。拡張機能の詳細については、を[拡張ポイントの使用](#)参照してください。

- **interface-identifier** (プリセット値は off) : アドレスを生成するためにサーバーがクライアント (link-local) アドレスから **interface-identifier** を使用するかどうかを制御します。一時アドレスとプレフィックスの委任では無視されます。
- **random** (プリセット値は on) : サーバーが、RFC 3041 アルゴリズムを使用してアドレスを生成するかどうかを制御します。プレフィックスの委任では無視されます。
- **best-fit** (プリセット値は on) : 使用可能で最も適切なプレフィックスをサーバーが最初に委任するかどうかを制御します。アドレスでは無視されます。

サーバーがクライアントに割り当てるアドレスが必要な場合、クライアント要求、予約、拡張、インターフェイス識別子、およびランダムなアドレスが見つかるまで、フラグは次の順序で処理されます。サーバーは、クライアントにプレフィックスをデリゲートする必要がある場合、クライアント要求、予約、拡張、最適なプレフィックスが見つかるまで、フラグを次の順序で処理します。

- **restrict-to-reservations** : クライアント (またはリース) 予約に対してプレフィックスが制限されるかどうかを制御します。
- **restrict-to-admin-allocation** : プレフィックスが次に使用可能なアドレスを割り当てる管理要求に制限されるかどうかを制御します。設定されている場合、サーバーは、クライアントに事前に割り当てられている場合にのみ、このプレフィックスからのアドレスを持つクライアントに応答します。
- **max-leases** : プレフィックスで許可されている、予約されていないリースの最大数。新しいリースを作成する必要がある場合、サーバーは制限を超えていない場合にのみ作成します。制限を超えると、サーバーはクライアントに新しいリースを作成したり、新しいリースを提供したりできません。SNMP トラップも有効にした場合、**max-leases**値は使用済みアドレスと使用可能なアドレスのパーセンテージも計算します。



ヒ 最大リースの値を予想される最大値に設定して、SNMP アドレストラップが意味のある結果を返すようにします。

- **ignore-declines** : IPv6 アドレスを参照する DHCPv6 DECLINE メッセージまたは、このプレフィックスからの委任されたプレフィックスにサーバーが応答するかどうかを制御します。有効にすると、サーバーはこのプレフィックスのリースに関するすべての拒否を無視します。無効(プリセット値)または未設定の場合、サーバーは、クライアントにリースされている場合、DECLINE メッセージで要求されるすべてのアドレスまたは委任されたプレフィックスを UNAVAILABLE に設定します。
- **expiration-time** : プレフィックスの有効期限が切れる日時。この日時以降、サーバーは新しいリースを許可せず、このプレフィックスから既存のリースを更新することもしません。

[平日]月の日 hh:mm[:ss]年"の形式"で値を入力します。たとえば"Dec31、23:59"などです。2006"の有効期限属性については、説明を[プレフィックステンプレートの作成と編集](#)参照してください。

- **free-address-config** : このプレフィックスで予期しない空きアドレスイベントをキャプチャするトラップを識別します。構成されていない場合、サーバーは親リンクのフリー・アドレス構成属性値を探します。この属性が構成されていない場合、サーバーはv6-default フリー・アドレス設定属性を調べられます。
- **deactivated** : プレフィックスがクライアントへのリースを延長するかどうかを制御します。非アクティブ化されたプレフィックスは、リースをクライアントに拡張せず、範囲内のすべてのアドレスを個別に非アクティブ化されたかのように扱います。プリセット値はfalse (アクティブ化) です。
- **max-pd-balancing-length** : **prefix-delegation** プレフィックスのバランスをとる際にフェールオーバー プール バランシングが考慮する、**prefix-delegation** プレフィックスの最大長を制御します。既定値は 64 で、プレフィックスの委任で許可されている最長プレフィックス長を超えることはありません。
- **allocation-group** : このプレフィックスが属している割り当てグループ。
- **allocation-group-priority** : 同じ割り当てグループ内の他のプレフィックスに対するこのプレフィックスの優先順位。デフォルト値はゼロです。
- **range-end** : リースの割り当てに使用されるプレフィックスアドレス範囲内のエンドアドレスを指定します (これがDHCPタイプのプレフィックスである場合)。設定されていない場合、プレフィックスアドレス範囲の最後に使用可能なアドレスが終了アドレスとして使用されます(**range-start**がプレフィックスとして指定されている場合を除き、**range-start**で指定された接頭語の最後のアドレスが使用されます)。
- **range-start** : リースの割り当てに使用されるプレフィックスアドレス範囲内の開始アドレスか、またはこれがDHCPタイプのプレフィックスの場合は範囲として使用されるプレフィックス (この場合は **range-end** を指定しない) を指定します。設定されていない場合、プレフィックス アドレス範囲の最初の使用可能なアドレスが開始アドレスとして使用されます。

範囲開始と範囲終了を使用すると、顧客は、ランダムなアドレスを割り当てる際にサーバーが使用するアドレスの範囲を制限できます。予約や拡張が提供するアドレスには影響しません。これらの属性は、完全に指定されたIPv6アドレスまたは非プレフィックスビット(プレフィックスの範囲またはアドレス属性に基づく)セットを持つIPv6アドレスです。たとえば、::1000 の場合、プレフィックスの範囲/アドレスが /96 以下です。



- 注
- 範囲開始も範囲終了も指定されていない場合、10.0より前の動作はランダムなアドレス割り当てに関して保持されます。
 - 範囲開始または範囲終了のどちらかを指定した場合、インターフェースID割り振りアルゴリズムが指定されている場合は、使用不可になります。

• embedded-policy : プレフィックスに埋め込まれたポリシー。

ローカルアドバンスドおよびリージョン Web UI

ステップ 1 [デザイン] メニューのPrefixesサブメニューDHCPv6の下で選択します。[DHCP v6 プレフィックスの一覧表示/追加] ページには、既存のプレフィックスが表示されます。

プレフィックスを作成するには、次の手順を実行します。

1. 現在のVPN以外で作成する場合は、Web UIの上部にある[設定]ドロップダウンリストのVPNサブメニューからVPNを選択します。
2. [プレフィックス] ウィンドウの[プレフィックスの追加]アイコンをクリックし、プレフィックス名とアドレスを入力して、ドロップダウンリストからプレフィックスの長さを選択します。
3. プレフィックスのアドレス範囲を指定する場合は、サブネットアドレスを入力し、プレフィックスの長さを選択します。
4. DHCPタイプを選択します(このセクションの上部にある属性の説明を参照)。デフォルトはDHCPです。
5. 事前設定済みのプレフィックステンプレートを適用する場合は、ドロップダウンリストから選択します。(適用されたテンプレートの属性値は、接頭辞に設定された値を上書きします)。
6. をAddIPv6クリックPrefixすると、リストに接頭辞が追加されます。
7. DHCPサーバーをリロードします。[DHCPv6 プレフィックスの一覧/追加] ページに戻ると、同期されるプレフィックスの数を示すメッセージが表示されます。

ステップ 2 プレフィックスから逆引きゾーンを作成するには、[逆方向の領域] タブをクリックします。このタブで、ゾーンテンプレートを選択し、 をReportクリックしますRun。

ステップ 3 プレフィックスを作成すると、[リース] タブをクリックして、プレフィックスのリースを表示および管理できます。[リース] タブで、クライアントルックアップキーのリースを表示し、名前をクリックして各リースを個別に管理できます。

ステップ 4 [予約] タブをクリックすると、プレフィックスの予約を表示および管理できます。各予約IPアドレスとルックアップキーを追加し、ルックアップキーが文字列かバイナリAdd Reservationかを指定して、 をクリックします。

ステップ5 プレフィックスを編集するには、[プレフィックス]ペインで名前をクリックします。[プレフィックスの編集]ページで、プレフィックス属性を編集するか、グループにプレフィックスを割り当てて優先順位を設定するか、新しいポリシーを作成するか、既存の埋め込みポリシーを編集します。

グループにプレフィックスを割り当て、優先順位を設定するには、次の手順に従います。

1. 配賦グループ属性フィールドにグループの名前を入力します。
2. [配賦グループ優先順位属性] フィールドに優先順位値を入力します。ここで値を入力しない場合は、既定値(0)が割り当てられ、このプレフィックスはグループ内で最も低い優先順位になります。

これらの属性は、詳細モードのアロケーショングループにあります [プレフィックス割り当てグループ \(24 ページ\)](#) (を参照)。

埋め込みポリシーを管理するには

1. またはCreateEmbedded、[NewPolicyプレフィックスのEditDHCP埋め込みポリシーの編集]ページを開きます。Existing Embedded Policy
2. 埋め込みポリシーのプロパティDHCPv6 ポリシー階層を変更します(「」を参照)。
3. Modify Embedded Policy をクリックします。次回[DHCPv6 プレフィックスの編集]ページが表示されたら、そのプレフィックスの埋め込みポリシーを編集できます。
4. Save をクリックします。

ステップ6 地域 Web UI では、プレフィックスをローカル クラスターにプッシュし、[DHCPv6 プレフィックスのリスト/追加] ページでプレフィックスを再利用できます。

- プレフィックスをプッシュするには、目的のプレフィックスを選択しPush、クリックして[IPv6 プレフィックスをプッシュ]ページを開きます。プレフィックスをプッシュするクラスタテンプレートまたはプレフィックステンプレートを選択し、をクリックしますPush Prefix。プレフィックスがプッシュされると、プレフィックスの予約はプレフィックスでプッシュされます。また、プレフィックスがリンク上にある場合、親プレフィックスがローカルクラスタに存在しない場合は、そのプレフィックスがプッシュされます。
- プレフィックスを再利用するには、目的のプレフィックスを選択し、Reclaim クリックして [IPv6 プレフィックスの再利用]ページを開きます。プレフィックスを再利用するクラスタテンプレートまたはプレフィックステンプレートを選択し、をクリックしますReclaim Prefix。プレフィックスが再利用されると、アクティブなリースがない場合、またはforce オプションが指定されている場合は、予約はプレフィックス付きで削除されます。それ以外の場合、プレフィックスは非アクティブになります。

(注) プレフィックスがユニバーサルリンクにある場合、そのプレフィックスは複数のクラスタにプッシュすることができ、ローカルでの変更は次のサーバーのリロードまで有効になりません。

CLI コマンド

prefix name create ipv6address/length を使用します。(このprefixコマンドは、以前のリリース dhcp-prefixのコマンドのシノニムです。DHCPサーバーをリロードします。次に例を示します。

```
nrcmd> prefix example-prefix create 2001:0db8::/32 [attribute=value]
nrcmd> dhcp reload
```

プレフィックスの作成中にプレフィックステンプレートを適用するには、`prefix name create ipv6address/length template=name`を使用します。既存のプレフィックス定義にテンプレートを適用するには、`prefix` 名前 `applyTemplate`テンプレート名を使用します。次に例を示します。

```
nrcmd> prefix example-prefix create 2001:0db8::/64 template=preftemp-1
nrcmd> prefix example-prefix applyTemplate template=preftemp-1
nrcmd> dhcp reload
```

上記の属性は通常の方法で設定および有効化できます。`prefix name addReservation ipv6address/length lookup-key [-blob|-string]`を使用して予約を追加します。`prefix`名前 `listLeases`を使用してリースを一覧表示します。



ヒント 追加のIPv6 リースの再設定構文については、[こちら](#)を参照してください。

`dhcp [getPrefixCount vpn 名前|all]`. VPN またはすべての VPN を指定できます。vpn 名前を省略すると、現在の VPN の数が返されます。

地域クラスターに接続すると、次のプッシュ・コマンドと再要求コマンドを使用できます。プッシュの場合、通常は1つのクラスターまたはフェールオーバーペアのみを指定でき、フェールオーバーペアのクラスターを再利用できません。ただし、プレフィックスがユニバーサルリンクにある場合は、クラスターとフェールオーバーペアの一覧を指定できます。

- プレフィックス名プッシュクラスター/フェールオーバーペア リスト[-template=テンプレート名] [-omitparents] [-omitchildren] [-レポート]
- プレフィックス名の再利用[クラスター/フェールオーバーペア リスト][[-force]][-omitchildren] [-report-only] [-report-only]

リンクの作成と編集

リンクを直接作成できます。リンクに設定できる属性は次のとおりです。

- name : ユーザーがリンクに割り当てた名前。
- vpn-id : リンクを含む VPN。
- description : リンクの説明テキスト。
- policy : クライアントに返信するときに使用する共有ポリシー。
- owner : リンクの所有者。
- region : このリンクのリージョン。

- **free-address-config** : このプレフィックスで予期しない空きアドレスイベントをキャプチャするトラップを識別します。構成されていない場合、サーバーはv6-default フリー アドレス設定属性を調べています。
- **interface** : このリンクに関連付けられたルーターインターフェイス。
- **type** : リンクのタイプ (トポロジ、ロケーション非依存、ユニバーサル)。
- **group-name** : リンクが属しているリンクのグループ。
- **embedded-policy** : クライアントに応答する際に使用される、単一で特定のリンク オブジェクト内に埋め込まれているポリシー。

ローカルアドバンスドおよびリージョン Web UI

ステップ 1 メニューから **Design**、**DHCPv6**サブメニューの下の **リンクの追加** を選択します。[DHCPv6 リンクの一覧表示/追加] ページには、既存のリンクが表示されます。

ステップ 2 リンクを追加するには、[リンク] ウィンドウの **リンクの追加** アイコンをクリックします。

ステップ 3 リンクの名前を入力します。

ステップ 4 リンクが接頭部の安定性の場合は、**リンクタイプ (type)** を選択し、**リンクグループ名 (group-name)** を指定します。リンクの種類は、既定ではトポロジ的です。これらの属性は、[DHCP v6 リンク テンプレートの編集] ページの **プレフィックスの安定性プレフィックス安定性 (22 ページ)**] 領域でも確認できます (リンクタイプとリンクグループの詳細についてはを参照してください)。

(注) リンク グループにはロケーションに依存しないリンクが 1 つ、VPN アドレス空間に 1 つのユニバーサルリンクしか設定できません。また、ユニバーサルタイプのリンクをリンクグループに割り当てることはできません。

ステップ 5 [リンクの追加 (Add Link)] をクリックします。

ステップ 6 新しいリンクの **リンクの編集** ページで、[使用可能] フィールドから **選択済** フィールドにリンクを移動して、リンクの定義済みのプレフィックスを選択します。

ステップ 7 リンクに新しいプレフィックスを追加するには、各プレフィックス名とアドレスをページの下部に入力し、**範囲**を指定し、**DHCP タイプ**と**テンプレート**を選択します **Apply Prefix**(必要な場合)。

ステップ 8 **Save** をクリックします。

ステップ 9 地域 Web UI では、ローカルクラスターへのリンクをプッシュし、[DHCP v6 リンクの編集] ページでリンクを再利用し、[DHCP v6 リンクの一覧/追加] ページの **レプリカ IPv6 アドレス空間** をプルできます。

- リンクをプッシュするには、目的のリンクを選択し **Push**、(ページの上部にある) をクリックして、プッシュリンクページを開きます。リンクをプッシュするクラスターまたはリンクテンプレートを**選択**し、**リンク** をクリックします **Push Link**。リンクがプッシュされると、リンク上のすべてのプレフィックスと、プレフィックス上のすべての予約もプッシュされます。
- リンクを再利用するには、目的のリンクを選択し、(ページの上部にある) をクリック **Reclaim** して **リンクの再利用** ページを開きます。リンクを再利用するクラスターまたはリンクテンプレートを**選択**し、**リンク** をクリックします **Reclaim Link**。リンクが再利用されると、アクティブなリースがない場合、予約、プレフィックス、およびリンクはローカルクラスターから削除されます。アクティブなリースが見つかつ

た場合、プレフィックスは無効になります。force オプションを使用すると、アクティブなリースがある場合にリンクとそのプレフィックスを削除できます。

(注) ユニバーサルリンクのみを複数のクラスターにプッシュできます。

- レプリカ IPv6 アドレススペースをプルするには、左側のリンクペインの上部にある[データのプル]アイコンをクリックして、[プルレプリカ IPv6 アドレススペースの選択]を開きます。データ同期モード(更新、完了、または正確)を選択Reportし、をクリックします。

ローカルでの変更は、次のサーバーの再ロードまで有効になりません。

CLI コマンド

link 名前 create を使用します。(link コマンドは、以前のリリースからの dhcp-link コマンドと同義です)。次に例を示します。

```
nrcmd> link example-link create [attribute=value]
```

リンクの作成時にリンクテンプレートを適用するには、link 名前名 template-root-prefix=[address] を使用 createtemplate=し、テンプレートが複数のプレフィックスを作成できる場合は、テンプレートルートプレフィックスを指定します。既存のリンク定義にテンプレートを適用するには、link 名前 applyTemplate テンプレート名[テンプレートルートプレフィックス]を使用します。

上記の属性は通常の方法で設定および有効化でき、リンクの表示とリスト表示を行うことができます。リンクに関連付けられたプレフィックスまたはプレフィックス名を一覧表示するには link、名前 listPrefixes または link 名前 listPrefixNames を使用します。

リージョナルクラスターに接続する場合は、下記の push コマンドや reclaim コマンドを使用することができます。プッシュの場合、通常は1つのクラスターまたはフェールオーバーペアのみを指定でき、クラスターまたはフェールオーバーペアを再利用できません。ただし、リンクがユニバーサルリンクの場合は、クラスターとフェールオーバーペアの一覧を指定できます。

- リンク名プッシュクラスター/フェールオーバーペア リスト[-template=プレフィックステンプレート名][-omitparents][-omitchildren][-report]
- リンク名の再利用[クラスター/フェールオーバーペア リスト][-force][-report]

DHCP ネットワークの管理

スコープを作成する場合は、サブネットとマスクに基づいてネットワークも作成します。スコープは同じサブネットを共有できるため、関連付けられたネットワークとスコープを表示すると便利です。これらのネットワークの管理は、ローカルクラスター機能のみです。また、作成されたネットワークの名前を編集することもできます。

関連項目

[ネットワークの一覧 \(34 ページ\)](#)

[ネットワークの編集 \(34 ページ\)](#)

ネットワークの一覧

[ネットワークの一覧] ページでは、スコープによって作成されたネットワークを一覧表示し、ネットワークが関連付けるスコープを決定できます。ネットワークは名前でもリストされ、Web UI はサブネットとマスクから作成します。このページでは、ネットワークを展開したり折りたたんだりして、関連するスコープを表示または非表示にできます。

基本モードで、[設計] メニューから Networks[] から [] を DHCPv4 選択して [DHCP ネットワーク ツリー] ページを開きます。このページでは、次の作業を行うことができます。

- ネットワークは名前のアルファベット順に表示されます。List the networks サブネットと割り当てられた選択タグを識別できます。ネットワークの横にある+プラス記号() をクリックすると、関連するスコープが表示されます。

すべてのネットワーク ビューを展開するには Expand All、 をクリックします。ネットワークビューをすべて折りたたんでネットワーク名だけを表示するには、Collapse All をクリックします。

- **ネットワーク名の編集**- ネットワーク名をクリックします。[ネットワークの編集 \(34 ページ\)](#) を参照してください。

DHCPv6 アドレス空間内のネットワークを表示するには、設計 > DHCPv6 メニューからネットワークを選択して、DHCPv6 ネットワーク ツリー ページを開きます。このページでは、「DHCPv6 リンクのリスト/追加」 ページと同様に、テンプレートおよびテンプレート・ルート接頭部を使用して DHCPv6 リンクを追加できます。リンクを追加すると、[DHCPv6 リンクの追加] ページが開きます。リンクを作成した後は、編集用の [DHCPv6 ネットワークの表示] ページでリンクを選択できます。



ヒント DHCP v6 ネットワーク ツリー ページを使用して、リンクをプッシュおよび再利用できます。目的のリンクの **プッシュ** または **再利用** アイコンをクリックします。詳細については、[リンクの作成と編集 \(31 ページ\)](#) の項を参照してください。

ネットワークの編集

ネットワーク名を編集できます。元の名前は、スコープで指定されたサブネットとマスクに基づいています。この名前は任意の説明文字列に変更できます。

[ローカル基本 (Basic)]または[アドバンスド (Advanced)]Web UI

ステップ 1 [デザイン]メニューから、[DHCPv4]サブメニューから[ネットワーク]を選択するか、DHCPv6サブメニューから[ネットワーク]を選択して、[DHCP ネットワーク ツリー] ページ (DHCP v4) または DHCP v6 ネットワーク ツリー ページ (DHCP v6) を開きます。

DHCPv6 の場合、DHCP v6 ネットワークページはネットワークを作成するためのものです。ネットワークの名前を入力し、必要に応じてテンプレートを選択し、テンプレートルートプレフィックス名を入力して、[リンクを追加ネットワークの一覧 (34 ページ)]をクリックします(を参照)。

ネットワークを編集する場合は、編集するネットワークの名前をクリックします。[DHCP v6 リンクの編集] ページが開きます。

ステップ 2 [保存 (Save)] をクリックします。
