リースの管理

リースは、Dynamic Host Configuration Protocol（DHCP）の中心となるものです。これらは、一定期間、個々のクライアントに割り当てられる IP アドレスです。DHCP サーバーは、有効な IP アドレス範囲を含む適切に構成されたスコープで、これらのリースを自動的に割り当てます。2つのクライアントが同じリースアドレスを持つ可能性はありません。予約とは、常に同じ IP アドレスを取得するリースです。

この章では、ネットワーク内のリースと予約を管理する方法について説明します。

- リース状態 （1 ページ）
- リース期間のガイドライン （3 ページ）
- DHCPv6 クライアントとリース （5 ページ）
- スコープでのリースの設定 （8 ページ）
- リースの表示 （8 ページ）
- クライアント予約の使用 （19 ページ）
- リース予約の作成 （22 ページ）
- リースと予約プロパティの詳細設定 （27 ページ）
- リースの照会 （39 ページ）
- アドレス レポートとリース レポートの実行 （47 ページ）
- 動的リース通知 （56 ページ）
- リース通知クライアントの例 （58 ページ）
- リース履歴データベース圧縮ユーティリティ （65 ページ）
- 柔軟なリース時間 （70 ページ）

リース状態

次の表に、IPv4 または IPV6 のリース状態を示します。

IPv4 リース状態

IPv4 リースは、次の表に示す状態のいずれかになります。

表 *1 : IPv4* リース状態

状態	説明
使用可能（Available）	リースに使用できる IP アドレス。
使用不可（Unavailable）	リース不可能。DHCPサーバーがリースを不可に設定する方法については、使用不可としてマークされているリースの処理 （37 ページ） を参照してください。
リース済み	クライアントにより保持されています。
提供済み（Offered）	クライアントに提供されています。
期限切れ（Expired）	リース猶予期間が期限切れになったときに使用できます。
非アクティブ（Deactivated）	リースが期限切れになった後、更新またはリースできません。リースの無効化 （13 ページ）を参照してください。
使用可能状態の保留中（Pending available）	フェールオーバーに関連します。サーバーがフェールオーバーパートナーと状態を同期するとすぐに、使用可能状態の保留中のリースが使用可能になります。 DHCP フェールオーバーの管理を参照してください。

IPv6 リース状態

リースは、次の表に記載されている状態のいずれかになります。

表 *2 : IPv6* リース状態

状態	説明
使用可能（Available）	リースに使用できる IP アドレス。
提供済み（Offered）	クライアントに提供されています。
リース済み	クライアントにより保持されています。
期限切れ（Expired）	リース猶予期間が期限切れになったときに使用できます。
使用不可（Unavailable）	リース不可能。何らかの競合のために使用できなくなりました。
解放（Released）	クライアントはリースを解放しましたが、サーバーはリースに猶予期間を適用するように構成されています。猶予期間が切れるまで、リースは利用できません。

状態	説明
その他の使用可能状態（Other available）	フェールオーバーに関連します。フェールオーバーパートナーによる割り当てには使用できますが、このサーバーでは割り当てには使用できません。
使用可能状態の保留中（Pending available）	フェールオーバーに関連します。サーバーがフェールオーバーパートナーと状態を同期するとすぐに、使用可能状態の保留中のリースが使用可能になります。プレフィックス委任リースのみに使用されます。
削除の保留中	フェールオーバーに関連します。保留中の削除状態のリースは、サーバーがフェールオーバー パートナーと状態を同期するとすぐにクライアントとの関連付けを解除されます。

リース期間のガイドライン

リース時間に適切な値を定義するには、ネットワーク上で次のイベントを検討します。

- DHCP オプションおよびデフォルト値に対する変更の頻度。
- IP アドレスを要求するクライアントと比較した、使用可能な IP アドレスの数。
- ネットワーク インターフェイス エラーの数。
- コンピュータがネットワークに追加および削除される頻度。
- ユーザーによるサブネット変更の頻度。

これらのイベントはすべて、クライアントがIPアドレスを解放したり、DHCPサーバーでリースが期限切れになる原因となる場合があります。その結果、アドレスは、再利用のためにフリー アドレス プールに戻る可能性があります。ネットワークで多くの変更が発生する場合、アクティブなネットワークには1~3日、非アクティブなネットワークには4日から10日の間のリース期間が推奨されます。このようなリース時間を割り当てると、クライアントがサブネットから離れるのに合った速さでIPアドレスが再割り当てされます。

もう1つの重要な要因は、接続されているコンピュータに対する使用可能なアドレスの比率です。たとえば、使用可能なアドレスが254個のクラスCネットワークでは、アドレスの再利用の要求が少なく、そのうち40個しか使用されません。このような状況では、2か月などの長いリース期間が適切な場合があります。一度に接続しようとしているクライアントが240~260人いれば、需要ははるかに高くなります。このような場合は、より多くのアドレス空間を構成する必要があります。その前まで、DHCP リース時間を 1 時間以下にしてください。

ヒント リース期間が短くなると、クライアントはリースを頻繁に更新するため、DHCPサーバーを継続的に使用できるようにすることが求められるようになります。DHCPフェールオーバー機能は、このようなレベルの可用性を保証するのに役立ちます。

永続的なリースを持つポリシーを作成する場合は注意が必要です。安定した環境でも、クライアント間で一定の売上高が発生します。ポータブル ホストの追加と削除、デスクトップ ホストの移動、およびネットワーク アダプタ カードの交換が可能です。永続的なリースを持つクライアントを削除する場合、IPアドレスを再利用するためには、サーバー構成に手動で介入する必要があります。管理者の介入なしにアドレスが最終的に回復されるように、6 か月などの長いリースを作成することをおお方が良いでしょう。

リース期間の推奨事項は次のとおりです。

- ケーブル モデムのリース期間を 7 日間 (604800 秒) に設定します。リースはプライベート アドレス空間から取得する必要があり、ケーブル モデムはめったに動かないはずです。
- 顧客宅内機器 (CPE) またはラップトップのリースは、パブリック アドレス空間から取得し、サーバーの負荷を軽減するためにできるだけ長いリースで、ユーザーの人口の習慣と一致する必要があります。
- リース時間を短くするには、より多くのDHCP要求および応答バッファーが必要です。最適なスループットを得るために要求バッファと応答バッファをDHCP要求と応答パケットバッファの設定設定します (を参照)。
- リース時間の優先許可ポリシー属性が無効 (通常の既定値) であることを確認して、サーバーがリース期間を決定できるようにします。有効にした場合でも、クライアントは、サーバーに対して構成した時間よりも短いリース時間のみを要求できます。一部のクライアントは、常に固定リース時間 (1 時間など) や以前と同じ時間を要求します。この種の要求は、クライアントが完全なリース時間を取得しなくなるという問題を引き起こし、サーバーに対するトラフィックを増やす可能性があります。
- リースの中間マークの前にリースを更新しようとするクライアントのリース延長を延期します。詳細については、リース拡張の保留 を参照してください。

リース日の制限

リース日の制限は、次の属性を使用して指定できます。

- *lease-retention-max-age*
- *lease-retention-min-age*

リース保持期間-最大年齢属性は、リース時間が制限されている過去 (現在の時刻から) の最長時間を指定します。これは、プライバシー保護のためのデータ保存制限を満たすために使用できます。指定しない場合、リース時間がどの程度前に戻るかに制限は適用されません。リースに対してリース保持制限を適用するには、リース保持期限をゼロ以外にする必要があるだけでなく、個々のリース自体がそのポリシーでリース保持制限属性を設定するポリシーに該当する必要があります。この値は、構成されている場合は 8 時間より大きくする必要があります。0 以外で 8 時間未満に設定されている場合は、8 時間に設定されます。

リース保持期間 -期限属性は、リース時間を制限できる最短の時間を、過去に指定します。その値は、リース保持 - 最大年齢より少なくとも 6 時間少なくする必要があります。この属性が有効で、ゼロ以外の値に設定されている場合、保有期間の制限の対象となるリース時間は、

リース保持期間 -*max-age*より古くなることはできません。リース保持期限*(max-age)*に向けて進むにつれて、過去には定期的にリース保持-最小年齢にリセットされます。この属性の構成は、既定では、リース保持期間 -最大期間より 6 時間少なくなるので、オプションです。また、属性値の差が 6 時間未満の場合は、リース保持期間 -最大年齢から 6 時間を引いた値が使用されます。

リース保持-最小とリース保持-最大年齢の間のリース期間に古い時間を維持するには、いくつかの処理が必要であり、これらの2つの値が近いほど、これらの属性の絶対値に関係なく、この処理が行われる頻度が高くなります。リース保持期間の日数を、リース保持期限の数日前に設定すると、リース保持期間の制限に専念する追加のサーバー処理が最小限に抑えられます。

これらの保存期間に影響を受けるクライアントのポリシーを 1 つ以上変更する必要があります。すべてのクライアントに適用するようにsystem_default_policyでこれを構成できます。しかし、これが問題ではないデバイスがある場合は、より選択的に設定することをお勧めします。この機能を有効にしているクライアントが少ないほど、作業が少ないため、サーバーのパフォーマンスへの影響が少なくなります。

ポリシー属性のリース保持制限は、そのポリシーに関連付けられているクライアントがリース日付の制限の対象かどうかを示します。この属性が有効で、DHCP サーバーのリース保持期限がゼロ以外の値に構成されている場合、このポリシーの対象となるリース期間は、リース保持期間 -最大年齢よりも古くなることはできません。リース保持期限に向けて進むにつれて、過去には定期的にリース保持-最小年齢にリセットされます。

プライバシー保護機能の使用を検討する際に覚えておくべきことは次のとおりです。

- 最初に有効(または特定の再構成)を行った場合、既存のリース履歴レコードは、リース保持限界フラグが設定されていないため、この機能の対象になりません。
- リース履歴のトリミング時間が調整される可能性があります。リース保持期間の上限とリース保存期間の差の約3分の2に設定されています。たとえば、6 時間の既定値を使用すると、トリミングは 4 時間ごとに行われます。
- システムのディスク入出力レートが上昇します。これは、サーバーがアクティブなリースレコードと履歴リースレコードの古い時間を更新する必要があるためです。この影響は、リース保持期間の最大値とリース保存期間の差を大きくすることで、ある程度まで減少します。
- スコープやプレフィックスの削除、範囲の調整などの構成変更が行われると、スコープまたはプレフィックスに関連付けられたリースは孤立したリースになります。これらの孤立したリースは、プライバシー保護の時間制限のためにトリミングされず、処理されません。孤立したリースを削除する必要があります。詳細については、孤立したリースの削除（15 ページ）を参照してください。

DHCPv6 クライアントとリース

DHCPv6 サーバーは、DHCPv4 のクライアントとリースに類似したクライアントとリースをサポートします。以下に、その主な違いを説明します。

- サーバーは、ハードウェア アドレスとクライアント ID を 1 つの一意のクライアント識別子に統合する DHCPv4 概念である DHCP 一意識別子 (DUID) によって DHCPv6 クライアントを識別します。
- DHCPv6クライアントは、複数のリースを持つことができます。つまり、複数のプレフィックスが単一のリンク上にあり、割り当てグループ属性を使用してグループ化されていない場合、サーバーは DHCPv4 のように、1 つのスコープからではなく、使用できる各プレフィックスからリースをクライアントに割り当てます。1つのリンク上の複数のプレフィックスが割り当てグループ属性を使用してグループ化されている場合、サーバーは、プレフィックスアロケーション グループ内で最も優先度の高いプレフィックスから、割プレフィックス割り当てグループり当てグループごとに1つのリースのみをクライアントに割り当てます (を参照)。
- サーバーは、最初のリースをDHCPv6クライアントに関連付けると最初に作成し、リースが関連付けられていないときにクライアントを削除します。これは、DHCPv4クライアントが 1 つのリースしか持てることができない点を除いて、DHCPv4 の動作と同じです。
- DHCPv6リースは動的に作成されます。サーバーは、構成時に使用できる可能性のあるすべてのリースを作成するわけではありません。

リースは次の場合に使用できます。

- **Nontemporary**：長く、かつ再生可能な可能性がある標準 IPv6 ユニキャスト**addresses**アドレス。
- **Temporary**：標準 IPv6 ユニキャスト アドレスですが、有効期間が非常に限られています (**addresses**更新不可能)。一時的なアドレスは、IPv6 (RFC 3041 を参照) のプライバシーの問題を解決します。
- **Delegated prefixes**：プレフィックスの委任に使用されます（RFC 8415 を参照）。

リースには、優先存続期間と有効な有効期間の両方があります。

- **Preferred**：主にクライアントを使用する場合、有効なアドレスが優先**lifetime**される時間。優先存続期間が満了すると、アドレスは非推奨になります。
- **Valid**：クライアントとサーバーの両方で使用される、アドレスが有効な状態のままの**lifetime**時間です。有効期間は推奨期間より長いか、または同じである必要があります。有効期間が切れると、アドレスは無効になります。有効な有効期間が切れると、リースは削除される資格があります。これは、DHCPv4 のリース時間と基本的に同じです。

DHCPv6 バインディング

バインドは DHCPv6 の新機能であり、複数のアドレス グループをクライアントに割り当てることができます。クライアント・バインディングは、次の 3 つのタイプのいずれかで構成されます。

- 一時的でない (IA_NA)
- 一時(IA_TA)

• プレフィックス委任（IA_PD）

バインディングは、一意の ID アソシエーション ID (IAID) から構成されます。リースは常にバインディングの下に存在します。したがって、クライアントには1つ以上のバインディングがあり、バインディングには1つ以上のリースがあります。サーバーは、最初にリースを追加するときにバインディングを作成し、それ以上リースがない場合はバインディングを削除します。最初のバインディングを追加するときにサーバーはクライアントを作成し、バインディングがなくなったときにクライアントを削除します。

リース アフィニティ

DHCPv4 の場合、リースが期限切れになった場合、またはサーバーがリースを解放すると、サーバーは、別のクライアントに割り当てられていない限り、そのアドレスに対してクライアントを記憶します。DHCPv6 の場合、IPv6 アドレス空間が大きいため、アドレス生成手法によっては、アドレスを別のクライアントに再割り当てする前に eons が渡される可能性があります。したがって、Cisco Prime Network レジストラーは、有効期限前に更新を要求しなくてもクライアントが同じアドレスを取得できるように、アフィニティ期間属性を提供します。

アフィニティ期間は、一部の環境では望ましいが、アフィニティー時間がゼロまたは非常に小さい場合には望ましくありません。アフィニティー期間中、リースは AVAILABLE 状態で、最後にリースされたクライアントに関連付けられます。この期間中にクライアントがリースを要求した場合、サーバーは同じリースを許可します (または、更新が禁止されている場合、クライアントはそのリースを明示的に取得しません)。

リースのライフ サイクル

リースには、州によって制御されるライフサイクルがあります。リースはクライアントに関連付けられている間のみ存在し、サーバーはそのクライアントに関連付けられていないと削除します。ライフサイクルと状態遷移は次のとおりです。

1. リースが生まれ、サーバーが次の場合にアドレスに関連付けられます。
    1. リースの予約を作成し、リースを AVAILABLE 状態にして、RESERVED としてマークします。この状態に関連付けられているタイマーはなく、サーバーは予約されている限りリースを削除しません。
    2. クライアントに ADVERTISE メッセージを送信し、リースを提供状態にします。リースは、オファーのタイムアウト後に DELETED 状態に移行します。
    3. クライアントに応答メッセージを送信し (要求、書き換え、または REBIND の場合)、リースをリース状態にします。リースの有効期間が経過すると、リースは期限切れ状態に移行します。
2. 提供されたリースは次の処理に移行します。
    1. LEASED 状態は、サーバーが REQUEST メッセージを受信し、リースの有効期間が経過した後に期限切れ状態に遷移します。
    2. 提供時間が経過した場合の DELETED 状態。
3. リースリース:

1. サーバーが要求、書き換え、または REBIND メッセージを受信すると、更新されます。リースの有効期間が新たに経過した後、リースは期限切れ状態に移行します(新しい有効な有効期間は 0 である可能性があります)。
2. サーバーが RELEASE メッセージを受信すると、RELEASE 状態に遷移します。リースは、リリース猶予期間が経過した後に AVAILABLE 状態に移行します。
3. サーバーが辞退メッセージを受信すると、UNAVAILABLE 状態に遷移します。サーバーは、タイムアウト時間が経過した後にリースを削除します。

4. 期限切れリースは、猶予期間の後にいずれかの利用可能な状態に移行します。サーバーは、アフィニティー期間が経過した後にリースを削除します。
5. 利用可能なリース:
    1. DELETE 状態に遷移し、サーバーは、アフィニティ期間が経過した後、メモリとリース データベースから削除します。
    2. [予約済み] の場合は削除できず、使用可能なまま残ります。
6. サーバーは LEASED、EXPIRED、RELEASED、または AVAILABLE リースをクライアントに再提供できますが、現在の状態のままですが、タイムアウトは少なくともオファータイムアウトまで延長されます。

DHCP フェールオーバーは、一般的にパートナーが認識するまでこれらの遷移が発生する可能性がある状態遷移の一部を複雑にします。追加のライフサイクルと状態の遷移 (フェールオーバー関連) は次のとおりです。

- AVAILABLE (または他の AVAILABLE) 状態に移行するには、パートナーが移行を確認する必要があるため、承認がパートナーから受信されるまで、PENDING AVAILABLE 状態が使用されます。
- クライアントからのリースの関連付けを解除するには、パートナーからの確認応答も必要であり、したがって、パートナーが状態変更を確認するまで、PENDING DELETE 状態が使用されます。

スコープでのリースの設定

スコープの IP アドレス範囲を設定した後、DHCP 割り当てから生じるリースを監視および調整できます。

リースの表示

リースを表示するには、スコープ内で*Cisco Prime Network Registrar 11.1* クイック スタート ガイドスコープの管理IP アドレスの範囲を作成する必要があります。

ローカルの基本 Web UI

[**デザイン**] メニューの**Scopes[DHCPv4]**サブメニューの下で [DHCP スコープの一覧/追加] ページを開き、スコープの**[リース]**タブをクリックします。ページが開き、各リースをクリックして管理できます。

「 リース状態 （1 ページ）状態」列の値の説明については、「」を参照してください。リースの有効期限に関するガイドラインについては、をリース期間のガイドライン （3 ページ）参照してください。

[DHCP スコープの編集] ページを開くには、リース IP アドレスをクリックします。

ローカル アドバンスド Web UI

メニューから**DesignScopesDHCPv4**サブメニューの下で選択し、[DHCP スコープの一覧/追加] ページを開きます。その後、スコープの**[リース]**タブをクリックします。または、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**Leases**開き、ページのタブをクリックします。

CLI コマンド

[vpn-name/]ipaddr **show**を使用して**lease**、IP アドレスに基づいて特定のリースのプロパティを表示します。**scope**名前付**listLeases**きスコープのすべてのリースを表示するには、名前を使用します。出力は両方のコマンドでほぼ同じです。特定の仮想プライベート ネットワーク (VPN) でリースを一覧表示できないことに注意してください。すべての VPN のすべてのリースがリストに表示されます。

リースに関連付けられた最新の MAC アドレス、または MAC アドレスに関連付けられているリースを表示できます。*[vpn-name/]addr* **macaddr**コマンドは**lease**、リースが予約されているかアクティブであるかにかかわらず、リースの MAC アドレスを表示します。**lease list –macaddr** *addr* [**-vpn**=*vpn-name*] コマンドは、その MAC アドレスの IP アドレスがアクティブにリースされた (予約されていない) 場合にのみリース データを一覧表示します。**lease list -lansegment**また、*ADDR*マスクおよびaddrマスクコマンドを使用して**lease list -subnet**、LAN セグメントおよびサブネット別のリースを一覧表示することもできます。

リース データのインポートとエクスポート

CLI を使用して、テキスト ファイルに対してリース データをインポートしたり、テキスト ファイルからエクスポートしたりできます。

前提条件のインポート

リースをインポートする前に、次の構成手順を実行する必要があります。

1. インポートするリースの DHCP サーバーでスコープを構成します。

2. リースのホスト名をインポートの一部として DNS に動的に入力する場合は、DHCP サーバーからの動的更新を許可するように DNS サーバーのゾーンを構成します。
3. DHCP サーバーをインポート モードに設定して、リース インポート中に他のリース要求に応答しないようにします。
4. すべての時間フィールドに対して、1970 年 1 月 1 日の GMT の午前 0 時からの秒数、または日、月、日付、時刻、年の形式 (2002 年 4 月 15 日 15:35:48) のいずれかを使用します。
5. リースをインポートした後、DHCP サーバーをインポート モードから外し、他のリース要求に応答できるようにします。

（注） 永続リースオプションを無効にすると、永久リースのインポートは失敗します。必要に応じて **policy** *name* **enable permanent-leases**を使用してこのオプションを有効にします。

インポートとエクスポート コマンド

コマンドと**import leases**コマンドは、特殊なファイル形式を使用します。 **export leases** ファイル内の各レコードまたは行は、1 つの DHCP クライアントを表します。

```
field-1|field-2|field-3|...|field-13
```

垂直線 (|) 区切り文字とフィールド値の間にスペースを使用しないでください。少なくとも最初の4つの必須フィールドを含める必要があります。さらに値を指定する場合は、13個のフィールドが存在するように、残りのNULLフィールドをすべて垂直線(|)で区切る必要があります。フィールドは次の順序で示されます。

1. *aa*の MAC アドレス :*bb*:*cc*:*dd*:*ee*:*ff*形式 (必須)
2. MAC アドレス タイプ（必須）
3. MAC アドレスの長さ (必須)
4. ドット付き 10 進形式の IPアドレス、*.b.c.d* (必須)
5. リース開始時間 (グリニッジ標準時、GMT) (オプション)
6. リース有効期限 (GMT) (オプション)
7. 許容延長時間 (GMT) (オプション)
8. 最終トランザクション時間 (GMT) (オプション)
9. DHCP サーバーの IP アドレス（任意）
10. ホスト名（ドメイン無し）（任意）
11. ドメイン名（任意）
12. クライアント ID (オプション)
13. VPN 名 (省略した場合は、グローバル VPN が使用されます)

すべての時間フィールドに対して、1970 年以降の秒数または日月-日付/時刻の年形式(例:2007 年 4 月 9 日(月 9/16:35:48))を使用します。

リースをインポートする場合、DHCPサーバーがリースを受け入れないか、通信障害がリースパケットをドロップする可能性があります。後者の場合、サーバーはインポートを数回再試行し、約1分後に失敗を報告します。インポートが失敗した場合は、DHCPサーバーのログ ファイルを調べて、エラーの原因となったリースを見つけます。インポート ファイルに戻り、問題

のあるエントリを含めてすべてのリース エントリを削除し、リース のインポートを繰り返します。

を使用**export leases**する場合は、現在のリースと期限切れのリースの状態を出力ファイルに書き込むか、現在のリースのみを書き込むか選択できます。次の例は、Cisco Primeネットワークレジストラー DHCP サーバーからのリースデータエクスポートの一部を示しています。レコード間の空白行は、わかりやすくするために例に表示されます。実際の出力には含まれていません。

例: リースデータエクスポート

```
00:60:97:40:c1:96|1|6|204.253.96.103|Wed Aug 30 08:36:57 2000|Fri Sep 01 13:34:05 2000|
Wed Aug 30 08:36:57 2000|Fri Sep 01 09:34:05 2000|204.253.96.57|nomad|cisco.com|
00:d0:ba:d3:bd:3b|blue-vpn
00:d0:ba:d3:bd:3b|1|6|204.253.96.77|Thu Aug 17 13:10:11 2000|Fri Sep 01 14:24:46 2000|
Thu Aug 17 13:10:11 2000|Fri Sep 01 10:09:46 2000|
204.253.96.57|NPI9F6AF8|cisco.com|blue-vpn
00:d0:ba:d3:bd:3b|1|6|204.253.96.78|Fri Jun 23 15:02:18 2000|Fri Sep 01 14:11:40 2000|
Fri Jun 23 15:02:18 2000|Fri Sep 01 09:56:40 2000|
204.253.96.57|JTB-LOCAL|cisco.com|blue-vpn
```

インポート ファイルのリース期間

リース インポート要求の場合、DHCP サーバーが次の場合は、次のようになります。

- インポートモードで有効になっており、リースがまだクライアントにリースされていない場合、サーバーはクライアントが指定したリース時間を受け入れます。
- インポートモードでは、リースは既にクライアントにリースされ、サーバーに対して遅延リースエクステンションが有効になり (デフォルト)、要求は更新時刻 (T1) より前に到着します。

  要求が T1 の後に到着すると、サーバーはクライアントに要求されたものを何でも与えます。有効期限から約 2 分以内に、遅延リース延長は動作しません。

- インポートモードに対して有効になっていませんが、サーバーで構成された時間よりも長いリース時間を受け入れることはありません。
  - 要求に適用可能なポリシーに対してリース時間の優先を許可が有効になっている場合、サーバーはクライアントからのリース時間を短く受け入れます。サーバーエキスパートモードのクライアント要求最小リース時間属性を設定して、リース時間のフロアを作成できる場合でも、リース時間を短くすることは、サーバーに許容されます。
  - 適用可能なポリシーでリース時間の優先を許可する機能が有効になっていない場合、サーバーは着信パケットの dhcp-lease-time 要求を無視し、サーバー設定を使用します。

インポート ファイルに DNS ゾーン名が指定されている場合、サーバーは DNS を更新するときにゾーン名を使用しません。ファイルがホスト名を指定する場合、クライアントまたはクライアント・クラスのエントリーのホスト名指定がホスト名をオーバーライドしない限り、サーバーは DNS の更新時にホスト名を使用します。

クライアントのホスト名は、DNS 更新に使用する DNS 更新構成オブジェクトに関連付けられているゾーン以外のゾーンにする必要があります。これは、クライアントまたはクライアントクラスのエントリでゾーンを指定することによってのみ、DHCP サーバーに表示できます。

アドレス提供前のホストへの ping 実行

DHCP サーバーでインターネット制御メッセージ プロトコル (ICMP) エコー メッセージ機能 (別名**ping**) を使用して、IP アドレスに応答するユーザーがいるかどうかを確認してから、それを割り当てる(*ping-clients*属性を使用)することができます。*ping-clients*属性は、サーバーがリースを提供する前にアドレスに対して ping を試行するかどうかを制御します。有効にした場合は、*ping* タイムアウト属性も設定する必要があります。このテストにより、DHCP サーバーは、アドレスを割り当てる前に、そのアドレスが使用されていないかどうかを確認できます。

を**ping**使用すると、2 つのクライアントが同じアドレスを使用するのを防ぐことができます。クライアントが ping に応答すると、DHCP サーバーはそのアドレスを利用不可としてマークし、別のアドレスを提供します。このテストは、パワーアップされたクライアントに対してのみ機能します。クライアントがリースを持ち、電源を切ることは可能です。

DHCP サーバーで*ping* クライアント属性を構成することもできます。この属性は、スコープで明示的に構成されていない場合、スコープの*ping-clients*属性の既定値を制御します。

（注） スコープを構成している場合は、スコープ固有の構成が優先されます。明示的な構成を持たないスコープは、グローバル設定を前提としています。

ping タイムアウト期間は重要です。ping は、特定の IP アドレスを使用しているクライアントがないことを確認するのに役立つため、各 ping はタイムアウト期間全体を待機する必要があります。この ping タイムアウト期間はオファーの前に来るので、指定された時間はサーバーのパフォーマンスに大きな影響を与えます。

- この時間を長く設定しすぎると、リースオファリングプロセスが遅くなります。
- この時間を短く設定しすぎると、IP アドレスを使用して別のクライアントを検出する ping パケットの有効性が低下します。

IP アドレスを提供する前に ping ホストを実装するには、次の方法でスコープを変更します。

- pingクライアント属性を有効にします。この機能はデフォルトでは無効になっています。
- pingタイムアウト属性を設定しています。デフォルトでは 300 ミリ秒です。

サーバーは、正常な ECHO 応答を受信する IP アドレスを使用できなくなります。DHCP サーバー属性の*ignore-icmp-errors* (プリセット値) を有効にすることで、このアクションを制御できます。DHCP サーバーは、IP アドレスを使用不可にする理由として、ICMP DEST_UNREACHABLEを使用し、ICMP ECHO 要求を送信した後に受信するエラーメッセージをTTL_EXPIREDします。

リースの無効化

リースを非アクティブ化すると、クライアントはリースから移動します。リースが使用可能な場合、このリースを非アクティブ化すると、DHCPサーバーがクライアントにリースを渡すことを防ぎます。リースがアクティブ (クライアントによって保持されている) の場合、非アクティブ化すると、クライアントがリースを更新し、サーバーが別のクライアントにリースを渡すことを防ぎます。リースを非アクティブ化できるのは、サーバーが実行中の場合だけです。DHCP サーバーは、リースを直ちに非アクティブ化します。

ヒント　Windows クライアントがリースを強制的に解放するには、**ipconfig /release** をクライアントマシンで実行します。

（注）　DHCPv4 リースの場合、リースは再びアクティブ化されるまで非アクティブ化されたままになります。DHCPv6 リース (アドレスまたはプレフィックスの委任) の場合、クライアントがリースから削除されると、リースが自動的にアクティブになるという動作が少し異なります。したがって、DHCPv6 非アクティブ化リースをアクティブ化する必要はありません。ただし、これは、現在のリースが終了した後にリースが使用可能であり、クライアントに関連付けられていないリースを非アクティブ化できないことを意味します。DHCPv6 予約が非アクティブ化された場合、その予約を再度使用するためには、その予約をアクティブにする必要があります。

ローカル Web UI

リースを非アクティブ化するには、[スコープ] の [**リース**] タブでリースのアドレスリースの表示 （8 ページ）をクリックし**Deactivate**(を参照) 、[ ] をクリックします。リースが非アクティブ化として表示されるようになりました。リースを再アクティブ化するには、**Activate**をクリックします。同様の方法で、DHCPv6 リースを非アクティブ化することもできます。

CLI コマンド

リースを非アクティブ化するには**lease**、[*vpn-name*/]*ipaddr* **deactivate**を使用します。リースを再アクティブ化するには、[**lease** *vpn-name*/]*ipaddr***activate**を使用します。

DHCPv6 リースを非アクティブ化するには、**lease6** [*vpn-name*/]*addr* **非アクティブ化**を使用します。DHCPv6 リースを再アクティブ化するには、**lease6** *[vpn-name/]addr* **アクティブ化**を使用します (ただし、クライアントがリースから削除されたときに自動的にこれが行われるため、DHCPv6 リースは通常再アクティブ化する必要はありません)。

範囲からのリースの除外

IPアドレス範囲は、定義上、連続している必要があります。既存の範囲からリースを除外するには、範囲を2つに分割する必要があります。新しい範囲は、元の開始範囲と終了範囲のアドレスと除外するアドレスの間のアドレスで構成されます。

⚠

注意 除外されたアドレスに現在アクティブなリースがある場合は、まず のリースの無効化（13ページ）手順に従って、そうでない場合は警告メッセージが表示されます。アクティブなリースを削除すると、削除されたアドレスが後で再構成され、再割り当てされた場合、重複する IP アドレスが生じる可能性があります。サーバーを再ロードした後、リースに関する情報は存在しなくなります。

ローカルの基本 Web UI

スコープ アドレス範囲からリースを除外するには、次の手順を実行します。

ステップ 1 **Design** メニューで、[DHCPv4] サブメニューから **Scopes** を選択し、[DHCPスコープの一覧/追加（List/Add DHCP Scopes）] ページを開きます。

ステップ 2 [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 [範囲（Ranges）] 領域で、削除する IP アドレス範囲の横にある [削除（Delete）] アイコンをクリックします。

ステップ 4 除外された IP アドレスの直前に終了する範囲を追加します。

ステップ 5 除外された IP アドレスの直後に始まる別の範囲を追加します。

ステップ 6 [保存（Save）] をクリックしてスコープを保存します。

ステップ 7 DHCP サーバーをリロードします。

ローカル アドバンスド Web UI

スコープ アドレス範囲からリースを除外するには、基本モードと同じ操作が存在します。

CLI コマンド

スコープ アドレス範囲からリースを除外するには、リース範囲 (**scope** *name* **listRanges**) を検出 **lease** し、リースを非アクティブ化します (*[vpn-name/]ipaddr* **deactivate**) 、 その IP アドレス**scope**(*name* **removeRange** *start end*) の範囲だけを削除します。その後、結果の範囲が適切に分割されます。

次の例では、範囲から 192.168.1.55 アドレスを削除します。リースが VPN が定義されたスコープ内にある場合は、セッションに対して VPN を明示的に定義するか、または VPN プレフィックスを**lease**コマンドに含めることができます。

```
nrcmd> session set current-vpn=red
```

```
nrcmd> scope examplescope1 listRanges

nrcmd> lease red/192.168.1.55 deactivate

nrcmd> scope examplescope1 removeRange 192.168.1.55 192.168.1.55

nrcmd> scope examplescope1 listRanges
```

孤立したリースの削除

孤立したリースを削除するには、次の手順を実行します。

始める前に

スコープやプレフィックスの削除、または範囲の調整などの設定変更が行われると、スコープまたはプレフィックスに関連付けられているリースが孤立したリースになります。これらの孤立したリースは、日付の制限に違反しないように定期的に更新されません。

リース日付制限機能を使用する場合は、孤立リースが存在しないようにします (または定期的に消去します)。

ステップ 1 DHCP 属性の削除-孤立リースを有効にする:

```
nrcmd> dhcp enable delete-orphaned-leases
```

ステップ 2 DHCP サーバーをリロードします。

```
nrcmd> dhcp reload
```

ステップ 3 DHCP 属性の削除-孤立リースの設定を解除する:

```
nrcmd> dhcp unset delete-orphaned-leases
```

ステップ 4 DHCP サーバーをリロードします。

```
nrcmd> dhcp reload
```

サーバー全体のリースの検索

Cisco プライムネットワーク レジストラーを使用すると、サーバー全体でリースを検索できます。検索は、ネットワーク用に構成された1つ以上のリースを対象とするリース属性の組み合わせを指定できるフィルターメカニズムです。リース履歴検索機能はローカルおよび地域の両方のクラスターで使用できますが、アクティブなリース検索機能はローカルクラスターでのみ使用できます。検索機能は、DHCPv4 と DHCPv6 のリースに対して個別に提供されます。

Cisco プライムネットワーク レジストラーを使用して、アクティブなリースを検索することもできます。

ローカル アドバンスド Web UI

DHCPv4 リースを検索するには、次の手順を実行します。

ステップ 1 メニューから**Operate**サブ**DHCPv4 Current Leases** メニューの下を**Reports**選択して、[DHCP リース検索] ページを開きます。

（注） DHCP リース検索ページを開くには、[DHCP リース履歴検索] ページの [検索] ボタンをクリックします (**Reports**サブメニューの **[DHCPv4 リース履歴]** を選択して [DHCP リース履歴検索] ページを開きます)。このボタンをクリックすると、リース履歴検索ページとアクティブなリース検索ページを切り替えることができます。

ステップ 2 アドレスなど、ドロップダウン リストから、[フィルタ属性（Filter Attribute）] を選択します。DHCPv4 と DHCPv6 には、フィルター属性の個別のリストがあります。また、アクティブリースと履歴リースでは、フィルタ属性のセットが異なります。

属性は、要素として選択するとグレー表示されます。

ステップ 3 ドロップダウンリストから、フィルタ タイプを選択します。少なくともバイナリまたは正規表現を選択できますが、選択したフィルタ属性に応じて、リストに次の 1 つ以上を含めることができます。

- バイナリ - 値はバイナリ表記です。
- [日付の範囲] - 日付値の範囲、日付と時刻から日付と時刻を指定します。
- 整数 - 値は整数です。
- 整数の範囲 - 整数値の起き値から整数値の To 値。
- IP Address：値は IP アドレスです。
- IP 範囲:IP アドレスの [宛先] 値から IP アドレスの値。
- IP サブネット:値は IP サブネットです。
- 正規表現 - 値は正規表現構文の正規表現です。(正規表現の一般的な使用方法については、『』の「管理者の設定」の章 *Cisco Prime Network Registrar 11.1 Administration Guide*を参照してください。

ステップ 4 選択したタイプに基づいて値を入力します。フィルタをクリアするには、**Clear Filter** をクリックします。

ステップ 5 **Add**クリック**Element**すると、検索要素が [フィルター要素] リストに追加されます。フィルター表示を展開し、要素の横にある**[削除]** アイコンをクリックすると、要素を削除できます。

ステップ 6 要素のリストを作成したら、それらの要素を検索して、結果を得るための要素をまとめて検索できます。**Search** をクリックします。

ステップ 7 検索の結果として得られるリースのテーブルを確認し、各アドレス、状態、MACアドレス、ホスト名、フラグ、および有効期限を示します。必要に応じて、ページサイズを変更して、さらにエントリを表示します。リースは IP アドレスで順序付けられます。

ヒント　フィルターエレメントは、検索のために一緒に AND されます。検索結果が期待どおりの結果を得られない場合は、フィルター要素リストをもう一度確認し、結果を妨げる可能性のある要素を削除します。

ローカル アドバンスド Web UI

DHCPv6 リースを検索するには、次の手順を実行します。

ステップ 1　メニューから**Operate**、**DHCPv6 Current Leases**サブメニューの下**Reports**で選択し、DHCP v6 リース検索ページを開きます。

DHCPv6 LeaseHistoryサブメニューの下**Reports**で選択した場合は、DHCP v6 リース検索ページに移動することもできます。**DHCPv6 LeaseHistory**サブメニューの下で**Reports**選択すると、DHCP v6 リース履歴検索ページが表示されます。[DHCP v6 リース検索] ページに移動するには、[検索] ボタンをクリックする必要があります。

ステップ 2　アドレスなど、ドロップダウン リストから、[フィルタ属性（Filter Attribute）] を選択します。

ステップ 3　ドロップダウン リストから、フィルタ タイプを選択します。少なくともバイナリまたは正規表現を選択できますが、選択したフィルタ属性に応じて、リストに次の 1 つ以上を含めることができます。

- バイナリ - 値はバイナリ表記です。
- [日付の範囲] - 日付値の範囲、日付と時刻から日付と時刻を指定します。
- 整数 - 値は整数です。
- 整数の範囲 - 整数値の起き値から整数値の To 値。
- IPv6 アドレス:値は IPv6 アドレスです。
- IPv6 プレフィックス:値は IPv6 プレフィックスです。
- 正規表現 - 値は正規表現構文の正規表現です。（一般的な正規表現の使用方法については、*Cisco Prime Network Registrar 11.1 Administration Guide*の「管理者の設定」の章を参照してください）。
- [次の値を含む] - 値は IPv6 アドレスまたはプレフィックスです(IPv6 アドレスでのみ使用できます)。クエリは、指定したアドレスまたはプレフィックスを含むリースを一覧表示します。

ステップ 4　選択したタイプに基づいて値を入力します。フィルタをクリアするには、**Clear Filter** をクリックします。

ステップ 5　**Add**クリック**Element**すると、検索要素が [フィルター要素] リストに追加されます。フィルター表示を展開し、要素の横にある**[削除]** アイコンをクリックすると、要素を削除できます。

ステップ 6　要素のリストを作成したら、それらの要素を検索して、結果を得るための要素をまとめて検索できます。**Search** をクリックします。

ステップ 7 検索の結果として得られるリースのテーブルを確認し、各アドレス、状態、MACアドレス、ホスト名、フラグ、および有効期限を示します。必要に応じて、ページサイズを変更して、さらにエントリを表示します。リースは IP アドレスで順序付けられます。

CLI コマンド

DHCPv4 空間で**leaselist–macaddr**リースを検索するには、*mac-addr* [**–vpn**=*vpn-name*] を使用します。リースの MAC アドレスを指定します。VPN 指定を省略すると、現在の VPN に基づいて検索を行います。

DHCPv4 空間のリースの場合は、次**lease list**の構文を使用します。

```
nrcmd> lease list [-macaddr=mac-addr] [-cm-macaddr=cm-mac-addr]
       [-reservation-lookup-key=key] [-mac | -blob | -string]]
       [-vpn=vpn-name] [-count-only]
```

DHCPv4 スペース内のリースの場合は、次の **lease listbrief** 構文を使用します。

```
nrcmd> lease listbrief [-macaddr=mac-addr] [-cm-macaddr=cm-mac-addr]
       [-reservation-lookup-key=key] [-mac | -blob | -string]]
       [-vpn=vpn-name] [-count-only]
```

DHCPv6 空間のリースの場合は、次**lease6 list**の構文を使用します。

```
nrcmd> lease6 list[-duid=client-id]
       [-lookup-key=key] [-blob | -string]]
       [-reservation-lookup-key=key] [-blob | -string]]
       [-macaddr=mac-addr]
       [-cm-macaddr=cm-mac-addr]
       [-vpn=vpn-name] [-count-only]
```

DHCPv6 スペース内のリースの場合は、次の **lease6 listbrief** 構文を使用します。

```
nrcmd> lease6 listbrief[-duid=client-id]
       [-lookup-key=key] [-blob | -string]]
       [-reservation-lookup-key=key] [-blob | -string]]
       [-macaddr=mac-addr]
       [-cm-macaddr=cm-mac-addr]
       [-vpn=vpn-name] [-count-only]
```

オプション**–macaddr**と**–cm-macddr**オプションは、CableLabs DOCSIS*vendor-opts* オプション (DHCPv6 オプション 17) で識別されるリースを検索することです。たとえば、次の 2 つのコマンドの場合は、次のようになります。

```
nrcmd> lease6 listbrief -macaddr=01:02:03:04:05:06
nrcmd> lease6 listbrief -cm-macaddr=01:02:03:04:05:06
```

–macaddr 回線には、オプション 17 device-id サブオプション (36) に要求された MAC アドレスが含まれているリースがリストされます。–cm-macddr 行には、オプション 17 cm-mac-address サブオプション (1026) が要求された MAC アドレスと一致するリースがリストされます。(これらの番号順の DHCPv6 オプション一覧サブオプションの詳細については、を参照してください。

クライアント予約の使用

以前のバージョンのCisco Prime Networkレジストラーのバージョンでは、クライアントが必要とするリースを取得する唯一のオプションは、リース予約の作成 （22 ページ）リース予約を作成することでした(を参照)。クライアント(ごとに予約を作成するのは必ずしも簡単ではありません。また、Cisco Primeネットワーク レジストラー予約をデータベースに同期するプロセスも非常に複雑です。クライアント予約機能は、この複雑さを軽減するのに役立ちます。

Cisco Primeネットワーク レジストラー DHCP サーバーが DHCPv4 クライアントに IP アドレスを割り当てる際にサポートされている現在の機能は次のとおりです。

- クライアントのリースベースの予約が存在し、リースが使用可能な場合は、その予約が使用されます。
- それ以外の場合、クライアントがアドレスを要求し、そのアドレスが使用可能な場合は、そのアドレスが使用されます。
- それ以外の場合は、クライアントが使用できるスコープの1つからランダムアドレスが使用されます。

クライアント予約機能を使用すると、クライアントエントリ(Cisco Prime Networkレジストラーまたは LDAP に直接保存される)または拡張を通じて、アドレスを指定してプレフィックスを委任できます。また、クライアントは複数のスコープまたはプレフィックスに配置でき、サーバーはクライアントの場所に適したアドレスを選択します。

クライアント予約リースは、基本的に予約済みリースです。主な違いは、リースが予約されているクライアントが、クライアントの予約の場合にサーバーに知られていない点です。クライアント予約は、多数のクライアントのリースを構成する場合や、単一のクライアントに対して多数のリースを構成する場合に使用されます。

クライアントの予約は、次の3つの主要なメカニズムのいずれかを使用してCisco Primeネットワーク レジストラーに提供できます。

- 内部クライアント データベースの使用:リース予約と同じ問題がいくつか発生しますが、Cisco Prime Networkレジストラー内部クライアントデータベースが他の目的で既に使用されている場合は、より良いオプションになる場合があります。内部クライアント データベースが、クライアントを単独で維持する必要があり、予約を維持する必要が生じるためには、リース予約と比較すると、より有利になります。
- LDAP を使用する:Cisco Prime Network レジストラーは、LDAP リポジトリ(Cisco Prime Networkレジストラーの外部)でクライアントを検索することができ、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。
- エクステンションの使用:Cisco Prime Networkレジストラーは、エクステンションを使用して外部サーバーまたはデータベースと通信するように設定できます。

Cisco Prime Network レジストラークライアント データベースまたは LDAP 内で維持されるクライアントエントリには、クライアントが使用するはずのアドレスとプレフィックスを含めることができます。クライアント予約を指定する属性は次のとおりです。

1. **reserved-addresses**- クライアント用に予約されているアドレスのリストを指定します。使用可能なスコープに一致する最初の使用可能なアドレス (予約への制限が有効になっている必要があります) がクライアントに割り当てられます。
2. **reserved-ip6addresses**：クライアント用に予約されているアドレスのリストを指定します。使用可能なプレフィックスに一致する使用可能なすべてのアドレス (予約に制限が有効になっている必要があります) がクライアントに割り当てられます。
3. **reserved-prefixes**- クライアント用に予約されているプレフィックスのリストを指定します。使用可能なプレフィックスに一致する使用可能なすべてのプレフィックス (予約制限が有効になっている必要があります) がクライアントに割り当てられます。

（注） 上記の属性は VPN を示すものではなく、(クライアントが接続できる)すべての VPN に適用されます。したがって、VPN でクライアント予約を使用する場合は、予約済みアドレスが適切な VPN でのみ有効であることを確認するか(含まれるスコープまたはプレフィックスが存在し、予約が制限されているすべての VPN に適用されるため)、VPN ごとに一意のクライアントを確保する必要があります。

属性の予約制限は、スコープ、スコープテンプレート、プレフィックス、およびプレフィックステンプレートの各オブジェクトに追加され、クライアント予約を指定します。

LDAP のクライアントの場合、LDAP 属性名と対応するクライアント属性名との間のマッピングをセットアップする必要があります。

LDAP アドレス属性にクライアントの IPv4 アドレスリストが含まれている場合、**ldap** *servername* **setEntry query-dictionary** *ldap-attribute=cnr-client-attribute* を使用して、*reserved-addresses* 属性にマッピングします。次に例を示します。

```
nrcmd> ldap ldap-1 setEntry query-dictionary addresses=reserved-addresses
```

ローカル アドバンスド Web UI

スコープをクライアント予約に制限するには、次の手順を実行します。

1. [**デザイン**] メニューの**[DHCPv4]**サブメニューの [**スコープ**] を選択して、[DHCP スコープの一覧/追加] ページを開きます。スケジュールを作成するには、「スコープの作成」を参照してください。
2. [DHCP スコープの一覧/追加] ページの [その他の設定] グループで、[**予約制限**] 属性を有効にします。

   既存のスコープを変更してクライアント予約を指定するには、必要なスコープ名をクリックして [DHCP スコープの編集] ページを開きます。[その他の設定] グループの**[予約制限]** 属性の*[*有効] をクリックします。

フラグクライアント予約は、スコープがクライアント予約に制限されていることを示します。

スコープ テンプレートをクライアント予約に制限するには、次の手順を実行します。

1. [**デザイン**] メニューの**[DHCPv4]**サブメニューの [**スコープ テンプレート**] を選択して、[DHCP スコープ テンプレートの一覧/追加] ページを開きます。スコープスコープ テンプレートの作成と適用テンプレートを作成するには、「」を参照してください。
2. [DHCP スコープ テンプレートの一覧/追加] ページの [その他の設定] で [**予約制限**] 属性を有効にします。

   既存のスコープテンプレートを変更してクライアント予約を指定するには、必要なスコープ テンプレート名をクリックして[DHCP スコープ テンプレートの編集]ページを開きます。[その他の設定] グループの**[予約制限]** 属性の*[*有効] をクリックします。

プレフィックスをクライアント予約に制限するには、次の手順を実行します。

1. [**デザイン**] メニューの**[DHCPv6]**サブメニューの下にある**[プレフィックス]**を選択して、[DHCP v6 プレフィックスの一覧/追加] ページを開きます。
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、[IPv6 プレフィックスの追加] をクリックします。
3. [プレフィックス]ペインのプレフィックス名をクリックして、[DHCPv6 プレフィックスの編集] ページを開きます。[親以外の設定] グループの**[予約制限]** 属性を有効にします。

（注） 予約制限属性が有効になっているプレフィックスは、ライセンスが必要なアクティブリースの合計にはカウントされません。クライアント予約を受信するクライアントは、そのアクティブなリース数をカウントしますが、これは、リースが実際にクライアントによって保持されている場合にのみ発生します。

プレフィックス テンプレートをクライアント予約に制限するには、次の手順を実行します。

1. プレフィックスをクライアント予約に制限するには、[**デザイン**] メニューの**[DHCPv6]**サブメニューの [**プレフィックス テンプレート]**を選択して、[DHCP v6 プレフィックス テンプレートの一覧/追加] ページを開きます。
2. [プレフィックス テンプレート] ウィンドウの [**プレフィックス テンプレートの追加**] アイコンをクリックして、[プレフィックステンプレートの追加] ダイアログボックスを開きます。
3. プレフィックス テンプレート名を入力し、[**接頭辞テンプレートを追加**]ボタンをクリックします。
4. **[予約に制限]**属性を有効にする] をクリックします。

既存のプレフィックステンプレートを変更してクライアント予約を指定するには、クライアント予約に制限するプレフィックス テンプレート名をクリックします。*restrict-to-reservations* 属性に対して [有効（enabled）] をクリックします。

クライアント予約とリース予約の違い

クライアントの予約には、リース予約に関して次のような大きな違いがあります。

- 任意のアドレスに対してクライアント予約が 1 つだけであることを確認するための検証**はありません**。同じアドレスまたはプレフィックスを指定するクライアントが 2 つある場合は、どちらのクライアント要求が最初に到着しても、そのリースが許可されます。
- クライアント予約は、クライアントが DHCP 構成を完了した後にのみ、実際に存在します。リース予約は、クライアント トランザクションが発生しない場合でも知られているため、DHCP サービスをまったく提供しないクライアントにも使用できます。

  Cisco Prime Network Registrar は以下をサポートします。

  - 特定の IP アドレスのリース予約を作成する。
  - ケーブル ソース検証がケーブル モデム終端システム(CMTS)で正しく動作する IP アドレスに対して正しいケーブル モデムの MAC アドレスを設定します。

  これは、Cisco Prime Network レジストラー DHCP サーバーが DHCP クライアント トランザクションの前にリース予約を認識し、それらのアドレスに対する CMTS からの leasequery 要求に正しく応答するためです。これに対して、クライアント予約は DHCP サーバーに DHCP クライアント パケットが到着する前に DHCP サーバーに認識されません。クライアント登録のためにクライアント予約として構成された IP アドレスの leasequery は、IP アドレスがクライアント予約であることを (一般に) 認識しません。

  したがって、DHCP サーバーが正の応答を返すはずの leasequery は、クライアントがリースを要求していない場合でも、適切なケーブル モデム MAC アドレスを含む肯定的な結果を返す場合でも、クライアント予約では動作しません。

リース予約の作成

クライアントが常に同じリースを取得するようにするには、リース予約を作成します。リース予約の管理は、ローカル クラスターで dhcp-admin ロールを持つ管理者、または地域クラスターの dhcp 管理サブロールを持つ中央 cfg-admin ロールを持つ管理者のみが使用できます。

サーバーから DHCPv4 および DHCPv6 予約を照会することができます。

（注） すべてのリース予約は、ライセンスされた IP アドレスの数と比較されるアクティブなリースの合計にカウントされます。

DHCPv4 予約

DHCP編集モードが同期モードの場合、予約変更は自動的にDHCPサーバーに転送され、直ちに有効になります。

編集モードがステージングされると、ローカルクラスタの予約リストに対して行った変更は、親スコープを変更して、サーバーの再ロードが必要であることを示します。地域の予約リストに変更を行うと、親サブネットが変更されます。

ローカルの基本 Web UI

リース予約**Design**を表示するには、メニューから**ScopesDHCPv4**サブメニューを選択して[DHCPスコープの一覧表示/追加] ページを開き、[**予約**] タブをクリックします。

このページで引当を作成するには、リース用に予約するIPアドレスを入力し、[ルックアップキー] フィールドにルックアップ キーを入力します。ルックアップ キー エントリに応じて、MACアドレス(デフォルト)または文字列またはバイナリ ラジオボタンをクリックします。**Add Reservation** をクリックします。リースIPアドレス、ルックアップ キー、スコープの詳細は、[DHCP 予約の一覧/追加] ページに表示されます。

ローカル アドバンスド Web UI

DHCPv4 スコープのリース予約を表示するには、**Design**メニューからサブメニューの**Scopes**下を**DHCPv4**選択して[DHCP スコープの一覧/追加]ページを開きます。基本 Web UI に関する手順を実行します。

詳細モードでは、スコープに依存しない予約を作成するメカニズムも提供されます。DHCPv4スコープの予約を直接構成するには、次の手順を実行します。

ステップ 1 メニューから**DesignReservationsDHCPv4**サブメニューの下で選択し、[DHCP 予約の一覧表示/追加] ページを開きます。

ステップ 2 [予約] ウィンドウの**[DHCP 予約の追加]** アイコンをクリックし、リース用に予約するIPアドレスを入力します。

ステップ 3 ルックアップ キー エントリに応じて、MAC アドレス(デフォルト)または文字列またはバイナリ ラジオ ボタンをクリックします。**Save** をクリックします。

ヒント フィルタを使用して、表示されるリストのサイズを小さくすることができます。これを行うには、[フィルタタイプ（Filter Type）] ドロップダウン リストからフィルタ タイプを選択します。フィルターの値は、フィルターの種類の選択として設定されます。[フィルタの設定（Set Filters）] をクリックします。フィルタ タイプを「None」に設定するには、[フィルタのクリア（Clear Filter）] をクリックします。リースのIPアドレス、ルックアップキー、およびスコープの詳細は、[DHCP予約の一覧と追加（List/Add DHCP Reservations）] ページに表示されます。

（注） 複数の DHCP サーバーは、DHCP フェールオーバー パートナーでない限り、同じサブネット上に IP アドレスを配布しないでください。フェールオーバーを使用する場合、クライアント予約は各サーバーで同一である必要があります。存在しない場合、リース予約が存在するクライアントは、異なるサーバーから異なる IP アドレスのオファーを受け取ることができます。フェールオーバー同期機能は、パートナーの構成が一貫していることを確認するのに役立ちます。

CLI コマンド

予約コマンドを使用すると、Cisco プライムネットワーク レジストラーの DHCPv4 予約のグローバル リストにアクセスできます。

使用して新しいアドレスを作成します,**予約**[*vpn-name*/]アドレス**作成**{*macaddr* |検索キー}[**-mac**|**-ブロブ**|**-文字列**][属性=値..]

次に例を示します。

```
nrcmd> reservation white/192.168.1.110 create 00:d0:ba:d3:bd:3b
```

使用してアドレスを削除する**予約***[vpn-name/]*アドレス**削除**

次に例を示します。

```
nrcmd> reservation white/192.168.1.110 delete
```

を使用して属性を取得する、**予約**[*vpn-name*/]アドレス**取得**属性

次に例を示します。

```
nrcmd> reservation white/192.168.1.110 get value
```

使用して属性を設定する、**予約***[vpn-name/]*アドレス**セット**属性=値

次に例を示します。

```
nrcmd> reservation white/192.168.1.110 prefix=cm_prefix
```

使用して属性を設定解除する、**予約**[*vpn-name*/]アドレス**の設定解除**属性

次に例を示します。

```
nrcmd> reservation white/192.168.1.110 unset value
```

を使用してアドレスを表示**する予約***[vpn-name/]*アドレス**ショー**

次に例を示します。

```
nrcmd> reservation white/192.168.1.110 show
```

予約**リスト[VPN**名/]アドレスを使用して予約を表示する|**-マック**|**-キー**]。このコマンドは、ソート順を変更するために -key が指定されていない限り、予約をアドレス順に表示します。

次に例を示します。

```
nrcmd> reservation list white/192.168.1.110
```

予約の簡単な詳細を表示するには、**予約リストブリーフ**[**-macaddr**=*mac-addr*] [**-lookup-key**=ルックアップキー [**-mac** |**-ブロブ**|**-文字列**][**-vpn**=*VPN* 名][**-カウントのみ**]

次に例を示します。

```
nrcmd> reservation listbrief -lookup-key=d4:6a:a8:d3:e2:ea -mac
```

DHCPv6 リース予約

予約は、非一時アドレスとデリゲートされたプレフィックスにのみ適用されます。これらは、構成内のプレフィックスに関連付けられており、常に、構成済みのプレフィックスオブジェクトの下のアドレス (またはプレフィックス) に対して使用する必要があります。

予約は、別のプレフィックスのオブジェクト範囲内になっていない場合、プレフィックスのオブジェクト範囲の外側に置くことができます。ただし、新しいプレフィックスオブジェクトを追加する場合は、この影響を受けます。プレフィックスの新しい範囲に含まれている予約が存在する場合、プレフィックスは追加されません。これにより、EX_CONFLICTステータスになります。詳細は、リース予約の作成 （22 ページ）を参照してください。

（注） DHCPv4 予約の操作は、アドレスが v4 アドレスではなく v6 アドレスであることを除いて、DHCPv6 予約に似ています。また、DHCPv6 クライアントの主な ID は、MAC アドレスではなく、クライアント DUID です。DHCPv6 予約には、アドレスと委任されたプレフィックスが含まれます。

v6 予約リストで行った変更は、親プレフィックスを変更して、サーバーの再ロードが必要であることを示します。地域サーバーでは、DHCP編集モードが同期モードで、親プレフィックスがローカル クラスタに割り当てられている場合、変更は自動的にローカル クラスタに転送されます。これらの変更を有効にするには、サーバーの再ロードが必要です。

注意 複数の DHCP サーバーが同じプレフィックスに IP アドレスを配布する場合、予約は同一である必要があります。存在しない場合、予約が存在するクライアントは、異なるサーバーから異なる IP アドレスのオファーを受け取ることができます。

リース予約は、IP アドレスとルックアップ キーを組み合わせます。検索キーには、文字列値またはバイナリ BLOB を指定できます。

（注） サーバーが再ロードされるときに、既存のリースに競合する (または含まれている) 短いプレフィックスまたは長いプレフィックスを持つ新しいプレフィックス委任予約が追加された場合、予約は既存のリースの読み込みができなくなります。

ローカル アドバンスド Web UI

DHCPv6 プレフィックスの予約を表示するには、次の手順を実行します。

ステップ 1 DHCPv6 リース予約を表示するには、[**設計**] メニューの**Prefixes**サブメニュー**DHCPv6**の下で [DHCPv6 プレフィックスの一覧/ 追加] ページを開きます。

ステップ 2 [プレフィックス] ペインでプレフィックスを選択し、[**予約**] タブをクリックします。

ローカル アドバンスド Web UI

DHCPv6 プレフィックスの予約を直接設定するには、次の手順を実行します。

拡張モードでは、有効な親プレフィックスが指定されていない場合、CCM サーバーは自動的に適切な親プレフィックスを設定します。

ステップ 1 メニューから**DesignReservationsDHCPv6**サブメニューの下で選択し、DHCP v6 予約のリスト/追加ページを開きます。

ステップ 2 予約を作成するには、[予約] ウィンドウの**[DHCP v6 予約の追加]** アイコンをクリックし、リース用に予約する IP アドレスを入力し、[検索キー] フィールドにルックアップ キーを入力します。

ステップ 3 [検索キー] フィールドにバイナリ値を入力した場合は、[文字列] ラジオ ボタンをクリックするか、[バイナリ] ラジオ ボタンをクリックします。

ステップ 4 **Add Reservation** をクリックします。

ステップ 5 [予約] ウィンドウで、[**フィルターの種類**] ドロップダウン リストからフィルターの種類を選択します。[フィルタ値] フィールドに値を入力します。[フィルタの設定（Set Filters）] をクリックします。[フィルタの種類] を [なし] に設定するには、[**フィルタのクリア**] をクリックします。リース IP アドレス、ルックアップ キー、およびプレフィックスの詳細が[DHCP v6 予約の一覧/追加]ページに表示されます。

CLI コマンド

reservation6コマンドを使用すると、Cisco プライムネットワーク レジストラーの DHCPv6 予約のグローバル リストにアクセスできます。

グローバル リストの各予約に一致するプレフィックスが存在する必要があります。

を使用して新しいアドレスを作成します,**予約6**[*vpn-name*/]アドレス**作成**ルックアップキーを作成する [**-blob** |-**文字列**][属性=値..]

次に例を示します。

```
nrcmd> reservation6 white/2001:db8::1 create 00:03:00:01:01:02:03:04:05:06
```

使用してアドレスを削除する,**予約6** *[vpn-name/]*アドレス削除

次に例を示します。

```
nrcmd> reservation6 white/2001:DB8::1 delete
```

使用して属性を取得します,**予約6** [*vpn-name/*]アドレス**取得**属性

次に例を示します。

```
nrcmd> reservation6 white/2001:DB8::1 get value
```

使用して属性を設定する、**予約6** *[vpn-name/]*アドレス**セット**属性=値

次に例を示します。

```
nrcmd> reservation6 white/2001:DB8::1 set prefix=cm_prefix
```

使用して属性を設定解除します,**予約6** *[vpn-name/]*アドレス**の設定なし**の属性

次に例を示します。

```
nrcmd> reservation6 white/2001:DB8::1 unset value
```

使用してアドレスを表示する予約**6** *[vpn-name/]*アドレス**ショー**

次に例を示します。

```
nrcmd> reservation6 white/2001:DB8::1 show
```

予約を使用して予約を表示する予約**6リスト**[[VPN名/]アドレス|**-キー**]。このコマンドは、ソート順を変更するために -key が指定されていない限り、予約をアドレス順に表示します。

次に例を示します。

```
nrcmd> reservation6 list white/2001:DB8::1
```

使用して予約の簡単な詳細を表示します,**予約6リストブリーフ**[**-検索キー**=ルックアップキー [**-blob** |**-文字列**][**-vpn**=*VPN* 名][**-カウントのみ**]

次に例を示します。

```
nrcmd> reservation6 listbrief -lookup-key=def -string -vpn=vpn1
```

リースと予約プロパティの詳細設定

高度なリースと予約のプロパティを設定することができます。

- 現在リースされている IP アドレスの予約-現在リース済みのアドレスの予約 （28 ページ）
- リースの予約解除 -を参照してください。リースの予約解除 （29 ページ）
- MAC 以外のアドレスへのリースの延長:を参照してください。MAC 以外のアドレスへの予約の拡張 （30 ページ）
- リースの可用性の強制-「」を参照してください。リースを強制的に使用可能にする （33 ページ）

- リースの更新の抑制-「」を参照リース更新の抑制 （34 ページ）
- 利用不可とマークされたリースの処理 -「」を参照使用不可としてマークされているリースの処理 （37 ページ）
- 利用できないリースのタイムアウトの設定 -を参照してください。使用不可リースのタイムアウトの設定 （38 ページ）

現在リース済みのアドレスの予約

1 台目のクライアントにリースがある場合でも、別のクライアントに対して再使用している間に、そのクライアントの予約を削除できます。

ローカル アドバンスド Web UI

既存のリースを予約するには、次の手順を実行します。

ステップ 1 メニューの**DesignScopes**サブメニューの下**DHCPv4**でを選択し、スコープの名前を選択して [DHCP スコープの編集] ページを開きます。

ステップ 2 [リース] タブをクリックします。

ステップ 3 リースの IP アドレスをクリックします。

ステップ 4 IP アドレスがリースされていない場合 (使用可能な状態)、予約のルックアップ キーまたは MAC アドレスを入力します。

ステップ 5 **Make Reservation** をクリックします。[DHCP スコープの編集] ページで、リースが予約済みとして表示されます。

ステップ 6 [保存（Save）] をクリックしてスコープを保存します。

ステップ 7 予約を削除するには、[DHCP**Remove Reservation**スコープの編集] ページをクリックし、スコープを変更します。リースは予約済みとして表示されなくなります。

既存のリース予約の例

このCLIコマンドの例では、既存のリースから予約を作成します。これは、dhcp-editモードが同期に設定され、予約がサーバーに動的に追加されることを前提としています。

```
nrcmd> reservation 192.168.1.110 create 1,6,00:d0:ba:d3:bd:3b
nrcmd> lease 192.168.1.110 activate
```

クライアント 1,6,00:d0:ba:ba:d3:bd:3b は DHCPDISCOVER を行い、192.168.96.110 のオファーを受け取ります。クライアントは DHCPREQUEST を実行し、同じ IP アドレスに対する ACK メッセージを取得します。

時間が経過すると、クライアント 1,6,00:d0:ba:d3:bd:3b は、サーバーが確認する更新されるいくつかの DHCPREQUEST を実行します。次に、クライアントリースの有効期限が切れる前の時点で、予約を終了します。

```
nrcmd> lease 192.168.1.110 deactivate
nrcmd> reservation 192.168.1.110 delete
```

その後、その IP アドレスが最初のクライアントにリースされている場合でも、その IP アドレスに対して別のクライアントの予約を追加します。

```
nrcmd> reservation 192.168.1.110 create 1,6,02:01:02:01:02:01
nrcmd> lease 192.168.1.110 activate
```

このアクションにより、あるクライアントにリースされているが、別のクライアント用に予約された IP アドレスが作成されます。新しいクライアント (1,6,02:02:02:01:02:02:01) が元のクライアント (1,6,00:d0:d0:d3:bd:3b) の前に DHCPDISCOVER を実行した場合、新しいクライアントは 192.168.96.110 を取得しませんが、動的プールからランダムな IP アドレスを取得します。

元のクライアント (1,6,00:d0:ba:d3:bd:3b) が次の DHCPREQUEST/RENEW を 192.168.96.110 のリースに送信すると、NAK メッセージが表示されます。一般に、非確認メッセージを受信すると、クライアントは直ちに DHCPDISCOVER を送信します。DHCPDISCOVER を受信すると、サーバーは 192.168.96.110 の残りのリース時間をキャンセルします。

次に、サーバーはクライアントに 1,6,00:d0:ba:d3:bd:3b 適切なリースを提供します (192.168.96.110 以外の予約、動的リース (使用可能な場合) 、または何も (動的リースが利用できない場合) 。新しいクライアント (1,6,02:01:02:02:02:02:01) が受信したランダム IP アドレスを更新しようとすると、サーバーは予約済みアドレスを指定するため、NAK を送信します。新しいクライアントが DHCPDISCOVER を実行すると、192.168.96.110 予約アドレスが取得されます。

また、リースの可用性を強制することもできます (「」リースを強制的に使用可能にする （33 ページ）を参照)。ただし、これを行っても、元のクライアント (1,6,00:d0:d0:d3:bd:3b) が 192.168.96.110 を使用するのを停止しません。また、新しいクライアント (1,6,02:01:02:01:01:02:02:01) が 192.168.96.110 を取得するのを妨げるわけではありません。つまり、クライアントの予約は、予約が行われる IP アドレスのリース状態 (および実際のリース クライアント) とは無関係です。

したがって、あるクライアントに対して予約を行うと、別のクライアントがリースをすぐに失うわけではありませんが、クライアントは次回 DHCP サーバーに接続する際に NAK 応答を受信します (秒または数日)。また、IP アドレスを予約したクライアントは、他のクライアントが既に IP アドレスを持っている場合、そのアドレスを取得しません。代わりに、次の手順を実行するまで、別の IP アドレスを取得します。

- 受信するはずのIPアドレスは無料です。
- クライアントは更新として DHCPREQUEST を送信し、NAK 応答を受信します。
- クライアントが DHCP ディスカバリを送信します。

リースの予約解除

リース予約はいつでも削除できます。ただし、リースがまだアクティブな場合、クライアントは、有効期限が切れるまでリースを使用し続けます。別のクライアントのリースを予約しようとすると、警告が表示されます。

リージョンから最後の予約を削除すると、予約を選択して変更をローカル クラスターにプッシュすることはできません。親サブネットをプッシュして、予約リストを同期させて、予約のローカル コピーを削除する必要があります。

地域のDHCPv6予約にはプッシュ機能はありません。予約を再同期するには、常に親プレフィックスをプッシュする必要があります。地域削除アクションを同期する場合は、この方法が推奨されます。

ローカル アドバンスド Web UI

リースの予約を解除するには、[**デザイン**] メニューの**Reservations[DHCPv4]**サブメニューの下で [DHCP 予約の一覧/追加] ページを開き、削除する予約を選択した後に [**予約の削除**] アイコン (左ペイン) をクリックします。これにより、予約は確認なしで直ちに削除されます。

CLI コマンド

リースの予約を解除するには、[**reservation** *vpn/*]*ipaddr***delete**または**scope** *name* **removeReservation** {*ipaddr* |マカドル|検索キー}[**–mac** |**–blob** |**–string**]. それでも、次の対応を試してください。

- nrcmd 内部データベースから予約がなくなっていることを確認します。
- 予約を含むスコープでフェールオーバーを使用する場合:

1. 両方**reservation**のサーバーで [*vpn/*]*ipaddr* **delete**、**scope** または *name* **removeReservation** を使用します。
2. バックアップ サーバーで、ステージング dhcp 編集モードの場合は、 **lease** [*vpn/*]*ipaddr***delete-reservation**を使用します。
3. メイン サーバーで同じコマンドを使用します。

lease *ipaddr***delete-reservation**を発行した場合のみサーバー内部メモリに影響するため、この操作の結果を保存して、サーバーの再ロード後も保存します。

MAC 以外のアドレスへの予約の拡張

場合によっては、着信クライアント パケットの MAC アドレス以外のアドレスに基づいてリース予約を作成する必要があります。スイッチ ポートに接続されている DHCP クライアント デバイスは、MAC アドレスに関係なく、同じ IP アドレスを取得する必要があります。この方法は、工場出荷時のデバイスを同一のデバイス(異なる MAC アドレス)で置き換えるが、同じ IP アドレスを維持する場合に役立ちます。

クライアント ID の上書き

Relay エージェント情報オプション (82) からスイッチの MAC アドレスとポートを抽出し、そこからクライアント ID を作成するクライアント クラスオーバーライド クライアント *ID*属性で式を設定できます。着信パケットのクライアント ID に関係なく、IP アドレスを割り当てる ID は、同じスイッチ ポートを経由して着信するデバイスと同じです。属性に使用する式は、オプション 82 形式によって異なります。DHCP サーバーは、クライアント クラスにパケット

を割り当てると式を計算します。オーバーライドクライアント *ID*値は、その後のクライアントの ID になります。

（注） *[v6-]* オーバーライドクライアント *ID*式を使用する場合、クライアント ID による leasequery 要求は、クライアントのリースに関する情報を正しく取得するために、オーバーライドクライアント *ID*属性を指定する必要があります。

ただし、ポリシーで *use-client-id-for-reservations* 属性を有効にすると、サーバーはその要求のクライアント ID を *nn*:*nn*:*nn ...nn*:*nn* という形式の文字列に変換し、その文字列を使用して予約を検索します。

クライアントまたはクライアントクラスの環境への追加属性は、名前と値のペアとして指定された DHCP 拡張環境ディクショナリ (を参照拡張ポイントの使用) に属性値を送信する機能も提供します。クライアントまたはクライアント クラスのどちらでも、環境への追加のディクショナリ属性を構成できます。クライアントとクライアントクラスの両方でこの属性を構成する場合は、クライアントクラスで構成する名前と値のペアとは異なる名前を持つようにする必要があります。同じ環境辞書に入れられます (特定の名前に対して 1 つの値しか持てありません)。一般的に、この属性はクライアントまたはクライアント クラスでのみ構成し、両方で構成しないことをお勧めします。

ローカル アドバンスド Web UI

*[DHCP*クライアント クラスの編集] ページでオーバーライド クライアント ID 属性を**Design**確認できます (メニューから、**Client ClassesDHCP Settings**サブメニューの下でクライアント クラスの名前を選択します)。

また、DHCP サーバーのクライアント クラスルックアップ ID を設定して、すべてのパケットを特定のクライアント クラスに入れ、そこでオーバーライド クライアント *ID*式を設定する必要があります。**Operate** メニューから、**Servers** サブメニュー の **Manage Servers** を選択し、[DHCP] をクリックして、[ローカルDHCPサーバーの編集（Edit Local DHCP Server）] ページを開きます。クライアント クラス属性に、クライアントクラス検索 *ID*式を入力します。

予約にクライアント ID を使用するには、[DHCP ポリシーの追加] ページの [クライアント*ID* の予約] 属性を有効にするように**Design**ポリシーを構成します (メニューの**PoliciesDHCP Settings** []メニューの []をクリックし**Design**、[DHCP ポリシーの編集]ページをクリック**AddPolicies**します)。 **Policies DHCP Settings**

CLI コマンド

オーバーライドクライアント *ID*属性を設定するための構文は**client-class** 、*name* **set override-client-id="**式"です。クライアント クラス検索 *ID*属性を設定するための構文は式**dhcp set client-class-lookup-id="**です"。*use* クライアント *ID-for-*予約属性を設定するための構文は**policy name enable use-client-id-for-reservations**です。

予約の上書きの例

次の例は、予約のクライアント ID をオーバーライドする方法を示しています。

ステップ 1 予約のスコープを作成します。

a) サブネット アドレスを入力します。
b) 動的予約が必要な場合は、IP アドレス範囲を追加します。

ステップ 2 スコープの予約を追加します。

a) ルックアップ キーの値を含めます。
b) ルックアップ キーの種類をバイナリとして指定します。

ステップ 3 目的のポリシーを作成し、*use-client-id*-予約属性を有効にします。

ステップ 4 目的のクライアント クラスを作成します。

a) 前の手順で作成したポリシーを指定します。
b) パケットの内容に基づいて、目的のクライアント ID を持つ BLOB 値を返すオーバーライド クライアント*ID*属性の式を含めます。

ステップ 5 MAC アドレスを持つクライアントのリースを取得します。このクライアントはオーバーライド ID を取得します。

IPv6 リースの再設定

DHCPv6 リースの場合、RECONFIGURE メッセージをクライアントに送信して、サーバーに新しい構成パラメータまたは更新された構成パラメータがあることをクライアントに通知できます。適切な認証によって承認された場合、クライアントはサーバーと、更新、再バインド、または情報要求の応答トランザクションを開始して、新しいデータを取得できるようにします。

DHCPv6 ポリシーの再構成を有効にする方法の詳細DHCPv6 ポリシーの設定については、を参照してください。

ローカル アドバンスド Web UI

[プレフィックスの DHCP リースの一覧/追加**Reconfigure**] ページには、各リースのボタンが含まれるため、その特定のリースに対して再構成要求を開始できます。

CLI コマンド

再設定をサポートするために、Cisco Primeネットワーク レジストラー**lease6**には、コマンドの次の構文が含まれています。

```
lease6 [vpn-name/]ipaddr reconfigure [renew | rebind | information-request] [-unicast |
 -via-relay]
```

オプションは、クライアントがリコンフィグレーション メッセージに対して更新パケット、再バインドパケット、または情報要求パケットで応答するかどうか、およびサーバーがユニキャ

ストするかリレーエージェントを通過するかを決定します。および**lease6 show**コマンドは、これらの関連属性の値も表示します**lease6。 list**

- クライアント再構成キー- クライアントへのメッセージの再構成のためにサーバーが生成する 128 ビットキー。
- クライアント再構成キー生成時間: サーバーがクライアント再構成キーを生成した時刻。

ポリシーコマンドには、関連する 2 つの属性設定が含まれています。

- 再構成—(1)、許可しない(2)、または(3)サポートを再設定する必要があるかどうか。プリセット値は許可 (1) です。
- リレー経由で再構成— リレー エージェント上での再構成を許可するかどうか。プリセット値は false で、それによって再設定通知はサーバーからのユニキャストによって行われます。

リースを強制的に使用可能にする

現在のリースを強制的に使用可能にすることができます。ユーザーがリースを解放するか、または自分でリースを解放するように要求してから、そのユーザーの可用性を強制する必要があります。リースの可用性を強制する場合、サーバーの再ロードは必要ありません。

（注） リースが強制的に使用可能になった後、クライアントは DHCP サーバーに接続するまでリースを使用し続けます。

ローカル アドバンスド Web UI

リースの可用性を強制するには、次の手順を実行します。

ステップ 1 **Design** メニューで、**DHCPv4** サブメニューから **Scopes** を選択し、[DHCPスコープの一覧/追加（List/Add DHCP Scopes）] ページを開きます。

ステップ 2 リースがあるスコープの [リース（Lease）] タブをクリックします。

ステップ 3 [DHCPスコープの編集（Edit DHCP Scope）] ページでリースの IP アドレスをクリックします。

ステップ 4 [DHCPスコープの編集（Edit DHCP Scope）] ページで **Force Available** をクリックします。リースは、フラグ列に空の値を表示します。

CLI コマンド

リースの可用性を強制するには、 **lease** *vpn*/]*ipaddr***force-available**を使用します。**scope**名前 **clearUnavailable**を使用して、スコープ内のすべての **"利用不可"** リースを強制的に **"利用可能"** 状態に変更します。

リース更新の抑制

通常、Cisco Primeネットワーク レジストラー DHCP サーバーは、クライアントとそのリース IPアドレスとの関連付けを保持します。DHCPプロトコルは、この関連付けを明示的に推奨しており、通常は望ましい機能です。ただし、ISP などの一部の顧客では、長期間のリース関連付けを持つクライアントは、IPアドレスを定期的に変更する必要があるため、望ましくない場合があります。Cisco Prime Network レジストラーには、DHCP クライアントがリースの更新または再起動を試みたときに、リースアソシエーションを強制的に変更できるようにする機能が含まれています。

サーバーはクライアントにリースの変更を強制することはできませんが、DHCPRENEW 要求またはDHCPDISCOVER要求に基づいてクライアントに強制的に変更を強制することができます。Cisco Prime Network レジストラーには、クライアントに IP アドレスの変更を強制するために使用するインタラクションを選択できる設定オプションがあります。

- **Inhibiting all —lease**クライアント**が**リースされたアドレスを使用している間、リースの**renewals**延長を定期的に試みます。更新を行うたびに、サーバーはリースを拒否して、クライアントが IP アドレスの使用を停止することを強制できます。クライアントは、リースが終了すると終了するアクティブな接続を持っている可能性があるため、DHCP対話のこの時点での更新の禁止はユーザーに表示される可能性があります。
- **Inhibiting renewals - at** DHCP クライアントが再起動すると、有効期限のない有効なリースバインディングが記録されたか、有効な**reboot**リースが存在しない可能性があります。リースがない場合は、サーバーが最後に保持したリースを許可しないようにすることができます。クライアントに有効なリースがある場合、サーバーはそれを拒否し、クライアントは新しいリースを取得することを余儀なくされます。いずれの場合も、アクティブな接続はリースされたアドレスを使用しないため、禁止が目に見える影響を与えません。
- —更新**Effect**の禁止よりも予約が**on優先reservations**されます。クライアントに予約がある場合、更新禁止が構成されているかどうかにかかわらず、予約済み IP アドレスを引き続き使用できます。
- —更新禁止テストの後、クライアントクラスのテストが行われます。 **Effect on client-classes** クライアントが更新禁止によって IP アドレスの変更を強制された場合、クライアント・クラスの処理は、サーバーがクライアントに提供するアドレスに影響を与える可能性があります。

スコープまたはクライアントごとに、システム全体を設定できるポリシーのリース更新禁止を有効または無効にできます。禁止 *all-re-news*属性により、サーバーはすべての更新要求を拒否し、クライアントが DHCP サーバーに接続するたびに新しい IP アドレスを取得することを強制します。再起動時の更新を禁止属性は、クライアントがリースを更新することを許可しますが、サーバーは再起動するたびに新しいアドレスを取得するように強制します。これは、ディスカバーおよびINIT-REBOOT 操作にのみ適用されます。ディスカバーが含まれているのは、再起動時に INIT-REBOOT を使用する DHCP クライアントが少ないためです (ほとんどのクライアントはディスカバリを行うだけです)。

次の条件下では、更新が禁止されません。

- フェールオーバーを使用する場合、および開始状態がMCLTより短い時間から経過した時間。デフォルトの MCLT は 60 m です。

- フェールオーバーを使用する場合、フェールオーバーの状態は通常またはPARTNER-DOWNではありません。
- リースが AVAILABLE で、クライアント作成時間が更新禁止時間よりも短い時間である場合。更新禁止 -最大時間のデフォルト値は 60s です。
- リースが提供またはリースされ、要求がディスカバーまたはリクエスト選択であり、状態の開始時刻が更新禁止時間よりも短い時間である場合。*renewal-inhibition-max-time* のデフォルト値は、60 s です。

DHCP サーバーは、拒否する必要があるクライアント メッセージ (更新要求など) と再送信を表すメッセージを区別する必要があります。サーバーはメッセージを処理するときに、パケットが到着した時刻を記録します。また、クライアントにリースバインドを行った時刻と、そのバインドに関するクライアントからのメッセージを最後に処理した時刻も記録します。次に、パケットの到着時刻をリース バインディング時間 (開始状態時間) と比較し、バインディングの開始時刻から一定の時間間隔内にクライアントからのパケットを処理します。既定では、この時間間隔は 1 分です。

ローカル アドバンスド Web UI

リースの更新を禁止するには、[DHCP ポリシーの編集] ページでポリシーを**Design**作成し**Policies**(メニューから**[DHCP 設定]**サブメニューの下で選択し、ポリシーの名前を選択して、すべての更新を禁止するか、再起動時に更新を禁止する)を有効にします。(両方の属性は、無効にプリセットされています)。次に、ポリシーを変更し、[**保存**] をクリックして変更を保存します。

サーバー間でのリースの移動

サーバーの構成が、推奨される制限を超えるほど大きくなり、新しいDHCPサーバーにリースを移動する必要がある場合があります。リースを新しいサーバーに移動するか、既存のサーバーに移動するかによって、このタスクを実行する方法はさまざまです。これらの方法のどちらを使用する場合も、特別な考慮事項と慎重な実行が必要です。多くの場合、新しいサーバーは、構成全体と状態データベースを移動することによって最も簡単に実行できます。リースを別のサーバーに移動するには、leaseadmin ユーティリティを使用します。このユーティリティを使用すると、すべてのリースまたは選択したリースセットをエクスポートしたり、エクスポートしたリースセットをインポートしたりすることもできます。

⚠

注意 leaseadmin ユーティリティはローカル クラスタ (エクスポートまたはインポート) でのみ使用する必要があり、dhcp サーバーは leaseadmin ユーティリティを実行する前に停止する必要があります。

リースをあるサーバーから別のサーバーに移動できるようにleaseadminユーティリティがCisco Prime Network レジストラーに追加されました。このユーティリティは、DHCP サーバーと同じマシン上で実行する必要があり、データベースファイルの読み取りおよび変更を行うには、スーパーユーザー/ルート権限が必要です。このユーティリティでは、リース状態データベースに直接アクセスする必要があります。ただし、DHCPサーバーを停止しても、停止したサー

バーはリース状態データベースを開いたままにしているので、十分ではありません。データベースがまだ使用中のときにユーティリティが実行されると、leaseadminユーティリティは"リース状態データベースへの排他的アクセスを取得できませんでした"というエラーを報告します。デフォルトの場所は次のとおりです。

/opt/nwreg2/local/usrbin

コマンド プロンプトで上記の場所に移動し、次の構文を使用してユーティリティを実行します。

./leaseadmin <*options*>

次の表では、**leaseadmin** ユーティリティの修飾オプションについて説明します。

表 *3*: リース管理者コマンド オプション

オプション	説明
リースをエクスポートするには	
–e *filename*	ファイルにエクスポート
–x	未加工の出力形式を送信します (インポートに必要)。
–t {**current** | **history** | **detail** | **all** | **v6leases** | **v6history**}	エクスポートするレコードの種類を指定します。有効な値は次のとおりです。 **current**、**history**、**detail**、**all**、**v6leases**、および **v6history**
–s *subnet* | *prefix*	サブネットまたはプレフィックスにエクスポートするリース レコードを制限します。
リースをインポートするには	
–i *filename*	ファイルからのインポート。**-n**オプションと共に使用する場合は、VPNを指定します。
–o	-i（インポート）オプションと共に使用すると、既存のデータが上書きされます。
–c	レコードを圧縮します。
リースまたはサーバー DHCP 一意識別子 (DUID) を削除するには	
–d *address* | *subnet* | *prefix*	削除するアドレス、サブネット、またはプレフィックスを指定します。

オプション	説明
–d server-duid	サーバー DUID 情報をデータベースから削除することを指定します。 （注） server-duid 指定すると、自動生成された DHCPv6 サーバー DUID が存在する場合は、その DUID が削除されます。 リースデータベースが別フェールオーバーに関連する問題のトラブルシューティング時に避けるべき事項のローカルクラスタにコピーされる場合は、推奨しませんが、コピーされたデータベースに存在する可能性のある server-duid は、この操作を使用してサーバーの duid を削除することが重要です。 server-duid が削除されると、DHCP サーバーが始動すると、新しい server-duid が生成されます。これにより、クライアントが DHCPv6 再バインド要求の送信を開始するまで、古い server-duid をサーバー ID オプションとして指定したすべての DHCPv6 更新要求がドロップされます。 10.x 以降の場合、サーバーは一度削除されると、ローカルクラスターの UUID を使用し、クラスターの構成から利用できるようにリース データベースに格納されません。
全般オプション	
–n *vpn*	-e (エクスポート)、-i (インポート)、または -d (削除) オプションと共に使用する場合は、VPN を指定します。すべての VPN を含めるには、「all」を指定します。
–h *path*	データベースへの既定のパスをオーバーライドします。
–v	データベース バージョンを表示します。
–z{文字}= レベル	デバッグ出力レベルを設定します。

使用不可としてマークされているリースの処理

効果的なリースメンテナンスの側面の1つは、スコープ内の利用できないリースの数を決定することです。この数は予想よりも大きくなる場合があります。利用できないリースは、深刻な問題を示している可能性があります。リースが利用できない原因として、次のことが考えられます。

- 現在アクティブ***The DHCP server is configured for a ping before an offer, and the ICMP echo message is returned successfully***なクライアントがその *IP* アドレスを使用しているので、*DHCP* サーバーは使用不可能とマークします。 サーバーがアドレスを使用しないようにするには、クライアントにアドレスを提供する前に ping を無効にします。アドレス提供前のホストへの ping 実行 （12 ページ）を参照してください。

- —クライアントはローカル LAN セグメントの IP アドレスに対してアドレス解決(ARP)要求を行い、別のクライアントがそのアドレスに応答します。 **The server receives a DHCPDECLINE message from a client to which it leased what it considered to be a good IP address** クライアントは、DHCPDECLINE パケットを使用してサーバーにアドレスを返し、別の DHCPDISCOVER パケットを送信して新しいアドレスを取得します。サーバーは、クライアントから返されるアドレスを使用できないものとしてマークします。サーバーが DHCPDECLINE メッセージに応答しないようにするには、スコープ属性(無視拒否)を設定します。

- DHCPOFFER メッセージに続くすべての DHCPREQUEST メッセージがブロードキャストされるため、サーバーは他の DHCP サーバーに送信されたメッセージを見ることができます。 **The server receives “other server” requests from the client** サーバーは、パケット内の *server-id*オプションの値によってメッセージがメッセージに送信されることを認識しています。Cisco Prime Network レジストラーサーバーが、自身の IP アドレスが*server-id*オプションに表示されないという点で、別のサーバーに向けられたメッセージを認識する場合、メッセージ内のアドレスはサーバーが制御するアドレスであり、2 台のサーバーが同時にアドレスを管理しようとしていると考えています。次に、ローカルアドレスを利用不可としてマークします。この動作は、DHCP フェールオーバー構成では適用されません。2 つのサーバーが、同じ IP アドレスの一部またはすべてを使用して構成されているか、または(まれに) DHCP クライアントがパケットに誤った*server-id*オプション値を配置したかのどちらかです。

  クライアントが(実際に他のサーバーに送信されるパケットではなく)不正なサーバー *ID*オプションを送信していると考える理由がある場合、Cisco Prime Network レジストラーには、この動作を無効にするサーバー属性を持つことができます。

- —非常にまれで、サーバーの起動時に、サーバーがリースの設定中に、内部キャッシュのリフレッシュ中にディスクからリースデータを読み取る場合にのみ発生します。 **Inconsistent lease data** リース状態はリース済みとして表示されますが、リースにクライアント IDオプション値が設定されていない可能性があるなど、そのリース用のクライアントを構築するための不完全なデータが存在します。サーバーはデータに不整合があると見なし、IP アドレスを利用不可とマークします。リースを強制的に利用可能にする(CLI で **lease** *ipaddr* **force-available**コマンドを使用するなど) この問題を解決する必要があります。

使用不可リースのタイムアウトの設定

で使用不可としてマークされているリースの処理 （37 ページ）説明したように、リースが使用不能になった時点では、すべての利用不可能なリースは構成された時間だけその状態のままになり、その後も再び利用可能になります。ポリシー属性(利用不可タイムアウト)は、この時間を制御します。*system_default_policy*ポリシーでは、既定でこの値を 1 日に設定します。

このタイムアウト機能を持たない Cisco Prime Network レジストラーの旧リリースからのアップグレードを処理するために、サーバー レベルで特別なアップグレードタイムアウト属性、アップグレード不可タイムアウト(1 日に事前設定されている)が含まれます。アップグレード不可タイムアウト値は、Cisco Prime Network レジストラーのアップグレード前に使用不可能に設定されたリースに与えられるタイムアウトです。この設定は、実行中のサーバーのみに影響し、

データベースの書き換えは行いません。サーバーが再ロードせずに1日稼働している場合、前回のリロード時に存在していたすべての利用不可能なリースはタイムアウトになります。サーバーが1日未満でリロードすると、次のリロードでプロセス全体が再開されます。このプロセスは、アップグレード前に使用不可能に設定されたリースに対してのみ行われます。アップグレード後に利用不可になったリースは、前述のように、ポリシーから利用不可タイムアウト値を受け取ります。

リースの照会

Cisco Prime Network レジストラーは、シスコのルータと連携して、プロビジョニング機能を強化できます。この機能は、CISCO プライムネットワーク レジストラーが準拠する DHCP リースクエリ仕様(RFC 4388)で説明されています。Cisco uBR アクセス コンセントレータ リレー エージェントの実装の一部は、DHCP リース要求および応答から情報を収集して収集することです。この情報は、次の用途に使用されます。

- 加入者ケーブル モデムとクライアント MAC アドレスをサーバーが割り当てた IP アドレスに関連付けます。
- アップストリーム データグラムの送信元 IP アドレスを確認します。
- DOCSIS ベースライン プライバシー プロトコルを通じてユニキャスト ダウンストリーム トラフィックを暗号化します。
- uBR とサブスクライバ ホストに負担をかける可能性があり、悪意のあるクライアントが侵害する可能性がある、ダウンストリーム アドレス解決プロトコル (ARP) 要求のブロードキャストを避けてください。

uBR デバイスは、グリーニングを通じてすべての DHCP 状態情報をキャプチャするわけではありません。uBR デバイスは、ユニキャスト メッセージ (特に更新およびリリース) から収集できません。また、このデータは uBR のリブートまたは置換の間で保持されません。したがって、uBR デバイスの DHCP 状態情報の唯一の信頼できるソースは、DHCP サーバー自体です。

このため、DHCP サーバーは、DHCPINFORM メッセージに似たメッセージをサポートします。アクセス コンセントレータおよびリレー エージェントは、DHCP サーバーから、DHCPv4 アドレスおよび DHCPv6 アドレスに対してクライアント ロケーション データを直接取得できます。

リースクエリの実装

Cisco プライムネットワーク レジストラーは、次の 3 つのリースクエリ実装を提供します。

- DHCPv4 以前の RFC 4388 用のシスコ独自仕様DHCPv4 の 事前 RFC リースクエリ （40 ページ）
- RFC 4388 に準拠する DHCPv4 - 「」を参照してください。DHCPv4 の RFC 4388 リースクエリ （41 ページ）
- DHCPv6：「DHCPv6 のリースクエリ （42 ページ）」を参照

DHCPv4 のシスコ独自の実装と最新の RFC 準拠の実装は、わずかな方法でしか異なっており、共存します。DHCP サーバーは、同じポートで Leasequery 要求を受け入れ、両方の実装に指定されたデータを返します。DHCPv6 の実装は、RFC 5007 および RFC 5460 に準拠しています。

DHCP サーバーは、DHCPv4 および DHCPv6 のリースクエリ応答にリース予約データを含めることができます。Cisco Prime Network レジストラーは、予約済み DHCPv4 のデフォルトリース時間 (31536000 秒) を返し、応答で DHCPv6 リースのリースの有効期間を返します。IP アドレスが実際にリースされている場合、Cisco Primeネットワーク レジストラーは残りのリース時間を返します。

リースクエリは、すべての実装で有効にするように事前設定されています。それを無効にするには、エキスパートモード属性を無効にします。

DHCPv4 の 事前 RFC リースクエリ

リースクエリ メッセージには、通常、要求フィールドとオプションが含まれます。例として、リレー エージェントの再起動または交換後に、リレー エージェントがパブリック ブロードバンド アクセス ネットワークにダウンストリームのデータグラムを転送する要求を受信したとします。リレーエージェントはダウンストリーム ロケーションデータを持たなくなったため、リレー エージェントのゲートウェイ IP アドレス (*giaddr*) と、ターゲット クライアントの MAC アドレスまたは*dhcp* クライアント識別子(オプション 61) を含む DHCP サーバーに LEASEQUERY メッセージを送信します。DHCP サーバーは、クライアントを検出すると、クライアントの IP アドレスを leasequery への応答のクライアント アドレス (*ciaddr*) フィールドに返します。サーバーがクライアント アドレスを見つけられない場合は、DHCPNACK を返します。

DHCPv4 の事前 RFC 実装では、リクエスタは IP アドレス、クライアント ID オプション (61)、または MAC アドレスを問い合わせることができ、DHCPACK (返されたデータを含む) または DHCPNACK メッセージをサーバーから受信するか、サーバーがパケットをドロップします。要求に複数のクエリタイプが含まれている場合、DHCP サーバーは最初に見つかるクエリタイプに応答します。リクエスタからの*giaddr*値は、検索された*ciaddr*から独立しており、単にサーバーからの応答の戻り IP アドレスです。次の 3 つのクエリの種類があります。

- **IPaddress** ciaddr —要求パケットは ciaddr フィールドの IP アドレスを含**(**みます。 **)** DHCP サーバーは、そのアドレスを使用するために、最新のクライアントのデータを返します。*ciaddr*値を含むパケットは、MAC アドレス フィールド (*htype*、 *hlen*、および *chaddr*) または*dhcp* クライアント識別子オプションの値に関わらず、IP アドレスによる要求である必要があります。IP アドレスによるクエリは最も効率的な方法であり、最も広く使用されている方法であり、他の 2 つの方法は DHCP サーバーに負荷をかける可能性があります。
- *:* 要求パケットには *dhcp* クライアント識別子オプション値が含まれます。
  dhcp-client-identifier option (61) DHCP サーバーは、最後にアクセスされたクライアントの IP アドレス データを含む DHCPACK パケットを返します。要求が MAC アドレスを省略した場合、サーバーは、要求されたクライアント ID のすべての IP アドレスとデータを*cisco-leased-ip*オプション(関連付けられた *IP*とも呼ばれます)に返します。要求に MAC アドレスが含まれる場合、サーバーは*DHCP* クライアント識別子と MAC アドレスを IP アドレスのクライアントデータと照合し、そのデータを*ciaddr*フィールドまたは*cisco-leased-ip(*関連 *IP*とも呼ばれる)オプションに返します。

- : 要求パケットには、ハードウェア タイプ (htype) 、アドレス長 (hlen) 、およびクライアント ハードウェア アドレス (chaddr) フィールド、および空の ciaddr フィールドに MAC アドレスが含まれます。 **MAC address** サーバーは、応答パケットの*cisco* リース *IP(*関連付けられた *IP*とも呼ばれます)オプションの MAC アドレスのすべての IP アドレスと最新のリース データを返します。

RFC 前実装の DHCPメッセージ タイプオプション (53) の DHCPLEASEQUERY メッセージ番号は 13 です。この種類のメッセージをサポートしていないサーバーは、パケットをドロップする可能性があります。DHCPACK メッセージ応答には、*htype*、 *hlen*、および*chaddr*フィールドのリース所有者の物理アドレスが常に含まれます。要求に*ciaddr*が含まれている場合、返されるデータは常に*ciaddr*に基づいており、クライアント ID または MAC アドレスはベースにしません。

リクエスターは、アドレスに関する特定のオプションを要求するパラメーター要求リスト・オプション (55) を含めることができます。応答には、*dhcp-lease-time*オプション (51) と、クライアントが送信した*Relay-agent-info*オプション (82) の元の内容が含まれることがよくあります。サーバーがクライアントの有効なリースを検出しない場合、サーバーはオプション 51 を返さないため、リクエスタは有効なリースがあるかどうかを判断する必要があります。

サーバーからの DHCPACK には、次のリースクエリ オプションを含めることもできます。

- **シスコリース-*ip* (161)**- クライアントに関連付けられたすべての IP アドレスのデータ。関連付けられた *IP*オプション (および後で名前が変更された) とも呼ばれます。
- ***cisco* クライアントが要求したホスト名 (162)**:ホスト名オプション(12)またはクライアント *FQDN*オプション(81)でクライアントが要求したホスト名。要求されたホスト名は、RFC 4388 の実装で削除されました。
- ***cisco* クライアント-最後のトランザクション時間 (163)**:DHCP サーバーがクライアントに接続した最新の時間。

DHCPv4 の RFC 4388 リースクエリ

リースクエリは、2006年2月にDHCPv4の公式RFC 4388になりました。Cisco プライムネットワーク レジストラーは、RFC 4388 実装を前DHCPv4 の 事前 RFC リースクエリ （40 ページ）の RFC の実装と共に提供します (を参照) と、それらの間に競合はありません。ただし、RFC 4388 の実装には、いくつかの顕著な変更が含まれています。

- *DHCP* メッセージ タイプオプション (53) に含まれる DHCPLEASEQUERY メッセージ タイプは、メッセージ ID を 10 に変更し (ID 13 は DHCPLEASEACTIVE メッセージに与えられました)、応答メッセージは DHCPACK および DHCPNACK からより具体的に変更されました。
  - クエリの場合は 10 です。
  - 割り当てられていないアドレスの応答に対する DHCPLEASEUNASSIGNED (11)
  - 不明なアドレスの応答に対しては、DHCPLEASEUNKNOWN 不明 (12)
  - アクティブ・アドレスの応答に対する DHCPLEASEACTIVE (13)
- 応答オプション名と ID が変更され、*cisco* クライアントが要求した *host-name*オプションがドロップされ、応答オプションが 2 つしかないようになっていました。

- **クライアント最終トランザクション時間 (91)**:DHCP サーバーがクライアントに接続した最新の時間。
- **関連付け-*ip* (92)**—クライアントに関連付けられているすべての IP アドレスのデータ。

- クライアント ID または MAC アドレスによる照会の場合、要求には*dhcp* クライアント識別子オプション (61) または MAC アドレスのみを含めることができます。パケットに両方が含まれている場合、サーバーはそれをドロップします。

DHCPv6 のリースクエリ

Cisco プライム ネットワーク レジストラーは、RFC 5007 (UDP) と RFC 5460 (TCP、バルク) DHCPv6 の両方のリースクエリ機能

（注） RFC 5460 (TCP、一括) リースクエリ サポートを使用するには、IPv6 用のDHCP リスナーの設定 （63 ページ）DHCP リスナを作成する必要があります (を参照)。

DHCPv6 リースクエリのメッセージタイプは次のとおりです。

- LEASEQUERY (14)
- LEASEQUERY_REPLY (15)
- LEASEQUERY_DATA (17)
- LEASEQUERY_DONE (16)
- 240)

クエリは次の方法で行うことができます。

- QUERY_BY_ADDRESS (1)
- QUERY_BY_CLIENTID (2)
- QUERY_BY_RELAY_ID(3)
- QUERY_BY_LINK_ADDRESS(4)
- QUERY_BY_REMOTE_ID(5)

DHCPv6 LEASEQUERY_REPLYメッセージには、以下のオプションを 1 つ以上含めることができます。

- ***lq-query* (44)**—クエリが実行されています。要求でのみ使用されるオプションには、クエリの種類、リンク アドレス (0::0)、およびクエリに必要なデータを提供するオプションが含まれます。
- **クライアント データ (45)**- 単一のリンク上の単一のクライアントのデータをカプセル化します。クライアントデータには、これらのオプションまたはその他の要求されたオプションをいくつでも含めることができます。
- ***clt-time* (46)**—クライアント データ オプションにカプセル化されたクライアントの最後のトランザクション時間 (45);は、サーバーがクライアントと最後に通信した時間 (秒単位) を示します。

- ***lq-relay-data* (47)**—クライアントが最後にサーバーと通信したときに使用されるリレーエージェント データ。フィールドはピア アドレスとリレー メッセージです。このオプションには、さらにオプションを含めることができます。
- ***lq-client-link* (48)**—クライアントがバインディングを持つリンク。リンク アドレスが省略され、クライアントが複数のリンク上にあることが判明した場合に、クライアント クエリに対する応答で使用されます。
- ***option_lq_base_time***—バインド情報を送信した時点での DHCPv6 サーバーの現在の絶対時刻を指定します。

DHCPv6 LEASEQUERY_REQUESTメッセージには、以下のオプションを 1 つ以上含めることができます。

- ***option_lq_start_time***-指定した時間以降に更新されたバインド。このオプションは、オフライン期間中に発生したバインディング更新のリストに使用されます。
- ***option_lq_end_time***-指定された期間中に更新されたバインド。

DHCPv6 は、オプション要求オプション (*oro*) を使用して、リースクエリ応答のオプションのリストを要求します。

（注） クライアント ID による leasequery 要求では、[*v6-override-client-id*] 式を使用してクライアントのリースに関する情報を正しく取得する場合に、オーバーライドクライアント*ID*属性を指定する必要があります。

リースクエリの統計

リース クエリは、Web UI の[DHCP サーバーの統計情報] ページ (の「統計の表示」*Cisco Prime Network Registrar 11.1 Administration Guide*セクションを参照)、および CLI で**dhcp getStats**統計属性を提供します。リースクエリの統計は次のとおりです。

- **lease-queries**:指定された時間間隔で受信した RFC 4388 メッセージ ID 10 (または RFC 以前のメッセージ ID 13) DHCPv4 リースクエリ パケットの数。
- **lease-queries-active**: RFC 4388 DHCPLEASEACTIVE パケットの数。
- **lease-queries-unassigned**: RFC 4388 DHCPLEASEUN 割り当てパケットの数。
- **lease-queries-unknown**: RFC 4388 DHCPLEASEUNKNOWN パケットの数。
- **leasequeries**-受信した DHCPv6 リースクエリ パケットの数。
- **leasequery-replies**- 成功する場合と成功しない場合がある DHCPv6 リースクエリ パケットに対する応答の数。
- **tcp-current-connections**- DHCPv6 アクティブクエリおよびバルク リースクエリの DHCP サーバーへの現在開いている TCP 接続の数。
- **tcp-total-connections**- この時間間隔で DHCPv6 アクティブクエリおよびバルク リースクエリの DHCP サーバーに対して開かれた TCP 接続の数。

- **bulk-leasequeries**- この時間**bulk-leasequeries**間隔ですべての TCP 接続で受信した LEASEQUERY パケットの数。
- **bulk-leasequery-replies**- この時間間隔ですべての TCP 接続を介して送信された LEASEQUERY-REPLY パケットの数。
- **bulk-leasequery-data**- この時間間隔ですべての TCP 接続を介して送信された LEASEQUERY-DATA パケットの数。
- **bulk-leasequery-done**- この時間間隔ですべての TCP 接続を介して送信された LEASEQUERY-DONE パケットの数。
- **tcp-lq-status-unspec-fail**- この時間間隔で TCP を介して送信されるステータス コード UnspecFail(1) を持つ LEASEQUERY-REPLY パケットの数。
- **tcp-lq-status-unknown-query**: この時間間隔で TCP を介して送信される状態コードが不明なリースクエリ-応答パケットの数です。
- **tcp-lq-status-malformed-query**- この時間間隔で TCP を介して送信された、状態コードが異常である LEASEQUERY-REPLY パケットの数です。
- **tcp-lq-status-not-configured**- この時間間隔で TCP を介して送信される状態コードが未構成(9)の LEASEQUERY-REPLY パケットの数。
- **tcp-lq-status-not-allowed**-この時間間隔で TCP 経由で送信されるステータス コードが NotAllowed(10) の LEASEQUERY-REPLY パケットの数。
- **tcp-lq-status-query-terminated**: この時間間隔で TCP を介して送信された状態コードが[11]であるリースクエリ-応答/リースクエリ-DONEパケットの数。
- **tcp-connections-dropped**- DHCPv6 リクエスターによって TCP 接続がクローズ (またはリセット) されたために、この時間間隔で終了した TCP 要求の数。これは、通常の接続のクローズまたはサーバーの再ロードを除外します。
- **アクティブ リースクエリ**—この時間間隔内にすべての TCP 接続を介して受信される ACTIVELEASEQUERY パケットの数。
- **アクティブリースクエリ応答**-アクティブなリースクエリのこの時間間隔内にすべての TCP 接続を介して送信される LEASEQUERY-REPLY パケットの数。
- **アクティブ リース クエリ データ**-アクティブなリース クエリに対して、この時間間隔内にすべての TCP 接続を介して送信される LEASEQUERY-DATA パケットの数。
- **アクティブリースクエリ完了**-アクティブなリースクエリに対して、すべての TCP 接続を介して送信される LEASEQUERY-DONE パケットの数。
- **tcp-lq 状況データ欠落**-この時間間隔で TCP を介して送信される状態コード DataMissing(240) を持つ LEASEQUERY-REPLY パケットの数。
- **tcp-lq 状況キャッチアップ-完了**- この時間間隔で TCP を介して送信される状態コードが CatchUpComplete(241) の LEASEQUERY-DATA パケットの数。

リースクエリの例

次の例は、リンク アドレスがないクライアント ID による DHCPv6 UDP クエリのパケット トレースを示していますが、複数のリンクにアドレスが含まれています。出力の最初の部分はクエリ メッセージを示し、2 番目の部分は応答データを示します。*lq-query*オプションは、照会のタイプを識別します。要求のオプション要求オプション(*oro*)を使用して要求されたオプションのリストと、応答の*lq-client-links*オプションで返される 2 つのアドレスを確認します。

例: UDP リース クエリのパケット トレース

```
+- Start of LEASEQUERY (14) message (113 bytes)
| transaction-id 22
| lq-query (44) option (37 bytes)
| (query-type 2, link-address ::)
| client-identifier (1) option (10 bytes)
| 00:03:00:01:01:02:03:04:05:06
| oro (6) option (2 bytes)
| 47
| server-identifier (2) option (14 bytes)
| 00:01:00:01:13:06:6a:67:00:23:7d:53:e5:e3
| client-identifier (1) option (10 bytes)
| 00:03:00:01:01:03:05:07:09:11
| vendor-class (16) option (14 bytes)
| (enterprise-id 1760,
| ((00:08:41:49:43:20:45:63:68:6f)))
| vendor-class (16) option (14 bytes)
| (enterprise-id 1760,
| ((00:08:41:49:43:20:45:63:68:6f)))
+- End of LEASEQUERY message
+- Start of LEASEQUERY-REPLY (15) message (72 bytes)
| transaction-id 22
| server-identifier (2) option (14 bytes)
| 00:01:00:01:13:06:6a:67:00:23:7d:53:e5:e3
| client-identifier (1) option (10 bytes)
| 00:03:00:01:01:03:05:07:09:11
| lq-client-links (48) option (32 bytes)
| 2001:4f8:ffff:0:8125:ef1b:bdcb:4b4e,2001:4f8:ff00:0:e400:f92:1bfd:60fa
+- End of LEASEQUERY-REPLY message
```

次の例は、クライアント ID による DHCPv6 TCP クエリのパケット トレースを示しています。出力の最初の部分は要求メッセージを示し、2 番目の部分は最初のクライアントのバインディングデータを含む応答メッセージを示し、最後の部分はクエリが正常に終了したことを示します。返されるクライアントが複数ある場合、3 番目の部分は 2 番目の部分に続きます。

（注） リースクエリ-応答メッセージにバインディング データがない場合、パケットには LEASEQUERY-DONE メッセージは存在しません。

例: TCP リース クエリの例のパケット トレース

```
+- Start of LEASEQUERY (14) message (59 bytes)
| transaction-id 2
| lq-query (44) option (37 bytes)
| (query-type 2, link-address ::)
| client-identifier (1) option (10 bytes)
| 00:03:00:01:01:02:03:04:05:06
| oro (6) option (2 bytes)
| 47
| client-identifier (1) option (10 bytes)
| 00:03:00:01:01:03:05:07:09:11
+- End of LEASEQUERY message

+- Start of LEASEQUERY-REPLY (15) message (162 bytes)
| transaction-id 2
| server-identifier (2) option (14 bytes)
```

```
| 00:01:00:01:13:06:6a:67:00:23:7d:53:e5:e3
| client-identifier (1) option (10 bytes)
| 00:03:00:01:01:03:05:07:09:11
| client-data (45) option (122 bytes)
| client-identifier (1) option (10 bytes)
| 00:03:00:01:01:02:03:04:05:06
| clt-time (46) option (4 bytes)
| 5m54s
| iaaddr (5) option (24 bytes)
| (address 2001:4f8:ffff:0:8125:ef1b:bdcb:4b4e,
| preferred-lifetime 6d23h54m6s,
| valid-lifetime 1w6d23h54m6s)
| lq-relay-data (47) option (68 bytes)
| peer-address fcc0:a803::214:4fff:fec1:226a
| +- Start of RELAY-FORW (12) message (52 bytes)
| | hop-count 0,
| | link-address 2001:4f8:ffff::,
| | peer-address fe80::302:3ff:fe04:506
| | vendor-class (16) option (14 bytes)
| | (enterprise-id 1760,
| | ((00:08:41:49:43:20:45:63:68:6f)))
| +- End of RELAY-FORW message
+- End of LEASEQUERY-REPLY message
+- Start of LEASEQUERY-DATA (17) message (130 bytes)
| transaction-id 2
| client-data (45) option (122 bytes)
| client-identifier (1) option (10 bytes)
| 00:03:00:01:01:02:03:04:05:06
| clt-time (46) option (4 bytes)
| 5m33s
| iaaddr (5) option (24 bytes)
| (address 2001:4f8:ff00:0:e400:f92:1bfd:60fa,
| preferred-lifetime 6d23h54m27s,
| valid-lifetime 1w6d23h54m27s)
| lq-relay-data (47) option (68 bytes)
| peer-address fcc0:a803::214:4fff:fec1:226a
| +- Start of RELAY-FORW (12) message (52 bytes)
| | hop-count 0,
| | link-address 2001:4f8:ff00::,
| | peer-address fe80::302:3ff:fe04:506
| | vendor-class (16) option (14 bytes)
| | (enterprise-id 1760,
| | ((00:08:41:49:43:20:45:63:68:6f)))
| +- End of RELAY-FORW message
+- End of LEASEQUERY-DATA message

+- Start of LEASEQUERY-DONE (16) message (4 bytes)
| transaction-id 2
+- End of LEASEQUERY-DONE message
```

TCP バルク リースクエリと UDP リースクエリの違い

TCP バルク リースクエリと UDP リースクエリの違いは次のとおりです。

- UDP リースクエリは、IPv6 アドレスによるクエリとクライアント識別子によるクエリをサポートしています。ただし、TCP 一括リースクエリは 5 つのクエリタイプをすべてサポートします。つまり、IPv6アドレスによるクエリ、クライアント識別子によるクエリ、リレー識別子によるクエリ、リンク アドレスによるクエリ、およびリモート ID によるクエリです。

- UDP Leasequery では、サーバーが複数のリンク上のリレー エージェントのバインディングを検出した場合、DHCP サーバーは応答メッセージにOPTION_CLIENT_LINKオプションを送信します。リレー エージェントは、返された各リンク アドレスを使用してLEASEQUERY メッセージを再送信し、すべてのクライアントのバインディングを取得する必要があります。TCP一括リースクエリでは、サーバーは異なるリンク上のクライアントの複数のバインディングを返します。ただし、OPTION_CLIENT_LINKは、一括リースクエリの応答ではサポートされていません。

アドレス レポートとリース レポートの実行

IP アドレスとリースに関する次のレポートを実行できます。

- **アドレスの使用法**-「」を参照してください。アドレス使用状況レポートの実行 （47 ページ）
- **リース履歴**-参照IP リース履歴の実行 （47 ページ）
- **現在の使用状況**：「リース使用率レポートの実行 （54 ページ）」を参照
- **リース通知**— 「」を参照してください。リース通知の受信 （55 ページ）

アドレス使用状況レポートの実行

アドレス使用状況レポートには、リースが割り当てられている IP アドレスが表示されます。

ローカル アドバンスド Web UI

IP アドレスのリースを表示するには、[DHCP スコープの編集] ページ**Design**(メニューの**Scopes[DHCPv4]**サブメニューの下で選択) をクリックし、スコープの**[DHCP**リースの一覧] タブを開きます。特定のリースを管理するには、ページで該当する IP アドレスをクリックします。

CLI コマンド

指定したサーバーの IP アドレスの使用状況を表示**report**するには、 を使用します。

ヒント　まだ自動化された方法で使用**lease-notification**していない場合は、サーバーの**lease-notification available=100%**状態のスコープごとの簡潔な概要を試してください。

IP リース履歴の実行

特定のデータベースから IP リース履歴データを抽出して、特定の IP アドレスの過去の割り当て情報を確認することができます。クライアントがリースを発行した時間、クライアントまたはサーバーがリースの期限切れ前にリリースした時間、およびサーバーがリースを更新したか

どうか、およびどのくらいの期間をクライアントがリースを発行したかの履歴ビューを取得できます。

Cisco プライムネットワーク レジストラーは、IP 履歴データのクエリを制御するクライアントを提供します。このクライアントを使用すると、次のことができます。

- 特定の時間の間に特定の IP アドレスに関連付けられた MAC アドレスを取得します。
- IP 履歴データベース全体をカンマ区切りファイルとして参照してください。
- リース履歴の属性 (リース履歴の詳細レポート) を表示するIP リース履歴の照会 （49 ページ）- を参照してください。

レコードの IP 履歴データベースをトリミングするために、データベースのサイズが限界なく拡大しないようにするには、追加の管理機能を使用する必要があります。

（注） 既存のリースの状態が変更された場合 (予約済み IP アドレスとして構成されている場合や、非アクティブ化された場合など)、その変更は地域でのリース履歴の変更として表示されません。詳細コレクションが無効になっている場合、リース履歴の変更は、リースがリース済みからリースされていない状態に遷移するか、別のクライアントに割り当てられている場合にのみ表示されます。

ローカル クラスタでのリース履歴録音の有効化

ローカル クラスタ DHCP サーバーのリース履歴記録を明示的に有効にする必要があります。DHCP サーバーは、IP 履歴記録エラーを通常の DHCP ログ ファイルに記録します。

ローカルクラスタでリース履歴が有効になっている場合、サーバーのパフォーマンスとリース状態データベースのサイズに影響します。リースが終了(有効期限が切れたり解放されたり)するたびに、リース用の履歴レコードが作成されます。クライアントが長期間にわたって更新するリースでは、履歴レコードは作成されません。各リース履歴レコードのサイズは多くの要因に依存しますが、1 レコードあたり約 1 KB の見積もりが適しています。リースが終了するレートとリース履歴が保持される期間によっては、リース履歴レコードの数が多く作成され、かなりのディスク領域が必要になる可能性があります。これは、アクティブなリースに必要なスペースよりも多くの注文が大きくなる可能性があります。

ローカル アドバンスド Web UI

リース履歴の記録を有効にするには、次の手順を実行します。

ステップ 1 メニューから**DeployDHCPServer[DHCP]**サブメニューの下で選択し、[DHCPサーバーの管理]ページを開きます。

ステップ 2 [DHCP**Local DHCP Server**サーバー] ペインで をクリックします。

ステップ 3 [ローカル DHCP サーバーの編集] ページで、リース履歴属性を探します。

- *Lease History (ip-history)*：v4 のみ（DHCPv4）、v6 のみ（DHCPv6）、またはその両方のリース履歴データベースを有効または無効にします。
- *ip-history-max-age*：収集するリース履歴の最大経過期間。リース履歴が v4 のみに設定されている場合、v6 のみ、または両方の DHCP サーバーが定期的にリース履歴レコードを調べ、この経過時間のしきい値より古いリース履歴バインドを持つレコードを削除します。

ステップ 4 **Save** をクリックします。

ステップ 5 サーバーをリロードします。

CLI コマンド

リース履歴の記録を有効にするには、 を使用**dhcp set ip-history=<value> (v4-only, v6-only, both, or disable)**して IP アドレスの IP (リース) 履歴の記録を明示的に有効にする必要があります。

IP リース履歴の照会

リースを取得したら、その履歴を照会できます。IP リース履歴は、ローカル または地域のクラスターから照会できます。DHCP サーバーを含むローカル クラスターを地域クラスターの一部としてセットアップし、地域クラスターからのリース履歴データのポーリングを有効にします (の「リース履歴収集の有効化」セクション*Cisco Prime Network Registrar 11.1 Administration Guide*を参照)。

地域クラスター Web UI のクラスターのポーリング基準は、「 」の「ポーリング使用率およびリース履歴データ」セクションで説明されている属性を使用して調整できます。 *Cisco Prime Network Registrar 11.1 Administration Guide*

また、リース履歴データのクエリの選択基準も、以下のセクションで説明します。

ローカル アドバンスドおよびリージョン アドバンスド Web UI

IPv4 リース履歴を照会するには、次の手順を実行します。

ステップ 1 メニューから**Operate**[**レポート**]**DHCPv4 Lease History**サブメニューの下で[DHCPリース履歴検索]ページを開きます。

（注） ローカルの詳細 Web UI の [検索（Search ）] ボタンを使用して、[DHCP リース検索（DHCP Lease Search）] ページに移動できます。このボタンを使って、リース履歴の検索ページとアクティブ リースの検索ページを切り替えられます。

ステップ 2 ドロップダウン リストから [フィルター] 属性と [タイプ] を選択し、[値] フィールドで選択したフィルター タイプの値を入力します。

ステップ 3 **Search** をクリックし、リースの一覧を表示します。

ローカル アドバンスドおよびリージョン アドバンスド Web UI

IPv6 リース履歴を照会するには、次の手順を実行します。

ステップ 1 メニューから**Operate**[レポート]**DHCPv6 Lease History**サブメニューの下で[DHCP v6 リース履歴検索]ページを開きます。

（注） ローカルの詳細 Web UI の [検索（Search ）] ボタンを使用して、[DHCP リース検索（DHCP v6 Lease Search）]ページに移動できます。このボタンを使って、リース履歴の検索ページとアクティブリースの検索ページを切り替えられます。

ステップ 2 ドロップダウン リストから [フィルター] 属性と [タイプ] を選択し、[値] フィールドで選択したフィルタータイプの値を入力します。

ステップ 3 **Search** をクリックし、リースの一覧を表示します。

（注） 地域サーバーは、最新のポーリングと同じ最新のリース履歴のバージョンのみを検索します。最新のデータの場合、最新のリース履歴データを取得するために、地域の明示的なリース履歴ポーリングを実行する必要があります。

iphist ユーティリティの使用

ユーティリティを使用して、ローカルおよび地域クラスタの IP 履歴データベースを照会し、結果を標準出力またはファイルに**iphist**送ることができます。デフォルトの場所は次のとおりです。

/opt/nwreg2/local/usrbin

コマンド プロンプトで上記の場所に移動し、次の構文を使用してユーティリティを実行します。

iphist[オプション *]*{イパドル|**all**} [開始日 |**start** [終了日|**end**]]

IPアドレスは単一のアドレスまたはキーワード**all**であり、開始日は現地時間またはデータベースの最も早**start**い日付のキーワードで、終了日はデータベースの最後の日付のローカル時刻またはキーワード**end**です。ただし、ローカル時間を指定する**–l**オプションを使用しない限り、出力は既定でグリニッジ標準時 (GMT) に設定されます。

コマンド オプションの完全な一覧が下の表に表示されます。

***表 4 : iphist* コマンド オプション**

オプション	説明
–N *username*	管理者ユーザー名。省略すると、ユーザー名の入力を求められます。

オプション	説明
–P *password*	管理者パスワード。省略した場合は、パスワードを入力するように求められます。
–C *cluster* [**:***port*]	宛先サーバーとオプションの SCP ポート。
–6	出力 DHCPv6 リース
–a	リース属性の可視性 3 を表示します。
–f 形式	出力行の形式。デフォルトの形式は次のとおりです。**"address,client-mac-addr,binding-start-time,binding-end-time"**
–t	タイトル行として印刷形式を指定します。
–n *namespace*	アドレスの名前空間を指定します。
–o *file*	出力をファイルに送信します。
–l	デフォルトの UTC/GMT ではなく、現地時間で出力を表示します。
–i	指定した IPv6 アドレスを含むデリゲートされたプレフィックスの出力 **–**を表示します (6 のみ)。
–s{自己|パートナー}	リースを自己またはパートナーに制限します。
–v	出力バージョンを表示します。
–zデバッグ引数	デバッグ出力レベルを設定します。

日付では次の構文を使用できます (スペース文字を含める場合は引用符が必要です)。

- 月/日/年@時間:分:秒(例えば、8/28/2007@10:01:15)、時間オプション
- 月/日/年時:分:秒(例えば、"8/28/2007 10:01:15")、時間オプション
- 月の日の時間:最小:秒年(例えば、8月 28 10:01:15 2007)、秒オプションで
- キーワード**start**、 **end**、 **now** 、または (現在の時刻の場合)

日付フィルターは、その間にアクティブだったリースに出力を制限することを目的としています。つまり、開始日より前に終了しない限り、指定した開始日より前に開始できます。また、指定した終了日以降は開始できません。たとえば、次のコマンドを呼び出します。

```
# ./iphist -N user -P password all "Aug 28 00:00 2008" "Dec 31 23:59:59 2008"
```

次のリースの場合。

リース 1	Begin	2008 年 1 月 1 日	終了（End）	2008 年 6 月 30 日
リース 2	Begin	2008 年 3 月 10 日	終了（End）	2008年9月01日
リース 3	Begin	2008年6月01日	終了（End）	2008年9月30日

リース 4	Begin	2009 年 1 月 1 日	終了（End）	2009 年 3 月 10 日

リース 2 とリース 3 は、どちらもクエリの指定された開始日の後に終了するため、リース 2 とリース 3 のみを返します。他の 2 つは、指定された開始日より前に終了するか、クエリの指定された終了日より後に開始されるため、範囲外です。

各行の値は、DHCP サーバーが格納する特定のリース オブジェクトによって異なります。*format* コマンドを使用して、含める**iphist–f**値を指定できます。

*format*引数は、出力行のテンプレートを提供する名前をコンマで区切った引用符で囲まれたリース属性名のリストです。デフォルトの出力は*ipaddress*、クライアント-*mac-addr*、バインディング開始時、バインディング終了時です。

次に例を示します。

```
# ./iphist -f "address,client-mac-addr,binding-start-time,binding-end-time" all
```

出力は、オペレーティングシステムに適した改行シーケンスで終了する行のシーケンスです（UNIX では \n）。各行には、単一のリース レコードにデータが含まれます。行の形式は、通常、引用符で囲まれたコンマ区切り値です。引用符の内側にリテラルの円記号 (\) または引用符 (") を使用するには、前に 1 つのバックスラッシュ (\) を付けます。属性の新しい行は**\n**として印刷されます。

次の表は、出力に含めることができる一般的なリース オブジェクト属性の一部を示しています。また、コマンドのヘルプも**lease**参照してください。完全なリストを取得するには、**iphist -a**を使用します。

表 *5: IP* 履歴クエリの出力属性

リース属性	説明
address	リースの IP アドレス。
binding-start-time	リース バインドの開始時刻。
binding-end-time	リース バインドの終了時刻。
client-binary-client-id	クライアントの MAC アドレスのバイナリ形式。
client-dns-name	DHCP サーバーによって認識されるクライアントの最新の DNS 名。
client-domain-name	クライアントが存在するドメイン。
client-flags	クライアント フラグの数。
client-host-name	クライアントが要求したホスト名。
client-id	クライアントが要求したクライアント ID またはクライアント用に合成されたクライアント ID。
client-last-transaction-time	クライアントがサーバーに最後に接続した日時です。

リース属性	説明
client-mac-addr	クライアントが DHCP サーバーに提示した MAC アドレス。
client-os-type	リースされたクライアントのオペレーティングシステム。
expiration	リースが期限切れになった日付と時刻。
フラグ（*Flags*）	予約済みまたは非アクティブ化。
lease-renewal-time	クライアントがリース更新を発行する予定の時間を最小限に抑えます。
lease-rebinding-time	クライアントが再バインド要求を発行する予定の最小時間。
relay-agent-circuit-id	回線 *ID*サブオプション (1) の内容。
relay-agent-option	最新のクライアント対話からのオプションの内容。
relay-agent-remote-id	リモート *ID*サブオプションの内容 (2)。
relay-agent-server-id-override	サーバー IDオーバーライド・サブオプションの IP アドレス。
relay-agent-subnet-selection	サブネット選択サブオプションの IP アドレス。
relay-agent-vpn-id	*vpn-id*サブオプションの内容。
start-time-of-state	リースの状態が変更された日時です。
state	使用可能な、期限切れ、リース、提供、または使用不可のいずれか。
vendor-class-id	クライアントが要求したベンダー クラス ID。
vpn-id	VPN の識別子 (存在する場合)。

リース履歴データのトリミング

リージョン クラスターで IP 履歴トリミングを有効にした場合、IP 履歴データベースは自動的にトリミングされ、ディスク領域を再利用できます。各履歴レコードには有効期限があります。DHCP サーバー自体、および履歴データの DHCP サーバーをポーリングする CCM 地域サーバーには、トリミングが必要です。

CCM サーバーは、一定の期間を経過したリース履歴データを一定の間隔でトリミングする、地域クラスターでバックグラウンドトリミングを実行します。トリミング間隔はデフォルトで 24 時間に設定され、年齢 (トリミング前にどのくらいさかのぼるか) は 24 週に設定されます。ローカル クラスタの DHCP サーバーは、毎日自動トリミングを実行し(現地時間の午前 3 時)、デフォルトで 4 週間のデータを格納します。

リージョン Web UI

リース履歴データをトリミングするには、中央の構成管理者である必要があります。

ステップ 1 **Operate** メニューの [サーバー（Servers）] サブメニューの下から **Manage Servers** を選択し、[サーバーの管理（Manage Server）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ウィンドウの **CCM**をクリックして、[ローカルCCMサーバーの編集（Edit Local CCM Server）] ページを開きます。

ステップ 3 [リース履歴の設定（Lease History Settings）] セクションで次の属性（入力する値には **s**、**m**、**h**、**d**、**w**、**m** または **y** 接尾辞を使用可能）を設定します。

- *lease-hist-trim-interval*：古いリース履歴データを自動的にトリミングする頻度（デフォルトは毎日）。0 に設定すると、自動的にリースがトリミングされません。境界値は 0 ～ 1 年です。
- *lease-hist-trim-age*：*lease-hist-trim-interval* が 0 に設定されていない場合に古いリース履歴データを自動的にトリミングするのに遡る期間（デフォルトは 24 週間）。境界値は 1 日から 1 年です。

ステップ 4 即時トリミングを強制するには、ページの下部にある [トリム/コンパクト入力（Trim/Compact Inputs）] セクション（圧縮はDHCP使用率データでのみ使用可能）を見つけます。トリム/コンパクト年齢を希望の値に設定します。この期間は、リース履歴データをトリミングするのにどのくらいの時間が経過します。この値に対する境界はありません。ただし、非常に小さい値(1m など)を設定すると、最新のデータをトリミングまたは圧縮しますが、これは望ましくない場合があります。実際、ゼロに設定すると、収集されたデータがすべて失われます。値を大きくし過ぎる (10y など) に設定すると、データのトリミングや圧縮が行えなくなる可能性があります。

ステップ 5 すぐにトリミングする場合は、 を**Trim All Lease History**クリックします。

*IP-history-max-age*属性を設定することで、DHCP サーバー自体が実行するトリミングを調整できます。*ip-history*が設定されている場合、DHCP サーバーは、リース バインディングの変更に応じて、時間の経過と同時にデータベース レコードを蓄積します。このパラメーターは、データベースに保持される履歴レコードの経過時間の制限を設定します。サーバーは定期的にリース履歴レコードを調べ、このパラメーターに基づいて経過時間のしきい値を設定し、しきい値より前に終了したバインディングを表すレコードを削除します。プリセット値は 4 週間です。

リース使用率レポートの実行

リース使用率レポートには、アドレスブロック、サブネット、およびスコープの現在の使用率が表示されます。両方のユーザー インターフェイスについては使用率履歴レポートの生成、「」を参照してください。

ローカル アドバンスド Web UI

アドレス・スペース機能のページから、アドレス・ブロック、サブネット、およびスコープの現在の使用率を表示します。

CLI コマンド

リース使用率レポートを表示するには、**report**を使用します。

リース通知の受信

CLIは、使用可能なIPアドレスの数が特定のしきい値以下の場合に通知を送信する機能を提供します。この**lease-notification**コマンドは、使用可能なリースの数が特定のしきい値に達した場合または下回った場合に通知が発生するタイミングを、使用可能な属性を使用して指定します。レポートをユーザーに電子メールで送信できます。対話的にコマンドを使用できますが、主にUNIX**cron** タスクなどの自動化された手順で使用します。

次の例では、リース通知を examplescope の空きアドレスが 10% に落ちたときの設定を行います。特定の Windows メール ホストで、受信者のビリー、ジョー、および Jane にレポートを送信します。

```
nrcmd> lease-notification available=10% scopes=examplescope recipients=billy,joe,jane
mail-host=mailhost
```

出力は、説明ヘッダー、空きアドレスの数がしきい値以下の各スコープの行を含むテーブル、および要求されたスコープとクラスターに関連する可能性のある警告で構成されます。

Cisco プライムネットワーク レジストラーでは、特に指定しない限り、デフォルトでデフォルト クラスタと .nrconfig ファイルが使用されます。コマンドの構文については、コマンドのヘルプを**lease-notification**参照してください。

リース通知を自動的に実行する

cron(1)コマンドを実行するコマンドを**crontab(1)**に指定することで、**定期的にリース通知**を実行することができます。

crontabに指定したこの例では、月曜日から金曜日までの 00:15 および 12:15 (午前 0 時と正午の 15 分後) に**リース通知**を実行します (これは単一のコマンド ラインを含みます)。

```
15 0,12 * * 1-5 . .profile; /opt/nwreg2/local/usrbin/nrcmd lease-notification
available=10\% config=/home/jsmith/.nrconfig addresses=192.32.1.0-192.32.128.0
recipients=jsmith,jdoe@example.com >/dev/null 2>&1
```

UNIX の**crontab -e**コマンドを実行して、**クロンタブ**編集を実行できます。**ed(1)**を使用する場合を除き、コマンドを実行する前にEDITOR環境変数を設定します。詳細については、**crontab(1)**のマニュアルページを参照してください。

crontabコマンド行でCLIコマンドの絶対パスを指定する必要があることに注意してください。どの**nrcmd**コマンドを使用して、ご使用の環境の完全なパスを判別できます。

また、**crontab**を使用してリース通知**コマンド**を実行すると、**nrcmd**コマンドは、CNR_CLUSTER、CNR_NAME、およびCNR_PASSWORDのユーザー環境変数を無視します。他のビューアは実行中のコマンドを表示できるため、セキュリティ上の理由から、コマンドラインの**-P**オプションを使用してパスワードを指定しないでください。

crontab -eを実行しているユーザーのホーム ディレクトリ内の .profile またはその他のファイルから**nrcmd**コマンドを実行するクラスターのクラスター名、ユーザー、およびパスワードの情報を指定します。次に例を示します。

```
CNR_CLUSTER=host1
export CNR_CLUSTER
CMR_NAME=admin1
export CNR_NAME
CNR_PASSWORD=passwd1
export CNR_PASSWORD
```

。**crontab**エントリの .profile 指定は、ファイルを明示的に読み取ります。最初のドット (.) は、ファイルを読み取るシェルコマンドで、少なくとも 1 つのスペース文字を使用してそれに従う必要があります。**nrcmd**が実行されている場所とは異なるクラスター (またはクラスター) で通知する場合は、次の情報を指定します。

- クラスタを使用して構成ファイルをチェックインしますリース通知用の設定ファイルの指定 （56 ページ）(を参照)。
- このセクションの冒頭にあるサンプル**の crontab**項目のように完全に指定されたパス。

chmod go-rwx *config-file* UNIX コマンドを使用してアクセス権を変更することにより、他のユーザーが作成した .profile および構成ファイルの内容を調べたり変更したりできないようにすることができます。

リース通知用の設定ファイルの指定

構成ファイルを省略する場合は**lease-notification**、現在のディレクトリ、ホームディレクトリ、最後に /var/nwreg2/{local | regional}/conf ディレクトリで既定の .nrconfig ファイルを探します。Cisco プライムネットワーク レジストラーは、最初に検出されたファイルを使用します。ファイルの各行は、文字 # (コメント)、角かっこで囲まれたセクション ヘッダー、またはパラメーターと値のペアまたはその継続で始まる必要があります。Cisco プライムネットワーク レジストラーは、各行から先頭のスペース文字を取り除き、空白行を無視します。

動的リース通知

DHCPv4 および DHCPv6 動的リース通知機能により、外部クライアント アプリケーションは DHCP サーバーの IP アドレス バインディング アクティビティに関する更新を受信できます。この機能を使用すると、特定のリースアクティビティが発生したときに、リースアクティビティを使用して外部データベースを更新したり、合法的傍受などのアクションをトリガしたりできます。

（注） 動的リース通知は、現在のリース状態情報のみを提供します。すべてのリース状態の変更が報告されることを保証するものではありません。DHCP サーバーへの接続がダウンまたは輻輳状態の場合など、特定の条件下でリース状態の変更が失われます。

動的リース通知機能は、追加機能をサポートするためにDHCPサーバーを拡張し、サンプルクライアント(Javaで書かれている)を含み、リース状態情報をMySQLデータベースに格納して機能を示します。

動的リース通知の使用

動的リース通知を使用するには:

1. ローカル クラスターにdhcp リスナ オブジェクトを作成する必要があります。dhcp リスナオブジェクトは、サーバーが着信TCP接続をリッスンするポートと、これらの接続のその他DHCP リスナーの設定 （63 ページ）の属性を指定します(を参照)。DHCP リスナー オブジェクトを作成した後、DHCP サーバーを再ロードする必要があります。
2. 動的リース通知クライアントは、DHCPサーバーとのTCP接続を確立し、次のいずれかの要求を行う必要があります。
   - 一括リースクエリ- この要求は、特定の時点以降に状態が変化したDHCPサーバー内のすべてのリースの現在の状態を取得するために行われます。時間が指定されていない(または、時刻にゼロが指定されている)とき、すべてのリースの現在の状態が送信されます。これは、DHCPサーバーが1つの要求に応答してクライアントにすべてのリースを配信する点が異なる点を除いて、UDPベースのDHCPv4リースクエリ(RFC 4388)とDHCPv6リースクエリ(RFC 5460)に似ています。通常、バルク リースクエリは、外部データベースを初期化するために使用されます。また、アクティブなリースクエリが何らかの中断を起こした後、そのデータベースを最新の状態にする場合にも使用されます。
   - アクティブリースクエリ: この要求は、DHCPサーバーが行うすべての今後の重要なリース変更に対するリース状態情報を取得するために行われます。DHCPサーバーが重要なリース状態情報をデータベースに書き込む場合、リース状態情報はTCP接続を介して送信されます。
   - アクティブ リース クエリ(キャッチアップ付き)- この要求は、将来のリース状態の変更と、最近変更されたリースの最新データを取得するために行われます。動的リース通知クライアントは、動的リース通知クライアントやDHCPサーバーの再起動時など、接続損失の短い期間に失われた最近変更されたリースの最新データを取得できます。キャッチアップを伴うアクティブなリースクエリは、リースの現在の状態のみをフェッチします。これは、見逃した可能性のあるすべての中間リース状態変更に関するデータをフェッチしません。

DHCPサーバーは、リースクエリ メッセージのストリームで、リース状態情報を動的リース通知クライアントに送信します。バルク リースクエリの場合、DHCPサーバーが処理する時間が与えるとすぐにリース状態情報が送信されます。アクティブなリースクエリの場合、リース状態の変更が発生すると、リース状態情報が送信されます。動的リース通知クライアントは、これらのメッセージを処理して、データベースの更新などの適切なアクションを実行できます。

（注） DHCPサーバーは複数の動的リース通知クライアントをサポートしていますが、複数のクライアントがDHCPサーバーのリースパフォーマンスに影響を与える可能性があるので、クライアント数を最小限に抑えることをお勧めします。

フェールオーバー構成では、DHCPクライアントと対話するアクティブフェールオーバーパートナーのみが、動的リース通知クライアントに対して、アクティブな leasequery 要求を使用して動的リース通知の更新を送信します。したがって、完全な情報を受信するには、動的リース通知クライアントが両方のフェールオーバー パートナーに接続する必要があります。

サーバーは、dhcp リスナの*leasequery-send-all*属性に基づいて、アクティブなリースクエリ通知のキューにリースが登録されているかどうかを判断します。この属性が有効になっている場合、DHCPサーバーは常にアクティブなリースクエリ クライアントに通知を送信します。この属性が無効または未設定の場合、DHCP サーバーは、アクティブな leasequery クライアントで正確な状態を維持するために必要な通知のみを送信します。

また、エクステンションを使用してリースクエリ通知を制御することもできます。拡張機能は、アクティブリースクエリ制御要求および応答データディクショナリ項目を使用して、アクティブな*leasequery*通知用にリースがキューに入拡張ポイントの使用れられていないかどうかを決定できます。

リース通知クライアントの例

Cisco プライム ネットワーク レジストラーは、スタンドアロンのサンプル Java クライアントを提供します。スタンドアロンのサンプル Java クライアントは、1 つ以上の DHCP サーバーからリース状態データを収集し、最新のリース データで SQL データベースを更新します。サンプルの Java クライアントは、両方のフェールオーバー パートナーからのリース状態の更新を受け入れ、最新のリース状態情報が SQL データベースに含まれることを確認するように設計されています(更新が正しい順序で受信された場合でも)。サンプルJavaクライアントを使用する場合、バルクおよびアクティブなリースクエリ プロトコルの詳細を知る必要はありません。サンプル Java クライアントソースが提供されています。したがって、サンプルの Java クライアントがニーズを満たさない場合は、独自の実装ではなく、変更することをお勧めします。

サンプル Java クライアントは、すべてのリースの状態を取得するために初めてサーバーに接続するときに、バルク・リース照会を実行します。サンプル Java クライアントがサーバーと通信したことがある場合、キャッチアップを使用してアクティブなリースクエリを試行します。サンプル Java クライアントは、キャッチアップを伴うアクティブなリースクエリが、クライアントがしばらくダウンしていたか、DHCPサーバーが再ロードされた場合など、キャッチアップ データが使用できないという場合にのみ、バルク リースクエリを実行します。

サンプル Java クライアントは、複数の VPN および複数のサーバーを持つ構成をサポートしています。ただし、サンプルの Java クライアントでは、これらのサーバー間のリースは VPN および IP アドレスに関して一意であると想定しています。2 つのサーバーが VPN またはグローバル名前空間で同じ IP アドレスをリースしている場合、SQL データベースには 2 つのリースのうちの 1 つだけのレコードが含まれます。これは、フェールオーバー ペアではなく、2 つの

独立した DHCP サーバーに適用されます。また、SQL データベースを最新の状態に保つために、フェールオーバー ペアの両方のフェールオーバー パートナーと通信するようにサンプルの Java クライアントを構成する必要があります。

（注） サンプル Java クライアントは、インストール・パス/例/dhcp/cnrnotify.jar で入手できます。cnrnotify-readme.txt という名前のテキストファイルも、そのディレクトリに用意されており、最初に読み取る必要があります。

例/dhcp/cnrnotify.jar は、次の zip ファイルを含む zip ファイルです。

- サンプル Java クライアントソースコードと Javadoc ドキュメント。
- たとえば、lnc.properties ファイルと lnc6.properties ファイルを指定します。(使用可能なプロパティの詳細については、-listprops オプションを指定してクライアントを実行します。
- Cisco Prime ネットワーク レジストラー実装のための一括およびアクティブなリースクエリ インターネット ドラフト。
- Cisco Prime Network レジストラー専用リース情報に使用されるメッセージ値、オプションコード、ベンダー固有のデータを詳しいドキュメント。インターネット割り当て番号機関(IANA)は、バルクおよびアクティブリースクエリインターネットドラフトで使用されるメッセージおよびオプションコードにまだ値を割り当てていないため、Cisco Prime Network レジストラーで使用される値について説明します。

これらの項目を抽出するには、Winzip などの zip ツールを使用して cnrnotify.jar ファイルを開きます。(cnrnotify-readme.txt ファイルを参照してください)。Javadoc を抽出するには、次の使用をお勧めします。

```
jar xvf cnrnotify.jar docs_notify
```

上記のコマンドは、ドキュメントを抽出するために使用されます。

DHCPv4 サブサブ オプション コード

次の表は、DHCPv4 リースクエリの要求時に使用されるサブサブ オプション コードの一覧です。これらのコードは cnrnotify-プロトコル-numbers.txt ファイルに存在し、cnrnotify.jar zip ファイルで使用できます。

表 *6 : DHCPv4* サブ-サブ オプション コード

サブサブ オプション コード	オプション名	オプション タイプ
1	oro	サブサブ オプション番号の 1 バイト以上
2	状態	バイト
3	data-source	バイト
4	start-time-of-state	基準時間からの過去の期間
5	ベースタイム	絶対時間(1970年からの秒)

サブサブ オプション コード	オプション名	オプション タイプ
8	クライアント クラス名	文字列 (ゼロ終了なし)
9	パートナー-最終トランザクション時間	base-time からの経過時間
10 0xa	client-creation-time	base-time からの経過時間
11 0xb	制限 ID	制限 ID を含む blob
12 0xc	バインディング開始時刻	base-time からの経過時間
13 0xd	バインディング終了時刻	基準時からの将来/過去の期間を表す負/正の値
14 0xe	fwd-dns-config-name	文字列（0 で終了しない）
15 0xf	レブ・DNS-コンフィグ名	文字列（0 で終了しない）
16 0x10	client-override-client-id	クライアントのクライアント ID を含む blob
17 0x11	ユーザー定義データ	文字列（0 で終了しない）
18 0x12	scope-name	文字列（0 で終了しない）
19 0x13	フェールオーバー状態シリアル番号	4 バイト整数, ネットワークの順序
20 0x14	予約キー	blob、タイプバイトで始まる: • 0x2e、46: ゼロ終了なしの文字列 • 0x7、7:ブロブ
21 0x15	クライアント-prl	クライアントのパラメーター要求リスト、DHCPv4 オプション コードの BLOB

DHCPv6 サブサブ オプション コード

次の表は、DHCPv6 リースクエリの要求時に使用されるサブサブ オプション コードの一覧です。これらのコードは cnrnotify-protocol6-numbers.txt ファイルにも存在し、cnrnotify.jar zip ファイルで使用できます。

表 *7: DHCPv4* サブ-サブ オプション コード

サブサブ オプション コード	オプション名	オプション タイプ
1	oro	サブサブ オプション番号の 1 バイト以上

サブサブ オプション コード	オプション名	オプション タイプ
2	状態	バイト
3	data-source	バイト
4	start-time-of-state	基準時間からの過去の期間
5	ベースタイム	絶対時間(1970年からの秒)
8	クライアント クラス名	文字列 (ゼロ終了なし)
9	パートナー-最終トランザクション時間	base-time からの経過時間
10 0xa	client-creation-time	base-time からの経過時間
12 0xc	バインディング開始時刻	base-time からの経過時間
13 0xd	バインディング終了時刻	基準時からの将来/過去の期間を表す負/正の値
14 0xe	fwd-dns-config-name	文字列（0 で終了しない）
15 0xf	レブ・DNS-コンフィグ名	文字列（0 で終了しない）
16 0x10	検索キー	クライアントのクライアントIDを含むblob
17 0x11	ユーザー定義データ	文字列（0 で終了しない）
18 0x12	prefix-name	文字列（0 で終了しない）
19 0x13	フェールオーバー状態シリアル番号	4 バイト整数, ネットワークの順序
20 0x14	予約キー	blob、タイプバイトで始まる: • 0x2e、46: ゼロ終了なしの文字列 • 0x7、7:ブロブ
21 0x15	フェールオーバー パートナーの有効期間	base-time からの未来/過去の経過時間を表す負または正の値
22 0x16	フェールオーバー-次のパートナーの有効期間	base-time からの未来/過去の経過時間を表す負または正の値
23 0x17	フェールオーバーの有効期限	base-time からの未来/過去の経過時間を表す負または正の値

サブサブ オプション コード	オプション名	オプション タイプ
24 0x18	クライアントオロ	クライアントの ORO、 DHCPv6 の BLOB 2 バイト オプション コード

サンプル Java クライアントの要件

サンプル Java クライアントの要件は次のとおりです。

- JDK11
- JDK 11 の java.sql パッケージ。
- JDBC ドライバーと互換性のあるデータベースのインストール。データベースには、事前定義された列セットを含む特定のテーブルが存在する必要があります。

ヒント　テーブルが存在しない場合は、-cオプションを指定してクライアントを実行します。テーブルが作成されます。

MySQL の要件は次のとおりです。

- MySQL サーバーの最新バージョン。
- MySQL の JDBC コネクタ。
- サンプル Java クライアントの状況とエラーをログに記録するための log4j パッケージ。

（注）　MySQL-8.0.29 データベース、mysql-connector-java-8.0.29.jar、log4j-api-2.17.2.jar、および log4j-core-2.17.2.jar を使用することをお勧めします。

抽出され、lnc.properties ファイルが構成されたら、サンプルの Java クライアントを次の方法で実行できます。

ステップ 1　4 つの .jar ファイル（cnrnortify.jar、mysql-connector-java-8.0.29.jar、log4j-api-2.17.2.jar、および log4j-core-2.17.2.jar）をすべて同じディレクトリに配置します。

ステップ 2　同じディレクトリ内の lnc.properties/lnc6.properties ファイルを抽出します。

DHCPv4 クライアントの場合:

```
jar xvf cnrnotify.jar com/cisco/cnr/notify/lnc.properties
```

DHCPv6 クライアントの場合:

```
jar xvf cnrnotify.jar com/cisco/cnr/notify/lnc6.properties
```

ステップ 3　lnc.properties/lnc6.properties ファイルを構成します。

ステップ 4　Java実行可能ディレクトリが現在のパスにある場合、サンプル・クライアントは次の方法で実行されます。

DHCPv4 の場合:

```
java -cp .:cnrnotify.jar:mysql-connector-java-8.0.29.jar:log4j-api-2.17.2.jar:log4j-core-2.17.2.jar
 com/cisco/cnr/notify/LeaseNotificationClient
```

DHCPv6 の場合:

```
java -cp .:cnrnotify.jar:mysql-connector-java-8.0.29.jar:log4j-api-2.17.2.jar:log4j-core-2.17.2.jar
 com/cisco/cnr/notify/LeaseNotificationClient6
```

ローカル Web UI

Web UI は、構成属性を表示および管理し、関連サーバーの情報を表示します。リース クエリに関する統計情報は、[DHCP サーバーの統計情報] ページで確認できます。

ステップ 1 **Deploy** メニューで、[DHCP] サブメニューから **DHCP Server** を選択し、[DHCPサーバーの管理（Manage DHCP Server）] ページを開きます。

ステップ 2 [**統計情報**] タブをクリックして、[DHCP サーバーの統計情報] ページを開きます。

このページに、サーバー統計の詳細情報が表示されます。

CLI コマンド

既存の**dhcp getRelatedServers**コマンドは、DHCP リスナーとアクティブな接続に関する情報を提供するために拡張されます。

```
nrcmd> dhcp getrelatedservers
```

（注） このコマンドは、ローカル クラスターでのみ使用できます。

DHCP リスナーの設定

DHCP リスナ構成を使用して、TCP 接続を介して DHCP サーバーに対するアクティブおよびバルク リースクエリを有効にするようにオブジェクトを構成できます。DHCP サーバーが複数の TCP ポートでの接続のリッスンをサポートするか、サーバーが受信接続を受け入れるアドレスを制限する必要がない場合は、単一のオブジェクトで十分です。

ローカル アドバンスド Web UI

ステップ 1 メニューから**Deploy** 、**Listeners**サブメニューの下**DHCP**でを選択して、[DHCP TCP リスナーの一覧/追加] ページを開きます。

ステップ 2 [リスナー（Listeners）]ペインの[リスナーの追加（Add Listeners）]アイコンをクリックし、[名前（Name）]フィールドに名前を入力して、[TCPリスナーの追加（Add TCP Listener）] をクリックします。

ステップ 3 サーバーが接続を受け入れるインターフェイスを制限するために、アドレス/ip6address フィールドに IP アドレスを入力します。これは通常、指定されていません。IPv6 リスナーを設定する場合は、ip6address を入力します。アドレスと ip6 アドレスの両方が指定されていない場合は、IPv4 アドレス 0.0.0.0 が使用されます。

TCP 接続が受け入れられるアドレスを制限するには、アドレス (IPv4 の場合) または ip6address (IPv6 の場合) 属性を入力します。どちらの属性にも値が入力されていない場合、ホストの IPv4 アドレスへの IPv4 接続は受け入れられます。IPv6 経由の接続を指定するには、ip6address 属性に値を入力する必要があります (0::0ホストの IPv6 アドレスへの接続を受け入れる場合に使用できます。両方の属性ではなく、両方の属性にのみ値を入力できます。

（注） DHCP サーバーに対して IPv4 と IPv6 の両方のリスナーを指定することはできません。

ステップ 4 デフォルト値が適切でない場合は、ポートフィールドにポートの値を入力します。デフォルトのポートは、DHCPv4 のサーバーポートと DHCPv6 のサーバーポートです。

ステップ 5 *enable* 属性に対しては、[真（true）] または [偽（false）] ラジオボタンをクリックします。デフォルト値は true です。

ステップ 6 デフォルト値の 10 が適切でない場合は、*max-connections* の値を入力します。

ステップ 7 デフォルト値の 120 が適切でない場合は、*leasequery-backlog-time* の値を入力します。

ステップ 8 *leasequery-send-all* 属性に対しては、[真（true）] または [偽（false）] ラジオボタンをクリックします。デフォルト値は false です。

ステップ 9 [保存（Save）] をクリックします。

CLI コマンド

DHCP リスナ コマンドを次の表に示します。

表 *8: DHCP* リスナ コマンド

操作	コマンド
作成（Create）	**dhcp-listener** *name* **create** [*attribute=value*]
削除（Delete）	**dhcp-listener** *name* **delete**
一覧表示（List）	**dhcp-listener list**
名前の一覧表示（List the names）	**dhcp-listener listnames**
表示（Show）	**dhcp-listener** *name* **show**
設定（Set）	**dhcp-listener** *name* **set** *attribute=value* [*attribute=value ...*]
取得（Get）	**dhcp-listener** *name* **get** *attribute*

操作	コマンド
設定解除（Unset）	**dhcp-listener** *name* **unset** *attribute*
有効化（Enable）	**dhcp-listener** *name* **enable** *attribute*
無効化（Disable）	**dhcp-listener** *name* **disable** *attribute*

リース履歴データベース圧縮ユーティリティ

cnr_leasehist_compressユーティリティは、地域クラスタ(DHCPv4)リース履歴データベースを圧縮するために、Cisco Prime Network レジストラーに追加されました。このユーティリティは、データベース内のデータを直接圧縮するのではなく、既存のデータを、可能な限りコンパクトに最適化された新しいデータベースにコピーします。このユーティリティは、シスコ Web サイトの Cisco Primeネットワーク レジストラーダウンロード セクションからダウンロードできます。

注意 **cnr_leasehist_compress**ユーティリティは、地域のクラスターリース履歴データベースでのみ使用し、特に DHCPRELEASE パケットのためにデータベースが大幅に増加したと思われる場合に使用します。

コピー操作中に、このユーティリティを使用して次の操作を行うことができます。

- 一定の時間間隔より古いレコードをトリミングする - 通常は**–t**、このオプションを使用します。このオプションで指定する間隔は、ネットワークレジストラー時間間隔形式を使用します。たとえば、30**30d**日または**1y**1 年間です。
- 同じリースとクライアントに属するレコードのマージ: この**cnr_leasehist_compress** ユーティリティを使用して、IPアドレスのリースを解放した後にリースを解放したクライアントに属するレコードをマージします。通常、**–m** オプションを使用します。このオプションで指定する間隔は、ネットワークレジストラー時間間隔形式を使用します。たとえば、120**120s**秒または**2m**2 分間です。

  レコードのマージ中に、このユーティリティは、突然終了したリース履歴レコードや、バインドの終了時刻が正しくない(後続のリース操作によって発生した可能性がある)を修正します。レコードをマージするこのオプションは、サーバーに追加の負荷を生じさせる特定のルーター構成によって作成される膨大な数のレコードにも対応します。

ユーティリティを実行する**cnr_leasehist_compress** 前に、次の手順を実行します。

- ネットワークレジストラー地域クラスターを停止します。アクティブな地域クラスタデータベースでは動作しません。
- 既存のリース履歴データを単独で圧縮するために使用できることに注意してください。リージョン クラスターが将来のリース履歴レコードを収集する方法は変更されません。チャット クライアントが疑われる場合は、DHCP サーバーが DHCPRELEASE メッセージ

を処理しないことを確認します。このような場合は、ユーティリティを定期的に実行する必要があります。

- サービス プロバイダであり、一部のデバイスで DHCPDISCOVER、DHCPOFFER、DHCPREQUEST、DHCPACK のシーケンスを繰り返し生成するなどの既知の問題が発生し、30 以降に発生する可能性があるため、サービス プロバイダであり、ネットワーク内の地域リース履歴が増加していると疑われる場合に使用できます。メッセージを送信します。すべての DHCPRELEASE メッセージをドロップするか、または設定されたしきい値を超えるクライアントに属するメッセージをドロップするかを選択できます。
- 新しいデータベースは最適な方法で書き込まれます。新しいデータベースは、最初はかなりの速度で拡張できますが、追加のリース履歴レコードが収集された後、通常の状態に戻ります。

Cnr_leasehist_compress の実行に関する全般的なコメント

注意 この手順のすべての手順に慎重に従ってください。いずれかの手順を省略すると、リース履歴データが失われる可能性があります。各タスクに関連するリース履歴データベースをメモします。リース履歴レコードの数とレコードのトリミングまたはマージにかかる時間によっては、このユーティリティの実行に数時間または数日かかる場合があります。実行が完了する前にサーバーが再起動した場合は、実行中にユーティリティを中断できます。後で再開できます。ただし、前の実行で使用したのと同じオプションを指定する必要があります。

インストールパスは、Cisco Prime Network Registrar をインストールするパスです。

次の表に、このユーティリティの限定オプションを**cnr_leasehist_compress** 示します。

表 *9 : cnr_leasehist_compress* オプション

オプション	説明
–a	一時アクティブ データベース内のすべてのリース履歴レコードを、新しいデータベースのリース履歴レコードに追加します。
–c *limit*	クライアントに対してマージされたレコード数が指定数を超えた場合にレポートを生成します。**–f**このオプションを使用すると、これらのレコードはログファイルに転送されます。
–C	書き込み時にリースレコードを圧縮する (詳細については、CCM の *lease-hist-compression*を参照してください。
–d *path*	圧縮されたリース履歴レコードを含む新しい転送先データベースへのパスを指定します。
–e *attrlist*	除外されたマージ属性リストを上書きします。

オプション	説明
–f *file*	ほとんどのリース履歴レコードの警告をログ ファイルにリダイレクトします。
–g	*dbtxn-seq* 属性と *dbtxn-generation* 属性を使用して、宛先データベースに書き込まれているすべてのリース履歴レコードに割り当てられた番号順に新しいシーケンスを生成します。
–i *ipaddr*	特定の IP アドレスのレコードをログ ファイルに転送します。
–l *limit*	データベースが事前に設定された 20 ファイルの制限に達した後に、ログ ファイルをパージします。
–m *time-int*	特定**binding-start-time**のリースのが、以前のリースの**binding-end-time**期間内にある場合にリース レコードをマージします。このオプションの推奨値は、**120s** です。
–n	隣接するレコードをマージせずに比較します。
–p	詳細なリース履歴レコードを削除します。このオプションは、詳細リース履歴を有効にしている場合にのみ使用できます。 （注） シスコ プライム ネットワーク レジストラーは、詳細なリース履歴をサポートしなくなりました。ただし、詳細なリース履歴をサポートしているバージョンからのアップグレードの場合、このオプションは保持されます。
–q *records*	ユーティリティの実行中に生成される定期的な進行状況レポートの間隔を設定します。デフォルト値は **100000** です。次に例を示します。 `+00:00:18 Read 100000 records (0 bad); trimmed 6717; merged 73370; 19912 written (19.91%)`
–r *records*	ソース データベースから読み取られるレコードの数を制限します。
–s *path*	データを新しいデータベースにコピーするソース データベースを指定します。
–t *age*	特定の時間間隔より古いレコードをトリミングするための値を指定します。このオプションには、1**1y**年または**30d**30 日間など、標準のネットワークレジストラー時間間隔を使用します。
–v	バージョンを出力して終了します。
–w *records*	転送先データベースに書き込まれるレコードの数を制限します。
–y "*line attr*"	リース履歴レコードのダンプの幅を変更します。このオプションは推奨されません。ただし、132 列**132 30**の出力には値を使用できます。

オプション	説明
–z{文字**}**=レベル	標準のネットワーク レジストラーデバッグ トレース構文を使用して指定されたデータベースをデバッグします。

圧縮の実行

cnr_leasehist_compress ユーティリティを実行するには、次の手順を実行します。

ステップ 1 *LD_LIBRARY_PATH*にインストールパス/lib を追加して、ユーティリティにネットワーク レジストラーIP ライブラリへのアクセスを提供します。

```
$ bash
# export LD_LIBRARY_PATH=install-path/lib:$LD_LIBRARY_PATH
```

ステップ 2 ネットワークレジストラー地域クラスターを停止します。

```
# systemctl stop nwregregional
```

ステップ 3 元のインストールパス/data/leasehist ディレクトリの名前をインストールパス/data/oldleasehist に変更します。/leasehist ディレクトリは元のデータベースになります。

```
# mv install-path/data/leasehist
# install-path/data/oldleasehist
```

ステップ 4 新しいリースディレクトリを作成します。

```
# mkdir install-path/data/leasehist
```

ステップ 5 ユーティリティ **cnr_leasehist_compress** を 実行して、地域のクラスターがアクティビティを再開できるようにします。

```
# install-path/bin/cnr_leasehist_compress
> -r 0
> -s install-path/data/oldleasehist
> -d install-path/data/leasehist
> -p
```

注意 これらのコマンドを実行しても、元のデータベースは圧縮されません。**–r**この**0**オプションは、一時的なアクティブ・データベースを作成するようにユーティリティーに指示するので、非常に重要です。ユーティリティが元のデータベースを圧縮している間、地域クラスタはアクティブなままです。

ステップ 6 ネットワークレジストラーの地域クラスターを再起動します。

```
# systemctl start nwregregional
```

ただし、この時点では、元のデータベースからリース履歴データを取得することはできません。リージョンクラスターは、新しいリース履歴データを収集し、一時的にアクティブなデータベースに転送します。次に、このユーティリティは、新しいリース履歴データを新しいデータベースにマージします。

ステップ 7 インストールパス/data/newleasehist という新しいディレクトリを作成します。この /newleasehist ディレクトリが新しいリース履歴データベースになります。

```
# mkdir install-path/data/newleasehist
```

ヒント 地域クラスターが新しいデータベースにデータを取り込んだ後、必要に応じてこの新しいディレクトリを別のパーティションに作成し、最終的な場所にコピーできます。

ステップ 8 ユーティリティを**cnr_leasehist_compress**実行して、元のデータベースを新しいデータベースにトリミング、マージ、および圧縮します。

```
# install-path/bin/cnr_leasehist_compress
> -s install-path/data/oldleasehist
> -d install-path/data/newleasehist
> -t trim-time-interval
> -m merge-time-interval
> -f /tmp/cnr-compress.log
```

元のデータベースに詳細なリース履歴レコードが含まれている場合は、**–p**このオプションを使用して、これらのレコードを新規データベースに転送しないことがユーティリティーに許可されることを確認する必要があります。それ以外の場合、ユーティリティは実行されません。

（注） シスコ プライム ネットワーク レジストラーは、詳細なリース履歴をサポートしなくなりました。ただし、詳細なリース履歴をサポートしているバージョンからのアップグレードの場合、このオプションは保持されます。

ステップ 9 ユーティリティが元のデータベース全体を処理した後、新しいデータベースに新しいリース履歴レコードを追加するには、次のタスクを実行します。

（注） 次の手順を完了するまで、地域クラスターを再起動しないでください。次の手順でシステムが再起動する場合は、この手順を繰り返します。

a) Network Registrar のリージョン クラスタを停止します。

```
# systemctl stop nwregregional
```

b) このユーティリティ**cnr_leasehist_compress** を実行して、新しいリース履歴レコードを新しいデータベースに追加します。

```
# install-path/bin/cnr_leasehist_compress
> -a
> -s install-path/data/leasehist
> -d install-path/data/newleasehist
> -m merge-time-interval
> -f /tmp/cnr-append.log
```

注意 この**–a**オプションは、ユーティリティが一時アクティブ・データベースのリース履歴レコードを新規データベースのリース履歴レコードに追加する必要があることを示すため、重要です。元のデータベースに使用したのと同じマージ時間間隔値を使用することをお勧めします。

c) ユーティリティが新しく収集したリース履歴レコードを追加するタスクを完了したら、一時アクティブ データベース ディレクトリの名前をインストールパス/data/leasehist から *install-path*/data/tmpleasehist に変更します。

```
# mv install-path/data/leasehist
# install-path/data/tmpleasehist
```

d) 新しいデータベース ディレクトリの名前を変更します, インストール パス /data/newleasehist,インストール パス/data/leasehist として:

```
# mv install-path/data/newleasehist
# install-path/data/leasehist
```

ステップ 10 Network Registrar のリージョン クラスタを起動します。

```
# systemctl start nwregregional
```

ステップ 11 Network Registrarの Web UI を使用して、リージョン リースの履歴データを確認します。

ステップ 12 インストールパス/data/oldleasehist、および一時的なアクティブなデータベースをインストールパス/data/tmpleasehist にアーカイブします。データベースをアーカイブするときに、すべてのサブディレクトリとファイルを必ず含めます。

ステップ 13 元のデータベースと一時的なアクティブなデータベースを削除します。

```
# rm -rf install-path/data/oldleasehist
# rm -rf install-path/data/tmpleasehist
```

柔軟なリース時間

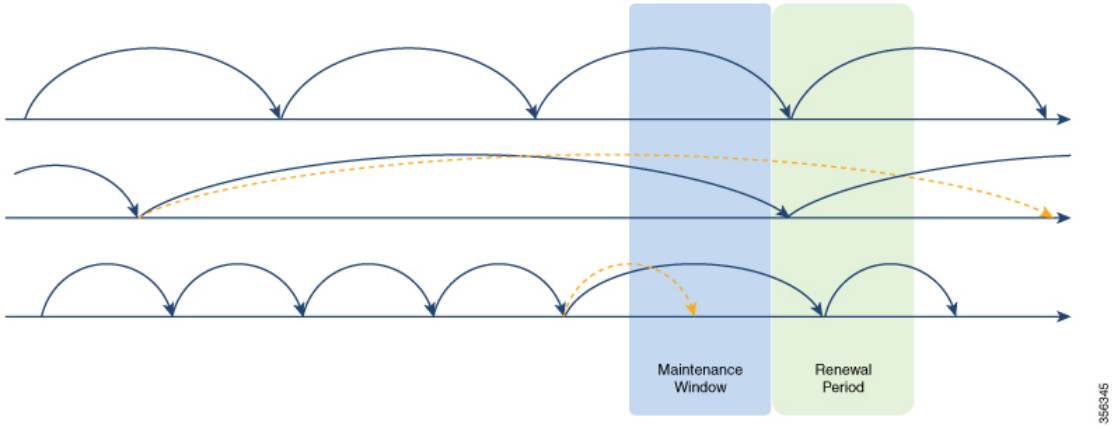
特定のネットワーク セグメントの番号を変更したり、構成の変更を迅速に有効にしたりする必要があるため、ネットワークの再構成が必要になる場合があります。通常、これは、変更の前にクライアントのリース時間を短縮し、変更を適用し、リース時間を元の値に戻すことによって行われます。つまり、更新時間を比較的狭いウィンドウ (メンテナンスウィンドウ) に圧縮し、サーバーの負荷を均等に戻す必要があります。これらの手順は手動で、エラーが発生しやすいものです。Cisco Prime Network レジストラーは、メンテナンス期間の前、中、および後の DHCP サーバーの更新負荷を軽減するために、このプロセスを自動化するのに役立ちます。

ネットワークの再設定のスケジューリング

Cisco Prime Network レジストラーでは、メンテナンス期間をスケジュールして、エラーが発生しやすく、リース時間のリセットを忘れないようにすることができます。必要なメンテナンス期間の開始時刻、終了時刻、および更新期間を設定できます。また、メンテナンス期間をサーバー全体に適用するか、特定のスコープ、リンク、またはプレフィックスにのみ適用するかを指定できます。サーバーは、この期間中にサーバーがシャットダウンする可能性があるため、保守期間の開始時刻と終了時刻の間にクライアントがDHCPサーバーに接続しようとするのを避けるために、リース、更新 (T1)、および再バインド (T2) の時間を調整しようとします。メンテナンス期間中、DHCPサーバーは最小リース時間を使用し、メンテナンス期間の後はリース時間を元の状態に戻しますが、更新は広がったままにします。再構成中および再構成後の更新は、サーバー負荷の急増を最小限に抑えるために適切に分散されます。最終的には、メンテナンス ウィンドウの構成を削除するか、新しい構成に置き換えることができます。サーバーは、過去に発生した保守を無視します。

図 1 : Maintenance Window （71 ページ）は、異なるリース時間を持つ 3 つのクライアントを示し、メンテナンスウィンドウと対話します。最初の(上)のケースでは、更新期間中にクライアントが入ってくるので、変更はありません。2 番目 (中央) の場合、サーバーは更新期間中にクライアントが更新されるように時間を短縮します。3 番目 (下位) の場合、サーバーはメンテナンス期間中にクライアントの更新を回避するために時間を増やします (サーバーに到達できない可能性があるため)。

図 *1 : Maintenance Window*



1 つのメンテナンスウィンドウを作成、編集、および削除できます。DHCP サーバーは、構成されている場合はメンテナンス ウィンドウを読み込みます。現在の時刻が終了時刻に更新期間を加算した場合 (すべてのクライアントが更新された構成を持つ必要があるメンテナンス期間の終了後の時間間隔) は、メンテナンスウィンドウをロードするために無視されます。また、リース更新の配布が有効になっていない場合も読み込まれません (を参照リース更新の配布（73 ページ）。メンテナンス期間が適用されるスコープ、リンク、またはプレフィックスの場合、サーバーは次のようにクライアントに送信されるリース時間または更新時間を変更します。

- メンテナンス期間の終了前にクライアントに与えられたリース時間は、メンテナンス期間の終了時刻に更新期間を加えた時間を超えないことを示します。
- メンテナンス期間の終了前にクライアントに与えられた更新時間は、メンテナンス期間の終了時刻に更新期間を 1/2 を加えた時間を超えないことをお知りください。
- メンテナンス期間の開始時刻と終了時刻の間に終了するクライアントに与えられたリース時間は、メンテナンス期間の終了後と終了時刻の前の時間間隔に時間を加えた後の間隔を 1/2 に加えた間隔の間のどこかで期限切れに調整されます。
- メンテナンス期間の開始時刻から終了時刻の間に発生するクライアントに与えられた更新時間は、メンテナンス期間の終了から更新期間の 1/2 までの間に更新をトリガーするように調整されます。

（注） フェールオーバー時間の制限は引き続き適用され、メンテナンス期間が原因で変更されません。これらの制限により、サーバーがリース、更新 (T1)、および一部のクライアントの再バインド (T2) の時間を最適化できなくなる可能性があります。

メンテナンス期間オブジェクトの追加

メンテナンス ウィンドウ オブジェクトを追加するには、次の手順を実行します。

ローカル アドバンスド Web UI

ステップ 1 [**展開**] メニューの**[DHCP]**サブメニューの [**メンテナンス ウィンドウ**] を選択します。[メンテナンス ウィンドウの一覧/追加] ページが開きます。

ステップ 2 左側のペインで [**メンテナンス ウィンドウの追加**] アイコンをクリックし、次のフィールドに詳細を入力します。

- **名前**：DHCP メンテナンス ウィンドウのオブジェクトの名前。
- **開始日**— メンテナンス期間が開始される日時。これは、DHCP サーバーが停止すると予想される場合です。
- **[終了日]**- メンテナンスウィンドウが終了する日時。これは、DHCP サーバーが再び利用可能になると予想される場合 (構成の変更が行われた後) です。
- **[更新期間]**- 影響を受けるすべてのクライアントが新しく構成された情報を受け取るためにサーバーに接続する必要があるメンテナンス期間の終了後の期間。

ステップ 3 [**メンテナンス ウィンドウの追加**] をクリックします。

ステップ 4 メンテナンスウィンドウを特定のスコープ、プレフィックス、またはリンクに適用する場合は、次の操作を行います。

- *[DHCP*スコープの一覧] ページで [一覧] を有効に設定したメンテナンス属性を持つスコープが、[スコープ] 領域の下に表示されます。メンテナンス期間を特定のスコープに適用するには、[**スコープの構成**] オプションの横にある**無効な**ラジオ ボタンをクリックし、[スコープ] 領域から必要なスコープを選択または追加します。**有効**にされたラジオ ボタンをクリックすると、構成内のすべてのスコープが現在のメンテナンス ウィンドウに参加します。
- [リスト/追加 DHCP v6 プレフィックス] または [リスト/追加 DHCP v6 リンク] ページでメンテナンス属性を持つプレフィックス/リンクが有効に設定されているリンクまたはプレフィックス領域の下に一覧表示されます。メンテナンス ウィンドウを特定のプレフィックスまたはリンクに適用するには、[**プレフィックス/リンクの設定**] オプションの横にある**無効な**ラジオ ボタンをクリックし、[リンク] 領域または[プレフィックス]領域から必要なリンクまたはプレフィックスをそれぞれ選択または追加します。**有効**なラジオ ボタンをクリックすると、構成内のすべてのプレフィックスとリンクが現在のメンテナンス ウィンドウに含まれます。

ステップ 5 [保存（Save）] をクリックします。

メンテナンスウィンドウオブジェクトの詳細は、メンテナンスウィンドウ編集ページで編集できます。メンテナンス ウィンドウ オブジェクトを削除するには、左側のウィンドウでメンテナンス ウィンドウ オブジェクトの名前を選択し、左側のウィンドウで[**選択したメンテナンス ウィンドウの削除**] アイコンをクリックして、削除を確認します。

（注） メンテナンス ウィンドウ オブジェクトを削除すると、スコープ、プレフィックス、およびリンクのメンテナンス属性もすべてクリアされます。

CLI コマンド

保守ウィンドウ オブジェクトを作成するには、**dhcp-メンテナンス ウィンドウ**名 **create** [属性 =*value* ..] コマンドを使用します。保守ウィンドウ オブジェクトを削除するには、**dhcp-メンテナンス ウィンドウ**名削除**コマンドを**使用します。

dhcp**メンテナンス ウィンドウクリア**を使用するメンテナンス [**dhcpv4** |**dhcpv6**]をクリックして、すべてのスコープまたはすべてのプレフィックス/リンクのメンテナンス フラグをクリアします。**dhcpv4**を指定すると、スコープのみがクリアされます。**dhcpv6**を指定すると、プレフィックス/リンクのみがクリアされます。どちらも指定しない場合、すべてクリアされます。

すべてのメンテナンス ウィンドウ コマンドの完全な一覧については、/docs ディレクトリの CLIGuide.html ファイルの**dhcp-maintenance-window**コマンドを参照するか、CLI の**ヘルプ dhcp-メンテナンス ウィンドウ**を使用してください。

リース更新の配布

DHCPサーバーは、リース更新の負荷が可能な限り均等に分散されるようにクライアントの更新を調整し、更新トラフィックの急増を回避します。更新トラフィックの急増は、多数のクライアントが一度に戻るメンテナンスウィンドウ、ネットワーク (または停電) の後に発生する可能性があります。そのようなスパイクを回避するために、この機能はデフォルトでは有効になっています。

サーバーは、バケット間隔内に更新するクライアント数を保持します。サーバーがクライアントの更新時間 (リース時間の 50%) を決定すると、そのバケットの値が標準 (クライアント数/(最新の更新時間/バケット間隔) を超えているかどうかを確認します。標準を超えると、サーバーは更新時間の 20 ~ 120% のランダムな値を選択し、そのバケットを標準と照らしてチェックします。このプロセスは、基準を下回るバケットが見つかるまで、または満たされていないバケットの時間が使用されるまで、限られた回数だけ繰り返されます。

（注） バケットが 10 更新/秒未満の場合、サーバーはその負荷を簡単に処理できるため、サーバーはカウントを調整しません。

図 *2:* リース更新の配布の例

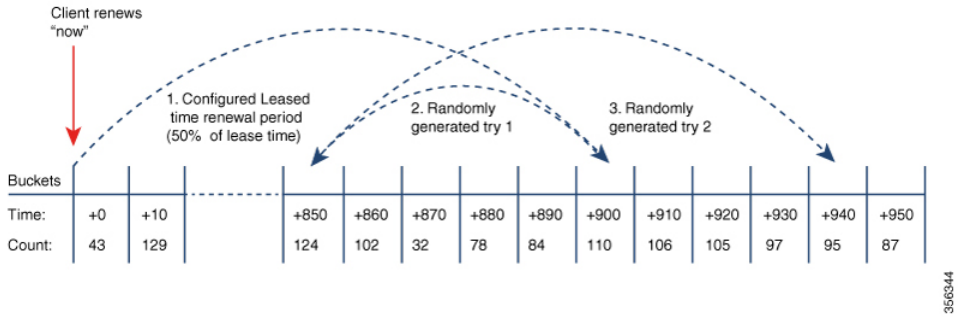


図 2 : リース更新の配布の例 （74 ページ）更新の配布機能の例を示します。この例では、クライアントの通常の更新時間 (リース時間の 50% が 1800 秒 = 900 秒) のバケットが、そのバケットの期間中に更新される予定クライアントのしきい値を超えた場合、サーバーは更新時間を調整します。ここでは、サーバーはランダムな代替更新時間(元の更新の20%から120%の間)を選択します。ただし、最初の試みもしきい値を超えているため、セカンダリ試行が試行され、更新時間 (944) がしきい値を下回るバケット内にあることが検出されます。クライアントには、その更新時間 (944 秒) が与えられます。

DHCPv4 の場合、この機能が有効になっている場合、サーバーは強制的に *dhcp* 更新時間オプション (58) と *dhcp* 再バインド時間オプション (59) を送信します。DHCPv6 の場合、サーバーは常に IA_NA および IA_PD オプションの T1/T2 フィールドを設定するので、その処理に影響はありません。

更新の配布機能の制御

更新の配布機能を制御するには、次の手順を実行します。

ローカルの高度な Web UI

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ウィンドウの [DHCP] をクリックし、[ローカルDHCPサーバーの編集（Edit Local DHCP Server）] ページを開きます。

ステップ 3 [分散更新（Distributed Renewals）] セクションで、次の属性を設定します。

- *distribute-renewals*：DHCP サーバーが更新時間を調整してサーバーの更新負荷を平滑化できるかどうかを制御します。

  （注） 設定されているポリシーの *dhcp-lease-time* オプション（51）または優先存続期間が 180 日より長く設定されている場合、サーバーはこの機能を有効にしません。

- *distribute-renewals-max-renewal-time*：サーバの更新負荷を円滑に調整するために、サーバーが更新を調整する際に使用する最大更新時間を制御します。この属性が設定されていない（または0）場合、サーバーは *dhcp-lease-time* オプションの 50%（51）またはすべての名前付きポリシーと組み込みポリシーの優先存続期間に基づいてこれを決定します。

- *distribute-renewals-bucket-interval*：サーバーの負荷を円滑にするために使用されるバケットの時間間隔を制御します。この属性が設定されていない場合、バケット数が 100,000 を超えない限り、サーバは 10 秒を使用します。この場合、サーバーは時間間隔を使用してバケットを最大 100,000 に制限します。

ステップ 4 [保存（Save）] をクリックします。

CLI コマンド

配布更新機能を無効にするには、dhcp を使用して**dhcp disable distribute-renewals** にします。配布更新機能を有効にするには、dhcp を**使用して配布更新を有効にします。また、dhcp set**コマンドを使用して、配布更新-最大更新時間および分散更新-バケット間隔の値を変更することもできます。

DHCP 更新レポートの表示

ローカル Web UI の [DHCP 更新レポート] ページには、DHCP サーバー上で予想される更新の負荷がグラフィカルに表示されます。これは、特定の時間間隔 (バケット) で将来更新される予定のクライアントの数を示します。

Web UI のダッシュボードから更新データを確認することもできます。詳細については、DHCP 更新データを参照してください。

DHCP 更新レポートを表示するには、次の手順を実行します。

ローカル Web UI

ステップ 1 [操作（Operate）] メニューの [サーバー（Servers）] サブメニューで [サーバーの管理（Manage Servers）] を選択して [サーバーの管理（Manage Servers）] ページを開きます。

ステップ 2 [サーバーの管理（Manage Servers）] ウィンドウの [DHCP] をクリックし、[ローカルDHCPサーバーの編集（Edit Local DHCP Server）] ページを開きます。

ステップ 3 [DHCP**更新レポート**] タブをクリックします。

ステップ 4 [バケット数]フィールドに、希望するバケット**数を入力します**。更新データが報告されるバケットの数を指定します。バケットは、その時間間隔中に更新する予定のクライアントを表します。

ステップ 5 [表示（Show）] をクリックします。

DHCP 更新データはグラフ形式で表示され、Y 軸に沿って特定の間隔で更新するクライアント数と X 軸に沿って日付/時刻のスタンプを更新します。

CLI コマンド

配布更新機能に関連する情報を報告するには、**dhcp getRenewalData** [*max-buckets*] を使用します。既定では、時間の経過に伴う予想されるクライアント更新数は、20 個のバケットに最も多く表示されますが、この値は希望する数を指定することでオーバーライドできます。

これは、設定に関するいくつかの情報と、各更新バケット内のクライアント数の(文字セル)グラフも表示します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。