CHAPTER 2

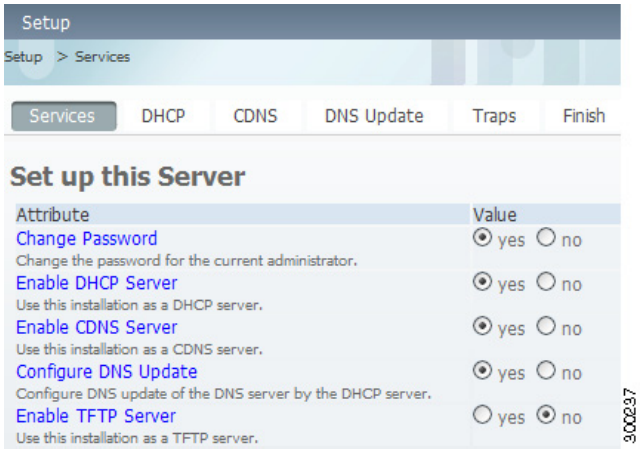
セットアップ Web UI の実行

Web ユーザ インターフェイス（UI）の Cisco Prime Network Registrar セットアップ インタビューでは、連続する一連のページで基本設定を行うことができます。これらのページの概要、設定シナリオ、および基本ナビゲーションの詳細については、第 1 章「セットアップ Web UI の概要」を参照してください。

サービスの設定

ローカルの基本ユーザ モードでメイン メニューの [Setup] をクリックすると、[Set up this Server] ページが開きます。すぐにセットアップ モードに移行し、[Basic] タブと [Advanced] タブが表示されなくなります（図 2-1（P.2-1）を参照）。

図 2-1　[Set up this Server] ページ（Setup）



このページでは、次の機能をイネーブルにするかディセーブルにするかを決定します。

- **管理者パスワードの変更**：セキュリティ上の理由から、Cisco Prime Network Registrar のインストール時または Cisco Prime Network Registrar Web UI への初回ログイン時に設定した値から管理者パスワードを変更する必要があります。詳細については、「管理者パスワードの変更」（P.2-2）を参照してください。
- **ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）サーバ**：DHCP には、Cisco Prime Network Registrar の重要な部分であるダイナミック アドレス割り当てのメカニズムが用意されています。DHCP をイネーブルにすると、DHCP セットアップの一連のページが表示されます。ディセーブルにすると、DHCP セットアップは省略されます。詳細については、「DHCP サービスの設定」（P.2-2）を参照してください。

- **キャッシング ドメイン ネーム システム（CDNS）サーバ**：CDNS には、ドメイン ネーム構造が用意されています。CDNS をイネーブルにすると、CDNS セットアップの一連のページが表示されます。ディセーブルにすると、CDNS セットアップは省略されます。詳細については、「CDNS サービスの設定」（P.2-7）を参照してください。
- **権威ドメイン ネーム システム（DNS）サーバ**：DNS には、ドメイン ネーム構造が用意されています。DNS をイネーブルにすると、DNS セットアップの一連のページが表示されます。ディセーブルにすると、DNS セットアップは省略されます。詳細については、「DNS サービスの設定」（P.2-9）を参照してください。
- **DNS 更新**：DNS 更新は、DHCP を使用したダイナミック アドレッシングの利点を永続的で固有の DNS ホスト名と組み合わせたものです。これにより、ネットワーク アクセスのための DNS ホストを自動的に設定できます。DHCP サーバは DNS サーバがリソース レコード（RR）を最新の状態に維持できるように DNS サーバに通知します。DNS 更新をイネーブルにすると、DNS 更新セットアップの一連のページが表示されます。ディセーブルにすると、DNS 更新セットアップは省略されます。詳細については、「DNS 更新の設定」（P.2-13）を参照してください。
- **Trivial File Transfer Protocol（TFTP）サーバ**：アドレスのプロビジョニングのためのファイルをケーブル モデムに転送できるように、TFTP サーバをイネーブル化する必要があります。TFTP をイネーブルにするのにセットアップ ページでさらに設定を行う必要はありません（「Setup Interview Report」（P.2-14）を参照）。

（注）　選択内容はログイン セッションを越えて保持されます。

選択内容に応じて次のページに移動するには [Next>>] をクリックし、セットアップを終了して [Setup Interview Report] ページに移動するには [Finish] をクリックします。

管理者パスワードの変更

セットアップ インタビューの [Set up this Server] ページで [Change Password] の値を [yes] に設定した場合は、[Change Password for User] ページが開きます。

パスワードの変更後は、次回以降の管理者ログインで新しいパスワードを使用します。

パスワードを変更しない場合は、[no] チェックボックスをオンにします。パスワードを変更するには、新しいパスワードを入力し、[Verify] フィールドにもう一度入力して確認します。[Next>>] または [Finish] をクリックすると、次のログイン セッションのために変更が送信されます（ある場合）。

DHCP サービスの設定

セットアップ インタビューの [Set up this Server] ページで [Enable DHCP Server] の値を [yes] に設定した場合は、適切な順序で [Set up DHCP] ページが開きます。このページは、ナビゲーション バーで [DHCP] をクリックした場合も開きます。

DHCP サーバを設定するには、このページで [Enable DHCP Server] の値が [yes] に設定されていることを確認します。すでに Cisco Prime Network Registrar でメイン DHCP サーバを設定し、そのサーバと同期している場合は、セットアップ プロセスによって、現在のホストがすでにバックアップ サーバであるためこれ以上の DHCP 設定が必要ないことが示されます。

次の項に基づいて設定値を選択し、[Next>>] をクリックします。セットアップ プロセスによって設定がアクティブになり、その後はスコープ（アドレス プール）設定用のページが表示されます。

DHCP フェールオーバーのイネーブル化

DHCP フェールオーバーの設定では、メイン サーバが何らかの理由でネットワークから切断された場合に処理を引き継ぐことができるバックアップ DHCP サーバを指定します。サーバは冗長ペアとして機能し、相互に通信してアドレスの重複割り当てを防ぎます。

フェールオーバー サービスを提供するには、[Enable DHCP Failover] の値を [yes] に設定します。セットアップ プロセスで既存の複雑なフェールオーバー設定が検出された場合は、セットアップ インタビューではフェールオーバーを設定できないことが通知されます。DHCP フェールオーバーがすでに拡張モードで設定され、次のいずれかの条件が満たされる場合、DHCP フェールオーバーを設定できません。

- 複数のフェールオーバー ペアが設定されている。
- 1 つのフェールオーバー ペアが存在し、main-server、backup-server、または network-match-list の値が設定されている。

フェールオーバー設定の詳細については、「DHCP フェールオーバーの設定」（P.2-4）を参照してください。

DHCP サービス クラスのイネーブル化

サービス クラスは、DHCP クライアントにディファレンシエーテッド サービスを提供します。最も一般的なサービスは次のとおりです。

- アドレス リース
- IP アドレス範囲
- クライアントにサービスを提供する DNS サーバのアドレス
- ホスト名の割り当て
- アクセス コントロールによるサービス拒否

セットアップ ページで定義したサービス クラスによって最終的に次のものが定義されます。

- サービス クラスと同じ名前の DHCP クライアント クラス。
- サービス クラスと同じ名前の DHCP ポリシー。
- 選択タグがサービス クラスとして定義されている場合は DHCP スコープの割り当て。

サービス クラス設定の詳細については、「DHCP サービス クラスの設定」（P.2-4）を参照してください。

サーバ ロギング モード

DHCP サーバは、メッセージ出力のモードを設定できるログ メッセージを提供します。[Server Logging Mode] オプションには、特定のロギング設定に変換される 4 つの値を指定できます。

- **normal-operations**（プリセット値）：通常のロギングが行われます。
- **high-performance**：高パフォーマンス ロギングが行われます。
- **debugging**：デバッグ ロギングが行われます。
- **customized**：特定のログ設定を求めるメッセージを表示し、その設定のみを記録します。

DHCP トラップのイネーブル化

DHCP サーバの SNMP トラップを設定すると、サーバが起動しているかどうか、パートナー通信のステータス、および特定の数の利用可能な下限フリー アドレスと上限フリー アドレスがあるかどうかを報告できます。DHCP トラップはデフォルトではイネーブルになっていないため、イネーブルにするにはこの値を [yes] に設定する必要があります。詳細については、「DHCP トラップの設定」（P.2-6）を参照してください。

DHCP フェールオーバーの設定

セットアップ インタビューの [Set up DHCP] ページで [Enable DHCP Failover] の値を [yes] に設定した場合は、適切な順序で [Set up DHCP Failover] ページが開きます。

[Enable DHCP Failover] のプリセット値は [yes] で、[DHCP Failover Role] は [main] にプリセットされています。現在のマシンのロールを [backup] に変更した場合は、このマシンに対するフェールオーバー設定をこれ以上行うことができません。（メイン サーバ マシンに対してフェールオーバー設定を実行し、そのマシンからフェールオーバー同期を実行するよう推奨するメッセージが表示されます）。同様に、Cisco Prime Network Registrar で複雑なフェールオーバー設定が検出された場合は、警告メッセージが表示され、フェールオーバー設定のセットアップをスキップする必要があります。

[Failover Partner] の値によって、リモート バックアップ サーバのアドレスとアクセス基準が決まります。そのサーバのクラスタがすでに存在する場合は、[Select existing cluster] ドロップダウン リストからクラスタを選択できます。既存のクラスタがない場合は、バックアップ サーバのクラスタを設定できます。

1. バックアップ DHCP サーバのホスト名または IP アドレスを入力します。
2. バックアップ サーバのアクセス基準として、管理者の名前とパスワード、SCP ポート番号（**1234** にプリセット）を入力します。
3. [Add Cluster] をクリックしてクラスタを追加します。

フェールオーバー ペアをパートナー サーバ間のリース割り当てがサーバごとにアドレス プールの 50% であるロード バランシング関係にするかどうかを決定します。このロード バランシングを有効にする場合は、[Load Balancing] の値を [yes]（プリセット値は [no]）に設定します。

設定値を選択するか入力し、[Next>>] をクリックして設定をアクティブにすると、他の DHCP 設定を実行できます。

DHCP サービス クラスの設定

セットアップ インタビューの [Set up DHCP] ページで [Enable DHCP Classes of Service] の値を [yes] に設定した場合は、適切な順序で [Set up DHCP Classes of Service] ページが開きます。

[Enable DHCP Classes of Service] のプリセット値は [yes] です。[Class of Service Usage] では、着信 DHCP パケットが着信パケットに基づいてサービス クラスを決定するか、このページで個別にクライアントを登録するかどうかを設定します。着信パケットによってサービス クラスを割り当てる場合は、*client-class-lookup-id* DHCP サーバ属性の式の設定など、拡張モードでいくつかの設定を行う必要があります。（「着信パケットに基づくサービス クラスの割り当て」（P.2-5）を参照）。

DHCP サービス クラスの値は、各サービス クラス名およびオプションで、サービス クラスを割り当てる DNS 正引きゾーンを設定するためのものです。追加するサービス クラスごとに [Add Class of Service] をクリックします。

設定値を選択するか入力し、[Next>>] をクリックして設定をアクティブにすると、他の DHCP 設定を実行できます。[Class of Service Usage] の選択肢：

- [Assign class of service based on incoming packet?]：ページに特別なヘルプ リンクが表示されます（「着信パケットに基づくサービス クラスの割り当て」（P.2-5）を参照）。
- [Register clients individually?]（プリセット値）：[List/Add DHCP Clients] ページが開きます（「クライアントの個別登録」の項を参照）。

クライアントの個別登録

[Set up DHCP Classes of Service] ページの [Class of Service Usage] 設定で [Register clients individually?] をイネーブルにした場合は、適切な順序で [List/Add DHCP Clients] ページが開きます。([List/Add DHCP Clients] ページの例については、『*User Guide for* Cisco Prime Network Registrar』の「See the *Configuring Clients*」の項を参照してください)。

このページでは、DHCP クライアントの名前を入力し、必要に応じてドロップダウン リストから設定済みのクライアント クラスを選択します。

- クライアント クラスも選択した場合は、それ以上設定を行わなくてもクライアントがリストの下に追加されます。
- クライアント クラスを選択しなかった場合は、[Add DHCP Client] ページが開きます。
- このページでアタシを入力する方法については、『*User Guide for Cisco Prime Network Registrar*』の「*Configuring Clients*」の項を参照してください。[Add DHCP Client] ページでクライアントの名前をクリックすると、[Edit DHCP Client] ページの基本モード バージョンが開きます（詳細については、『*User Guide for Cisco Prime Network Registrar*』の「*Editing Clients and Their Embedded Policies*」の項を参照してください)。

着信パケットに基づくサービス クラスの割り当て

[Set up DHCP Classes of Service] ページの [Class of Service Usage] 設定で [Assign class of service based on incoming packet?] をイネーブルにした場合は、[Set up DHCP Classes of Service] ページが情報ページに変わります。

着信パケットに基づくサービス クラスの割り当ては、セットアップ モードではクライアントの個別登録よりも使用頻度が低く、拡張モードでの設定を必要とします。このページで [Next] をクリックして、DHCP の次のセットアップ タスクに移動します。次のように進みます。

ステップ 1　セットアップ ページを最後まで完了し、セットアップ モードを終了します。

ステップ 2　[Advanced] をクリックして拡張モードを開始します。

ステップ 3　[DHCP] をクリックしてから [DHCP Server] をクリックします。

ステップ 4　[Manage DHCP Server] ページで [Local DHCP Server] リンクをクリックします。

ステップ 5　[Edit DHCP Server] ページで、[Client-Class] カテゴリの下にある *client-class-lookup-id* 属性の式の値を入力する（または、式を含むファイルへの参照を入力する）必要があります。この属性を設定してクライアントを区別する例を次に示します。

- **voip クライアント クラスに Cisco IP Phone を入力** : *dhcp-parameter-request-list* オプション（55）のバイト値が 150 または 122 の着信パケットを検索します。見つかった場合、クライアントに **voip** クライアント クラスを割り当てます。

```
(or
(if (search (byte 150) (request get-blob option 55)) "voip")
(if (search (byte 122) (request get-blob option 55)) "voip")
"<none>")
```

- **クライアント クラスに MAC アドレスの最初の 3 バイトを共有するクライアントを入力** : MAC アドレスが 01:02:03 で始まる着信パケットを検索し、**red** クライアント クラスを割り当てます。04:05:06 で始まる MAC アドレスに **blue** クライアント クラスを割り当てます。

```
(or
(if (starts-with (request get-blob chaddr) 01:02:03) "red")
(if (starts-with (request get-blob chaddr) 04:05:06) "blue")
"<none>")
```

- **msftclass クライアント クラスに Microsoft クライアントを入力**：*dhcp-class-identifier* オプション（60）の値が MSFT で始まる着信パケットを検索し、クライアントに **msftclass** クライアント クラスを割り当てます。

```
(or
(if (starts-with (request get-blob option 60) (as-blob "MSFT"))
"msftclass")
"<none>")
```

ステップ 6　[Modify Server] をクリックします。

ステップ 7　[Manage DHCP Server] ページの [Reload] アイコン（  ）をクリックしてサーバをリロードします。

DHCP トラップの設定

セットアップ インタビューの [Set up DHCP] ページで [Enable DHCP Traps] の値を [yes] に設定した場合は、適切な順序で [Set up DHCP Traps] ページが開きます。

[Enable DHCP Traps] のプリセット値は [yes] です。設定するトラップとトラップの設定方法を決定する必要があります。設定するトラップの種類は、[Select DHCP Traps] の値によって決まります。すべてのトラップを設定するか、次の項目を報告するトラップを選択して設定できます。

- サーバの起動と終了（server-start と server-stop）。
- フリー アドレスの検出日時（free-address-low と free-address-high）。
- DNS キューのサイズ（dns-queue-size）。
- パートナー サーバがダウンしているかアップしているか（other-server-down と other-server-up）。
- 検出された重複アドレス（duplicate-address）、アドレス競合（address-conflict）、またはフェールオーバー設定エラー（failover-config-error）。

フリー アドレスの検出トラップを設定した場合は、その設定も指定する必要があります。

- フリー アドレス設定の名前（display-only の値：**global**）
- フリー アドレスの決定方法：**scope**、**network**、または **scope-selection タグ**（プリセット値：**scope**）
- フリー アドレスの何パーセントが検出されたら low-threshold トラップを生成して高しきい値を再度イネーブルにするか（プリセット値：**20%**）
- フリー アドレスの何パーセントが検出されたら high-threshold トラップを生成して低しきい値を再度イネーブルにするか（プリセット値：**25%**）

設定値を選択するか入力し、[Next>>] をクリックして設定をアクティブにすると、DHCP アドレスのスコープを設定できます。

DHCP スコープの管理

セットアップ インタビューで DHCP サービスをイネーブルにし、DHCP フェールオーバー、サービス クラス、またはトラップの最後の設定ページを完了すると、[Manage Scopes] ページ（図 2-2（P.2-7）を参照）が開きます。スコープは、一般的なリース設定を指定するアドレス プールです。これらのスコープは、DHCP に必要です。

図 2-2　[Manage Scopes] ページ（Setup）

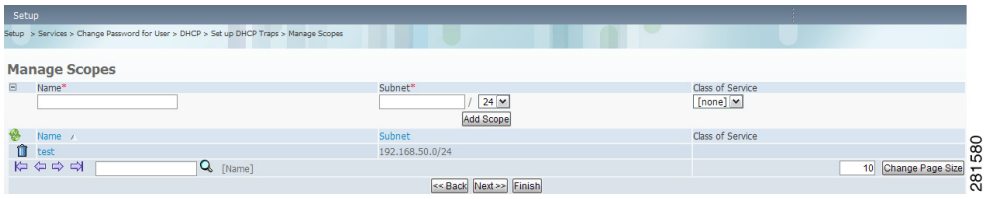


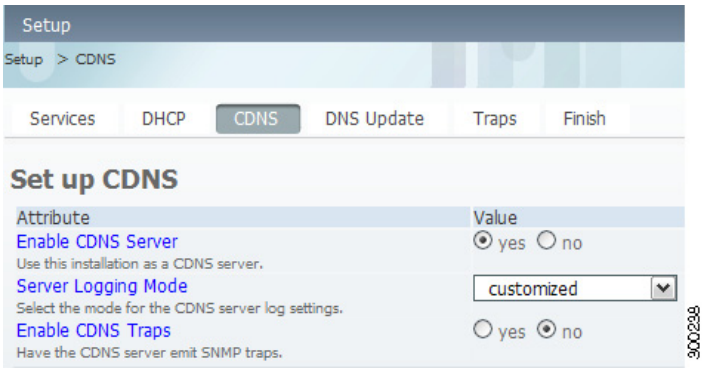
図 2-2 では、example-scope がすでに定義されています。スコープを定義するには、[Name] フィールドにスコープ名を入力し、そのサブネット アドレス（192.168.50/24 など）を [Subnet] フィールドに入力します。「DHCP サービス クラスの設定」（P.2-4）でサービス クラスを設定した場合は、[Class of Service] ドロップダウン リストからサービス クラスをスコープに関連付けることもできます。

[Add Scope] をクリックしてスコープを追加します。次に、[Next>>] をクリックして設定をアクティブにし、次の設定手順に進みます。たとえば、DHCP トラップを設定する場合は、次にトラップの受信側（「トラップの受信側の設定」（P.2-14）を参照）を設定できます。DNS サーバをイネーブルにした場合は、DNS サーバの設定ページに移動します（「DNS サービスの設定」の項を参照）。

CDNS サービスの設定

セットアップ インタビューの [Set up this Server] ページで [Enable CDNS Server] の値を [yes] に設定した場合は、適切な順序で [Set up CDNS] ページが開きます（図 2-4（P.2-9）を参照）。このページは、ナビゲーション バーで [CDNS] をクリックした場合も開きます。

図 2-3　[Set up CDNS] ページ（Setup）



次の項の情報に基づいて設定値を選択し、[Next>>] をクリックして設定をアクティブにします。その後、アクセス コントロールとトラップの設定用のセットアップ ページが表示されます。

CDNS サーバ ロール：

DNS サーバはキャッシング サーバにすることができます。

- **Caching**：ゾーンに対して権威を持たず、ゾーン情報のデータベースを保持しませんが、キャッシュおよび権威ネーム サーバへの照会によってクエリーに応答します。

サーバ ロギング モード

キャッシング DNS サーバはログ メッセージを提供し、ユーザがメッセージ出力のモードを設定できます。[Server Logging Mode] オプションには、特定のロギング設定に変換される 4 つの値を指定できます。

- **normal-operations**：通常のロギングが行われます。
- **high-performance**：高パフォーマンス ロギングが行われます。
- **debugging**：デバッグ ロギングが行われます。
- **customized**：特定のログ設定を求めるメッセージを表示し、その設定のみを記録します。

CDNS トラップのイネーブル化

CDNS サーバの SNMP トラップを設定すると、サーバが起動しているかどうかを報告する手段が提供されます。CDNS トラップはデフォルトではイネーブルになっていないため、イネーブルにするにはこの値を [yes] に設定する必要があります。詳細については、「CDNS トラップの設定」（P.2-9）を参照してください。

CDNS アクセス コントロールの設定

セットアップ インタビューの [Set up CDNS] ページで CDNS サーバを設定した場合は、適切な順序で [Set up CDNS Access Control] ページが開きます。

このページで、アクセス コントロール リスト（ACL）に基づいてクエリーとゾーン転送を制限できます。

- **dns-restrict-query-acl**：DNS サーバが受け入れるデバイス クエリーを制限するために使用されるグローバル ACL を提供します。クエリー クライアントは、ホスト IP アドレス、ネットワーク アドレス、およびその他の ACL に基づいて制限できます。プリセット値では、**任意の**クライアントによるクエリーの実行を許可します。複数の ACL 値はカンマで区切ります。
- **CDNS Forwarders**：キャッシング DNS サーバのフォワーダを設定する場合は、名前と IP アドレスを指定し、[Add Forwarder] をクリックします。
- **CDNS Resolution Exceptions**：CDNS サーバでドメイン外の特定の名前をルート ネームサーバに照会する通常の方法を使用しない場合は、解決例外を使用してルート ネームサーバをバイパスし、特定のサーバを対象にして名前解決を処理します。ネームサーバ名とそのカンマで区切られたアドレスを入力し、[Add Exception] をクリックします。

[Next>>] をクリックして設定をアクティブにし、CDNS サーバ設定を続行（または完了）します。

CDNS トラップの設定

セットアップ インタビューの [Set up CDNS] ページで [Enable CDNS Traps] の値を [yes] に設定した場合は、適切な順序で [Set up CDNS Traps] ページが開きます。

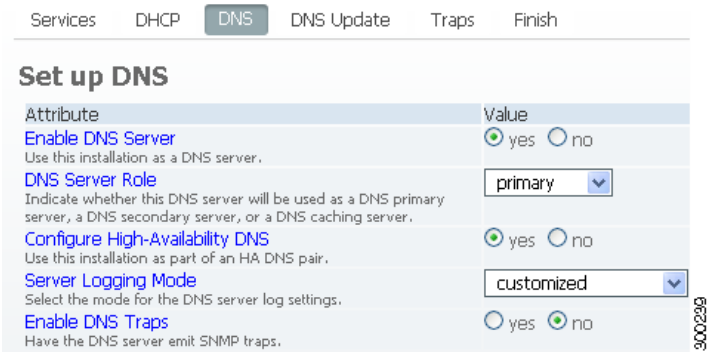
[Enable CDNS Traps] のプリセット値は [yes] です。設定するトラップとトラップの設定方法を決定する必要があります。設定するトラップの種類は、[Select CDNS Traps] の値によって決まります。[Select CDNS Traps] のプリセット値は [none] です。すべてのトラップを設定するか、サーバの起動と終了（server-start と server-stop）などを報告するトラップを選択して設定することもできます。

設定値を選択します。次に、[Next>>] をクリックして設定をアクティブにし、CDNS 設定を完了します。

DNS サービスの設定

セットアップ インタビューの [Set up this Server] ページで [Enable DNS Server] の値を [yes] に設定した場合は、適切な順序で [Set up DNS] ページが開きます（図 2-4（P.2-9）を参照）。このページは、ナビゲーション バーで [DNS] をクリックした場合も開きます。

図 2-4　[Set up DNS] ページ（Setup）



DNS サーバを設定するには、[Enable DNS Server] の値が [yes] に設定されていることを確認します。すでに他の場所でプライマリ DNS サーバを設定し、そのサーバと同期している場合は、セットアップ プロセスによって、現在の Cisco Prime Network Registrar ホストがすでにセカンダリ サーバまたはキャッシング サーバとして設定されているためこれ以上の DNS 設定が必要ないことが示されます。

次の項の情報に基づいて設定値を選択し、[Next>>] をクリックして設定をアクティブにします。その後、正引きおよび逆引き DNS ゾーン（High-Availability DNS サーバ用など）、ゾーン配信、およびアクセス コントロールの設定用のセットアップ ページが表示されます。

DNS サーバの役割

DNS サーバはプライマリまたはセカンダリ サーバにすることができます。

- **Primary**（プリセット値）：ゾーンに対して権威があり、このゾーン情報をデータベースに保持します。
- **Secondary**：プライマリ サーバのゾーン情報のコピーをロードします。プライマリは、セカンダリにゾーン情報の変更を通知し、セカンダリへのゾーン転送を実行します。

サーバがプライマリの場合は、そのサーバを High-Availability（HA）DNS サーバ設定に含めるかどうかを指定することもできます（「High-Availability DNS のイネーブル化」の項を参照）。サーバがセカンダリの場合は、そのサーバ専用のアクセス コントロールを設定できます。

High-Availability DNS のイネーブル化

High-Availability（HA）DNS サーバは、サーバがダウンしたときにフェールオーバーを提供します。この関係では、2 つ目のプライマリ サーバがメイン プライマリ サーバをシャドウイングするホット スタンバイになることができます。

HA DNS サービスを提供するには、[Enable High-Availability DNS] の値を [yes] に設定します。セットアップ プロセスで既存の複雑な HA DNS 設定が検出された場合、セットアップ インタビューでは HA DNS を設定できないことが通知されます。HA DNS がすでに拡張モードで設定され、次のいずれかの条件が満たされる場合、セットアップ ページでは HA DNS を設定できません。

- 複数の HA DNS サーバ ペアが設定されている。
- 1 つの HA DNS ペアが存在し、main-server または backup-server の値が設定されている。

HA DNS 設定の詳細については、「High-Availability DNS の設定」の項を参照してください。

サーバ ロギング モード

DNS サーバはログ メッセージを提供し、ユーザがメッセージ出力のモードを設定できます。[Server Logging Mode] オプションには、特定のロギング設定に変換される 4 つの値を指定できます。

- **normal-operations**：通常のロギングが行われます。
- **high-performance**：高パフォーマンス ロギングが行われます。
- **debugging**：デバッグ ロギングが行われます。
- **customized**：特定のログ設定を求めるメッセージを表示し、その設定のみを記録します。

DNS トラップのイネーブル化

DNS サーバの SNMP トラップを設定すると、サーバが起動しているかどうか、パートナー通信のステータス、パートナー設定、マスター通信、およびセカンダリ ゾーン ステータスを報告できます。DNS トラップはデフォルトではイネーブルになっていないため、イネーブルにするにはこの値を [yes] に設定する必要があります。詳細については、「DNS トラップの設定」（P.2-13）を参照してください。

High-Availability DNS の設定

セットアップ インタビューの [Set up DNS Server] ページで [Enable High-Availability DNS] の値を [yes] に設定した場合は、適切な順序で [Set up High-Availability DNS] ページが開きます。

[Enable High-Availability DNS] のプリセット値は [yes] で、[HA DNS Role] のプリセット値は [main] です。[DNS Role] は、この特定のマシンで実行するロールです。現在のマシンのロールを [backup] に変更した場合は、このマシンに対するフェールオーバー設定をこれ以上行うことができません。（メイン サーバ マシンに対してフェールオーバー設定を実行し、そのマシンから HA DNS 同期を実行するよう推奨するメッセージが表示されます）。同様に、Cisco Prime Network Registrar で複雑な HA DNS 設定が検出された場合は、警告メッセージが表示され、HA DNS 設定のセットアップをスキップする必要があります。

[HA Partner] の値によって、リモート バックアップ サーバのアドレスとアクセス基準が決まります。そのサーバのクラスタがすでに存在する場合は、[Select existing cluster] ドロップダウン リストからクラスタを選択できます。既存のクラスタがない場合は、バックアップ サーバのクラスタを設定できます。

1. バックアップ DNS サーバのホスト名または IP アドレスを入力します。
2. バックアップ サーバのアクセス基準として、管理者の名前とパスワード、SCP ポート番号（プリセット値は **1234**）を入力します。
3. [Add Cluster] をクリックしてクラスタを追加します。

設定値を選択するか入力し、[Next>>] をクリックして設定をアクティブにすると、DNS ゾーン配信を設定できます。

DNS ゾーン配信の設定

セットアップ インタビューの [Set up DNS] ページで DNS サーバをプライマリとして設定した場合は、適切な順序で [Set up DNS Zone Distribution] ページが開きます。

[DNS Secondary Server(s)] の値によって、現在の DNS プライマリのバックアップ セカンダリとなるサーバが決まります。セカンダリ サーバが存在する既存のクラスタをドロップダウン リストから選択するか、新しいクラスタを追加できます。新しいクラスタを作成するには、次の手順を実行します。

1. バックアップ DNS サーバのホスト名または IP アドレスを入力します。
2. バックアップ サーバのアクセス基準として、管理者の名前とパスワード、SCP ポート番号（プリセット値は **1234**）を入力します。
3. [Add Cluster] をクリックしてクラスタを追加します。

設定値を選択するか入力し、[Next>>] をクリックして設定をアクティブにすると、DNS サーバのゾーンを設定できます。

正引きゾーンの管理

セットアップ インタビューの [Set up DNS] ページで DNS サーバをプライマリとして設定した場合は、適切な順序で [Manage Forward Zones] ページが開きます。

正引きゾーンを定義するには、[Name] フィールドにゾーン名を、[Nameserver] フィールドにネームサーバ ドメイン名（ns1.example.com. など）を、[Contact E-Mail] フィールドにホストマスター名（hostmaster.example.com. など）を入力します。

[Add Zone] をクリックして [Add DNS Forward Zone] ページを開きます(『*User Guide for Cisco Prime Network Registrar*』の「*Configuring Primary Forward Zones*」の項を参照)。正引きゾーン データを追加し、[Add Zone] をクリックして [Manage Forward Zones] ページに戻ります。[Next>>] をクリックして設定をアクティブにすると、DNS サーバの逆引きゾーンを追加できます。

逆引きゾーンの管理

[Set up DNS] ページで DNS サーバをプライマリとして設定し、セットアップ インタビューで正引きゾーンを設定した場合は、適切な順序で [Manage Reverse Zones] ページが開きます。

Cisco Prime Network Registrar によってループバック逆引きゾーン（127.in-addr.arpa.）が自動的に作成されます。追加の逆引きゾーンを定義するには、[Name] フィールドにゾーン名を、[Nameserver] フィールドにネームサーバ ドメイン名（ns1.example.com. など）を、[Contact E-Mail] フィールドにホストマスター名（hostmaster.example.com. など）を入力します。（名前には最後のドットを含めて完全修飾名を使用してください)。

[Add Zone] をクリックして [Add DNS Reverse Zone] ページを開きます(『*User Guide for Cisco Prime Network Registrar*』の「*Adding Primary Reverse Zones*」の項を参照)。逆引きゾーン データを追加し、[Add Zone] をクリックして [Manage Reverse Zones] ページに戻ります。[Next>>] をクリックして設定をアクティブにすると、DNS サーバのアクセス コントロールを追加できます。

DNS アクセス コントロールの設定

セットアップ インタビューの [Set up DNS] ページで DNS サーバをプライマリまたはセカンダリとして設定した場合は、適切な順序で [Set up DNS Access Control] ページが開きます。

このページで、アクセス コントロール リスト（ACL）に基づいてクエリーとゾーン転送を制限できます。

- **dns-restrict-xfer-acl**：ゾーン転送を受け入れることができるユーザを指定するデフォルトの ACL。ゾーンに *restrict-xfer-acl* 属性を設定すると、この設定が上書きされます。この設定は、キャッシング サーバには適用されません。プリセット値は [none] です。複数の ACL 値はカンマで区切ります。

[Next>>] をクリックして設定をアクティブにし、DNS サーバ設定を続行（または完了）します。

DNS トラップの設定

セットアップ インタビューの [Set up DNS] ページで [Enable DNS Traps] の値を [yes] に設定した場合は、適切な順序で [Set up DNS Traps] ページが開きます。

[Enable DNS Traps] のプリセット値は [yes] です。設定するトラップとトラップの設定方法を決定する必要があります。設定するトラップの種類は、[Select DNS Traps] の値によって決まります。[Select DNS Traps] のプリセット値は [none] です。すべてのトラップを設定するか、次の項目を報告するトラップを選択して設定することもできます。

- サーバの起動と終了（server-start と server-stop）。
- HA DNS パートナーのアップ / ダウン状態（ha-dns-partner-up/ha-dns-partner-down）および設定エラー（ha-dns-config-error）。
- マスター サーバと転送サーバが応答しているか（masters-responding）応答していないか（masters-not-responding）。
- セカンダリ ゾーンが期限切れになっているかどうか（secondary-zone-expired）。
- フォワーダが応答しているか（forwarders-responding）応答していないか（forwarders-not-responding）。

設定値を選択します。次に、[Next>>] をクリックして設定をアクティブにし、DNS 設定を完了します。

DNS 更新の設定

セットアップ インタビューの [Set up this Server] ページで [Enable DHCP Server] の値を [yes] に設定し、[Enable DHCP Update] の値を [yes] に設定した場合は、適切な順序で [Set up DNS Update] ページが開きます。更新にローカル サーバを使用する場合は、[Enable DNS Server] も [yes] に設定しておく必要があります。前の基準が満たされている場合、このページはナビゲーション バーで [DNS Update] をクリックしても開きます。

このページでは、DNS 更新を有効にするために DNS サーバと DHCP サーバの関係を設定する必要があります。

- **DNS Server or HA Pair** : DNS 更新用に 1 つの DNS サーバまたは HA DNS サーバ ペアを設定できます。1 つのサーバの場合、値は **localhost** にプリセットされます。HA DNS ペアが定義されている場合、その設定名をドロップダウン リストから選択できます。新しいクラスタを定義するには、ホスト名、IP アドレス、管理者名、パスワード、および SCP ポート値（プリセット値 : 1234）をそれぞれのフィールドに入力し、[Add Cluster] をクリックします。
- **DHCP Server or Failover Pair** : DNS 更新用に 1 つの DHCP サーバまたは DHCP フェールオーバー サーバ ペアを設定できます。1 つのサーバの場合、値は **localhost** にプリセットされます。フェールオーバー パートナーシップが定義されている場合、その設定名をドロップダウン リストから選択できます。新しいクラスタを定義するには、ホスト名、IP アドレス、管理者名、パスワード、および SCP ポート値（プリセット値 : 1234）をそれぞれのフィールドに入力し、[Add Cluster] をクリックします。
- **Forward Zone Name** : DNS 更新を受信する正引きゾーンを定義する必要があります。ゾーンは DNS サーバまたは HA DNS ペアに定義されている必要があります。このフィールドにゾーン名を入力します。サービス クラスのゾーンを区別する場合は、複数のゾーンをカンマで区切ったリストを入力することもできます。それ以外の場合は、[example.com]（プリセット値）または [none] を [Forward Zone Name] ドロップダウン リストから選択できます。正引きゾーンに対して逆引きゾーンがすでに定義されている場合は、このページを完了すると、ポインタ（PTR）レコードが適切な逆引きゾーンにも書き込まれます。

- **Secure DNS Updates?**：トランザクション署名（TSIG）を使用して DNS 更新をセキュリティ保護する場合は、この値を [yes] に設定します（プリセット値は [no]）。この値をイネーブルにすると、DNS サーバは *dns-update-server-key* 属性に指定されている TSIG キーを使用するか、次の [Server Key] フィールドに定義されているキーを使用します。
- **Server Key** : [Secure DNS Updates] をイネーブルにし、TSIG キーが存在する場合は、ドロップダウン リストからキーを選択できます。キーが存在しない場合は、作成できます。[Name] フィールドにキー名を入力し、[Generate Key] をクリックします（この処理では Cisco Prime Network Registrar **cnr-keygen** ツールが使用されます）。キーを生成すると、その名前が [Select existing key] ドロップダウン リストに表示されます。

設定値を選択するか入力します。次に、[Next>>] をクリックして設定をアクティブにし、DNS 設定を完了します。

トラップの受信側の設定

[Set up this Server] ページで DHCP または DNS サーバをイネーブルにし、セットアップ インタビューの DHCP または DNS サーバのセットアップ ページでトラップをイネーブルにした場合は、適切な順序で [Set up Trap Recipients] ページが開きます。前の基準が満たされている場合、このページはナビゲーション バーで [Traps] をクリックしても開きます。

トラップを有効にするには、トラップ受信側（トラップ通知を受け取るホスト）を指定する必要があります。受信側ホストの識別名と IP アドレスを入力し、[Add Trap Recipient] をクリックします。[Next>>] をクリックして設定をアクティブにし、[Setup Interview Tasks] ページに移動します。

Setup Interview Tasks

[Setup Interview Tasks] ページは、セットアップ インタビューで設定に基づいて実行するタスクがある場合に開きます。たとえば、スコープを作成するには、DHCP サーバのリロードが必要になることがあります。このページには、タスク名、ID、およびタスクの最終実行日時が示されます。[Action] カラムには、タスクを選択するためのチェックボックスがあります。1 つ以上のタスクを実行するには、[Run Selected Tasks] をクリックします。クリックすると確認ページが開きます。このページで [Report and Exit] を実行すると、[Setup Interview Report] ページに移動します。

Setup Interview Report

[Setup Interview Report] ページは、セットアップ インタビューで最後に開くページです。このページには、インタビュー ページで実行したアクションの要約およびセッション時間と完了ステータスが表示されます。

[Exit Setup] をクリックするとメイン メニュー ページに戻ります。