DNS の設定

Domain Name System（DNS; ドメイン ネーム システム）は、DNS サーバから DNS プロトコルを介してホスト名を IP アドレスにマッピングできる分散データベースです。各固有の IP アドレスには、ホスト名を関連付けることができます。Cisco IOS ソフトウェアは、**connect**、**telnet**、**ping** EXEC コマンド、および関連する Telnet サポート操作で使用するための hostname-to-address マッピングのキャッシュを保守します。このキャッシュにより、名前とアドレスの変換プロセスが高速化されます。

機能情報の検索

ご使用のソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。最新の機能情報および警告については、ご使用のプラットフォームおよびソフトウェア リリースのリリースノートを参照してください。このモジュールに記載されている機能に関する情報を検索したり、各機能がサポートされているリリースに関するリストを参照したりするには、「DNS の機能情報」（P.15）を参照してください。

プラットフォームのサポートと、Cisco IOS および Catalyst OS ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

- 「DNS を設定するための前提条件」（P.2）
- 「DNS について」（P.2）
- 「DNS の設定方法」（P.4）
- 「DNS の設定例」（P.13）
- 「参考資料」（P.14）
- 「DNS の機能情報」（P.15）

DNS を設定するための前提条件

DNS を使用するには、ネットワークに DNS Name Server（NS; ネーム サーバ）が必要です。

DNS について

DNS を設定するには、次の概念について理解しておく必要があります。

- 「DNS の概要」（P.2）

DNS の概要

ネットワーク デバイスで、名前の割り当てを制御しないネットワークのデバイスとの接続が必要な場合、インターネットワーク全体でデバイスを一意に識別するデバイス名を割り当てることができます。インターネットのグローバル命名方式、DNS は、この作業を実行します。このサービスはデフォルトでイネーブルにされています。ここでは、DNS の概念および機能について説明します。

ネットワーク デバイスのホスト名

各固有の IP アドレスには、ホスト名を関連付けることができます。DNS は、ネットワーク ノードのホスト名を確立するために階層方式を使用します。これにより、クライアント/サーバ方式によるネットワークのセグメントのローカル制御が可能になります。DNS システムは、デバイスのホスト名をその関連する IP アドレスに変換することで、ネットワーク デバイスを検出できます。

ネットワークのグループのドメイン名

IP は、IP での検出によりデバイスを識別できる命名方式を定義します。これは、*ドメイン*に提供される階層命名方式です。インターネットでは、ドメインは、組織タイプまたは地理的情報に基づいたネットワークの一般的なグループ分けを示す命名階層ツリーの一部です。ドメイン名の区切りとしては、ピリオド（.）を使用します。たとえば、Cisco は、IP で *com* というドメイン名で識別される商業組織であるため、ドメイン名は *cisco.com* となります。このドメイン内の特定のデバイス、たとえば File Transfer Protocol（FTP; ファイル転送プロトコル）システムは、*ftp.cisco.com* で表されます。

ネーム サーバ

ドメイン名を追跡するため、IP は、ネーム サーバの概念を定義します。ネーム サーバは、ドメイン ツリーの名前空間部分に関する完全な情報を持ち、また場合によっては、ドメイン ツリーの他の部分からの情報を参照するときに使用できる他のネーム サーバへのポインタを含むプログラムです。ネーム サーバは、完全な情報を持つドメイン ツリーの部分を認識します。また、ネーム サーバは、ドメイン ツリーの他の部分に関する情報を保存することもできます。ドメイン名を IP アドレスにマッピングするには、まずホスト名を識別して、ネーム サーバを指定して、DNS サービスをイネーブルにする必要があります。

キャッシュ

名前をアドレスに変換するプロセスを高速化するため、ネーム サーバは、hostname-to-address マッピングに関するキャッシュと呼ばれるデータベースを保守します。これは、**connect**、**telnet**、**ping** EXEC コマンド、および関連する Telnet サポート操作により使用されます。キャッシュには、以前の応答の結果が保存されます。ネーム サーバは、クライアントが発行した DNS クエリーを受信すると、このローカル ストレージをチェックして、その回答をローカルで使用できるかどうか確認します。

ネーム リゾルバ

ネーム リゾルバは、クライアント要求に応答してネーム サーバから情報を抽出するプログラムです。リゾルバは、少なくとも 1 つのネーム サーバにアクセスできる必要があります。リゾルバは、ネーム サーバの情報を使用してクエリーに直接応答するか、他のネーム サーバへの参照を使用してクエリーを追跡します。リゾルバは、一般的に、ユーザ プログラムに直接アクセスできるシステム ルーチンです。そのため、リゾルバとユーザ プログラム間にプロトコルは必要ありません。

ゾーン

ドメイン名前空間は、DNS ツリーの委任ポイントである、*ゾーン*と呼ばれるエリアに分割されます。ゾーンには、他のゾーンに権限があるものを除き、特定のポイント以下のすべてのドメインが含まれます。

権限ネーム サーバ

ネーム サーバは、完全な情報を持つドメイン ツリーの部分の*認証局*と呼ばれます。ゾーンには、通常、権限ネーム サーバがあります（通常複数あります）。*権限ネーム* サーバは、ホスト テーブル情報が設定されるか、*ゾーン転送*を介してホスト テーブル情報を取得します（これは、セカンダリ DNS サーバが起動し、プライマリ サーバからそれ自体を更新するときに発生するアクションです）。

DNS の動作

組織は、多くのネーム サーバを使用できますが、インターネット クライアントは、ルート ネーム サーバが認識するネーム サーバだけをクエリーできます。他のネーム サーバは、内部クエリーだけに応答します。

ネーム サーバは、次に示すように、特定のゾーン内でローカルに定義されるホストの DNS サーバに対してクライアントが発行したクエリーを処理します。

- 権限ネーム サーバは、独自のホスト テーブルの永続的なエントリおよびキャッシュされたエントリを使用して、認証局のゾーン下にあるドメイン ネームの DNS ユーザ クエリーに応答します。認証局のゾーン下にあるが、その設定情報がないドメイン名にクエリーが発行された場合、権限ネーム サーバは、このような情報が存在しないことを示すだけです。
- 権限ネーム サーバとして設定されていないネーム サーバは、以前受信されたクエリー応答からキャッシュに保存された情報を使用して、DNS ユーザ クエリーに応答します。ルータがゾーンの権限ネーム サーバとして設定されていない場合、ローカルに定義されたホストの DNS サーバへのクエリーは、権限のない応答を受け取ります。

ネーム サーバは、特定のドメインに設定された転送および参照パラメータに従い、DNS クエリーに応答します（着信 DNS クエリーを転送するか、内部的に生成された DNS クエリーを解決します）。

DNS クエリーが解決のためにネーム サーバに転送された場合、該当する応答が受け取られるまで、またはタイムアウトになるまで、対応する DNS クエリーのためのメモリ スペースがいくつか保持されます。頻繁にクエリーを処理するときにフリー I/O メモリがなくならないようにするには、キューの最大サイズを設定します。

DNS の設定方法

ここでは、次の手順について説明します。

- 「ホスト名から IP アドレスへのマッピング」（P.4）
- 「DNS のカスタマイズ」（P.6）
- 「DNS スプーフィングの設定」（P.7）
- 「DNS サーバとしてのルータの設定」（P.8）
- 「ISO CLNS アドレスの DNS クエリーのディセーブル化」（P.11）
- 「DNS の確認」（P.12）

ホスト名から IP アドレスへのマッピング

ホスト名を IP アドレスにマッピングするには、次の作業を実行します。

hostname-to-address マッピング

ネーム サーバは、ドメイン名に関連する情報の追跡に使用されます。ネーム サーバは、hostname-to-address マッピングのデータベースを保守できます。各名前は、1 つ以上の IP アドレスにマッピングできます。このサービスを使用して、ドメイン名を IP アドレスにマッピングするには、ネーム サーバを指定する必要があります。

名前参照システムは、この作業で説明するコマンドを使用して静的に設定できます。DHCP など、Cisco IOS ソフトウェアの他のいくつかの機能は、名前参照システムの状態をダイナミックに変更できます。キャッシュにあるホスト名および DNS 設定を表示するには、**show hosts** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip host** *name* [*tcp-port-number*] *address1* [*address2 ... address8*]
4. **ip domain name** *name*
   または
   ip domain list *name*
5. **ip name-server** *server-address1* [*server-address2 ... server-address6*]
6. **ip domain lookup** [**source-interface** *interface-type interface-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip host** *name* [*tcp-port-number*] *address1* [*address2 ... address8*] **例：** `Router(config)# ip host cisco-rtp 192.168.0.148`	ホスト名キャッシュにスタティック hostname-to-address マッピングを定義します。 • 通常、数値アドレスではなく、シンボリック名によりネットワーク デバイスを参照する方が簡単です（Telnet のようなサービスは、ホスト名またはアドレスを使用できます）。ホスト名および IP アドレスは、スタティックまたはダイナミックに相互に関連付けることができます。 • 手動によりホスト名とアドレスの関連付けは、ダイナミック マッピングが使用できない場合に役に立ちます。

ステップ 4	**ip domain name** *name*
	または
	ip domain list *name*
	
	例：
	`Router(config)# ip domain name cisco.com`
	または
	
	例：
	`Router(config)# ip domain list cisco1.com`
		（任意）Cisco IOS ソフトウェアが未修飾ホスト名を完了するときに使用するデフォルトのドメイン名を定義します。
		または
		（任意）未修飾ホスト名を完了するデフォルトのドメイン名のリストを定義します。
		• Cisco IOS ソフトウェアがドメイン名要求を完了するときに使用するデフォルトのドメイン名を指定できます。単一のドメイン名またはドメイン名のリストを指定できます。完全なドメイン名を含まないホスト名には、名前が参照される前に、指定したデフォルトのドメイン名が追加されます。
		（注） ドメイン リストがない場合、**ip domain name** グローバル コンフィギュレーション コマンドで指定したドメイン名が使用されます。ドメイン リストがある場合、デフォルトのドメイン名は使用されません。**ip domain list** コマンドは、**ip domain name** コマンドと似ていますが、**ip domain list** コマンドの場合、システムが一致を検出するまでそれぞれをチェックする、ドメインのリストを定義できます。

	コマンドまたはアクション	目的
ステップ 5	**ip name-server** *server-address1* [*server-address2 ... server-address6*] **例：** `Router(config)# ip name-server 172.16.1.111 172.16.1.2`	DNS の名前情報を提供するためにネーム サーバとして機能できる 1 台以上のホスト（最高 6 台）を指定します。
ステップ 6	**ip domain lookup** [**source-interface** *interface-type interface-number*] **例：** `Router(config)# ip domain lookup`	（任意）DNS-based アドレス転送をイネーブルにします。 • DNS はデフォルトでイネーブルにされています。DNS がディセーブルの場合、このコマンドを使用します。

DNS のカスタマイズ

DNS 設定をカスタマイズするには、次の作業を実行します。

DNS Round-Robin の動作

DNS Round-Robin 機能のない複数サーバ設定の場合、多くのプログラムは、キャッシュ全体の Time to Live（TTL; 存続可能時間）に最初のホスト サーバ/IP アドレスを使用し、ホスト障害が発生した場合だけ、2 番めおよび 3 番めのホスト サーバ/IP アドレスを使用します。この動作により、大勢のユーザが TTL 時間中に最初のホストにすべて到達すると問題が発生します。たとえば、Network Access Server（NAS; ネットワーク アクセス サーバ）は、DNS クエリーを送信します。DNS サーバは、設定された IP アドレスのリストにより NAS に応答します。NAS は、指定時間内（たとえば 5 分）でこれらの IP アドレスをキャッシュします。5 分間の TTL 時間中にダイヤルインしたユーザは、すべて、リストの最初の IP アドレスにある 1 台のホストに到達します。

DNS Round Robin 機能を使用した複数サーバ設定では、DNS サーバは、ホスト名のキャッシュを使用してすべてのホストの IP アドレスを返します。キャッシュの TTL 中、ユーザはホスト間で分散されます。この機能は、設定されたホスト間でコールを分散することで、DNS クエリーの数を減らします。

スケジューリング アルゴリズムでは、プロセスは一定のサイクル順序でアクティブになります。子プロセスの終了や入出力操作など、他のイベントを待機するプロセスは、処理を続行できないため、制御をスケジューラに返します。（待機中の）イベントが発生する前に、プロセスの TTL がタイムアウトになった場合、このイベントは、他のすべてのプロセスがアクティブになるまで処理されません。

（注） DNS Round Robin 機能は、ルータの DNS 参照だけに適用され、このルータを示す別のクライアントには適用されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip domain timeout** *seconds*
4. **ip domain retry** *number*
5. **ip domain round-robin**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip domain timeout** *seconds* **例：** `Router(config)# ip domain timeout 17`	（任意）DNS クエリーへの応答を待機する時間を指定します。 • **ip domain timeout** コマンドが設定されていない場合、Cisco IOS ソフトウェアは、DNS クエリーへの応答を 3 秒間待機します。
ステップ 4	**ip domain retry** *number* **例：** `Router(config)# ip domain retry 10`	（任意）DNS クエリーの送信を試行する回数を指定します。 • **ip domain retry** コマンドが設定されていない場合、Cisco IOS ソフトウェアは、DNS クエリーを 2 回再試行します。
ステップ 5	**ip domain round-robin** **例：** `Router(config)# ip domain round-robin`	（任意）DNS サーバで Round Robin 機能をイネーブルにします。

DNS スプーフィングの設定

DNS スプーフィングを設定するには、次の作業を実行します。

DNS スプーフィングは、ルータをプロキシ DNS サーバとして機能させ、**ip dns spoofing** *ip-address* コマンドで設定された IP アドレスまたはクエリーの着信インターフェイスの IP アドレスのいずれかを使用して任意の DNS クエリーへの応答を「スプーフ」できるようにします。この機能は、Internet Service Provider（ISP; インターネット サービス プロバイダー）へのインターフェイスが稼動状態にないデバイスで役に立ちます。ISP へのインターフェイスが稼動状態になると、ルータは、DNS クエリーを実際の DNS サーバに転送します。

この機能は、DNS スプーフィングを有効にして、次の条件が満たされている場合に機能します。

- **no ip domain lookup** コマンドが設定されている。
- IP ネーム サーバ アドレスが設定されていない。
- 設定されているネーム サーバ アドレスに送信するための有効なインターフェイスまたはルートがない。

これらの条件が満たされていない場合、DNS スプーフィングは機能しません。

手順の概要

1. **enable**
2. **configure terminal**

3. **ip dns server**
4. **ip dns spoofing** [*ip-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dns server** **例：** `Router(config)# ip dns server`	ルータで DNS サーバをアクティブにします。
ステップ 4	**ip dns spoofing** [*ip-address*] **例：** `Router(config)# ip dns spoofing 192.168.15.1`	DNS スプーフィングを設定します。 • 独自のホスト名以外のホスト名にクエリーが発行された場合、ルータは、設定されている *ip-address* を使用して DNS クエリーに応答します。 • 独自のホスト名にクエリーが発行された場合、ルータは、着信インターフェイスの IP アドレスを使用して DNS クエリーに応答します。

DNS サーバとしてのルータの設定

DNS サーバとしてルータを設定するには、次の作業を実行します。

Cisco IOS ルータは、キャッシング ネーム サーバおよび独自のローカル ホスト テーブルの権限ネーム サーバとして機能して、サービスを DNS クライアントに提供できます。

キャッシング ネーム サーバとして設定される場合、ルータは、ネットワーク名をネットワーク アドレスを解決する他のネーム サーバに DNS 要求をリレーします。キャッシング ネーム サーバは、他のネーム サーバから学習した情報をキャッシュします。そのため、トランザクションごとに他のサーバにクエリーすることなく、要求にすばやく応答できます。

独自のローカル ホスト テーブルの権限ネーム サーバとして設定されている場合、ルータは、DNS クエリーのポート 53 でリスニングして、その独自のホスト テーブルの永続的なエントリおよびキャッシュされたエントリを使用して DNS クエリーに応答します。

権限ネーム サーバの役割

権限ネーム サーバは、通常、ゾーン転送を発行するか、同じゾーンの他の権限ネーム サーバからのゾーン転送要求に応答します。ただし、Cisco IOS DNS サーバは、ゾーン転送を実行しません。

権限ネーム サーバが、DNS クエリーを受信すると、次のようにクエリーを処理します。

- 認証局のゾーン下にないドメイン名に対するクエリーの場合、権限ネーム サーバは、IP DNS-based hostname-to-address 変換が **ip domain lookup** コマンドによりイネーブルにされているかどうかに基づいて、クエリーを特定のバックエンド ネーム サーバに転送するかどうかを判別します。
- 認証局のゾーン下にあり、設定情報があるドメイン名に対するクエリーの場合、権限ネーム サーバは、独自のホスト テーブルの永続的なエントリおよびキャッシュされたエントリを使用してクエリーに応答します。
- 認証局のゾーン下にあるが、設定情報がないドメイン名に対するクエリーの場合、権限ネーム サーバは、クエリーを転送せず、このような情報が存在しないことを示すだけです。

制約事項

分散ディレクタがイネーブルにされていない限り、ローカルで定義されたリソース レコードの TTL は、常に 10 秒に設定されます。これは、authority record パラメータが、**ip dns primary** コマンドを使用して DNS ネーム サーバに指定されているかどうかに関係ありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dns server**
4. **ip name-server** *server-address1* [*server-address2 ... server-address6*]
5. **ip dns server queue limit** {**forwarder** *queue-size-limit* | **director** *queue-size-limit*}
6. **ip host** [**vrf** *vrf-name*] [**view** *view-name*] *hostname* {*address1* [*address2 ... address8*] | **additional** *address9* [*address10 ... addressn*]}
7. **ip dns primary** *domain-name* **soa** *primary-server-name mailbox-name* [*refresh-interval* [*retry-interval* [*expire-ttl* [*minimum-ttl*]]]]
8. **ip host** *domain-name* **ns** *server-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip dns server** **例：** `Router(config)# ip dns server`	DNS サーバをイネーブルにします。
ステップ 4	**ip name-server** *server-address1* [*server-address2 ... server-address6*] **例：** `Router(config)# ip name-server 192.168.2.120 192.168.2.121`	（任意）他の DNS サーバを設定します。 • Cisco IOS リゾルバ ネーム サーバ • DNS サーバ フォワーダ **（注）** Cisco IOS ネーム サーバが権限のあるドメイン名だけに応答するように設定される場合、他の DNS サーバを設定する必要はありません。
ステップ 5	**ip dns server queue limit** {**forwarder** *queue-size-limit* | **director** *queue-size-limit*} **例：** `Router(config)# ip dns server queue limit forwarder 10`	（任意）DNS サーバ プロセスにより使用されるキューのサイズに制限を設定します。 • **director** キーワードは、Cisco IOS Release 12.4(24)T 以降から削除されました。
ステップ 6	**ip host** [**vrf** *vrf-name*] [**view** *view-name*] *hostname* {address1 [*address2 ... address8*] | **additional** *address9* [*address10 ... addressn*]} **例：** `Router(config)# ip host user1.example.com 192.168.201.5 192.168.201.6`	（任意）ローカル ホストを設定します。
ステップ 7	**ip dns primary** *domain-name* **soa** *primary-server-name mailbox-name* [*refresh-interval* [*retry-interval* [*expire-ttl* [*minimum-ttl*]]]] **例：** `Router(config)# ip dns primary example.com soa ns1.example.com mb1.example.com`	ドメイン（ゾーン）のプライマリ DNS ネーム サーバおよび Start of Authority（SOA）レコード ソース（ゾーンの開始を指定します）としてルータを設定します。 **（注）** 分散ディレクタがイネーブルにされていない限り、ローカルで定義されたリソース レコードの TTL は、常に 10 秒に設定されます。
ステップ 8	**ip host** *domain-name* **ns** *server-name* **例：** `Router(config)# ip host example.com ns ns1.example.com`	（任意）関連するドメインに対して DNS サーバがクエリーされたときに返される Name Server（NS; ネーム サーバ）リソース レコードを作成するようにルータを設定します。 • この設定が必要になるのは、システムに権限があるゾーンが他のネーム サーバからもサービスが提供される場合だけです。

例

ここでは、ルータがその独自のローカル ホスト テーブルの権限ネーム サーバとして設定されていて、**debug domain** コマンドが有効な場合に記録されるデバッグ出力の例を示します。

- 「DNS クエリーを別のネーム サーバにリレーするときのデバッグ出力：例」（P.11）
- 「ローカル ホスト テーブルからの DNS クエリーにサービスを提供するときのデバッグ出力：例」（P.11）

（注） DNS-based X.25 ルーティングの場合、**debug x25 events** コマンドは、X.25 アドレスが DNS サーバを使用して IP アドレスに解決されるときに発生するイベントを記述する機能をサポートします。**debug domain** コマンドを **debug x25 events** とともに使用すると、全体的な DNS-based X.25 ルーティング データ フローを観察できます。

DNS クエリーを別のネーム サーバにリレーするときのデバッグ出力：例

次に、ルータがその独自のローカル ホスト テーブルの権限ネーム サーバとして設定されている場合に DNS クエリーを別のネーム サーバにリレーするときの **debug domain** コマンドの出力例を示します。

```
Apr  4 22:18:32.183: DNS: Incoming UDP query (id#18713)
Apr  4 22:18:32.183: DNS: Type 1 DNS query (id#18713) for host 'ns1.example.com' from
192.0.2.120(1283)
Apr  4 22:18:32.183: DNS: Re-sending DNS query (type 1, id#18713) to 192.0.2.121
Apr  4 22:18:32.211: DNS: Incoming UDP query (id#18713)
Apr  4 22:18:32.211: DNS: Type 1 response (id#18713) for host <ns1.example.com> from
192.0.2.121(53)
Apr  4 22:18:32.215: DOM: dom2cache: hostname is ns1.example.com, RR type=1, class=1,
ttl=86400, n=4
Apr  4 22:18:32.215: DNS: Forwarding back A response - no director required
Apr  4 22:18:32.215: DNS: Finished processing query (id#18713) in 0.032 secs
Apr  4 22:18:32.215: DNS: Forwarding back reply to 192.0.2.120/1283
```

ローカル ホスト テーブルからの DNS クエリーにサービスを提供するときのデバッグ出力：例

次に、ルータがその独自のローカル ホスト テーブルの権限ネーム サーバとして設定されている場合にローカル ホスト テーブルからの DNS クエリーにサービスを提供するときの **debug domain** コマンドの出力例を示します。

```
Apr  4 22:16:35.279: DNS: Incoming UDP query (id#8409)
Apr  4 22:16:35.279: DNS: Type 1 DNS query (id#8409) for host 'ns1.example.com' from
192.0.2.120(1279)
Apr  4 22:16:35.279: DNS: Finished processing query (id#8409) in 0.000 secs
```

ISO CLNS アドレスの DNS クエリーのディセーブル化

International Organization for Standardization（ISO; 国際標準化機構）Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）アドレスの DNS クエリーをディセーブルにするには、次の作業を実行します。

ルータで IP および ISO CLNS の両方がイネーブルにされているときに、ISO CLNS Network Service Access Point（NSAP; ネットワーク サービス アクセス ポイント）アドレスを使用する場合、RFC 1348 で説明されているように、DNS を使用してこれらのアドレスをクエリーできます。この機能は、デフォルトでイネーブルにされています。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip domain lookup nsap**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ip domain lookup nsap** **例：** `Router(config)# no ip domain lookup nsap`	ISO CLNS アドレスの DNS クエリーをディセーブルにします。

DNS の確認

DNS 設定を確認するには、次の作業を実行します。

1. **enable**
2. **ping** *hosts*
3. **show hosts**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**ping** *hosts* **例：** `Router# ping cisco-rtp`	基本ネットワーク接続を診断します。 • DNS 設定が指定された後で、ホスト名を使用してデバイスを ping または telnet することで DNS サーバを確認できます。
ステップ 3	**show hosts** **例：** `Router# show hosts`	デフォルトのドメイン名、名前検索サービスの方式、ネーム サーバ ホスト名のリスト、およびキャッシュに格納されているホスト名とアドレスのリストを表示します。 • DNS を使用して名前が解決されたら、**show hosts** コマンドを使用して、キャッシュされたホスト名と DNS 設定を表示します。

DNS の設定例

ここでは、次の設定例について説明します。

- 「IP アドレスの例」（P.13）
- 「ホスト名から IP アドレスへのマッピング：例」（P.13）
- 「DNS のカスタマイズ：例」（P.13）
- 「DNS スプーフィングの設定：例」（P.13）

IP アドレスの例

次に、いくつかの代替ドメイン名のドメイン リストを確立する例を示します。

```
ip domain list example.com
ip domain list example1.edu
ip domain list example2.edu
```

ホスト名から IP アドレスへのマッピング：例

次に、hostname-to-address マッピング プロセスを設定する例を示します。IP DNS-based 変換が指定され、ネーム サーバのアドレスが指定され、デフォルトのドメイン名が提供されます。

```
! IP DNS-based hostname-to-address translation is enabled
ip domain lookup
! Specifies hosts 192.168.1.111 and 192.168.1.2 as name servers
ip name-server 192.168.1.111 192.168.1.2
! Defines cisco.com as the default domain name the router uses to complete
! Set the name for unqualified hostnames
ip domain name cisco.com
```

DNS のカスタマイズ：例

次に、指定された順序で 3 つの各 IP アドレスに company.example.com への Telnet を接続できるようにする例を示します。この指定順序では、最初にホスト名が参照されるときに 10.0.0.1 に接続され、2 回目にホスト名が参照されるときに 10.1.0.1 に接続され、3 回目にホスト名が参照されるときに 10.2.0.1 に接続されます。いずれの場合も、最初のアドレスが失敗した場合、他の 2 つのアドレスへの接続が試行されます。これは、Telnet コマンドの標準の動作です。

```
Router(config)# ip host company.example.com 10.0.0.1 10.1.0.1 10.2.0.1
Router(config)# ip domain round-robin
```

DNS スプーフィングの設定：例

次の例では、ルータは、任意の DNS クエリーへの応答をスプーフするように設定されています。

```
ip dns server
ip dns spoofing
no ip domain lookup
interface e3/1
 ip address 10.1.1.1 255.255.255.0
```

参考資料

ここでは、DNS に関する関連資料について説明します。

関連資料

関連項目	参照先
DNS コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS IP Addressing Services Command Reference*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	—

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存の MIB のサポートはありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1348	『*DNS NSAP RRs*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

DNS の機能情報

表 1 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(1) 以降で導入または変更された機能だけを示します。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのサポートの導入時期に関する詳細については、コマンド リファレンス マニュアルを参照してください。

Cisco IOS ソフトウェア イメージは、Cisco IOS ソフトウェア リリース、機能セット、プラットフォームそれぞれに固有です。プラットフォーム サポートと Cisco IOS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスするには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザ名やパスワードを忘れた場合は、ログイン ダイアログボックスで [Cancel] をクリックし、表示される説明に従ってください。

（注） 表 1 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 1　DNS の機能情報

機能名	リリース	機能情報
DNS スプーフィング	12.3(2)T	この機能は、ルータをプロキシ DNS サーバとして機能させ、**ip dns spoofing** *ip-address* コマンドで設定された IP アドレスまたはクエリーの着信インターフェイスの IP アドレスのいずれかを使用して任意の DNS クエリーへの応答を「スプーフ」できるようにします。 次のセクションで、この機能に関する情報を参照できます。 • 「DNS スプーフィングの設定」 この機能により、次のコマンドが導入されました。**ip dns spoofing**。