ダイナミックホストコンフィギュレーションの概要

インターネットアクセスを求めるすべてのホストは、IPアドレスを持っている必要があります。インターネット管理者は、新しいユーザーおよびコンピュータが別のサブネットに移動したすべてのユーザーに対して、次の操作を実行する必要があります。

1. 正当な IP アドレスを選択します。
2. アドレスを個々のデバイスに割り当てます。
3. デバイス構成パラメーターを定義します。
4. DNS データベースを更新し、デバイス名を IP アドレスにマッピングします。

これらのアクティビティは時間がかかり、エラーが発生しやすいため、動的ホスト構成プロトコル (DHCP) が発生します。DHCP を使用すると、IP アドレスを個別に割り当てる負担から解放されます。これは、TCP/IP の使用時に必要な設定の量を減らすため、Internet Engineering Task Force（IETF）によって設計されました。DHCP はホストに IP アドレスを割り当てます。また、接続しているインターネットネットワークの情報をホストが操作および交換するために必要なすべてのパラメータを提供します。

DHCP は TCP/IP 構成情報をローカライズします。また、DHCP を使用するように構成されたシステムに IP アドレスを自動的に割り当てることによって、TCP/IP 構成データの割り当てを管理します。したがって、各ホストを個別に構成しなくても、ホストがインターネットにアクセスできることを確認できます。

この章は、次の項で構成されています。

DHCP の仕組み

DHCP は、デバイス構成をサーバー レベルでグローバル アドレス プールに移行することで、動的アドレス割り当てを可能にします。DHCP はクライアント サーバー モデルに基づきます。クライアント ソフトウェアはデバイスで実行され、サーバー ソフトウェアは DHCP サーバーで実行されます。

サンプル DHCP ユーザー

Beth のワークステーション (bethpc) が DHCP で構成された後、次のアクションは、最初に起動したときに発生します。

1. 彼女の PC はネットワーク上の DHCP サーバーから IP アドレスを自動的に要求します。
2. DHCP サーバーは、IP アドレス、割り当てられたリース時間、その他インターネットを使用するために必要な構成データを含むリースを提供します。リースされたアドレスを他人が使用することはなく、彼女の PC でのみ有効です。
3. アドレスのリースが期限切れになる前に、bethpc は、リースを提供したサーバーからリース延長を要求することによってアドレスを更新できます。（通常、このプロセスは、最初に割り当てられたリース時間が約半分経過した時点で始まります）。これにより、有効期限が延長されます。リース時間の約 85% までにリースを更新できない場合、bethpc は、少し異なる要求の送信を開始して、使用可能なサーバーからリースの更新を試みます。サーバーに到達できない場合、Bethpc はリース期間が終了するまでリースを使用し続けます。

   まとめると、クライアントには 3 つの重要な時間があります。

   - **リース有効期限（Lease Expiration Time）（有効なライフタイム（Valid Lifetime））**：リースの有効期限が切れになるタイミング。これは常にクライアントに明示的に伝達されます。
   - **Renewal Time（T1）（更新時期）**：リースが許可されたサーバー、または最後にリースが延長されたサーバーで、クライアントが更新プロセスを開始できるタイミング。DHCPv4 の更新はユニキャストです。DHCPv6 の場合、クライアントは、リースが許可されたサーバー、または最後にリースが更新されたサーバーを指定します。

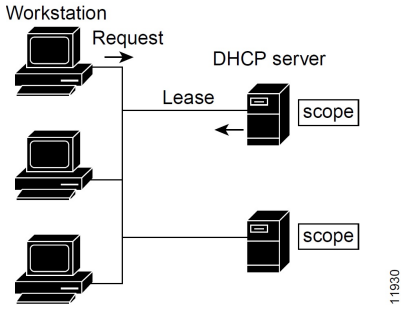
     更新時期（T1）は、サーバーによって明示的に通知されるか、またはクライアントが生成します。デフォルトでは、リース時間の 50% です。
   - **Rebinding Time（T2）（再バインド時期）**：クライアントが再バインドプロセスを開始できるタイミング。更新プロセスと似ていますが、単一のサーバーに制限されなくなりました。DHCPv4 の場合、これらの要求はブロードキャストされます（したがって、リレーによってピックアップされ、両方のフェールオーバーパートナーに転送されます）。DHCPv6 の場合、クライアントはサーバーを指定しないため、どのサーバーも応答できます。

再バインド時期（T2）は、サーバーによって明示的に通信されるか、またはクライアントが生成します。通常、リース時間の約 87.5%（DHCPv4 の場合）または、約 85%（DHCPv6 の場合）です。

4. ベスが別の部署に移動し、PC が別のサブネットに移った場合、現在のアドレスは期限切れになり、他のユーザーが利用できるようになります。新しい場所で自分の PC を起動すると、サブネット上の適切な DHCP サーバーからアドレスがリースされます（下の画像を参照）。

DHCP サーバーに正しい構成データが存在する限り、DHCP を使用するワークステーションまたはサーバーの構成が正しく行われなくなります。したがって、トレースが困難な、不適切に構成されたデバイスやサーバーからネットワークの問題が発生する可能性が低くなります。

図 *1* : ホストは *IP* アドレスを要求します



この例では、異なるサブネット上のアドレスを提供する一連の DHCP サーバーを含む DHCP プロトコルを示します。アドレス プールの管理をさらに簡単にするために、多くの場合、ネットワーク ルーターは、中央の DHCP サーバーにクライアント メッセージを転送する DHCP リレー エージェントとして構成されます。このサーバーは、サブネットのグループのアドレス プールで構成されています。

標準 DHCP 管理

DHCP を使用するには、ネットワーク上に少なくとも 1 つの DHCP サーバーが必要です。サーバーをインストールした後:

- DHCP サーバーが DHCP クライアントに提供できる IP アドレスのスコープを定義します。どのアドレスが使用されているか、どのアドレスが使用可能かを追跡する必要はなくなりました。
- 最初の DHCP サーバーがダウンした場合に、配布を共有したりリースを処理したりするようにセカンダリ サーバーを構成します。これは DHCP フェールオーバーと呼ばれます。DHCP フェールオーバーの管理の詳細についてはDHCP フェールオーバーの管理、を参照してください。

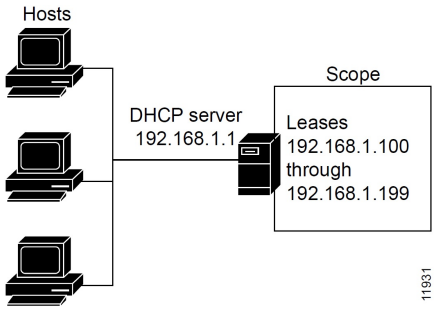
Leases

DHCP の最も大きな利点の 1 つは、IP アドレスを持つデバイスを動的に構成し、割り当てられたアドレスにリースを関連付けることができることです。DHCP は、ネットワーク内でアドレスを配布および再利用するための自動化された、信頼性が高く安全な方法を提供するリース メカニズムを使用しますが、管理者の介入はほとんど必要ありません。システム管理者は、ネットワークの特定のニーズに合わせてリース ポリシーを調整できます。

リースは、スコープと呼ばれるアドレス プールにグループ化され、要求ホストで使用できる IP アドレスのセットを定義します。リースは予約可能 (ホストは常に同じ IP アドレスを受け取る) または動的 (ホストは、スコープ内で次に使用可能な未割り当てのリースを受け取る) できます。サイトの DHCP サーバーは、アドレス 192.168.1.100 から 192.168.1.199 をリースするように構成されています (下の図を参照)。

スコープに構成されたアドレスよりも多くのネットワーク デバイスを使用しない場合は、ネットワーク トラフィックと DHCP サーバーの負荷を軽減するために、1 ~ 2 週間など、長いリース時間を定義できます。

図 *2: DHCP* サーバーからのリースを要求する *DHCP* ホスト



スコープとポリシー

スコープには、サブネットのアドレスのセットと、必要な構成パラメーターが含まれます。動的アドレス指定を行う各サブネットに対して、少なくとも 1 つのスコープを定義する必要があります。

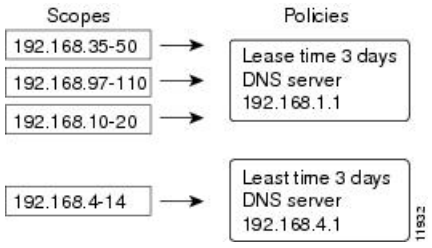
ポリシーには、DHCP サーバーがクライアントに通信するリース時間およびその他の構成パラメータが含まれます。ポリシーを使用して、要求に応じて DHCP サーバーがクライアントに提供する DHCP オプションを構成します。ポリシーを使用すると、DHCP サーバーがスコープごとに個別に指定しなくても、スコープに対して正しいオプションをすべて提供できます (下の図を参照)。

スコープとポリシーの違いは、スコープには、アドレスに関するサーバー情報 (どのアドレスが使えなくなっているか、リースを提供する前にクライアントに ping を実行するかどうかなど) が含まれることです。ポリシーには、ローカル DNS サーバーのリース期間やアドレスなどのクライアント構成データが含まれます。

ポリシーは、サーバー上に複数のスコープがある場合に特に便利です。すべてのスコープまたは選択したスコープに適用されるポリシーを作成できます。Cisco Prime Network レジストラー

ポリシー階層は、最も限定的なポリシーから最も具体的なポリシーを定義する方法です。たとえば、通常は各ポリシーにルーターオプションを指定します。このようなスコープ固有のポリシーは、スコープ埋め込みポリシーで定義できます。リース時間を参照するような、より一般的なポリシーは、システム全体のポリシーに適用できます（「DHCP ポリシーの設定」を参照）。ポリシーの割り当てを処理する拡張機能を作成することもできます（「DHCP サーバーの動作に影響を与える拡張機能の使用」を参照）。

図 *3:* スコープとポリシー



リンクとプレフィックス

明示的な DHCPv6 構成オブジェクトは、リンクおよびプレフィックスです。

- **Link**:1 つ以上のプレフィックスを持ち、DHCPv6 クライアントにポリシーを適用できる追加レイヤを追加できるネットワーク セグメント。
- **Prefix**— IPv4 のスコープに相当します。プレフィックスに関連付けられたリンクは、別のプレフィックスではなくリンクの名前を付ける点を除いて、プライマリ スコープに似ています。

スコープの場合と同様に、同じ IPv6 プレフィックスに対して複数のプレフィックス オブジェクトを作成できます。ただし、明示的な開始アドレスと終了アドレスを持つ複数の範囲をサポートするのではなく、プレフィックスは、プレフィックス オブジェクトと同じ長さ、または長い IPv6 プレフィックスである必要がある 1 つの範囲のみをサポートします。たとえば、2001:/64 のプレフィックスを 2001::/96 の範囲で定義すると、サーバーは 2001:0:0:0:0:0:0:0 から 2001:0:0:0:0:0:ffff のみアドレスを割り当てることができます。範囲:

- 2の累分に制限される。
- 一意である必要があります (別の VPN を除き、他の範囲で複製することはできません)。
- 以下で説明するプレフィックスの委任プレフィックスを除き、別の範囲に含めたり含めたりすることはできません。
- 以下で説明するプレフィックスの委任プレフィックスを除き、指定されていない場合は完全な IPv6 プレフィックスです。

プレフィックスの委任プレフィックス オブジェクトが指定されていない範囲で定義されている場合、プレフィックス委任プレフィックス以外のプレフィックスが含まれている可能性があり、有効範囲は次のいずれかになります。

- 同じ IPv6 プレフィックスを持つ他のプレフィックスが存在しない場合は、完全な IPv6 プレフィックス

- 同じ IPv6 プレフィックスを持つプレフィックス オブジェクトの他のすべての範囲が IPv6 プレフィックスから削除された場合に残るプレフィックス。

リンクを作成するのは、異なる IPv6 プレフィックスを持つ複数のプレフィックス オブジェクトがリンク上に存在する場合だけです。サーバーが設定をロードするときに、プレフィックスに明示的なリンクがない場合、サーバーはLink-vpn.name/]という名前の暗黙的なリンクを検索または作成します。同じIPv6プレフィックスを持つすべてのプレフィックス オブジェクトは、リンクを指定しないか、同じリンクを明示的に指定する必要があります。

DHCPv6 対応サーバーは、DHCPv6 の VPN アドレス空間をサポートします。リンクオブジェクトとプレフィックスオブジェクトの両方を VPN に割り当てることができます。ただし、リンク上のすべてのプレフィックスは同じ VPN ID を使用する必要があります。現在、DHCPv6 VPN オプションがないため、クライアントまたはクライアント クラスの*override-vpn*属性を使用して、クライアントに VPN からのアドレスを割り当てることのみが可能です。

関連項目

リンクとプレフィックスの決定

アドレスの生成

委任プレフィックスの生成

プレフィックス安定性

シスコ プライムネットワーク レジストラー DHCP 実装

Cisco プライムネットワーク レジストラー DHCP サーバーは、ネットワーク上のホストに IP アドレスを自動的に割り当てる信頼性の高い方法を提供します。DHCP クライアント設定を定義し、Cisco Prime Network レジストラーデータベースを使用して、クライアント IP アドレスの割り当ておよびその他のオプションの TCP/IP およびシステム設定パラメータを管理できます。TCP/IP 割り当て可能なパラメーターには、次のものがあります。

- ホスト内の各ネットワーク アダプタ カードの IP アドレス。
- 物理 (サブネット) ネットワーク識別子である IP アドレスの一部のサブネット マスク。
- サブネットを他のネットワーク セグメントに接続するデフォルト ゲートウェイ (ルーター)。
- ドメイン名など、DHCP クライアントに割り当てることができる追加の構成パラメータ。

Cisco プライムネットワーク レジストラーは、DHCP サーバー ソフトウェアをインストールすると、データベースを自動的に作成します。WEB UI または CLI を使用して、DHCP スコープとポリシーを定義するときにデータを追加します。

Cisco Prime Network レジストラー DHCP サーバーは、仮想プライベート ネットワーク(VPN)およびサブネットのアドレスをオンデマンド アドレス プール用のプール マネージャ デバイスに割り当てることもサポートしています。これらの機能の詳細については、以下の項で説明します。

関連項目

バーチャル プライベート ネットワーク （7 ページ）
サブネットの割り当てと DHCP アドレス ブロック

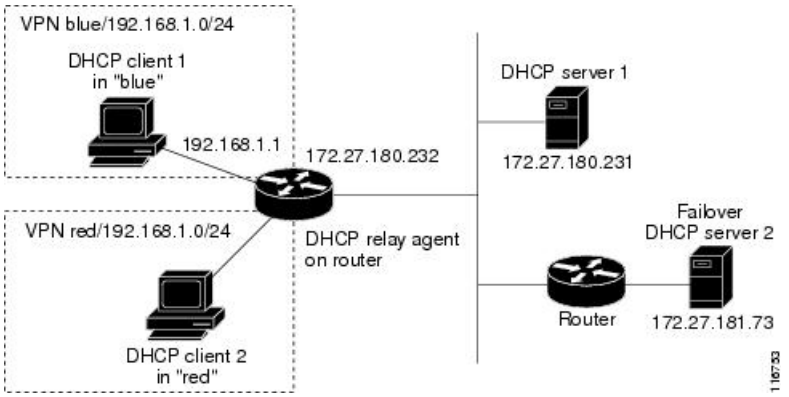
バーチャル プライベート ネットワーク

仮想プライベート ネットワーク（VPN）では、別々のネットワークの 2 つのプールが同じ DHCP サーバーが使用する同じアドレス空間をプライベート ネットワーク アドレスを使用して保持できます。これにより、貴重なパブリック アドレスを使用しなくても、アドレス リソースを節約できます。ただし、これらの VPN アドレスには、他の重複する IP アドレスと区別するために特別な指定子が必要です。クライアントと同じ VPN 上にない Cisco Prime Network レジストラー DHCP サーバーは、リースとアドレスをクライアントに割り当てることができ、1 つの VPN から別の VPN にアドレスを区別できます。

Cisco Primeネットワーク レジストラー DHCP サーバーおよび Cisco IOS DHCP リレー エージェントに加えられた変更を通じて、DHCP サーバーは複数の VPN 上のクライアントにサービスを提供できます。VPN は、DHCP サーバー オブジェクトのセットを区別し、他のアドレス空間にある同じオブジェクトから独立しています。同じアドレスを含む複数の VPN を定義できます。Cisco IOS リレー エージェントで設定された VPN 識別子に基づいて VPN を作成します。

次の図は、一般的な VPN 対応 DHCP 環境を示しています。DHCP リレー エージェントは、アドレス空間が重複する 2 つの異なる VPN(青と赤)にサービスを提供します。リレー エージェントは、VPN ブルーのインターフェイス アドレス 192.168.1.1 を持ち、DHCP サーバー 1 には 172.27.180.232 として知られています。DHCP クライアント 1 からの要求を VPN ブルーで処理するサーバーは、クライアントとは異なるネットワークまたはネットワーク セグメント上に配置でき、DHCP Server 2 でフェールオーバー構成に入ることができます（「DHCP フェールオーバーの管理」を参照）。リレー エージェントは、リレー エージェントと Cisco Prime Network レジストラー管理者の間で調整された、DHCP サーバーへのクライアント アドレス要求の特別な識別ルートを識別できます(RFC 6607 を参照)。DHCP サーバーは、両方の VPN 上のクライアントに重複する IP アドレスに基づいてリースを発行できるようになりました。

図 *4 :* バーチャル プライベート ネットワーク *DHCP* 構成

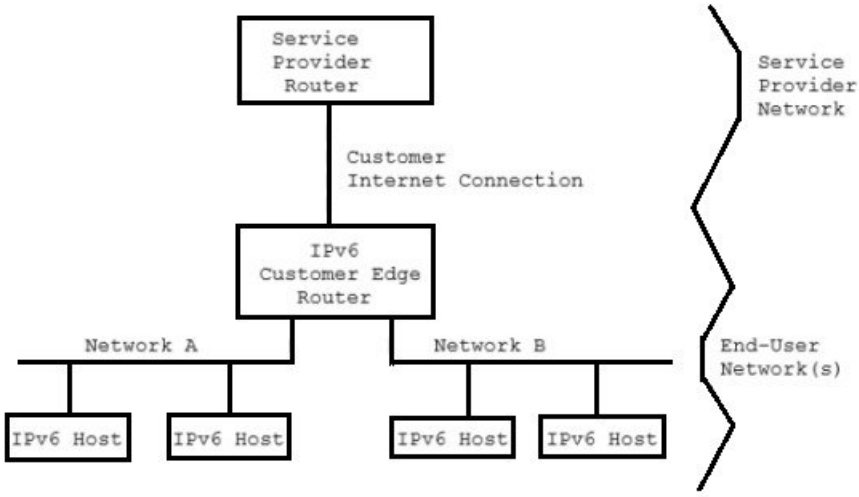


プレフィックス委任

プレフィックスの委任を使用すると、DHCPv6サーバーから要求元デバイスへのプレフィックスの委任が可能になります。プレフィックス委任は、顧客宅内機器(CPE)デバイスにプレフィックスを割り当てるサービスプロバイダによって使用されます。ISPは、プレフィックスをサブスクライバーに委任するためにも使用されます。

操作中に、要求側デバイスに委任するIPv6プレフィックスがDHCPv6サーバーに提供されます。要求側のデバイスは、DHCPv6サーバーにプレフィックスを要求します。DHCPv6サーバーは、委任のプレフィックスを選択し、要求側のデバイスにプレフィックスを付けて応答します。要求側のデバイスは、委任されたプレフィックスを担当します。たとえば、要求元のデバイスは、デリゲートされたプレフィックスからそのインターフェイスのいずれかにサブネットを割り当て、そのリンクのプレフィックスの通知の送信を開始できます。各プレフィックスには有効な有効期間と優先存続期間が関連付けられており、要求側のデバイスがプレフィックスを使用できる時間の長さに関する合意が構成されます。要求元のデバイスは、デリゲートされたプレフィックスの有効期間の延長を要求でき、プレフィックスの有効期間が期限切れになった場合に委任されたプレフィックスの使用を終了する必要があります。

図 *5:* エンドユーザーネットワークのモデルトポロジ



DNS 更新

DHCPはIPアドレスの配布の負担から解放されますが、DHCPクライアントの名前とアドレスを使用してDNSサーバーを更新する必要があります。DNS更新は、名前とアドレスを最新の状態に保つタスクを自動化します。Cisco Prime Network レジストラー DNS アップデート機能を使用すると、名前とアドレスの関連付けが発生または変更されたときに、DHCPサーバーは対応するDNSサーバーに伝えることができます。クライアントがリースを取得すると、Cisco Prime Network レジストラーはDNSサーバーにホスト データを追加するように指示します。

リースの期限が切れた場合、またはホストがリースを終了すると、Cisco Prime Network レジストラーは DNS サーバーにアソシエーションを削除するように指示します。

通常の動作では、DHCP を介してクライアントのアドレスが変更される頻度に関係なく、DNS を手動で再構成する必要はありません。Cisco プライムネットワーク レジストラーは、クライアント デバイスが提供するホスト名を使用します。また、Cisco Prime Network レジストラーで、クライアントを提供しないクライアントの名前を合成したり、クライアントルックアップ機能を使用してクライアントに事前設定されたホスト名を使用したりすることもできます。

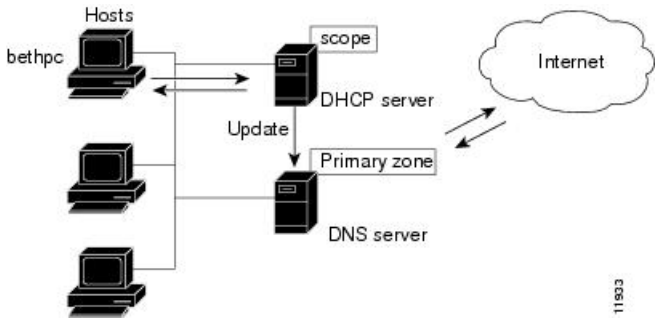
DHCPv4 および DHCPv6 DNS 更新のユース ケースが異なるために、ホスト名の更新を処理するためにサーバーの設計が異なりました。したがって、ホスト名の DHCPv4 および DHCPv6 DNS 更新の動作の違いが予想されます。

DNS へのリース取得の影響

ExampleCo の場合、管理者は DHCP サーバーにスコープを作成し、100 のリースを割り当てます (192.168.1.100 から 192.168.1.199)。各デバイスは、その所有者名を取得します。また、管理者は、DNS 更新を使用するように DHCP サーバーを構成し、それに対応する構成済み DNS サーバーに関連付けます。管理者は、DNS サーバー データベースに名前を入力する必要はありません。

月曜日の朝、ベス（bethpc のユーザー）は、アドレスなしでウェブサイトにログインしようとします。ホストが起動すると、アドレス要求をブロードキャストします(下の画像を参照)。

図 *6 :* 企業の *DNS* 更新



DHCP サーバーは次のようになります。

1. 次に使用可能な(未割り当て)IPアドレス(192.168.1.125)を bethpc に与えます。
2. ホスト名とアドレス (bethpc 192.168.1.125) で DNS サーバーを更新します。

ベスはウェブサイトにアクセスできるようになりました。さらに、Beth のコンピュータ名を自分の IP アドレスに変換する必要があるプログラム、または逆の方法で DNS サーバーにクエリを実行することもできます。

リース再獲得の DNS への影響

ベスは再び彼女のホストを起動するために彼女の旅行から戻ったとき:

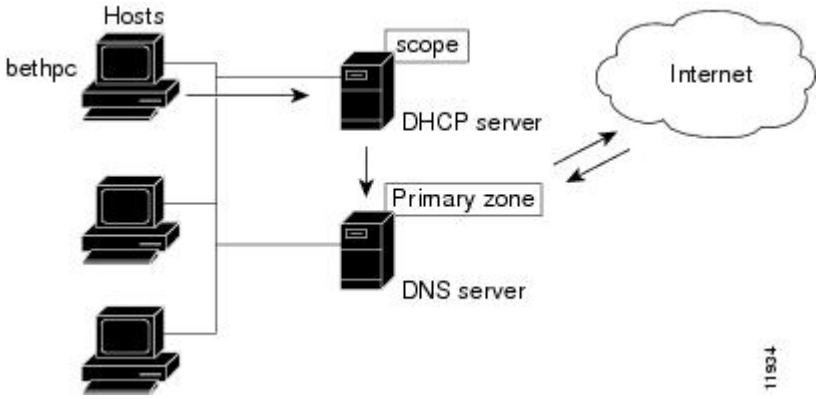
1. 彼女の PC は IP アドレスをブロードキャストします。
2. DHCP サーバーは、ホストが正しいネットワーク上にあるかどうかを確認します。その場合、サーバーはアドレスを発行します。正しくない場合は、正しいネットワーク上のサーバーがアドレスを発行します。
3. DHCP サーバーは、ホストとアドレスのデータを使用して DNS サーバーを再度更新します。

リースのリリースによる DNS への影響

その日の後半,ベスは町を出て行く必要があることを知りました。彼女は、3日後に期限切れになるリースアドレスをまだ持っているホストをオフにします。リースが解放されると、DHCP サーバーは次の処理を行います。

1. IP アドレスが他のユーザーに対して利用可能になったことを確認します(下の図を参照)。
2. ホスト名とアドレスを削除して DNS サーバーを更新します。DNS サーバーは、bethpc またはそのアドレスに関するデータを保存しなくなりました。

図 *7:* リースの放棄



DHCP フェールオーバー

Cisco Prime Network レジストラーフェールオーバープロトコルは、何らかの理由でメインサーバーがオフラインになった場合に、バックアップ DHCP サーバーが引き継がれるように設計されています。8.2 より前のバージョンでは、このプロトコルは UDP ベースで、IPv4 経由でのみ動作し、DHCPv4 のみをサポートしていました。8.2 以降、このプロトコルは TCP ベースで、IPv4 または IPv6 のいずれかを使用するように構成でき、単一の接続で DHCPv4 と DHCPv6 の両方をサポートします。DHCP サーバーは、両方を使用するように構成されている場合、IPv4 と IPv6 の両方のトランスポートを試行し、最初に起動した接続を使用します。既存の DHCP クライアントは、どのサーバーが要求に応答するかを知らなくても、リースを維持および更新できます。

フェールオーバー ペアは、Cisco Prime Network レジストラーのローカル クラスタとリージョン クラスタで作成および同期できます。詳細については、DHCP フェールオーバーの管理 を参照してください。

フェールオーバーによるアドレスの割り当て

ネットワーク パーティションが相互に通信できるが、相互通信できないネットワーク パーティションにもかかわらず、フェールオーバー ペアを動作させるには、単一サーバーの実行に必要なアドレスよりも多くのアドレスを使用できるようにする必要があります。メイン サーバーを構成して、各スコープまたはプレフィックス委任アドレス プールで現在使用可能な (割り当てられていない) アドレスの割合をパートナーに割り当てます。これらのアドレスは、メイン サーバーで使用できなくなります。パートナーは、メイン サーバーとの間で話ができないときに、メイン サーバーがダウンしているかどうかを知らない場合に、これらのファイルを使用します。ただし、フェールオーバー パートナーが通信中に、定期的にこれらのプールのバランスを調整します。

バックアップ サーバーは、メイン サーバーがダウンしているかどうかをバックアップが認識しない期間に到着したすべての新しいDHCPクライアントの要求を満たすのに、各スコープまたはプレフィックスから十分なアドレスを必要とします。フェールオーバー ペアの既定のバックアップの割合は 50% です。これにより、フェールオーバー中に他のパートナーのアドレス数が同じになります。

PARTNER-DOWN 状態の間でも、バックアップ サーバーはリースの有効期限とクライアントの最大リードタイム(MCLT)、小さな追加のタイム バッファを待ってから、リースを再割り当てします。これらの時間が経過すると、バックアップ サーバーは次の機能を提供します。

- アドレスのプライベート プールからのリース。
- アドレスのメイン サーバー プールからのリース。
- 新しいクライアントへのリースの期限が切れています。

稼働時間内に、管理スタッフが COMMUNICATIONS INTERRUPTED 状態に 2 時間以内に応答してメイン・サーバーが稼働しているかどうかを判別できる場合、バックアップ・サーバーは、新規DHCPの数に対して妥当な上限をサポートするのに十分なアドレスを必要とします。この 2 時間の間に到着する可能性のあるクライアント。

営業時間外に、管理スタッフが同じ状況に 12 時間以内に応答でき、DHCP クライアントから以前に知られていなかった到着率も少ないと考えると、バックアップ サーバーは妥当な上位をサポートするのに十分なアドレスを必要とします。この 12 時間の間に到着する可能性のあるDHCP クライアントの数に制限されます。

したがって、バックアップ サーバーが単独で制御するアドレスの数は、ピーク時およびピーク時以外に指定されたアドレスの数のうち、それぞれで現在利用可能な(未割り当て)アドレスの割合で表されるアドレスの数です。スコープまたはプレフィックス。

（注） DHCP フェールオーバー ペアの既定の使用セーフ期間が有効になり、既定のセーフ期間は 4 時間です。これにより、フェイルオーバー・パートナーが 4 時間の COMMUNICATIONS-INTERRUPTED 状態の場合、安全期間が経過した後に自動的に PARTNER-DOWN 状態になります。

クライアントクラス

Cisco Prime Networkレジストラークライアントおよびクライアント クラスの機能を使用して、共通のネットワークに接続されているユーザーに差別化されたサービスを提供できます。管理基準に基づいてユーザー・コミュニティをグループ化し、各ユーザーが適切なサービス・クラスを受け取れるようにすることができます。

Cisco Prime Network レジストラークライアント クラス機能を使用して、設定パラメータを制御できますが、最も一般的な用途は次のとおりです。

- **Lease periods**：一連のクライアントがアドレスを保持する期間。
- **IP address ranges**：クライアントアドレスを割り当てるリースプールの元。
- **DNS server addresses**：クライアントが DNS クエリを送信する場所。
- **DNS hostnames**：クライアントを割り当てる名前。
- **Denial of service**：許可されていないクライアントにリースを提供するかどうか。

クライアントクラスの機能を使用する 1 つの方法は、訪問者がネットワークの一部 (すべてではない) にアクセスできるようにすることです。たとえば、ExampleCo の訪問者である Joe がラップトップをexample.com ネットワークに接続しようとすると、Cisco Prime Network レジストラーはラップトップを外部として認識します。ExampleCo は、ネットワーク全体へのアクセス権を持つクライアントの1つのクラスを作成し、サブネットへのアクセス権を持つ別の訪問者クラスを作成します。Joeが標準訪問者アクセス以上のものを必要とする場合は、ラップトップを Cisco Prime Network レジストラーシステム管理者に登録し、適切なサービスを使用して別のクラスに追加できます。

次のセクションでは、DHCPが通常アドレス割り当てを処理する方法、およびクライアント クラス機能を有効にして DHCP がアドレス割り当てを処理する方法について説明します。

クライアントクラスなしの DHCP 処理

クライアント クラスの処理を適用する方法を理解するには、DHCPサーバーがクライアント要求を処理する方法を理解しておくと役立ちます。サーバーは、次の3つのタスクを実行できます。

- IP アドレスを割り当てます。
- 適切な DHCP オプション(構成パラメータ)を割り当てます。
- 必要に応じて完全修飾ドメイン名 (FQDN) を割り当て、その名前で DNS サーバーを更新します。

以下は、その DHCP サーバーによる追加処理です。

1. 定義されたスコープからクライアントにアドレスを割り当てる: クライアントのアドレスを選択するには、DHCP サーバーが要求パケットの内容に基づいてクライアント サブネットを決定し、そのサブネットに適したスコープを見つけます。

   1 つのサブネットまたは複数のネットワーク セグメント (マルチネット化) に複数のスコープがある場合、DHCP サーバーはラウンドロビン方式でこれらのスコープの中から選択するか、DHCP サーバー のアドレス割り当て優先順位機能を使用してスコープの選択の優先順位割り当て優先順位を使用した複数スコープの設定を変更できます (を参照してください)。サーバーは、スコープを選択した後、そのスコープから使用可能な (割り当てられていない) アドレスを選択します。

   1. 定義されたポリシーから DHCP オプション値を割り当てます。Cisco プライムネットワーク レジストラーでは、オプションをグループ化するポリシーを使用します。ポリシーには、スコープ固有とシステムの既定の 2 種類があります。クライアントが要求する DHCP オプションごとに、DHCP サーバーは定義された順序で値を検索します。
   2. スコープ固有のポリシーにオプションが含まれている場合、サーバーはその値をクライアントに返し、検索を停止します。
   3. 見つからない場合、サーバーはシステムのデフォルト・ポリシーを調べ、その値を戻し、検索を停止します。
   4. どちらのポリシーにもこのオプションが含まれている場合、サーバーはクライアントに値を返さないので、エラーをログに記録します。
   5. サーバーは、要求されたオプションごとにこのプロセスを繰り返します。

2. DNS 更新が有効な場合、サーバーはクライアントに FQDN を割り当てます。DNS アップデートを有効にした場合、Cisco Prime Network レジストラーは DNS ホスト テーブルにクライアント名とアドレスを入力します。DNS 更新 （8 ページ）を参照してください。クライアント名は次のことができます。

   - クライアント リース要求で指定された名前 (既定値)。
   - その MAC アドレス (ハードウェア アドレス、たとえば、00:d0:ba:d3:bd:3b)。
   - デフォルトのプレフィックス*dhcp*または指定したプレフィックスを使用する一意の名前。

クライアントクラスがある DHCP 処理

DHCP サーバーのクライアント クラス機能を有効にすると、要求処理は IPクライアントクラスなしの DHCP 処理 （12 ページ）アドレス、オプション、およびドメイン名を割り当てるのと同じ 3 つのタスクを実行しますが、機能が追加されます。以下は、その DHCP サーバーによる追加処理です。

1. **Considers the client properties and client-class inclusion before assigning an address**：通常の DHCP 処理と同様に、DHCP サーバーはクライアント サブネットを決定します。次に、サーバーは、クライアント クラスが定義されているか、またはこのクライアントの MAC アドレスがデータベースに存在するか確認します。次の場合：

1. クライアント クラスの検索 ID 式によって定義されたクライアント クラスは、このクライアント クラスのメンバーになります。
2. MACアドレスなし、デフォルトのクライアントを使用します。たとえば、既定のクライアントではクライアント クラス名を Guest に設定し、クライアント クラスは、クライアントが許可されるネットワーク操作を制限できます（オプションとアドレスの選択を使用）。
3. MAC アドレスがなく、デフォルトのクライアントも、サーバーは通常の DHCP 処理を通じてクライアントを処理します。
4. クライアント指定子はありませんが、MAC アドレスは、MAC アドレスはクライアント指定子に変換されます。既定のクライアントが定義されている場合、不明なクライアントが既定のクライアントにマップされます。

スコープには、クライアントからアクセス可能なサブネット上のアドレスが必要です。つまり、クライアントクラスに関連付ける選択タグが必要です。同じクライアントを異なるアドレス プールに割り当てるには、別々のスコープを使用する必要があります。

たとえば、スコープにはEmployeeまたはGuestの選択タグが付いていますが、両方は使用できません。この場合、各サブネットには 2 つのスコープがあります。1 つは選択タグ Employee、もう 1 つはゲストです。各スコープには、ユーザー グループに適切なアクセス権を提供する、関連付けられたポリシーとアドレス範囲が異なります。

2. **Checks for** :通常**client-class**の DHCP 処理では、サーバーはスコープ固有の DHCP オプションとシステムデフォルトの DHCP オプションをチェックします。 **DHCP options** クライアント クラスでは、まずクライアント固有のオプションとクライアント クラス固有のオプションもチェックします。
3. **Provides additional -FQDN**クライアントが要求するホスト名を使用する通常の名前割り当てプロセスを超えて、サーバーは次のことができます。 **assignment options**
   - それをオーバーライドする明示的なホスト名を指定します。
   - クライアントが要求したホスト名を削除し、置き換えないようにします。
   - クライアントの MAC アドレスからホスト名を合成します。

クライアントクラスへのスコープの定義

クライアント クラスを使用する動機付けの要因は、1 つまたは別のアドレス プールからクライアントにアドレスを提供することです。もう 1 つの動機として、クライアントに異なるオプション値またはリース時間を提供することが考えられます。クライアントに別のプールからアドレスを提供するには、複数のスコープを定義する必要があります。

サブネット上で複数のスコープを取得するには、同じネットワーク セグメントから取得する必要があります。ネットワークは、Cisco Primeネットワーク レジストラーでは直接設定されませんが、スコープ設定から推測されます。スコープが関連付けられるようになる (最終的には同じネットワークに入る):

- **Implicitly**-2 つのスコープのネットワーク番号とサブネット マスクが同じ。これらのスコープは、明示的な構成なしで同じネットワーク上で自然に終了します。

- **Explicitly**- 1 つのスコープは、別のスコープに対するセカンダリとしてマークされます。これは、セカンダリとしてマークされたスコープに、プライマリとは無関係のネットワークとサブネットマスクがある場合に必要です。たとえば、通常のルーティング可能なネットワークセグメントに10.0.0.0ネットワークアドレスのセットを配置する場合が考えられます。

Cisco Prime Network レジストラー DHCP サーバーがデータベースからスコープ設定を読み取ると、すべてのスコープがネットワークに配置され、この情報がログに記録されます。同じネットワーク番号とサブネット マスクを持つスコープは同じネットワークに終わり、セカンダリ スコープはプライマリ スコープ ネットワークに終わります。

ネットワークとスコープの選択

DHCP パケットが到着すると、サーバーは、受信元のアドレスを決定します。

- DHCPv4 パケットが到着すると、サーバーはゲートウェイ アドレス (*giaddr*) を決定します (もしあれば、BOOTP リレーを介して送信されたパケットの場合)。
- DHCPv6 の詳細については、リンクとプレフィックスの決定を参照してください。
- DHCP クライアントが DHCP サーバーも直接接続されているネットワーク セグメント上にある場合、ブロードキャストパケットが到着したインターフェイスのインターフェイス アドレス。

いずれの場合も、DHCPサーバーはゲートウェイまたはインターフェイスアドレスからネットワークを決定します。次に、ネットワークに複数のスコープがある場合、サーバーはDHCPクライアントにアドレスを割り当てるスコープを決定します。常に、このタイプのクライアントにアドレスを割り当てることができるスコープを探します。たとえば、DHCPクライアントにはDHCPをサポートするスコープが必要で、BOOTPクライアントはBOOTPをサポートするスコープを必要とします。クライアントがDHCPクライアントであり、DHCPをサポートするスコープが複数あり、それぞれが使用可能な (割り当てられていない) アドレスを持つ場合、DHCP サーバーは、それらのスコープのいずれかから IP アドレスをラウンドロビン方式で、または割り当て優先順位によって割り当てます。

選択タグとクライアントクラスを使用すると、次のIPアドレスを割り当てるようにDHCPサーバーを構成できます。

- ネットワーク上の 1 つ以上のスコープを 1 つのクラスのクライアントに対して行います。
- 異なるクラスのクライアントに対するスコープの異なるセット。

後者の場合、ゲートウェイまたはインターフェイスアドレスによってネットワークが決まります。クライアントクラス機能は、選択タグのメカニズムを通じて、使用するネットワーク上のスコープを決定します。

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。