DHCP サーバーの管理

この章では、DHCPサーバーパラメータの一部を設定する方法について説明します。クライアントがアドレス割り当てにDHCPを使用できるようにするには、少なくとも1つのスコープをサーバーに追加する必要があります。この機能については、スコープ、プレフィックス、リンク、ネットワークの管理で説明しています。

Cisco Prime Network Registrar のフェールオーバー プロトコルは、メイン サーバーが何らかの理由でオフラインになった場合に、バックアップのDHCPサーバーがメイン サーバーを引き継いで動作できるように設計されています。DHCP フェイルオーバーを設定するには、DHCP フェールオーバーの管理を読みます。

DHCP サーバーの設定

DHCPサーバーの設定では、サーバーのプロパティ、ポリシーおよび関連するDHCPオプションを設定する必要があります。Cisco Prime Network Registrar では以下が必要です。

- DHCP サーバーの IP アドレス
- 1 つ以上のスコープ (スコープの管理を参照) および および/またはプレフィックス

一般的な設定時の注意事項

DHCP サーバーを構成する前に考慮すべきガイドラインを次に示します。

- Separate the DHCP server from secondary DNS servers used for DNS updating：大規模ゾーン転送時に DHCP サーバーが悪影響を受けないようにするには、セカンダリ DNS サーバーとは異なるクラスタで DHCP サーバーを実行する必要があります。
- Lease times：リース期間のガイドラインを参照してください。

DHCP サーバー インターフェイスの設定

DHCP サーバーを設定するには、Cisco Prime Network レジストラーの のデフォルトを受け入れるか、データを明示的に指定します。

- Network interface：イーサネット カードの IP アドレス(静的で、DHCP によって割り当てられていないもの)
- Subnet mask：インターフェイス ネットワーク メンバーシップを識別します。サブネット マスクは通常、インターフェイス アドレスのネットワーク クラスに基づいていますが、ほとんどの場合 255.255.255.0 です。

既定では、DHCP サーバーはオペレーティング システムのサポートを使用して、コンピュータ上のアクティブなインターフェイスを自動的に列挙し、それらのすべてをリッスンします。サーバー・インターフェースを手動で構成することもできます。DHCP サーバーが存在するマシン上の NIC カードに割り当てられたすべての IP アドレスを静的に構成する必要があります。マシンは BOOTP または DHCP クライアントであってはなりません。

（注） DHCP に使用するインターフェイスを制限する必要がある場合を除き、特定の DHCP サーバー インターフェイスを構成しないことをお勧めします。サーバーが使用可能なインタフェースを自動的に検出できるようにします。

ローカル アドバンスド Web UI

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

ステップ 2 [マネージャーサーバー（Manager Servers）] ウィンドウで [ローカルDHCPサーバー（Local DHCP Server）] を選択します。

ステップ 3 [ネットワークインターフェイス（Network Interfaces）] タブをクリックして、サーバーに構成できるネットワーク インターフェイスを表示します。デフォルトでは、サーバーはこれらすべてのものを使用します。

ステップ 4 インターフェイスを設定するには、インターフェイスの [構成] 列の [編集（Edit）] アイコンをクリックします。これにより、インターフェイスが [構成済みインターフェイス] テーブルに追加され、編集または削除できます。

ステップ 5 設定されたインターフェイスの名前をクリックすると、[DHCPサーバーネットワークインターフェイスの編集（Edit DHCP Server Network Interface）] ページが開き、インターフェイスのアドレスとポートを（エキスパート モードで）変更できます。

ステップ 6 Save をクリックして変更を保存します。

ステップ 7 Revert をクリックして、[サーバーの管理（Manage Servers）] ページに戻ります。

CLI コマンド

DHCPdhcp-interfaceサーバーが DHCP クライアントをリッスンするネットワーク インターフェイス カードの IP アドレスを手動で制御するために使用します。デフォルトでは、DHCP サーバーは自動的にすべてのサーバー ネットワーク インターフェイスを使用するため、このコマンドを使用して、使用するネットワーク インターフェイスをより詳細に指定します。

構成変更の妥当性をトラブルシューティングして確認する。

- DHCP サーバーをリロードします。
- dhcp_startup_logファイルまたはname_dhcp_1_logファイルを確認してください。

ログの設定の詳細については、DHCP サーバーの調整 （19 ページ）を参照してください。

詳細なサーバー属性の定義

カスタム DHCP オプションを含む、高度な DHCP サーバー属性を設定できます。

DHCP サーバーをセットアップするには、次の手順を実行します。

1. スコープまたはプレフィックスを構成します。
2. サーバーをリロードします。

関連項目

詳細な DHCP サーバー属性の設定 （3 ページ）

スコープの BOOTP の有効化 （46 ページ）

BOOTP クライアントの移動または廃止 （46 ページ）

動的 BOOTP の使用 （46 ページ）

BOOTP リレー （47 ページ）

詳細な DHCP サーバー属性の設定

次の表は、ローカル クラスタ Web UI および CLI で設定できる高度な DHCP サーバー属性を示しています。

表 *1 : DHCP* の詳細属性

詳細パラメータ	アクション	説明
max-dhcp-requests	設定/設定解除	DHCP クライアントおよびフェールオーバー パートナーからのパケット受信に DHCP サーバーが割り当てるバッファの数を制御します。この設定が大きすぎると、DHCP アクティビティのバーストによって、処理前に古くなった要求でサーバーが詰まる可能性があります。その結果、クライアントが新しいリースを取得しようとしてパフォーマンスが著しく低下し、バーストの処理能力に影響を与える処理負荷が増大します。バッファの設定が低いと要求が調整され、サーバーのスループットに影響する可能性があります。サーバーがバッファを使い果たした場合、パケットは破棄されます。 負荷が高いと予想される場合 (定常状態または頻繁なストレス時間が発生した場合)、または高速マルチプロセッサ システムがある場合は、バッファーを増やすという優れた規則または経験があります。

詳細パラメータ	アクション	説明

		非フェールオーバー展開では、既定の設定 (500) で十分です。フェールオーバー展開では、DHCP ログが要求バッファの数が常に多いことを示している場合は、この数を 1000 に増やすことができます。また、DHCP 応答の数(max-dhcp-responsesパラメーターを参照) を要求バッファーの 4 倍に変更する必要があります。
		
		LDAP クライアントルックアップを使用する場合、バッファは、LDAP 接続の合計数と各接続に許可される要求の最大数で定義された LDAP ルックアップ・キュー・サイズを超えないようにする必要があります。LDAP サーバーの容量をサービス クライアントルックアップに合わせて LDAP キューのサイズを設定します。
		
		次のログ メッセージが頻繁に発生し、短期的なトラフィックの急増 (電源復旧後など) と関連しない場合は、属性の値を増やすことを検討してください。
		
		`4493 DHCP ERROR "DHCP has used xx of its yy request buffers: the server is dropping a request."`
		`4494 DHCP WARNING "DHCP has used xx of yy request packets. Requests will be ignored if no packet buffers are available."`
		`5270 DHCP WARNING "DHCP has used xx of its yy request buffers: the server is congested -- will not keep the client last-transaction-time to within value but will keep it to within value seconds."`
		
		必須。デフォルトは 500 です。

詳細パラメータ	アクション	説明

max-dhcp-responses	設定/設定解除	DHCP クライアントに応答し、DHCP パートナー間でフェールオーバー通信を実行するために DHCP サーバーが割り当てる応答バッファーの数を制御します。
		
		非フェールオーバー展開では、既定の設定の 2 倍の要求バッファー数で十分です。フェールオーバー展開では、これを増やして要求バッファの 4 倍になるようにすることができます。一般に、応答バッファの数を増やしても問題はありませんが、以前に推奨された比率を下回ると、サーバーの応答性に悪影響を及ぼす可能性があります。
		
		次のログ メッセージが頻繁に発生し、短期的なトラフィックの急増 (電源復旧後など) と関連しない場合は、属性の値を増やすことを検討してください。
		
		`4721 DHCP ERROR "DHCP has used all xx response packets. A request was dropped and they will continue to be dropped if no responses are available."`
		`5289 DHCP WARNING "DHCP has used xx of yy response packets. Requests will be dropped if no responses are available."`
		
		必須。デフォルトは 1000 です。

max-ping-packets	設定/設定解除	サーバーがクライアントに対する Ping 要求を開始するために使用できるバッファの数を制御します。スコープ レベルで Ping アドレスオプションを有効にした場合、パケットバッファは ICMP メッセージの送受信に使用されます。ping を有効にした場合、ping 要求のピーク負荷を処理するのに十分な ping パケットが割り当てられている必要があります。デフォルトは 500 ping パケットです。

詳細パラメータ	アクション	説明
defer-lease-extensions	有効にする/ 無効にする	DHCP サーバーが、期限の半分未満のリースを拡張するかどうかを制御します。これは、リース状態データベースへのディスク書き込みの回数を最小限に抑えるのに役立つパフォーマンスチューニング属性です。デフォルト値はオン、または true です。つまり、途中でリースを更新するクライアントは、残りの部分だけを取得でき、延長されません。リース拡張の保留 （9 ページ）を参照してください。
last-transaction-time-granularity	設定/設定解除	last-transaction-time-granularity 属性のデフォルト値が 60 秒から 1 週間に変更されました。この新しいデフォルトは、クライアントと最後のトランザクション時間が、クライアントが最後にサーバーと通信した時刻を正確に反映していない可能性があることを意味します。 クライアントがサーバーに通信するたびに更新されるこの属性に展開が依存する場合、展開に対して適切な値に last-transaction-time-granularity 属性を明示的に設定する必要があります。 defer-lease-extensions を無効にすると、last-transaction-time-granularity 属性を効率よく使用できません。したがって、遅延リース延長を無効にした場合、デフォルト値の変更は影響を受けません。 サーバーの負荷が高く、要求バッファまたは応答バッファが不足している場合、負荷を軽減するためにサーバーは一時的に last-transaction-time-granularity の値を 1 年に設定します。

詳細パラメータ	アクション	説明
discover-queue-limit	設定/設定解除	DHCPDISCOVER および SOLICIT クライアント要求にいつでも使用できる要求バッファの割合の制限を指定します。要求バッファの構成された割合を超えると、追加の DHCPDISCOVER および SOLICIT クライアント要求は破棄されます。DHCPDISCOVER/SOLICIT 要求で使用できる要求バッファを制限することにより、サーバーは DHCPREQUEST/REQUEST 要求を処理するために使用可能な要求バッファを持っていることを保証し、これにより、電源復旧や CMTS の再起動後など、アクティビティのスパイク中にクライアントをオンラインにするのに必要な時間を大幅に短縮できます。 DRL（Discriminating Rate Limiter）属性は、判別レートリミッタの機能を制御します。判別レート リミッターはデフォルトで有効になっており、DHCP サーバーが新しいトランザクションの起動よりも DHCP トランザクションの完了を優先します。多くの場合、これによりすべてのクライアントをオンラインにする時間が短縮されます。アクティビティの要約ロギングが有効になっている場合、レート制限のためにドロップされた DHCPDISCOVER (DHCPv4) および送信請求 (DHCPv6) パケットの数は DRL:number として報告されます。 DHCPv4 統計には、新しいキュー限定検出ドロップ・カウンターが含まれており、DHCPv6 統計には新しいキュー制限付き送信請求ドロップ・カウンターが含まれています。これらのカウンタは、ドロップされたパケットを監視するために使用されます。

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

ステップ 1 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 [DHCPサーバー（DHCP Server）] ペインからサーバーを選択します。

ステップ 3 [ローカルDHCPサーバーの編集（Edit Local DHCP Server）] ページで属性を追加または変更します。
ステップ 4 変更を加えた後に Save をクリックします。

CLI コマンド

現在のサーバーパラメータを表示するには、 dhcp show および dhcp get attribute を使用し、 dhcp set attribute=value [attribute=value ...]、dhcp unset attribute、dhcp enable attribute、および dhcp disable attribute を使用してこれらを変更します（上の表を参照してください）。

リース拡張の保留

遅延リース拡張属性 (事前設定値) を有効にすると、DHCP サーバーは DHCP トラフィックの突然のフラッディングに対する応答を最適化できます。このようなトラフィックスパイクが発生する可能性のあるネットワーク イベントの例としては、ケーブル インターネット サービス プロバイダ (ISP) データ センターで電源障害が発生し、その結果、すべてのケーブル モデム 終端システム (CMTS) が一度にリブートする場合があります。この場合、CMTS に接続されたデバイスは、すぐにオンラインに戻ってくると、DHCP トラフィックが大量に生成されます。

遅延リース拡張属性が有効になっていると、DHCP サーバーは、通常は T1 の前 (通常はリースの途中で) 前に発生するクライアントの更新要求のリースの有効期限の延長を延期する可能性があります。クライアントに構成されたリース時間を完全に設定する代わりに、サーバーは既存のリースの残りの時間を許可します。リースの有効期限の絶対値は変更されないため、サーバーは、サーバーのスループットが大幅に向上するデータベース更新を回避できます。もう 1 つの利点は、リースの有効期限を延長してフェールオーバー パートナーを更新する必要がないようにすることです。

クライアントが T1 以降 (通常は有効期限の途中) にある場合、この属性を有効または無効にしても効果はなく、サーバーは常にリース有効期限の延長を試みます。ただし、フェールオーバーやその他のプロトコル制限により、サーバーが構成された時間の間、リースを延長できなくなる可能性があります。

（注） リース拡張を延期すると、DHCP RFC に準拠したままサーバーのパフォーマンスが大幅に向上します。

リース拡張を延期する場合は、ポリシー属性のリース時間の変更をデフォルトの無効のままにするか、有効な場合は無効に変更することをお勧めします。

サーバーの観点から、次の 3 つの状況について説明します。

- Clientサーバーが遅れると、クライアントが要求を再送信することがretries可能です。DHCP サーバーは、これらの情報を再送信として認識するのに十分な情報を保持しておらず、それぞれが完了するまで処理を行い、再び完全なリース期間を与え、データベースを更新します。サーバーが既に遅れている場合、余分な作業を行うと状況が悪化します。これを防

ぐために、DHCP サーバーは、遅延リース拡張属性の状態に関係なく、30 秒未満のリースを延長しません。

- Client:クライアントリースの有効な更新時間は、設定された更新時間とクライアントの再起動間隔の最小値rebootsです。多くのインストールでは、更新時間が何日も設定されている場合でも、クライアントは 1 日あたり 1 回または 2 回 (一般的なケーブル ネットワークで) 新しいリースを取得する場合があります。遅延リース拡張属性を設定すると、これらの早期更新がデータベース トラフィックを引き起こさないようにすることができます。
- —DHCP サーバーがリースに関して DHCP クライアントにプロアクティブに接続する方法がないため、DHCP サーバーで短いリース時間を設定して、ネットワークの番号変更、アドレスの再割り当て、またはネットワークの再構成(DNS サーバーアドレスの変更など)をタイムリーに行う手段を提供できます。 Artificially short renewal times 目標は、許容できないデータベース更新のオーバーヘッドを発生させることなく、これを行えるようにすることです。

複雑な問題として、サーバーはクライアントから最後に聞こえた時刻も追跡します。最後のトランザクション時間と呼ばれるサイトでは、デバッグの補助としてこの情報を使用することがあります。この時間を維持するには、クライアントとのやり取りごとにデータベースへの書き込みが必要です。最後のトランザクション時間粒度属性は、設定する属性です。(表 1 : DHCP の詳細属性の属性の説明を参照してください)。これは主にデバッグ支援であるため、値は完全に正確である必要はありません。さらに、インメモリ コピーは常に正確であるため、データベース内のexport leases –serverデータが最新でない場合でも、現在の情報を表示するために使用できます。

DHCP 転送の設定

Cisco Prime Network レジストラー DHCP サーバーは、クライアントごとに別の DHCP サーバーへの DHCP パケットの転送をサポートします。たとえば、特定の MAC アドレス プレフィックスを持つ特定のクライアントからのアドレス要求を別の DHCP サーバーにリダイレクトする場合があります。これは、転送先のサーバーが管理するサーバーではない場合に役立ちます。これは、複数のサービス プロバイダが同じ仮想 LAN 上のクライアントに DHCP サービスを提供する環境で発生します。

DHCP 転送を有効にするには、拡張スクリプトを実装する必要があります。DHCP サーバーは、指定されたクライアントをインターセプトし、転送コードを呼び出し、転送されたサーバー アドレスの指定されたリストをチェックします。その後、要求自体を処理するのではなく、要求を転送します。dhcpattachExtensionをdhcp使用して、DHCP サーバーとの間で拡張機能を接続およびデタッチdetachExtensionします。

DHCP 転送機能は次のように機能します。

1. DHCP が初期化されると、サーバーは UDP ソケットをオープンし、それを使用して転送されたパケットを送信します。複数の IP アドレスを持つサーバーをサポートするために、ソケット アドレスのペアは、INADDR_ANY と任意のポート番号で構成されます。これにより、クライアントはサーバーの IP アドレスのいずれかを使用できます。

2. DHCP サーバーは、クライアントから要求を受信すると、次の拡張ポイント スクリプトを処理します。

   • post-packet-decode
   • pre-client-lookup
   • post-client-lookup

   DHCP サーバーはこれらのスクリプトを処理するに従って、次の文字列の環境ディクショナリをチェックします。

   ```
   cnr-forward-dhcp-request
   ```

3. その文字列が見つかったとき、値true (有効) を持つサーバーは、その転送コードを呼び出します。
4. 転送コードは、次のキーを持つ文字列の環境ディクショナリをチェックします。

   ```
   cnr-request-forward-address-list
   ```

   この例のように、コロンで区切られたポート番号を使用して、コンマで区切られたIPアドレスのリストが必要です。

   ```
   192.168.168.15:1025,192.168.169.20:1027
   ```

   デフォルトでは、サーバーは DHCPv4 のサーバーポートと DHCPv6 の v6 サーバーポートに転送します。クライアント要求全体のコピーを各IPアドレスとポートに順番に送信します。リスト内の要素のいずれかが無効な場合、サーバーはリストの解析を停止します。
5. 転送コードが戻った後、サーバーは要求の処理を停止します。ただし、クライアント参照後の拡張ポイント スクリプトでは、この操作によって、クライアント エントリの詳細を含むオプションのログ メッセージが作成される場合があります。

   次のTCL拡張スクリプトの一部の例では、要求の情報に基づいて別のサーバーに要求を転送するようにDHCPサーバーに指示します。同じ環境に複数のデバイスプロビジョニングシステムがある場合は、このようなスクリプトを使用できます。この場合、ルーターがブロードキャスト要求を転送するDHCPサーバーで拡張スクリプトを実行します。スクリプトは、他のサーバーが要求を処理する必要がある場合は、その要求を処理する必要がある場合、その要求を転送するように元のサーバーに指示します。

   サンプル スクリプトでは、MAC アドレス プレフィックスの静的マッピングを使用して、特定のベンダーから特定のシステムにモデムを送信します。

```
proc postPktDecode {req resp env} {
  set mac [$req get chaddr]
  set addrs ""
  # Very simple, static classifier that forwards all requests from devices
  # with a mac-address vendor-id of 01:0c:10 to the DHCP servers at
  # 10.1.2.3 and 10.2.2.3:
  switch -glob -- $mac {
    01:0c:10* {
      set addrs "10.1.2.3,10.2.2.3"
    }
  }
  # If we decide to forward the packet, the $addrs var will have the IP
  # addresses where to forward the packet:
  if {$addrs != ""} {
    # Tell the DHCP server to forward the packet...
    $env put cnr-forward-dhcp-request true
    # ...and where to forward it:
```

```
        $env put cnr-request-forward-address-list $addrs
        # No more processing is required.
        return
      }
    }
```

より柔軟なスクリプトでは、Cisco Prime Network レジストラークライアントエントリなどのクライアントごとの設定オブジェクトを使用して、どのDHCPサーバーが要求を取得するかを指定できます。

（注） DHCP 転送は DHCPv4 でのみ使用できます。DHCPv6 用ではありません。

DHCPv6 サーバー属性の編集

DHCPv6 に関連する DHCP サーバー属性を編集できます。これらの属性は次のとおりです。

- v6-client-class-lookup-id：DHCPv6 クライアント要求に基づいて client-class を決定し、設定済みの client-class の名前または <none>（式で client-class を指定しない場合）の文字列を返す式。属性にはプリセット値がありません。
- max-client-leases：DHCPv6 クライアントがリンクで保持できるリースの最大数。この属性を使用して、クライアントを 1 つのリースのみに制限しないでください。プリセットは 50 です。

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

[展開（Deploy）] メニューの [DHCP] サブメニューの下で 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。[ローカルDHCP サーバー（Local DHCP Server）] リンクをクリックして [DHCPサーバーの編集（Edit DHCP Server）] ページを開き、前述の DHCPv6 属性値を変更して、 Save をクリックします。

CLI コマンド

dhcp を使って前述の DHCPv6 サーバー属性を表示し、dhcp set attribute=value [attribute=value ...] を使用して変更します。

DHCP サーバーの動作に影響を与える拡張機能の使用

Cisco プライムネットワーク レジストラーは、拡張、プログラムを通じて、TCL または C/C++ で記述できる DHCP サーバーの動作を変更およびカスタマイズする機能を提供します。拡張機能は、要求パケットまたは応答パケットを変更し、環境ディクショナリに保存されている環境変数を使用して、サーバーと対話します（詳細は、拡張ポイントの使用を参照してください）。

たとえば、BOOTP 構成を使用する異常なルーティング ハブがある場合があります。このデバイスは、イーサネット・ハードウェア・タイプ (1) および MAC アドレスを指定した BOOTP 要求をchaddrフィールドに出します。その後、同じ MAC アドレスを持つ別の BOOTP 要求を送信しますが、ハードウェアタイプはトークンリング (6) です。通常、DHCP サーバーは、ハードウェア タイプ 1 の MAC アドレスとタイプ 6 の MAC アドレスを区別し、異なるデバイスであると見なします。この場合は、DHCP サーバーが同じデバイスに対して 2 つの異なるアドレスを配布することを防ぐための拡張機能を作成する必要があります。

次のいずれかの拡張を記述することで、2 つの IP アドレスの問題を解決できます。

- DHCP サーバーがトークン リング (6) ハードウェア タイプ のパケットをドロップする原因となるもの。
- トークン リング パケットをインターネット パケットに変更し、終了時に再度切り替えるパケット。この拡張は複雑になりますが、DHCP クライアントは DHCP サーバーからのリターンを使用できます。

関連項目

拡張機能の作成 （13 ページ）

拡張機能を使用した通信量の多いクライアントの防止 （15 ページ）

拡張機能の作成

TCL または C/C++ で拡張機能を記述できます。

- TCL—拡張機能を書き込むのが少し簡単で迅速になります。拡張が短い場合、TCL の解釈された性質はパフォーマンスに重大な影響を与えません。TCL で拡張機能を記述すると、サーバーをクラッシュさせる可能性のあるバグが発生する可能性が低くなります。
- C/C++ : 外部プロセスとの通信を含む、可能な限り最大のパフォーマンスと柔軟性を提供します。ただし、C/C++ API の複雑さが増し、拡張機能のバグがサーバーをクラッシュさせる可能性が TCL よりも高くなります。

特定の拡張ポイントで拡張機能を作成します。拡張ポイントには、要求、応答、環境という 3 種類のディクショナリが含まれています。これらの辞書の 1 つ以上は、次の拡張ポイントごとに使用できます。

1. init-entry：拡張ポイントは、DHCP サーバーが拡張機能を設定または構成解除するときに呼び出します。これは、サーバーの起動、停止、または再ロードのときに発生します。このエントリ ポイントのシグネチャは、拡張機能の他のエントリ ポイントと同じです。DHCPv6 処理に必要です。辞書:環境のみ。
2. pre-packet-decode：最初の拡張ポイントは、要求が到着したときに DHCP サーバーが検出し、パケットをデコードする前に呼び出します。辞書: 要求と環境。
3. post-packet-decode：入力パケットを書き換えます。使用するディクショナリは要求と環境です。
4. post-class-lookup：クライアントクラスに対する client-class-lookup-id 操作の結果を評価します。使用するディクショナリは要求と環境です。

5. pre-client-lookup：検索を行うクライアントに影響を与えます(検索を禁止したり、既存のデータを上書きするデータを提供したりすることなど)。使用するディクショナリは要求と環境です。
6. post-client-lookup：クライアント クラスの処理から入力された内部サーバー データ構造を調べるなど、クライアントクラスのルックアッププロセスの動作を確認します。DHCP サーバーが追加の処理を行う前に、この機能を使用してデータを変更することもできます。使用するディクショナリは要求と環境です。
7. generate-lease：DHCPv6 アドレスまたはプレフィックスを生成および制御します。辞書: 要求、応答、および環境。
8. check-lease-acceptable：リース受入テストの結果を変更します。細心の注意を払って行ってください。使用するディクショナリは、要求、応答、環境です
9. lease-state-change：リース状態が、これを変更するタイミングを細心の注意を払って決定します。辞書:応答と環境。
10. pre-packet-encode：応答で DHCP クライアントに返送されるデータを変更するか、DHCP 応答を送信するアドレスを変更します。使用するディクショナリは、要求、応答、環境です
11. post-packet-encode：サーバーがパケットをクライアントに送信する前、またはパケットをドロップする前に、サーバーがパケットを検査して変更できるようにします。使用するディクショナリは、要求、応答、環境です
12. post-send-packet：DHCP 要求/応答サイクルの重大な時間制約の外部で実行する処理用のパケットを送信した後に使用されます。使用するディクショナリは、要求、応答、環境です
13. environment-destructor：エクステンションが保持している可能性のあるコンテキストをクリーンアップできます。使用するディクショナリは環境です。

DHCP サーバーを拡張するには、次の手順を実行します。

ステップ 1 Tcl、C、または C++ で拡張機能を記述し、サーバー拡張ディレクトリにインストールします。

- Tcl—/var/nwreg2/local/extensions/dhcp/tcl
- C or C++—/var/nwreg2/local/extensions/dhcp/dex

これらの拡張機能は、TCL または C/C++ 拡張用の適切なディレクトリに配置するのが最適です。次に、ファイル名を構成するときに、ファイル名自体をスラッシュ（/）を使用せずに入力します。

サブディレクトリに拡張子を配置する場合は、パス区切り記号を付けてファイル名を入力します。

（注） 作成した拡張機能は、/var/nwreg2/local/extensions/dhcp/... エリアに追加する必要があります。Cisco Prime Network Registrar に同梱されている拡張機能は、/opt/nwreg2/local/extensions/dhcp エリアにあります。サーバーは、最初に /var/nwreg2/local/extensions/dhcp/... ディレクトリで拡張機能を検索し、次に /opt/nwreg2/local/extensions/dhcp/... ディレクトリで拡張機能を検索します。

ステップ 2 Web UI の [DHCP拡張の一覧/追加（List/Add DHCP Extensions）] ページを使用するか（[詳細設定（Advanced）] モードで [展開（Deploy）] メニューから、[DHCP] サブメニューの下の [拡張（Extensions）] を選択して

[DHCP拡張の一覧/追加（List/Add DHCP Extensions）] ページを開きます）、または CLI の**拡張**コマンドを使用して、DHCP サーバーがこの拡張機能を認識するように構成します。

ステップ 3 dhcp attachExtension を使用して、構成済みの拡張機能を 1 つ以上の DHCP 拡張ポイントに接続します。

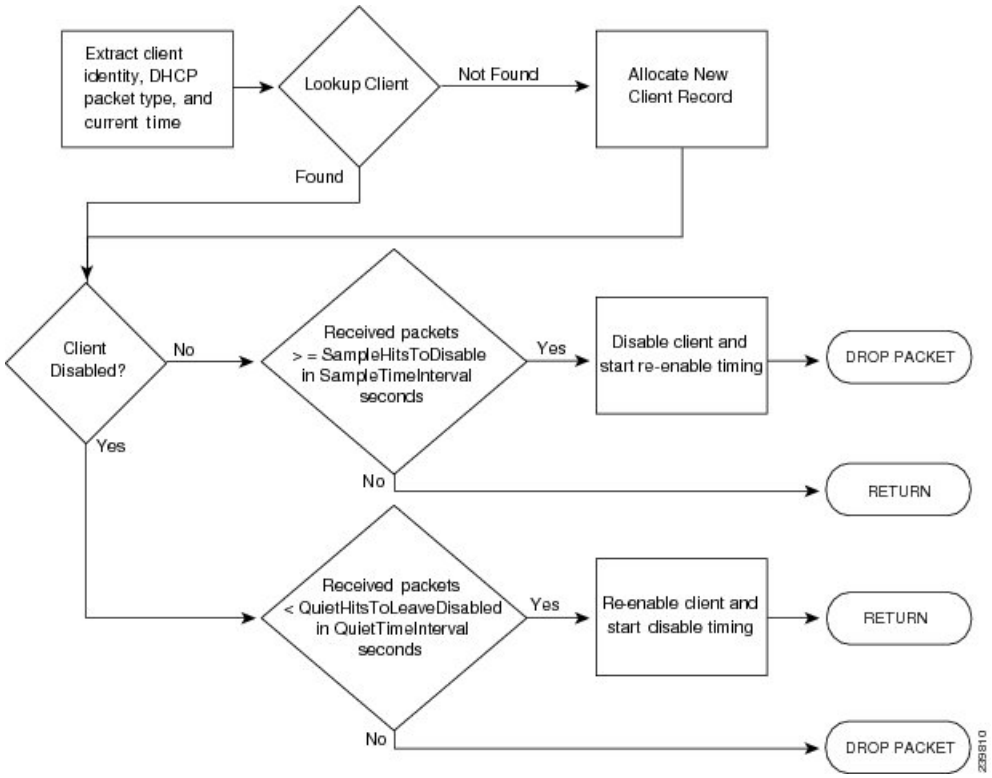
ステップ 4 サーバーをリロードします。

拡張機能を使用した通信量の多いクライアントの防止

拡張の効果的な使用方法の一例として、不要なトラフィックでサーバーがオーバーフローしているクライアントから保護することが挙げられます。ChattyClientFilter 拡張機能を使用すると、これらのチャット クライアント パケットを処理する作業の多くをサーバーが行う必要がないようにすることができます。ネットワーク内に多数のクライアントがある場合は、この拡張機能の実装を検討してください。

ChattyClientFilter 拡張機能は、 Cisco Prime Network Registrar インストールの インストールパス/examples/dhcp/dex ディレクトリで使用可能であり、コンパイル済みのため install-path/extensions/dhcp/dex/dexextension.so または install-path/extensions/dhcp/dex/dexextension.dll ですぐに使用できます。この拡張は、MAC アドレスに基づいてクライアント要求をモニターリングし、ある間隔で特定数を超えるパケットを生成したクライアントを無効にします。あるクライアントを無効にすると、サーバーではそのパケットが破棄されます。ただし、サーバーはそのクライアントのトラフィックを引き続きモニターリングするため、完全に無視するわけではありません。特定の間隔でクライアントが生成するパケット数が特定数を下回り始めたことをサーバーが検出すると、クライアントが再度有効になり、パケットの受信が再開されます。

図 *1:* チャット クライアント フィルタ フロー



クライアントを無効および再度有効にする基準は、ChattyClientFilter拡張の引数で設定します。デフォルトでは、サーバーは30秒以内に15個を超えるパケットを受信すると、クライアントを無効にします。サーバは、10秒以内に送信するパケットが5個未満の場合に、クライアントを再び有効にします。これらのデフォルト値は控え目な値であるため、すべての状況が保護されるわけではありませんのでご注意ください。たとえば、サーバーは3秒ごとにパケットを送信するクライアントを無効にはしません。数回の再送信があったとしても、クライアントが6個を超えるパケットを短い間隔で送信する必要がないためです。

チャット クライアントが疑われる場合は、DHCP サーバー ログを確認して着信レートを確認し、次の表に示す引数を ChattyClientFilter コードに適切に設定します。

表 *2:* 引数を使用します。

チャティクライアントフィルタ引数	説明
–c	環境ディクショナリのdrop属性が「true」に設定されている場合、パケットを無視します。デフォルトでは無視されません。

チャティクライアントフィルタ引数	説明
–d packet-count seconds	指定された時間間隔で指定された数を超える数を受信した場合は、DHCPRELEASE パケットを破棄します。デフォルトでは無効になっています。 サーバーはクライアントが指定された間隔でパケットの送信を中断するまで DHCPRELEASE パケットをドロップし続けます（DHCPv4 クライアントのみ）。 基本的な式は、時間間隔は少なくとも(パケットカウント+ 2)*30秒でなければならないということです。
–h packet-count	SampleHitsToDisable：デフォルトでは 15 パケットです。
–i seconds	SampleTimeInterval：デフォルトでは 30 秒です。
–l packet-count	QuietHitsToLeaveDisabled：デフォルトでは 5 パケットです。
–m seconds	クライアントが無効になる最大時間を秒単位で設定します。デフォルト 0 ～無制限。
–n	更新または再バインドする場合はクライアントをNAKs します。デフォルトではオフになっています。クライアントが、サンプルヒットを超える場合、無効にするクライアントは、DHCP 要求を行う、サーバーはパケットを破棄する代わりに DHCPNAK を送信します。 これにより、何らかの理由でリースを更新できないクライアント(ケーブル モデムなど)の問題を解決できます。DHCPNAK を送信すると、クライアントは DHCP ステート マシンを再起動して DHCPDISCOVER を送信します。 この引数を使用する場合は、拡張ポイントに ChattyClientFiltercheck-lease-acceptableをアタッチする必要があります。（DHCPv4 クライアントのみ）。
–q seconds	QuietTimeInterval：デフォルトでは 10 秒です。
–r seconds	StatisticsInterval：デフォルトでは 300 秒（5 分）です。この引数は、無効にして再び有効にしたクライアント数の定期的なログ記録の頻度を制御します。
-s	ドロップされたパケットをサイレントに破棄します。デフォルトではオフになっています。

チャティ クライアントフィルタ引数	説明
-t	指定した場合、チャッティ クライアント フィルタは DHCPv6 クライアントの DUID-LLT の「時刻」を無視します（クライアント ID オプション（1））。フィルターは、DUID-LLT 内の時間をゼロ（00:00:00:00）に変更します。 これは、DUID-LLT を使用するクライアントがこの値を正しく保存しないため、複数のクライアント ID を生成しない場合に使用できます。 **注**：これは、サーバーがこれらのクライアントを処理する方法を変更しません。
–w port	指定したポートで Web アクセスを有効にします。正のポート番号を指定すると、接続はローカルホストに制限されます。負のポート番号を指定した場合は、ポートの絶対値が使用され、接続が制限されません。
-4	DHCPv4 パケットのみをフィルタします。デフォルトは両方です。
–6	DHCPv6 パケットのみをフィルタします。デフォルトは両方です。

（注） h、-i、-l、および-q のデフォルトは、単一のタイプの不適切なクライアントに対処するように設計されていたため、ほとんどの状況に適している可能性は低い。通常の状態に対して間隔とパケット ヒット カウントを長くすると、妥当な結果が得られます。i 120 -h 8 -q 120 -l 8 などの値は、120 秒の期間にわたってクライアントに 8 パケットを許可します。通常の DHCP ディスカバー/オファー/要求/ACK は、クライアントからのパケットが 2 パケットのみです。つまり、ChattyClientFilter を適切に使用するには、特定のネットワーク条件に合わせてこれらの値を調整する必要があります。Cisco Web サイトの Cisco Prime Network レジストラーダウンロード セクションから利用できるログスキャン ツールを使用すると、クライアントのアクティビティを分析するのに役立ちます。

引数の設定と拡張機能の有効化の詳細については、ChattyClientFilter.cpp ファイルのコメントを確認してください。ほとんどの場合、post-packet-decode 拡張ポイントにアタッチします（–n 引数を使用する場合、check-lease-acceptable も含まれます）。

ChattyClientFilter のサンプルの使用例は、DHCPv4 クライアントから送信された DHCPRELEASE パケットをドロップして、リース履歴データベースが境界外に拡張されないようにすることです。

このシナリオでは、–d引数を使用します。設定は次のようになります。

```
nrcmd> extension dexChattyClientFilter create dex libdexextension.so
dexChattyClientFilter
init-entry=dexChattyClientFilterInitEntry
init-args="-d 2 120"

nrcmd> dhcp attachextension post-packet-decode dexChattyClientFilter
```

このセットアップにより、サーバーは、120 秒間隔で同じクライアントからこれらのパケットのうち 2 つ以上を受信した場合に DHCPRELEASE パケットを廃棄し、クライアントが DHCPRELEASE を少なくとも 120 秒間送信しない場合に DHCPRELEASE 処理を再開します。

Cisco Prime Network レジストラーは、チャッティー クライアント フィルタによって監視または無効になっている(ドロップされるトラフィック)クライアントに関する情報を取得するために使用できるミニ Web サーバーをサポートします。一般的な要求は、http://127.0.0.1:<port>/web ブラウザーに入力されたレポートです。

Web サーバーは、次の要求をサポートします。

- status：統計レポートを返します。
- report：統計レポートと完全なクライアントレポートを返します。クライアント レポートには、現在監視されているすべてのクライアントと無効になっているクライアントが含まれます。
- disabled-report：レポートと同じですが、無効なクライアントのみが返されます。
- flush：レポートと同じですが、すべてのクライアントが内部監視および無効リストから削除されます。
- csv-client-list：（監視および無効のクライアントを含む）CSV 形式を使用してクライアント リストを返します。
- csv-disabled-client-list：csv クライアントリストと同じですが、現在無効になっているクライアントのみが含まれます。
- xml-client-list：XML を使用してクライアント リストを返します（監視対象クライアントと無効なクライアントを含む）。
- xml-disabled-client-list：XML を使用して無効なクライアントリストを返します。

（注） この Web サーバーは非常に基本的なサーバーの実装です。上記のリクエストのみをサポートします。

DHCP サーバーの調整

DHCP パフォーマンスを調整するうえで役立つヒントは、次のとおりです。

- 最適なスループットを得るための要求 (最大 dhcp-request) および応答 (max-dhcp-responses) バッファを設定します。詳細については、表 1 : DHCP の詳細属性 を参照してください。
- 遅延リース拡張属性を有効にします。これにより、データベースへの書き込みが減少します。
- 最後のトランザクション時間粒度属性を、リース間隔の半分より大きい値として、最低60秒以上に設定します。
- プロダクション リースを提供するポリシーのリース時間の優先許可属性を無効にします。

- ログ記録とデバッグの設定を最小限にします。ログ記録が必要な場合は、次の表に示すように、制御された数の属性を持つ DHCP サーバーのlog-settings属性を使用します。

表 *3 : DHCP* ログの設定

ログ設定 (数値同等)	説明
default (1)	DHCP サーバーのいくつかの部分で低レベルのログを提供します。デフォルトを設定解除すると、このログは表示されません。
activity-summary (20)	サマリー メッセージを 1 分ごとに表示します。これは、no-xxx ログ設定の多くが有効になっているときに、各DHCP メッセージに対応するログ メッセージに必要な負荷を課すことなく、サーバーでのアクティビティを把握するのに役立ちます。これらのメッセージの期間は、 DHCP サーバー プロパティのアクティビティの概要 - 間隔を使用して構成できます。
client-criteria-processing (9)	有効なリースを見つけるためにスコープが検査される場合、またはスコープを調べて、既にリースを持っているクライアントに対して引き続きリースが許容できるかどうかを判断するたびに、ログ メッセージが出力されます。クライアント クラススコープの条件の処理を構成またはデバッグする場合に非常に便利です。これは、ログに記録される情報の適度な量を引き起こし、当然として有効にしておく必要があります。
client-detail (8)	すべてのクライアント クラスクライアントルックアップ操作の終了時に、単一行をログに記録します。この行には、クライアントに対して検出されたデータと、クライアントのクライアント クラスで検出されたデータの合成が表示されます。クライアント クラスの構成をセットアップする場合や、クライアント クラス処理で問題をデバッグする場合に便利です。
dns-update-detail (7)	サーバーが各 DNS 更新を送信し、更新メッセージへの応答を受信する場合に、メッセージをログに記録させます。
dropped-waiting-packets (15)	最大待機パケットの値がゼロ以外の場合、IP アドレスのキュー長がmax-waiting-packetsの値を超えると、パケットがドロップされることがあります。ドロップ待機パケットが設定されている場合、サーバーは、IPアドレスのキューから待機パケットをドロップするたびにメッセージをログに記録します。
failover-detail (10)	ほとんどのフェイルオーバー・トランザクションで、サーバーが単一のメッセージをログに記録するようにします。ログに記録される情報は、フェールオーバーがどのように動作しているかを理解するのに非常に役立ちます。

ログ設定 (数値同等)	説明
incoming-packet-detail (4)	DHCP サーバーが受信したすべての DHCP パケットの内容が、人間が判読可能な方法で解釈され、ログ ファイルに出力されます。これにより、入力パケットに対して組み込みの DHCP パケット スニッファが有効になります。この設定が有効になると、ログ ファイルがいっぱいになり、非常に急激に切り替わります。この設定は DHCP サーバーのパフォーマンスに大きな影響を与えるため、当然のことながら有効にしておく必要はありません。
incoming-packets (2)	この設定 (既定ではオン) では、着信パケットごとに 1 つの回線メッセージが記録されます。これは、DHCP サーバーまたは BOOTP リレーを最初に構成する場合に、DHCP サーバーがパケットを受信していることを即座に肯定する機能が存在する場合に特に便利です。
ldap-create-detail (13)	DHCP サーバーが LDAP サーバーに対してリース状態エントリの作成または削除を開始し、応答を受信し、結果メッセージまたはエラー メッセージを取得するたびに、ログ メッセージが表示されます。
ldap-query-detail (11)	DHCP サーバーが LDAP サーバーに対する照会を開始し、応答を受信し、結果またはエラー・メッセージを取得するたびに、ログ・メッセージが表示されます。
ldap-update-detail (12)	DHCP サーバーが LDAP サーバーに対する更新リース状態を開始し、応答を受信し、結果メッセージまたはエラー メッセージを取得するたびに、ログ メッセージが表示されます。
leasequery (14)	leasequery パケットが内部エラーなしで処理され、ACK または NAK が発生したときにログ メッセージが表示されます。
minimal-config-info (24)	サーバーの始動時または再ロード時に印刷される構成メッセージの数を削減します。特に、すべてのスコープについてメッセージをログに記録するわけではありません。
missing-options (3)	この設定 (既定ではオン) は、DHCP クライアントによって要求されたオプションがポリシーで構成されていないため、DHCP サーバーから提供できない場合に、メッセージがログに記録されます。
no-dropped-bootp-packets (18)	ドロップされたすべての BOOTP パケットに対して通常ログに記録される単一行メッセージが表示されないようにします。
no-dropped-dhcp-packets (17)	DHCP 設定が表示されないためにドロップされたすべての DHCP パケットに対して、通常は 1 行メッセージが記録されます。(無効であるためにドロップされたパケットに関連付けられたメッセージについては、無効なパケットがないを参照してください)。

ログ設定 (数値同等)	説明
no-failover-activity (19)	通常のアクティビティと、フェールオーバー用に記録された警告メッセージが表示されないようにします。重大なエラー ログ メッセージは、このログ設定とは無関係に表示され続けます。
no-failover-conflict (25)	フェールオーバー パートナー間の競合がログに記録されない原因になります。
no-invalid-packets (21)	無効であるために廃棄された DHCP パケットごとに、通常は 1 行のメッセージが記録されます。(DHCP サーバーの構成によってドロップされたパケットに関連付けられたメッセージについては、ドロップなしの dhcp パケットを参照してください)。
no-reduce-logging-when-busy (22)	通常、DHCP サーバーは、非常にビジー状態になったとき (つまり、使用可能な受信バッファの 2/3 以上を使用した場合 (それ自体は設定可能な値)、ログを減らします。成功メッセージ、ドロップなし dhcp パケット、ドロップなし bootp パケット、非フェイルオーバ アクティビティ、無効なパケットを設定し、アクティビティサマリー以外のすべてをクリアします。ログ記録アクティビティを設定しない場合、サーバーはこれを行いません。サーバーがビジー状態になくなったとき (つまり、使用可能な受信バッファの 1/3 しか使用していない場合) に、以前の設定が復元されます。
no-success-messages (16)	正常な発信 DHCP 応答パケットごとに通常ログに記録される単一行メッセージが表示されないようにします。正常な発信 DHCP 応答パケットの場合にのみ、ログに影響します。
no-timeouts (23)	リースまたはオファーのタイムアウトに関連付けられたメッセージがログ ファイルに表示されないようにします。
outgoing-packet-detail (5)	DHCP サーバーによって送信されるすべての DHCP パケットの内容が、人間が判読可能な方法で解釈され、ログ ファイルに出力されます。これにより、出力パケットに対して組み込みの DHCP パケット スニッファが有効になります。この設定が有効になると、ログ ファイルがいっぱいになり、非常に急激に切り替わります。この設定は DHCP サーバーのパフォーマンスに大きな影響を与えるため、当然のことながら有効にしておく必要はありません。
unknown-criteria (6)	クライアント エントリが見つかったときに、そのクライアントの現在のネットワークの場所に適したスコープに見つからない選択条件を指定するたびに、単一行のログ メッセージが表示されます。

ログ設定 (数値同等)	説明
v6-lease-detail (27)	サーバーが DHCPv6 リースアクティビティに関する個々のメッセージをログに記録します (非サクセス メッセージ、またはタイムアウトなしに応じてクライアント タイムアウト イベントに応じて、クライアントトランザクションごとに1つのメッセージに加えて、または代わりに)。

- クライアント キャッシュの設定を検討してください（「クライアントのキャッシュ パラメータの設定」を参照してください）。
- サーバーのパフォーマンスを監視するためにサーバーの統計情報を確認します（『Cisco プライムネットワーク レジストラー 11.0 管理ガイド』の「統計の表示」セクションを参照）。
- スコープ割り当ての優先順位を設定することを検討してください（「割り当て優先順位を使用した複数スコープの設定」を参照してください）。
- アドレスを提供する前にホストに ping を実行する場合は、ping タイムアウト期間の調整を検討してください（アドレス提供前のホストへの ping 実行を参照）。
- パフォーマンスを向上させるには、選択タグの数を制限することを検討してください。
- ライトウェイト ディレクトリ アクセス プロトコル（LDAP）サーバーを使用している場合は、「LDAP を使用するように Cisco Prime Network Registrar を設定する」で説明するパフォーマンスの問題を考慮してください。
- DHCP フェールオーバーを使用する場合は、負荷分散機能の使用を検討してください（「ロード バランシングの設定」を参照）。

ヒント　DHCP サーバー属性の変更に従って、サーバーの再ロードを行ってください。

DHCP に関連するサーバーの一覧 - フェールオーバー、DNS、LDAP、TCP リスナー サーバー

関連するフェイルオーバー、DNS、LDAP、またはTCPリスナー・サーバーがある場合（フェールオーバー サーバー ペアの設定を参照）これらのサーバーの属性にアクセスできます。

ローカル Web UI

[フェールオーバー ペア（Failover Pairs）]ページで、[フェールオーバーサーバの管理（Manage Failover Servers）]タブをクリックし、[関連サーバ（Related Servers）]タブをクリックするか、[DHCPサーバの管理（Manage DHCP Server）]ページ（[操作（Operate）]>[サーバ（Servers）]

>[サーバの管理（Manage Servers）]）の [関連サーバ（Related Servers）] タブをクリックして、[DHCP関連サーバー属性（DHCP Related Server Attributes）] ページを開きます。このページには、サーバーが配置されている通信とフェールオーバーの状態が表示されます。次の表に、このページの属性を示します（このページを表示するには、dhcp-management サブロールを使用して中央 cfg-admin ロールを割り当てる必要があります）。

表 *4:* 関連サーバーの属性

関連サーバー属性	説明
関連サーバーの種類	関連サーバーの種類: DHCP、DNS、または LDAP。
関連サーバーの IP アドレス	関連するサーバーの IP アドレス。DHCP フェールオーバーパートナーの場合は、このリンクをクリックして [フェールオーバー関連サーバーの表示（View Failover Related Server）] ページを開きます。
設定	通信の状態：なし、OK、または中断。
要求	DNS または LDAP 関連のサーバーにのみ適用され、これらのサーバーからの要求の数です。
状態	DHCP フェールオーバー：なし、起動、通常、通信中断、パートナーダウン、潜在的な競合、回復、一時停止、または回復完了 高可用性 (HA) DNS の場合—送信更新、プローブ、または ha 状態不明。正常に更新されたサーバーのみが、Send-Update 状態になることができます。更新を送信していないパートナー サーバーは、常にプローブまたは不明な状態になります。クライアントの動作がない場合に DHCP サーバーが起動すると、両方の DNS サーバーが不明な状態になることが多くなります。これは、DHCP サーバーが DNS 更新を実行しようとすると変更されます。
パートナーの役割	DHCP フェールオーバーの場合のみ、パートナーのフェールオーバーロール (メインまたはバックアップ)。
パートナーの状態	DHCP フェールオーバーの場合のみ、パートナーの状態：なし、起動、通常、通信中断、パートナーダウン、潜在的競合、回復、一時停止、または回復完了
更新応答の完了	DHCP フェールオーバーの場合のみ、完了した更新応答の割合 (未解決の更新応答がある場合にのみ有効)。

表 *5: DHCP* 関連のフェールオーバー サーバーの属性

DHCP 関連のフェールオーバー サーバー属性	説明
General attributes	

DHCP 関連のフェールオーバー サーバー属性	説明
failover-pair-name	このサーバーを管理するために使用するフェールオーバー ペア オブジェクトの名前。
current-time	このオブジェクトを返すサーバー上の現在の時刻。
comm-state	なし、OK、または中断。
smoothed-time-delta	ローカル サーバーとパートナー サーバーの時間差。ローカル・サーバー時刻がパートナー・サーバー時刻より前にある場合、属性値は正の値になります。ローカル・サーバー時刻がパートナー・サーバー時刻より遅れている場合、属性値は負になります。サーバーが通信していない場合は、最後に確認された属性値が記録されます。
最大クライアントリードタイム	このシステム上の現在の最大クライアントリードタイム(MCLT)。
sequence-number	フェールオーバー オブジェクト全体で固有のシーケンス番号は、リース内のシーケンスと異なる場合、リースは、sf-to-date のリース フラグとは無関係に「最新ではない」と見なされます。
負荷分散バックアップ-pct	現在のフェールオーバーロードバランシングのバックアップの割合。バックアップの割合が 0 の場合、フェールオーバーの負荷分散は使用されていない (無効)。
Local server information	
our-ipaddr	このサーバーへのインターフェイスの IPv4 アドレス。
our-ip6address	このサーバーへのインターフェイスの IPv6 アドレス。
role	このオブジェクトを返すサーバーのフェールオーバー ロール (なし、メイン、またはバックアップ)。
state	ローカルサーバーの状態：なし、起動、通常、通信- 中断、パートナーダウン、潜在的な競合、回復、一時停止、または回復完了

DHCP 関連のフェールオーバー サーバー属性	説明
start-time-of-state	現在のフェールオーバー状態が開始された時刻。
start-of-comm-interrupted	このパートナーが通信中断状態に入った時刻。これはリロード全体で有効ですが、開始時点の状態が最新のサーバーのリロードよりも早い時間を持つことはありません。
est-end-recover-time	update-request-in-progress がないに設定されている場合に有効です。表示された場合、更新要求が完了した場合にサーバーがリカバリ完了状態に入る時刻。表示されない場合、更新要求が完了するたびにサーバーはリカバリ完了に入ります。
use-other-available	false または未設定の場合、このサーバーは他の使用可能なリースを使用できません。true の場合、サーバーは他の使用可能なリースを使用できます。常に有効ですが、パートナーダウン状態の場合にのみ true にする必要があります。
use-other-available-time	パートナーダウン状態で、使用可能な使用が偽または未設定の場合、使用する他の使用可能な時間は true になります。
safe-period-remaining	セーフ期間の残り時間 (秒単位)。0 に設定されていない場合、このサーバーは現在、パートナーに対して安全な期間を実行しています。
load-balancing-local-hba	ローカルサーバーの現在のハッシュバケット割り当て(通常はハッシュバケット番号の範囲として表示されます)。(RFC 3074 を参照してください。
request-buffers-in-use	統計情報の計算時に DHCP サーバーが使用しているフェールオーバー要求バッファの数。
decaying-max-request-buffers-in-use	最近使用されたフェイルオーバー要求バッファーの最大数。
request-buffers-allocated	フェールオーバー機能をサポートするためにサーバーが割り当てた要求バッファの数。

DHCP 関連のフェールオーバー サーバー属性	説明
connection-start-time	最新の接続が開始された時刻。この値は、接続が開始されるたびに設定され、接続が終了してもクリアされません。
connection-end-time	最新の接続が終了した時刻。この値は、接続が終了するたびに設定され、新しい接続が開始されたときにクリアされません。
Partner server information	
ipaddr	パートナー サーバーの IP アドレス。
ip6address	パートナー サーバーの IPv6 アドレス。
partner-role	このオブジェクトを返すサーバーのパートナーのフェールオーバー ロール (なし、メイン、またはバックアップ)。
partner-state	フェールオーバー 関係のパートナーの最後の状態：なし、スタートアップ、ノーマル、通信中断、パートナーダウン、潜在的な競合、回復、一時停止、または回復完了
start-time-of-partner-state	パートナーの現在のフェールオーバー状態が開始された時刻。
est-partner-end-recover- time	パートナーの状態が[回復]の場合、パートナーが MCLT をタイムアウトして回復状態を終了する時期の予測値。
last-comm-ok-time	このサーバーが最後に通信が OK であると判明した時刻。
load-balancing-partner- hba	パートナーサーバーの現在のハッシュバケット割り当て(通常はハッシュバケット番号の範囲として表示されます)。（「RFC 3074」を参照）。
partner-vendor-major- version	パートナー サーバーからのベンダー ID メジャー バージョン。
partner-vendor-minor- version	パートナー サーバーからのベンダー ID マイナー バージョン。
Update requests sent to partner	

DHCP 関連のフェールオーバー サーバー属性	説明
update-request- outstanding	None または unset の場合、サーバーはパートナーのキューに更新要求を持っていません。Noneに設定されていない場合、フェールオーバー パートナーの更新要求がキューに入れられます。有効な値は、なし、更新、および更新すべてです。
update-request-start-time	update-request-outstanding 要求が開始された時刻。
update-request-done-time	更新要求の最後の完了時刻。
v6-update-response-in-progress	応答の種類と発生元。
v6-update-response-percent-complete	現在の IPv6 更新の応答の完了率。
v6-update-response-start-time	v6 更新-進行中の応答で言及された IPv6 更新応答が開始された時刻。
v6-update-response-done-time	最新の IPv6 更新応答がパートナー サーバーに対して行われた更新を送信した時刻。
Update requests processed for partner	
update-response-in- progress	このサーバーが更新応答を処理している場合は、応答の種類と発生元に関する情報を提供します。
update-response-percent- complete	更新-応答の未解決が表示された場合は、現在の更新の応答の達成率。
update-response-start- time	更新応答の進行中に記載された更新応答が開始された時刻。
update-response-done- time	最新の更新の応答が、パートナー サーバーに対して行われた更新を送信した時刻です。
Load Balancing Counters	
load-balancing-processed- requests	負荷分散の対象となる、IPv4 と IPv6 の両方のサーバー処理要求の数。このカウンタには、サーバーから NORMAL 状態への最新の遷移後に行われた要求のみが含まれます。
load-balancing-dropped- requests	負荷分散の対象となる、IPv4 と IPv6 の両方のサーバー ドロップ要求の数。このカウンタには、サーバーが Normal 状態に遷移した最新の移行後に行われた要求のみが含まれます。

DHCP 関連のフェールオーバー サーバー属性	説明
load-balancing-processed- total	サーバーが処理した IPv4 と IPv6 の両方の要求のうち、ロード バランシングの対象となるものの数。このカウンタには、このサーバーが最後に開始または再ロードされてからの要求が含まれます。
load-balancing-dropped- total	サーバーがドロップした IPv4 と IPv6 の両方の要求のうち、ロード バランシングの対象となるものの数。このカウンタには、このサーバーが最後に起動またはリロードされてからの要求が含まれています。
Binding Update or Ack Counters (this connection)	
binding-updates-sent	フェールオーバー パートナーに送信されたバインド更新 (BNDUPD) メッセージの数。
binding-acks-received	フェールオーバー パートナーから受信したバインド確認 (BNDACK) メッセージの数。
binding-updates-received	フェールオーバー パートナーから受信したバインド更新 (BNDUPD) メッセージの数。
binding-acks-sent	フェールオーバー パートナーに送信されたバインド確認 (BNDACK) メッセージの数。
v6-binding-updates-sent	最後に確立された接続の開始以降にフェールオーバー パートナーから受信した IPv6 バインディング更新 (BNDUPD6) メッセージの数。
v6-binding-acks-received	最後に確立された接続の開始以降にフェールオーバー パートナーから受信した IPv6 バインディング確認 (BNDACK6) メッセージの数。
v6-binding-updates-received	最後に確立された接続が開始されてから、フェールオーバー パートナーから受信した IPv6 バインディング更新（BNDUPD6）メッセージの数。
v6-binding-acks-sent	最後に確立された接続の開始以降にフェールオーバー パートナーに送信された IPv6 バインディング確認 (BNDACK6) メッセージの数。
バインディング更新/ACK カウンタの合計	

DHCP 関連のフェールオーバー サーバー属性	説明
binding-updates-sent-total	最新の統計リセット以降にフェイルオーバー・パートナーに送信された IPv4 バインディング更新 (BNDUPD) メッセージの数。
binding-acks-received-total	最新の統計リセット以降にフェールオーバーパートナーから受信した IPv4 バインド確認 (BNDACK) メッセージの数。
binding-updates-received-total	最新の統計リセット以降にフェイルオーバー・パートナーから受信した IPv4 バインディング更新 (BNDUPD) メッセージの数。
binding-acks-sent-total	最新の統計リセット以降にフェールオーバーパートナーに送信された IPv4 バインド確認 (BNDACK) メッセージの数。
v6-binding-updates-sent-total	最新の統計リセット以降にフェイルオーバー・パートナーに送信された IPv6 バインディング更新 (BNDUPD6) メッセージの数。
v6-binding-acks-received-total	最新の統計リセット以降にフェールオーバーパートナーから受信した IPv6 バインディング確認 (BNDACK6) メッセージの数。
v6-binding-updates-received-total	最新の統計リセット以降にフェイルオーバー・パートナーから受信した IPv6 バインディング更新 (BNDUPD6) メッセージの数。
v6-binding-acks-sent-total	最新の統計リセット以降にフェールオーバーパートナーに送信された IPv6 バインディング確認 (BNDACK6) メッセージの数。
フロー制御カウンター (この接続)	
current-binding-updates-in-flight	現在、現在処理中 (送信) されているバインド更新の数 (IPv4 と IPv6 の両方)。

DHCP 関連のフェールオーバー サーバー属性	説明
current-binding-updates-queued	現在キューに入っているバインド更新の現在の数 (IPv4 と IPv6 の両方)。 通常、この数は（総リースのパーセンテージとして）小さいはずですが、更新を必要とする多数のリースがある場合（パートナーのいずれかが停止した後に統合された場合など）、またはパートナーが更新の処理に時間がかかる場合は、大きくなる可能性があります。この数がリースの合計数を超えることはありません。 この数が 1000 を超えるか、リースの 10%（いずれか大きい方）を超える場合、あるいはさらに増加し続けている場合には、懸念が生じます。通常、これはフェールオーバーパートナーで要求の処理に大きな遅延が発生していることを意味します（通常はディスクの遅延が主な問題です）。
maximum-binding-updates-in-flight	一度に処理中 (送信) されたバインディング更新 (IPv4 と IPv6 の両方) の最大数。
maximum-binding-updates-queued	一度にキューに入れられたバインディング更新の最大数 (IPv4 と IPv6 の両方)。
last-binding-update-sent-time	最後のバインディング更新 (IPv4 または IPv6) が送信された時刻。
last-binding-ack-received-time	最後の IPv4 または IPv6 バインディング確認応答 (NAKed かどうか) を受信した時刻。
last-binding-update-received-time	最後のバインディング更新 (IPv4 または IPv6) を受信した時刻。
last-binding-ack-sent-time	最後の IPv4 または IPv6 バインディング確認 (NAKed かどうか) が送信された時刻。

表 *6 : DNS* 関連のフェールオーバー サーバーの属性

DNS 関連サーバー属性	説明
General attributes	
current-time	このオブジェクトを返すサーバー上の現在の時刻。

DNS 関連サーバー属性	説明
ipaddr	IP アドレス
comm-state	なし、OK、中断の 3 つの値が考えられます。 DHCP とリモート サーバー間の通信の状態。'OK' は、DHCP サーバーがリモート サーバーとの通信に成功したことを示します。'中断' は、DHCP サーバーがリモート サーバーとの通信に失敗したことを示します。
dns-server-state	プローブまたは SEND-UPDATE の 2 つの値があります。 PROBE は、DHCP サーバーがこのサーバーと通信を試みていないか、ダウンしていると判断され、プローブがアクティブであることを示します (これは、DHCP サーバーが 1 つの更新要求を送信するだけであることを意味します)。 SEND-UPDATE は、サーバーが通信しているように見え、DHCP サーバーが多くの要求を送信できることを意味します。
probe-polling-event-id	ゼロ。
要求	リモート サーバーで現在未処理の要求の数。
HA DNS Configuration information	
ha-dns-role	この DNS サーバーが果たす役割です。値は、スタンドアロン DNS、HA-MAIN、または HA バックアップです。 DNS サーバーは、スタンドアロン DNS、または HA-DNS が使用されている場合は HA-Main または HA-Backup にすることができます。
dns-timeout	動的 DNS 更新を再試行する前に、動的 DNS 更新に対する DNS サーバーからの応答を DHCP サーバーが待機するミリ秒数です。
max-dns-retries	DHCP サーバーが DNS サーバーに動的更新を送信しようとする回数。

DNS 関連サーバー属性	説明
ha-dns-failover-timeout	DHCP サーバーがフェールオーバーを実行して次の DNS サーバーを使用して動的更新を実行するまで、DHCP サーバーが DNS サーバーからの応答を待機する最大時間 (秒) です。デフォルト値は 30 秒です。
ha-dns-probe-timeout	cnr-ha-dns が有効になっている場合、HA-DNS サーバーがコミュニケーション中断状態または同期中の場合、DHCP サーバーはこのタイマーを使用して HA-DNS サーバー間のオーバーオーバーの遅延を調整し、遅延を軽減します。デフォルト値は 3 秒です。
ha-dns-probe-retry	cnr-ha-dns が有効になっている場合、DHCP サーバーは、HA-DNS サーバーが COMMUNIATION-INTERRUPTED 状態または同期中の場合に、この再試行回数と ha-dns プローブタイムアウトを使用して、HA-DNS サーバー間でのオーバーオーバーの遅延を調整し、遅延を軽減します。再試行のデフォルト値は 1 です。

表 *7: TCP* リスナおよび接続関連サーバーの属性

TCP リスナーと接続関連サーバー属性	説明
TCP リスナ関連サーバー属性	
ipaddr	リスナーがバインドされているアドレス。これは 0.0.0.0 である可能性があります。
comm-state	通信の状態。これは常に何もありません。
ip6address	リスナーがバインドされている IPv6 アドレス。これは 0::0 である可能性があります。
name	サービスの名前。
port	リスナーがバインドされるポート番号。このポートへの着信接続が処理されます。
total-connections	受信接続の総数。
current-connections	現在アクティブな接続の数。

TCP リスナーと接続関連サーバー属性	説明
rejected-connections	アクティブな接続の最大数を超えたなど、拒否された着信接続の総数。
TCP 接続関連のサーバー属性	
ipaddr	接続のリモート エンドのアドレス。
comm-state	通信の状態。これは常にOKです。
ip6address	接続のリモート エンドの IPv6 アドレス。
name	この接続が受け入れられたサービスの名前。
port	接続のリモート エンドのポート番号。
total-requests	受信した要求メッセージの総数。
current-requests	アクティブな要求の数。
current-state	接続の現在の状態です。
total-replies	送信した応答メッセージの総数。
start-time	接続が確立した時刻。
last-receive-time	受信した最後のバイトの時刻。
last-send-time	最後に送信されたバイトの時刻。
total-bytes-received	この接続で受信した合計バイト数。
total-bytes-sent	接続を介して送信された合計バイト数。
our-ipaddr	接続のローカル エンドのアドレス。
our-ip6address	接続のローカル エンドの IPv6 アドレス。
our-port	接続のローカル エンドのポート番号。

その他のコントロールは、次のページで使用できます。

- [関連サーバー（Related Server）] タブのデータを更新するには Refresh Data をクリックします。
- パートナーが通信が中断したフェールオーバー状態の場合、[関連サーバー（Related Server）] タブで、パートナーダウン日の設定の入力フィールドに関連付けて Set Partner Down をクリックできます。この設定は、start-of-communications- interrupted の値に初期化されます（通常の Web UI モードでは、この日付を初期化された日付より前の値に設定することはできません。エキスパート Web UI モードでは、この値を任意の日付に設定できます。Set

Partner Down をクリックした後は、[DHCPサーバーの関連サーバーの一覧（List Related Servers for DHCP Server）] ページに戻り、パートナーダウンアクションの結果を表示します。両方のパートナーをパートナー ダウン モードに設定しないでください。

- [DHCPサーバの関連サーバの一覧（List Related Servers for DHCP Server）] ページまたは [フェールオーバー関連サーバーの表示（View Failover Related Server）] ページから戻るには、Return をクリックします。

CLI コマンド

DHCPサーバーの関連サーバーを、値のサブセットと共に簡単なテーブル形式で一覧表示するには、dhcp getRelatedServers を使用します。完全な詳細を報告するには（テーブルではなく通常のオブジェクトフォーム表示で）dhcp getRelatedServers full を使用します。

バーチャル プライベート ネットワークの設定

このセクションでは、仮想プライベート ネットワーク(VPN)をサポートするようにCisco Prime Network レジストラー DHCP サーバーを設定する方法について説明します。

VPN の設定には、通常の DHCP ホスト IP アドレス指定に調整を加えることが関係します。VPN で使用するプライベート アドレス空間は、インターネット全体から見て一意ではない場合があります。このため、Cisco Primeネットワーク レジストラーは、VPN 識別子によって識別されるIPアドレスをサポートします。ルーター上のリレーエージェントもこの機能をサポートする必要があります。VPN 識別子は、クライアントが属する VPN を選択します。DHCP 用 VPN は現在 Cisco IOS ソフトウェアでのみサポートされており、最新バージョンでは、リレーされた DHCP メッセージに VPN ID を含めることができます。

関連項目

DHCP を使用した仮想プライベート ネットワークの設定 （35 ページ）

VPN とサブネット割り当ての調整パラメータ （43 ページ）

DHCP を使用した仮想プライベート ネットワークの設定

作成する VPN は、次の場合にフィルタリング メカニズムを提供します。

- 統合アドレス空間の表示（アドレス空間の表示を参照）
- 住所ブロックの一覧表示（アドレス ブロックの追加を参照）
- サブネットのリスト（アドレス ブロックとサブネットを参照）
- DHCP 使用率の照会（使用率履歴データの照会を参照）
- リース履歴の照会（IP リース履歴の実行を参照）

VPN を設定しない場合、Cisco Prime Network レジストラーは、各スコープでグローバル VPN 0 を使用します。

クライアントがリレー エージェントを使用して DHCP サーバーに IP アドレスを要求できるように VPN を構成するには、VPN を定義し、スコープを関連付ける必要があります。具体的には次のとおりです。

1. DHCP VPN トラフィックを処理するリレー エージェントが、DHCP のリレー エージェント情報オプション(82)のvpn-idサブオプションをサポートするバージョンの Cisco IOS ソフトウェアで設定されていることを確認します。
2. VPN が VPN ID または VPN ルーティングおよび転送インスタンス(VRF)名によって識別されることを、Cisco IOS リレー エージェント管理者と調整します。
3. VPN のスコープを作成します。

関連項目

標準 仮想プライベート ネットワーク （36 ページ）

仮想プライベート ネットワークの作成と編集 （37 ページ）

VPN の使用状況 （39 ページ）

標準 仮想プライベート ネットワーク

図 4は、VPN ブルーの一部として DHCP クライアント 1 を使用し、VPN クライアント 2 を VPN レッドで示す一般的な VPN シナリオを示しています。たとえば、VPN ブルーの DHCP クライアント 1 と VPN 赤のクライアント 2 の両方に同じプライベート ネットワーク アドレスがあります: 192.168.1.0/24。DHCP リレー エージェントには、2 つの VPN に含まれるゲートウェイ アドレスとグローバル アドレス(172.27.180.232)があります。2 つのフェールオーバー DHCP サーバーがあり、どちらも外部ゲートウェイ アドレスを介してリレー エージェントを認識しています。

サーバーがクライアントに VPN サポート アドレスを発行するために行われる処理は次のとおりです。

1. DHCP クライアント 1 は、その MAC アドレス、ホスト名、および要求された DHCP オプションを含む DHCPDISCOVER パケットをブロードキャストします。
2. アドレス 192.168.1.1 の DHCP リレー エージェントはブロードキャスト パケットをピックアップします。パケットにRelay エージェント情報オプション (82) を追加し、サブネットとして 192.168.1.0 を識別するサブネット選択サブオプションが含まれています。このパケットには、VPN を青で識別するvpn-idサブオプションも含まれています。DHCP サーバーは要求元のクライアントと直接通信できないため、server-id-overrideサブオプションには、クライアントによって認識されるリレー エージェントのアドレス (192.168.1.1) が含まれています。リレー エージェントはパケットの外部ゲートウェイ アドレス (giaddr) にも含まれます。
3. リレーエージェントは、DHCPDISCOVER パケットをサブネット上の構成済み DHCP サーバーにユニキャストします。
4. DHCP サーバー 1 はパケットを受信し、vpn-idおよびサブネット選択のサブオプションを使用して、適切な VPN アドレス空間から IP アドレスを割り当てます。サブネットと VPN で使用可能なアドレス 192.168.1.37 を検出し、パケットのyiaddrフィールド (クライアントに提供されるアドレス) に配置します。

5. サーバーは、GIADDR値で識別されるリレーエージェントにDHCPOFFERパケットをユニキャストします。
6. リレーエージェントは、リレーエージェント情報オプションを削除し、DHCPクライアント1にパケットを送信します。
7. DHCPクライアント1は、DHCPREQUESTメッセージをブロードキャストして、それが提供されたIPアドレスと同じIPアドレスを要求します。リレー エージェントは、このブロードキャスト メッセージを受信します。
8. リレー エージェントはDHCPREQUESTパケットをDHCPサーバー1に転送し、ユニキャストDHCPACKパケットをクライアントに返します。
9. リース更新の場合、クライアントはDHCPACKメッセージのDHCPサーバー識別子オプションで見つかったIPアドレスにDHCPRENEWパケットをユニキャストします。これは、リレーエージェントのアドレスである192.168.1.1です。DHCP リレー エージェントはパケットをDHCPサーバーにユニキャストします。サーバーは、最初に元のアドレスを提供したサーバーが必ずしも知らなくても、通常の更新処理を行います。サーバーはユニキャストDHCPACKパケットで応答します。リレー エージェントは、次に、ciaddrフィールド値で識別されるクライアントIPアドレスにDHCPACKパケットを転送します。

   リレーエージェント情報オプション(82)のサーバーIDオーバーライドサブオプションが存在する場合、DHCPサーバーはその値を使用して応答パケットのdhcp-server-identifierオプションの値と比較します。DHCPクライアントユニキャストが行うパケットは、サーバーではなくリレー エージェントに直接送信されます(実際にはクライアントからはアクセスできない可能性があります)。パケットにserver-id-overrideサブオプションが含まれている場合、フェイルオーバー環境の両方のパートナーはリースを更新できます。

仮想プライベート ネットワークの作成と編集

VPNとそのインデックスを設定するには、次の手順を実行します。

ステップ1 リレー エージェントのVPN IDまたはVRF名によってVPNが設定されていることをCisco IOSリレー エージェント管理者と調整します。これはCiscoプライムネットワーク レジストラーでVPNを識別する方法を決定します。

ステップ2 IOSスイッチまたはルータで設定されているVPNにDHCPクライアントをプロビジョニングできるように、VPNを作成します。

ステップ3 VPNインデックスを入力**します。**関連付けられたIDも一意である必要があります。

インデックスを追加するには、次の手順に従います。

- Local cluster（Advanced）：[設計（Design）]メニューの[DHCP設定（DHCP Setting）]サブメニューの[VPN]を選択して、[VPNの一覧/追加（List/Add VPNs）]ページを開きます。VPNに、クラスター内の数値キー識別子と一意の名前を指定します。

- Regional cluster：VPNを含むローカルクラスタを追加します（[操作（Operate）]メニューの[サーバー（Servers）]サブメニューの下の[クラスタの管理（Manage Clusters）]を選択します）。次に、[設計（Design）]メニューの[VPN]を選択します。[VPNの一覧/追加（List/Add VPNs）]ページが開きます。このページでVPNを作成するか、ローカル クラスタからVPNをプルできます。

- VPN を作成する場合は、数値キー識別子と一意の名前を指定します。
- ローカル クラスタから VPN をプルする場合は、[VPNの一覧/追加（List/Add VPNs）] ページの [VPN] ウィンドウで [データのプル（Pull Data）] アイコンをクリックし、選択したクラスタから特定の VPN またはすべての VPN をプルします。

[VPNの一覧/追加（List/Add VPNs）] ページの [プッシュ（Push）] または [すべてプッシュ（Push All）] アイコンをクリックして、VPN をクラスターにプッシュすることもできます。次に、[VPNデータをローカルクラスターにプッシュ（Push VPN Data to Local Clusters）] ページで、VPN をプッシュする同期モードとクラスターを選択します。

- CLI で、vpn name create key を使用します。次に例を示します。

```
nrcmd> vpn blue create 99
```

ステップ 4 VPN ID または VRF 名で適切な VPN 識別子を指定します。一方のみでかまいません。

- VPN ID を使用する場合は、VPN の vpn-id 属性値を設定します。値は IETF RFC 2685 に従って、通常は 16 進数で、 oui:index の形式です。この 3 オクテット VPN 組織固有識別子 (OUI) で構成され、その後に、VPN の所有者または ISP に対応し、その後にコロンが続きます。その後、VPN 自体の 4 オクテット インデックス番号が続きます。VPN ID の値を [VPNのリスト/追加（List/Add VPNs）] ページに追加します。CLI で、vpn-id 属性を設定します。次に例を示します。

```
nrcmd> vpn blue set vpn-id=a1:3f6c
```

- VPN ルーティングおよび転送(VRF)インスタンス名を使用する場合は、VPN のVRF 名属性値を設定します。シスコのルータは、VRF 名を頻繁に使用します。[VPNのリスト/追加（List/Add VPNs）] ページに VRF 名の値を追加します。CLI で、vrf 名属性を設定します。次に例を示します。

```
nrcmd> vpn blue set vrf-name=framus
```

ステップ 5 VPN の説明を追加します (オプション)。

ステップ 6 Add VPN をクリックします。VPN を編集して、[VPN の編集] ページの値を変更できます。

ステップ 7 VPN のスコープを作成します。

識別のために、VPN 名とスコープ名をできるだけ類似する必要があります。

1. Web UI の [デザイン（Design）] メニューから DHCPv4 サブメニューの下の [スコープ（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。
2. Web UI の上部にある [設定（Settings）] ドロップダウン リストの下にある [VPN] サブメニューから VPN を選択します。スコープの作成時に VPN を設定した後は、VPN を変更することはできません。

   CLI で、次の 3 つの方法のいずれかで、スコープがどの VPN に属しているかを特定します。

   - VPN 名は vpn属性(VPN ID をスコープに適用) で使用します。
   - vpn-id属性を介した VPN ID 自体。
   - コマンド ラインで VPN またはその ID を省略した現在のセッション VPN 名。

現在のセッションのデフォルト VPN を設定するには、セッション セット current-vpnを使用します。その後、スコープの通常のアドレス範囲と必要なオプションのプロパティを設定できます。次に例を示します。

```
nrcmd> scope blue-1921681 create 192.168.1.0 255.255.255.0 vpn=blue
```

または

```
nrcmd> scope blue-1921681 create 192.168.1.0 255.255.255.0 vpn-id=99
```

または

```
nrcmd> session set current-vpn=blue
nrcmd> scope blue-1921681 create 192.168.1.0 255.255.255.0
```

実行されるアクション（Then）

```
nrcmd> scope blue-1921681 addRange 192.168.1.101 192.168.1.200
nrcmd> scope-policy blue-1921681 setOption routers 192.168.1.1
```

ステージング DHCP 編集モードの場合は、すべての VPN とスコープを作成した後で DHCP サーバーをリロードします。

VPN の使用状況

VPN 名は、IP アドレス(リース)、スコープ、サブネットなど、Cisco Prime Network レジストラーの多くの DHCP オブジェクトを修飾するために使用されます。たとえば、リース名には次の構文を使用できます。

vpn/ipaddress

たとえば、red/192.168.40.0

VPN には、予約語globalとallを除く任意の一意のテキスト文字列を使用できます。データをリースglobalするall場合に使用できます。VPNglobalは [なし] VPN にマップされます。VPNallは、特定の VPN と [なし] VPN の両方にマップされます。

CLI では、オブジェクトの定義時に VPN またはその ID を省略すると、VPN は デフォルトで session set current-vpnによって設定された値になります。Web UI では、現在の VPN が定義されていない場合、デフォルトで [none] VPN が使用され、定義済み VPN の外部のすべてのアドレスが含まれます。

これらのオブジェクトには、関連する VPN プロパティがあります。

- Address blocks：アドレス ブロックの VPN を定義します。Design > DHCPv4 メニューから Address Blocks を選択して、[DHCPアドレスブロックの一覧/追加（List/Add DHCP Address Blocks）] ページを開きます（詳細モードで使用できます）。Web UI の上部にある [設定（Settings）] ドロップダウン リストの下にある [VPN] サブメニューから VPN を選択します。CLI で、作成およびdhcp-address-block属性設定コマンドを使用します。次に例を示します。

  ```
  nrcmd> dhcp-address-block red create 192.168.50.0/24

  nrcmd> dhcp-address-block red set vpn=blue

  nrcmd> dhcp-address-block red set vpn-id=99
  ```

（注） オブジェクトを作成する前に、vpn-id 値を dhcp アドレス ブロックを作成する必要がある VPN に設定します。vpn-id が常に現在の VPN であると仮定しないでください。

- Clientsand :外部ではなく、Cisco Prime Network レジストラー IP Express 内で VPN をプロビジョニングするのが最善の場合client-classesがあります。 この機能をサポートするために、クライアントまたはクライアント クラスの VPN を指定できます。次の 2 つの属性が提供されます。
  - default-vpn —着信パケットにvpn-idまたはvrf-name値がまだない場合にパケットが取得する VPN。属性は、クライアントおよびクライアント クラスで使用できます。
  - override-vpn —着信パケットのvpn-idまたはvrf-name値に何が提供されても、パケットは何を取得します。この属性は、クライアントとクライアントクラスで使用できます。クライアント クラスで優先 VPN を指定し、クライアントの既定の VPN を指定した場合、クライアント クラスのオーバーライド VPN がクライアントの既定の VPN よりも優先されることに注意してください。

  ローカル クラスタでClients、Client ClassesDesign>DHCPSettingsメニューから選択するか(詳細モードで利用可能)。クライアント クラスまたはクライアントを作成または編集し、default-vpn属性値とオーバーライド VPN属性値を入力します。

  地域クラスターで -Client ClassesDesign>DHCPSettingsメニューから (詳細モードで使用可能) を選択します。クライアントクラスを作成またはプルしてから編集し、default-vpn属性値とオーバーライド VPN属性値を入力します。

  CLI で、作成およびclient-class属性設定コマンドを使用します。次に例を示します。

  ```
  nrcmd> client 1,6,00:d0:ba:d3:bd:3b set default-vpn=blue

  nrcmd> client-class CableModem set override-vpn=blue
  ```

  たとえば、ケーブル モデムの導入では、override-vpn属性を使用してケーブル モデムをプロビジョニングできます。クライアント クラスはケーブル モデムのスコープを決定し、スコープは uBR の VPN を決定します。ケーブル モデムを介したユーザー トラフィックは、vpn-idサブオプションを設定して、特定の VPN を使用します。オーバーライド VPN 値は、クライアントに設定されたデフォルト VPNもオーバーライドします。

- Leases：リースのリスト、リースの表示、またはリース属性の取得。

  CLI で、リースをインポートするにはimport leases 、filenameを使用します。ファイル内の各リース エントリには、行の末尾に VPN を含めることができます。この機能が見つからない場合、Ciscoプライムネットワーク レジストラーは[none]VPNを割り当てます。（リース データのインポートとエクスポートも参照してください）。

  ```
  nrcmd> import leases leaseimport.txt
  ```

  VPN を含むようにアドレスまたはリースデータをエクスポートするには –vpn オプションの export leases を使用します。VPN 値の予約語 global または all

  - Global：定義された VPN（[none] VPN）の外部にあるアドレス。

- All：[なし] VPN を含むすべての VPN。

VPN を省略すると、エクスポートは によって設定された現在のsession set current-vpnVPN を使用します。現在の VPN が設定されていない場合、サーバーは [none] VPN を使用します。

```
nrcmd> export addresses file=addrexport.txt vpn=red

nrcmd> export leases -server -vpn red leaseexport.txt
```

- Scopes：DHCP を使用した仮想プライベート ネットワークの設定 （35 ページ） で説明しているとおり、範囲には VPN 名とその ID を含めることができます。

> 注 スコープの作成時に VPN を設定した後は、VPN を変更することはできません。

- Subnets：サブネットの一覧表示、サブネットの表示、またはサブネットの vpn 属性または vpn-id 属性の取得は VPN を示します。DHCP サブネットの割り当ての設定 （42 ページ） を参照してください。
- DHCP server：vpn-communication 属性が有効な場合（デフォルト）、DHCP サーバーは、DHCP リレーエージェント機能を強化して、DHCP サーバーと異なる VPN 上にある DHCP クライアントと通信できます。この機能は、リレー・エージェント情報オプション（82）のserver-id-override サブオプションによって示されます。

> 注 DHCP サーバーは、VPN に存在するクライアントに対して ping を実行しません。

サブネットの割り当ての設定

このセクションでは、オンデマンド アドレス プールのサブネット割り当てをサポートするように Cisco Prime Network レジストラー DHCP サーバーを設定する方法について説明します。

サブネット割り当てとは、クライアント (通常はルーターまたはエッジ デバイス) にサブネットをリースし、DHCP サービスを提供できるようにする方法です。この方法は、個々のクライアントアドレスの管理とともに使用したり、その代わりに使用できます。サブネット割り当てを使うと、DHCP インフラストラクチャによるサブネットのダイナミックな管理によって、IP アドレスのプロビジョニング、集約、特性評価、配布を大幅に改善できます。DHCP を介したサブネット割り当ては現在、Cisco IOS ソフトウェアでのみサポートされており、最新バージョンにはオンデマンド アドレス プール機能が組み込まれています。

（注） DHCP フェールオーバーには、DHCPv4 サブネット割り当ては含まれません。

関連項目

DHCP サブネットの割り当ての設定 （42 ページ）
VPN とサブネット割り当ての調整パラメータ （43 ページ）

DHCP サブネットの割り当ての設定

次のセクションでは、DHCP サーバーを使用してサブネット割り当てを設定する例を示します。図5は、プロビジョニング デバイスに割り当てられたサブネットを使用したサブネット割り当ての構成例と、従来の DHCP クライアント/サーバー構成を示しています。

サブネットを割り当てる前に、DHCP サーバーはまずクライアントが接続している VPN を次の順序で決定します。

1. サーバーは、着信 VPN オプションを検索し、VPN の値を使用します。
2. VPN オプションが見つからない場合、サーバーは Relay Agent サブオプション値を使用し、VPN をサブネット アドレスと結合して一意の識別子を形成します。
3. リレー エージェント サブオプションが見つからない場合、サーバーはクライアント・クラス情報 (選択タグ) を探します。

DHCP サブネット割り当てを構成するには、次の手順を実行します。

ステップ 1 サブネットの DHCP アドレス ブロックを作成し、初期サブネット マスクとその増分を設定し、他のサブネット割り当て要求属性を設定します。また、ポリシーを関連付けるか、組み込みポリシーを定義します。

- VPN を使用する場合は、vpn 属性または vpn-id 属性を指定できます（DHCP を使用した仮想プライベート ネットワークの設定 （35 ページ）を参照）。
- サーバーは、要求パケットにサブネット アロック DHCP オプション (220) の存在を使用して、パケットがサブネット割り当て要求であることを判断します。サーバーまたは VPN に addr ブロック使用選択タグ属性を設定する場合は、サブネット名サブオプション (3) を選択タグとして使用するようにサーバーを構成できます。
- オプションで、DHCP サーバーまたは VPN オブジェクトの addr ブロック -default-selection-tags属性を設定して、デフォルトの選択タグを設定できます。これは、アドレスを割り当てる 1 つ以上のサブネットを識別します。リレー エージェントがサブネットに関連付けられた VPN 文字列 (VPN オプションまたはリレー エージェント サブオプションを使用して) を送信する場合、その文字列を addr ブロック -default-選択タグ値の 1 つとして持つアドレス ブロックは、そのサブネットを使用します。
- サーバーと VPN の場合のデフォルトの動作では、DHCP サーバーは、クライアントが既に使用しているアドレス ブロックを使用して、クライアントにサブネットを割り当てようとします。addr ブロック

使用クライアント アフィニティ属性を無効にすると、サーバーはクライアントメッセージ内の他の選択データに基づいて、適切なアドレス ブロックからサブネットを提供します。

- 1 つの LAN セグメント上で複数のアドレス ブロックの構成をサポートする場合 (プライマリ スコープとセカンダリ スコープの使用に似ています)、セグメント名属性文字列値を DHCP アドレス ブロックに追加します。リレー エージェントは、単一のサブネット選択アドレスを送信するときに、そのセグメント名文字列値でタグ付けされたアドレス ブロックを選択します。ただし、LAN セグメント機能 (addr ブロック - lan-segments)をサーバーレベルまたは VPN レベルで明示的に有効にする必要もあります。
- ポリシーを関連付ける代わりに、アドレス ブロック埋め込みポリシーのプロパティを設定できます。クライアント、クライアント クラス、スコープの組み込みポリシーと同様に、アドレス ブロック ポリシーの属性を有効にしたり、無効にしたり、設定したり、設定を解除したり、取得したり、表示したりできます。また、DHCP オプションの設定、設定解除、取得、および一覧表示、およびベンダー オプションの設定、未設定、および一覧表示を行うこともできます。アドレス ブロックの埋め込みポリシーを削除すると、埋め込みポリシーのすべてのプロパティが解除されることに注意してください。

ステップ 2 サーバーは、リレー エージェント要求に基づいてサブネットを割り当てることに注意してください。要求されていない場合、既定のサブネット サイズは 28 ビットのアドレス マスクです。DHCP アドレス ブロックの既定サブネット サイズ属性を設定することで、必要に応じてこの既定値を変更できます。

次に例を示します。

```
nrcmd> dhcp-address-block red set default-subnet-size=25
```

ステップ 3 DHCP サーバーが作成するサブネットは、アドレス ブロックから制御できます。vpn-name/netipaddress/mask の形式でサブネットを識別し、vpn-nameはオプションです。サブネット制御には、リースと同様にサブネットのアクティブ化と非アクティブ化が含まれます。同様に、サブネットを強制的に使用できるようにし、その前に、サブネットが割り当てられたクライアントがサブネットを使用しなくなったことを確認する条件を満たすことができます。まず、作成されたサブネットを表示します。

ステップ 4 DHCP サーバーをリロードします。

VPN とサブネット割り当ての調整パラメータ

VPN およびオンデマンド のアドレス プールに対して、これらの調整パラメータを検討してください。

- Keep orphaned leases that have nonexistent VPNs：Cisco Prime Network レジストラー は、通常、関連付けられた VPN を持たないリースを Cisco Prime Network レジストラー 状態データベースに保持します。この変更は、 DHCP 属性の delete-orphaned-leases を有効にすることで変更できます。サーバーは、クライアントをリースに関連付けるリース状態データベースを保持します。スコープの変更によって既存のリースが無効になった場合、リース データベースには孤立したリース エントリが含まれます。サーバーは、このデータを使用してクライアントをリースに再関連付けしようとするので、通常はリースの期限が切れても削除されません。この欠点の 1 つは、リース データベースがディスク領域を過剰に消費する可能性があります。delete-orphaned-leases 属性を有効にすると、このようなリース デー

タベースエントリは、次回のサーバーの再ロード時に削除されます。ただし、この属性を有効にする場合は、リースを無効にレンダリングすると、サーバーが空きであると考えられるリースを使用するクライアントが発生する可能性があるため、注意が必要です。これにより、ネットワークの安定性が損なわれます。

- Keep orphaned subnets that have nonexistent VPNs or address blocks：これはデフォルトの動作ですが、DHCP 属性 DHCP を有効にして delete-orphaned-subnets を有効にすることで変更できます。DHCP サーバーは起動すると、サブネットのデータベースを読み取り、各サブネットの親 VPN とアドレスブロックの検索を試みます。この属性が有効な場合、サブネットがサーバーで構成されなくなった VPN を参照している場合、またはサーバーがサブネットを含む親アドレスブロックを見つけることができない場合、サーバーは状態データベースからサブネットを完全に削除します。
- Keep the VPN communication open：これはデフォルトの動作ですが、DHCP 属性 vpn-communication を無効にすることで変更できます。サーバーは、拡張 DHCP リレーエージェント機能を使用して、サーバーとは異なる VPN 上に存在するクライアントと通信できます。これは、リレーエージェント情報オプション(82)のvpn-idサブオプションの出現によって通知されます。サーバーがサーバーとは異なる VPN 上のクライアントと通信する必要がない場合は、vpn 通信属性を無効にできます。通常、その動機は、不正な DHCP クライアント アクセスを防止することで、ネットワーク セキュリティを強化することです。

BOOTP の設定

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

Cisco プライムネットワーク レジストラーを BOOTP サーバーのように動作するように設定できます。また、BOOTP では通常静的アドレス割り当てが必要ですが、IP アドレスを予約するか(したがって静的割り当てを使用する)、または BOOTP クライアントに IP アドレスを動的に割り当てるかを選択できます。

関連項目

BOOTP について （45 ページ）
スコープの BOOTP の有効化 （46 ページ）
BOOTP クライアントの移動または廃止 （46 ページ）

BOOTP について

BOOTP パケットを返すように DHCP サーバーを構成する場合、オプション領域以外のフィールドで、BOOTP はDHCP パケットの情報を必要とすることに注意してください。BOOTP デバイスは、DHCP パケットのブート ファイル(file)、 サーバー IP アドレス (siaddr)、およびDHCP パケットのサーバー ホスト名 (sname) フィールドに情報を必要とします (RFC 2131 を参照)。

すべての Cisco Prime Network レジストラー DHCP ポリシーには、ファイル、siaddr、または snameフィールドに直接返す情報を設定できる属性があります。Cisco Prime Network レジストラー DHCP サーバーは、ポリシー オプションを設定し、BOOTP デバイスに返すファイル、sname、またはsiaddrの値を決定する設定パラメータもサポートしています。

Cisco Prime Network レジストラーは、オプションと、DHCP クライアントに返すオプション、sname、またはsiaddrの値を設定できる、類似の設定パラメータをサポートしています。これは、DHCP 要求のdhcp パラメータ要求オプションで DHCP クライアントによって要求されるオプションに追加されます。したがって、BOOTP と DHCP の両方の応答パケットをデバイスに適切に設定できます。

ステップ 1 BOOTP 属性に使用する値を決定します。

- file：起動ファイルの名前
- siaddr：サーバー IP アドレス
- sname：任意のサーバーホスト名

ステップ 2 BOOTP クライアントに返すオプションとその値のリストを決定します。

ステップ 3 BOOTP 要求に関連付けるポリシーに、次の値を設定します。

- BOOTP クライアントに送信する属性（packet-siaddr、packet-file-name、packet-server-name）。
- BOOTP クライアントに戻すサーバー アドレスやドメイン名などのオプション値。
- BOOTP クライアントに返すフィールドとオプションのリスト。

ステップ 4 関連するスコープを BOOTP 処理用に使用可能にします。

ステップ 5 このスコープで、要求するBOOTP クライアントのアドレスを指定する場合は、動的BOOTP 処理を有効にします。動的BOOTP を有効にしていない場合は、このスコープでアドレスを指定する各BOOTP クライアントに予約を行う必要があります。

スコープの BOOTP の有効化

スコープに対して BOOTP 処理を有効にすることができます。ローカル クラスタ Web UI で作成されたポリシーに対して特定の属性と BOOTP 応答オプションを設定するか、または名前 policycreate[属性=値] とpolicy名前set属性=値[属性=値..] を使用して BOOTP を設定します。ポリシー属性とオプションをカンマ区切りリストとして設定します。属性は、クライアントブートプロセスで使用するエンティティです。

- packet-siaddr：次のサーバーの IP アドレス
- packet-file-name：ブートファイルの名前
- packet-server-name：サーバーのホスト名

サーバーは、これらの属性値の最初のインスタンスをポリシー階層に調べています。

CLI policy 名 setOption<opt-name|id>value[-blob] [-roundrobin] には、値の前に空白 (等号ではない) が必要です。-roundrobinが有効な場合、DHCP サーバーは、異なる回転順序で複数の値を含むオプションデータを返すように指示します。特定のクライアントは常に同じ順序を取得しますが、異なるクライアントは、クライアント識別子に基づいてオプションに対して構成された複数の値の順序の異なる「ローテーション」を取得します。

また、必要に応じて BOOTP および動的ブート・ブート・ブート・プログラムを使用可能にし、DHCP サーバーが BOOTP 要求を使用して DNS サーバーを更新することを確認します。次のオプションがあります。

- オプション dhcp-lease-time を設定します。
- dynamic-bootp 属性を有効にします。
- update-dns-for-bootp 属性を有効にします。
- update-dns-for-bootp 属性を有効にします。

BOOTP クライアントの移動または廃止

BOOTP クライアントを移動または使用停止にした場合、そのリースを再利用できます。BOOTP クライアントを使用停止にするには、そのリース予約をスコープから削除し、リースを強制的に使用可能にする必要があります。

ローカル クラスター Web UI でリースを使用するように強制するかscope、nameremoveReservation を使用します (ipaddr |マカドル|検索キー)[-mac |-**ブロブ**|-**文字列**]およびlease[VPN 名/]ipaddrforce-availableを CLI で実行します。

動的 BOOTP の使用

動的 BOOTP を使用する場合、その他の制限が適用されます、スコープ内のアドレスの使用には、BOOTP クライアントが永続的に割り当てられ、無期限のリースを受信します。

DHCPフェールオーバーを使用している場合、スコープの動的ブートオプションが有効になっていないサーバーが PARTNER-DOWN 状態になると、メイン サーバーとバックアップ サーバーのどちらで最初に使用できるかに関係なく、そのスコープから使用可能な IP アドレスを割り当てることができます。ただし、dynamic-bootpオプションが有効な場合、メインサーバーとバックアップサーバーは、独自のアドレスのみを割り当てることができます。したがって、dynamic-bootpオプションを有効にするスコープでは、フェールオーバーをサポートするためにより多くのアドレスが必要になります。

動的ブートを使用する場合:

1. 動的 BOOTP クライアントを単一のスコープに分離します。DHCP クライアントがそのスコープを使用できないようにします。ローカル クラスター Web UI で、スコープの BOOTP 属性の下で、dhcp属性を無効にします。CLI で、scope name disable dhcp を使用します。
2. DHCP フェールオーバーを使用している場合は、DHCP サーバーのフェールオーバー動的bootp-backup-percentage属性を設定して、このスコープのバックアップ サーバに対して、より大きな割合のアドレスを割り当てます。この割合は、通常のバックアップの割合よりも 50% も高くなる可能性があります。

BOOTP リレー

BOOTP リレーをサポートするルーターは、通常、DHCP サーバーを指すアドレスを持ちます。たとえば、Cisco ルータを使用している場合、特定のマシンのアドレスを含む IPヘルパー アドレスという用語が使用されます。この場合、このアドレスを使用して、すべての BOOTP (および DHCP) ブロードキャスト パケットを転送します。このアドレスは、ホストに最も近いルーターで構成してください。

ヒント DHCP クライアントが DHCP サーバーからアドレスを受信していない場合は、ネットワーク設定、特にルータまたはリレー エージェントの設定をチェックして、ネットワーク デバイスが Cisco Prime Network レジストラー DHCP サーバー アドレスを指す設定になっていることを確認します。