IP アドレッシング：DNS コンフィギュレーション ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2016 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

DNS の設定 3

機能情報の確認 3

DNS を設定するための前提条件 4

DNS に関する情報 4

DNS の概要 4

DNS ビュー 6

関連付けられた VRF からのビュー使用制限クエリー 6

内部生成された DNS クエリーの解決するためのパラメータ 7

着信する DNS クエリーを転送するパラメータ 7

DNS ビュー リスト 8

DNS 名グループ 10

DNS ビュー グループ 10

DNS の設定方法 11

IP アドレスへのホスト名のマッピング 11

DNS のカスタマイズ 14

ISO CLNS アドレスに対する DNS クエリーの無効化 15

DNS の確認 16

DNS ビューの定義 17

DNS ビューの確認 20

DNS ビュー リストの定義 21

DNS ビュー リストの変更 24

すでに使用中の DNS ビュー リストへのメンバーの追加 24

すでに使用中の DNS ビュー リスト メンバーの順序変更 26

デバイスの DNS サーバに対するデフォルト DNS ビュー リストの指定 28

デバイス インターフェイスに対する DNS ビュー リストの指定 29

DNS クエリー転送時の送信元インターフェイスの指定 30

DNS の設定例 31
例：代替ドメイン名を使用したドメイン リストの作成 31
例：IP アドレスへのホスト名のマッピング 32
例：DNS のカスタマイズ 32
例：異なるビュー使用制限によるスプリット DNS ビュー リストの設定 32
DNS の設定に関する追加情報 33
DNS の設定の機能情報 34
VRF-Aware DNS 37
機能情報の確認 37
VRF-Aware DNS に関する情報 38
Domain Name System; ドメイン ネーム システム 38
VRF マッピングおよび VRF-Aware DNS 38
VRF-Aware DNS の設定方法 39
VRF-Aware DNS を有効にするための VRF テーブルの定義とネーム サーバへの割り当て 39
IP アドレスへの VRF 固有ホスト名のマッピング 41
VRF 固有ネーム キャッシュでのスタティック エントリの設定 42
VRF テーブル内のネーム キャッシュ エントリの確認 43
VRF-Aware DNS の設定例 44
例：VRF 固有ネーム サーバの設定 44
例：VRF 固有ドメイン名リストの設定 44
VRF 固有ドメイン名設定の例 44
VRF 固有 IP ホストの設定の例 45
その他の参考資料 45
VRF-Aware DNS の機能情報 46
Service Discovery Gateway 49
Service Discovery Gateway に関する情報 49
サービス アナウンスの再配布とサービス拡張 49
サブネット間でのサービス拡張：概要 50
サブネット間にサービスを拡張するためのフィルタ オプションの設定 51
サブネット間でのサービス拡張 54
Service Discovery Gateway の設定方法 56

サービス検出に対するフィルタ オプションの設定 56
サービス検出フィルタの適用とサービス検出パラメータの設定 58
インターフェイスに対するサービス検出フィルタの適用 61
サービス インスタンスの作成 63
Service Discovery Gateway の確認とトラブルシューティング 65
Service Discovery Gateway の設定例 67
例：サービス検出に対するフィルタ オプションの設定 67
例：サービス検出フィルタの適用とサービス検出パラメータの設定 67
例：インターフェイスに対するサービス検出フィルタの適用 67
例：複数のサービス検出フィルタ オプションの設定 67
例：サービス インスタンスの作成 69
Service Discovery Gateway に関する追加情報 69
Service Discovery Gateway の機能情報 71

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

有効な 2 つのリリースとしての Cisco IOS XE リリース 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジ ルーティング用）が、1 つのバージョンの統合されたリリース（Cisco IOS XE 16）へと展開（マージ）されています。これにより、スイッチングおよびルーティング ポートフォリオの広範なアクセスおよびエッジ製品が盛り込まれた 1 つのリリースが実現しました。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術的構成ガイドが製品のランディング ページに表示される場合は、その機能がお使いのプラットフォームでサポートされていることを示します。

第 2 章

DNS の設定

ドメイン ネーム システム（DNS）は、DNS サーバから DNS プロトコルを使用してホスト名を IP アドレスにマッピングできる分散データベースです。一意の各 IP アドレスにホスト名を関連付けることができます。Cisco IOS XE 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ホスト名からアドレスへのマッピングのキャッシュを維持します。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。

- 機能情報の確認，3 ページ
- DNS を設定するための前提条件，4 ページ
- DNS に関する情報，4 ページ
- DNS ビュー，6 ページ
- DNS ビュー リスト，8 ページ
- DNS 名グループ，10 ページ
- DNS ビュー グループ，10 ページ
- DNS の設定方法，11 ページ
- DNS の設定例，31 ページ
- DNS の設定に関する追加情報，33 ページ
- DNS の設定の機能情報，34 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

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 ネーム サーバ（NS）が必要です。

DNS に関する情報

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

一意の各 IP アドレスにホスト名を関連付けることができます。DNS は、階層方式を使用して、ネットワーク ノードのホスト名を確立します。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となります。DNS システムは、デバイスのホスト名をそれに関連付けられた IP アドレスに変換して、ネットワークデバイスを見つけることができます。

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。インターネット上のドメインは、組織のタイプや場所に基づく一般的なネットワークのグループを表す命名階層ツリーの一部です。ドメイン名は、ピリオド（.）を区切り文字として使用して構成されています。たとえば、シスコは、インターネットでは *com* ドメイン名で表される営利団体であるため、そのドメイン名は *cisco.com* です。このドメイン内の特定のデバイス、たとえばファイル転送プロトコル（FTP）システムは *ftp.cisco.com* で識別されます。

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。ネーム サーバは、ドメイン ツリーの他の部分の情報を格納している場合もあります。IP アドレスにドメイン名を

マッピングするには、最初にホスト名を示し、そのあとにネームサーバを指定して、DNSサービスを有効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、ホスト名からアドレスへの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。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を確認します。

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

組織内では、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、その権限ゾーン内のドメイン名を求める DNS ユーザ照会に、自身のホストテーブル内にキャッシュされた永久的なエントリを使用して応答します。クエリーで求められているのが、自身の権限ゾーン内であるが、設定情報が登録されていないドメイン名の場合、権限ネーム サーバは単に、その情報が存在しないと返信します。

- 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、以前に受信した照会への返信からキャッシュした情報を使用して、DNS ユーザ照会に応答します。ゾーンの権限ネーム サーバとして設定されたデバイスがない場合は、ローカルに定義されたホストを求める DNS サーバへのクエリーには、正規の返信は送信されません。

ネームサーバは、特定のドメインに設定された転送パラメータおよびルックアップパラメータに従って、DNS 照会に応答します（着信 DNS 照会を転送するか、内部的に生成された DNS 照会を解決します）。

DNS セキュリティ

DNS 公開キー（DNSKEY）RR セットと委任署名者（DS）RR セットの代替シーケンスが署名済みデータのチェーンを形成し、チェーン内の各リンクが次のリンクを保証します。DNSKEY RR は DS RR を対象とした署名を確認するために使用され、DS RR が認証されるようにします。DS RR には別の DNSKEY RR のハッシュが含まれており、この新しい DNSKEY RR が DS RR 内のハッシュと一致すると認証されます。

DNS ビュー

DNS ビューは、DNS クエリーをどのように処理するかを指定する一連のパラメータです。DNS ビューにより、次の情報を定義します。

- VRF への関連付け
- 内部生成された DNS クエリーの解決するためのパラメータ
- 着信する DNS クエリーを転送するパラメータ
- クエリーへの応答、または DNS 応答のキャッシングに使用する内部ホスト テーブル

（注） DNS ビューとビュー リストの最大数は、シスコ デバイスのメモリによって異なります。DNS ビューおよびビュー リストに大きい値を設定するとデバイス メモリの消費量が増えます。またビュー リスト中のビュー数に大きい値を設定すると、デバイスのプロセッサ時間が長くなります。最適なパフォーマンスを得るには、スプリット DNS クエリーの転送やクエリー解決のニーズをサポートために必要な数のビューやビュー リスト メンバーを設定します。

関連付けられた VRF からのビュー使用制限クエリー

DNS ビューは常に VRF（グローバル VRF または名前付きの VRF）と関連付けられ、特定の VRF に一致するインターフェイスに到着した DNS クエリーの処理でのビューの使用を制限します。

- グローバル VRF に関連付けられた DNS ビューは、グローバル アドレス空間にあるインターフェイスに到着した DNS クエリーを処理する場合に限って使用できます。

- 名前付き VRF に関連付けられた DNS ビューは、ビューに対応する VRF に一致したインターフェイスに到着する DNS クエリーを処理する場合に限り使用できます。

（注） ビューを定義した後、さらに別の制約（「DNS ビュー」を参照）を適用することもできます。また、個別のケースごとに異なる制約を追加することにより、1 つのビューを何度も参照することができます。ただし、DNS ビューと VRF との関連付けは、DNS ビューの定義で指定されるため、VRF 固有のビュー使用制限は、DNS ビューの定義自体の特性を表すものです。したがって、この制限をビューから切り離すことはできません。

内部生成された DNS クエリーの解決するためのパラメータ

- ドメイン ルックアップ：内部生成されたクエリーのホスト名を解決する場合の DNS ルックアップのイネーブルまたはディセーブル
- デフォルト ドメイン名：ドットのないホスト名に追加するデフォルト ドメイン
- ドメイン検索リスト：ドットのないホスト名を探すときのドメイン名のリスト
- マルチキャスト ルックアップのドメイン名：マルチキャスト アドレス ルックアップに使用する IP アドレス
- ドメイン ネーム サーバ：内部生成されたクエリーのドメイン名を解決するときに使用するネーム サーバ リスト
- リゾルバ送信元インターフェイス：内部生成されたクエリーのドメイン名を解決するときに使用する送信元インターフェイス
- IP アドレスのラウンドロビン ローテーション：ホスト名のルックアップ時に毎回、キャッシュ中のドメイン名に関連付けられた別の IP アドレス使用イネーブルまたはディセーブル

着信する DNS クエリーを転送するパラメータ

次のパラメータにより、着信 DNS クエリーを転送する方法を定義します。

- クエリーの転送：着信 DNS クエリー転送のイネーブルまたはディセーブル
- フォワーダ アドレス：着信 DNS クエリーを転送するときに使用する IP アドレス リスト
- フォワーダ送信元インターフェイス：着信 DNS クエリーを転送するときに使用する送信元インターフェイス

場合によってデバイスでは、スプリット DNS 機能によって DNS クエリーの転送に使用する送信元インターフェイスを設定したときに、DNS クエリーが、設定したインターフェイスでは転送されないことがあります。この場合は、送信元インターフェイスによって DNS クエリーを転送し、次の点について検討してください。

- 転送送信元インターフェイスが設定され、DNS フォワーダが設定されていない場合、DNS クエリーはブロードキャスト アドレスに転送されます。
- 転送されたクエリーの送信元 IP アドレスは、**dnsforwardingsource-interface***interface* コマンドを使用して、設定されたインターフェイスのプライマリ IP アドレスに設定する必要があります。このような設定が存在しない場合は、転送された DNS クエリーの送信元 IP アドレスが発信インターフェイスのプライマリ IP アドレスになります。DNS の転送は、DNS 転送に設定された送信元インターフェイスがアクティブ状態の場合に限り、実行されます。
- DNS リゾルバ機能に対する DNS クエリーの送信元 IP アドレスは、**domainresolversource-interface***interface-typenumber* コマンドを使用して設定します。DNS アドレスが設定されていない場合、クエリーは、定義済みの送信元インターフェイスにブロードキャストされます。DNS の解決は、DNS 解決に設定された送信元インターフェイスがアクティブ状態の場合に限り、実行されます。設定手順については「DNS クエリー転送時の送信元インターフェイスの指定」を参照してください。

DNS ビュー リスト

DNS ビュー リストは、リスト中の個別のメンバーに対し、追加的な使用制限を指定できる DNS ビューの順序付きリストです。オプションの使用制限の範囲は、特定の DNS ビュー リストに含まれる個別のメンバーだけに制限されます。デバイスが、ある DNS クエリーに応答しなければならない場合、Cisco IOS ソフトウェアは、DNS ビュー リストを使用して、DNS クエリーの処理に使用する DNS ビューを選択します。

（注） サポートされる DNS ビューとビュー リストの最大数は特に制限されず、シスコ デバイスのメモリ容量に依存します。DNS ビューおよびビュー リストに大きい値を設定するとデバイス メモリの消費量が増えます。またビュー リスト中のビュー数に大きい値を設定すると、デバイスのプロセッサ時間が長くなります。最適のパフォーマンスが得られるように、スプリット DNS クエリーの転送やクエリー解決のニーズをサポートするにあたって必要な数を超えるビューやビュー リスト メンバーを設定しないようにしてください。

DNS ビュー リストのメンバーをチェックする順序

DNS ビュー リストを使用して、特定の DNS クエリーを処理する DNS ビューを選択すると、Cisco IOS ソフトウェアは、ビュー リストの各メンバーを、リストで指定された順序に従ってチェックします。さらに処理すべきクエリーでのビューの使用を許可する制限のうち、最初のビュー リスト メンバーを選択します。

ビュー リストの DNS ビューに定義された使用制限

DNS ビュー リスト メンバーは、アクセス コントロール リスト（ACL）で定義した使用制限とともに設定できます。ACL では、クエリー ホスト名またはクエリーの送信元ホスト IP アドレスに基づいて、対応するビュー リスト メンバーの選択に使用するルールを指定します。スプリット

DNS ビュー リストの定義では、2 種類の ACL がサポートされます。これらの ACL については、「DNS 名グループ」で説明します。

（注） 複数の DNS ビュー リストを定義できます。たとえば、各リストにある個別の使用制限に特定の DNS ビューを関連付けることができます。また、個々の DNS ビュー リストに個別の DNS ビューを組み込むこともできます。

DNS ビュー リストの選択

DNS キャッシング ネーム サーバとして動作しているデバイスで、ある DNS クエリーへの応答が必要になると、Cisco IOS ソフトウェアは、DNS ビュー リストを使用して、クエリーの処理に使用できる DNS ビューを特定します。

- DNS ビュー リストが設定されているインターフェイスに到着する着信クエリーに対して、デバイスが応答している場合は、このインターフェイス固有の DNS ビュー リストが使用されます。
- 特定の DNS ビュー リストが設定されていないインターフェイスに到着する着信クエリーに対して、デバイスが応答している場合は、デフォルトの DNS ビュー リストが使用されます。

内部生成されたクエリーに対して、デバイスが応答している場合、ビューの選択には DNS ビュー リストを使用せず、グローバル DNS ビュー リストを使用して、クエリーを処理します。

DNS ビュー リストのデフォルト設定、またはインターフェイスへの割り当てについては、「DNS ビュー グループ」で説明しています。

DNS ビュー リスト メンバーの選択

ビュー リストのメンバーは、デバイスが応答している DNS クエリーの特性に対して、1 つずつ順番に比較されます。

1. クエリーがビュー以外の VRF から送られてきた場合、このビューでクエリーを処理することはできないため、ビュー選択プロセスは、ビュー リストの次のメンバーに移ります。
2. 追加のビュー使用制限は、任意のビュー リスト メンバーに対するオプションの設定として指定します。

クエリー リストで、追加のビュー使用制限が指定されていない場合は、このビューを使用してクエリーを処理するため、ビュー選択プロセスは終了します。

ビュー リストで、追加のビュー使用制限が指定されている場合は、クエリーが個々の使用制限に比較されます。

- クエリーの特性が、いずれかのビュー使用制限に該当する場合は、このビューでクエリーを処理することはできないため、ビュー選択プロセスは、ビュー リストの次のメンバーに移ります。
- クエリー特性がビュー使用制限をすべてクリアしている場合は、このビューを使用してクエリーを処理します。ビュー選択プロセスが終了します。

- ビュー選択プロセスが、クエリーを処理できるビュー リスト メンバーを検出できないまま、選択された DNS ビュー リストの最後まで到達すると、デバイスはこのクエリーを廃棄します。

クエリーの処理には、使用制限がクエリー特性に適合する最初の DNS ビュー リスト メンバーが使用されます。

DNS 名グループ

スプリット DNS 機能では、DNS ビューの使用を制限するときに適用する 2 種類 ACL がサポートされます。ビュー定義自体に含まれる VRF 固有の使用制限に加え、DNS 名リスト、または標準 IP ACL（あるいはその両方）を DNS ビュー リスト メンバーに適用して、ビュー使用制限を指定します。

（注） この文脈で「グループ」という語は、ビュー リスト メンバーに対する使用制限として DNS 名リストまたは標準 IP ACL の指定を表すものとします。

クエリー ホスト名に基づく DNS のビュー使用制限

DNS名リストとは、ホスト名のパターンマッチング ルールの名前付きセットのほか、クエリーのホスト名が、ルール中のテキスト ストリング パターンに一致した場合に実行するアクションのタイプを指定する各ルールを加えたリストのことです。クエリーのホスト名が名前リストに一致する条件として、ホスト名は、マッチング パターンを明示的に許可するルールに一致していなければなりませんが、マッチング パターンを明示的に拒否するいずれのルールにも一致していてはなりません。

クエリー送信元 IP アドレスに基づく DNS のビュー使用制限

標準 IP ACL とは、ホスト IP アドレス マッチング ルールの名番号付きまたは名前付きセットのほか、IPアドレスが、ルール中のテキスト ストリング パターンに一致した場合に実行するアクションのタイプを指定する各ルールを加えたリストのことです。スプリット DNS 機能により、クエリーの送信元 IP アドレスに基づいて標準 ACL をビュー使用制限として使用できるようになります。送信元 IP アドレスが名前リストに一致する条件として、IP アドレスは、マッチング パターンを明示的に許可するルールに一致していなければなりませんが、マッチング パターンを明示的に拒否するいずれのルールにも一致していてはなりません。

DNS ビュー グループ

スプリット DNS 機能では、2 つの方法によって、Cisco IOS ソフトウェアが、着信 DNS クエリーの処理に使用する DNS ビューを選択するときの DNS ビュー リストを指定できます。特定の DNS ビュー リストを使用するように設定されたインターフェイスにクエリーが到着した場合は、イン

ターフェイス固有の DNS ビュー リストを使用します。これ以外の場合は、デフォルト DNS ビュー リストを使用します。

（注） この文脈で「グループ」という語は、インターフェイス固有の DNS ビュー リストとして示した DNS ビュー リスト、またはデバイスに対するデフォルト ビュー リストの指定を表すものとします。

インターフェイス固有のビュー リスト

デバイスインターフェイスには、DNS ビュー リストを対応付けることができます。このインターフェイスに着信 DNS クエリーが到着すると、Cisco IOS ソフトウェアは、該当するビュー リストを使用して、クエリーの処理に使用する DNS ビューを選択します。

デフォルト DNS ビュー リスト

DNS ビュー リストは、デバイスに対するデフォルトの DNS ビュー リストとして設定できます。特定の DNS ビュー リストを使用するように設定されていないインターフェイスに着信 DNS クエリーが到着した場合、Cisco IOS ソフトウェアは、デフォルトのビュー リストにより、クエリーの処理に使用する DNS ビューを選択します。

DNS の設定方法

IP アドレスへのホスト名のマッピング

ホスト名を IP アドレスに関連付けるには、次のタスクを実行します。

ネーム サーバを使用して、ドメイン名に関連付けられた情報を追跡します。ネーム サーバでは、ホスト名からアドレスへのマッピングのデータベースを維持できます。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。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **iphost***name*[*tcp-port-number*] *address1* [*address2 ...address8*] [*mx*nssrv]
4. 次のいずれかを実行します。
   - **ipdomainname***name*
   - **ipdomainlist***name*
5. **ipname-server***server-address1* [*server-address2...server-address6*]
6. **ipdomainlookup**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**iphost***name*[*tcp-port-number*] *address1* [*address2 ...address8*] [*mx*nssrv]
	
	例：
	
	`Device(config)# ip host cisco-rtp 192.168.0.148`
	`Device(config)# ip host test mx 1 mx_record`
	`Device(config)# ip host test ns ns_record`
	`Device(config)# ip host test srv 0 0 0 srv_record`
		スタティック ホスト名からアドレスへのマッピングをホスト キャッシュに定義します。
		
		• 通常は、数字のアドレスではなくシンボリック名でネットワーク デバイスを参照する方が簡単です（Telnet などのサービスでは、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。
		• ダイナミック マッピングが使用可能でない場合は、ホスト名をアドレスに手動で割り当てると便利です。
		• メール エクスチェンジャ（mx）は、特定のドメイン名宛の電子メールの処理を担うメール サーバを特定します。
		• ネーム サーバ（ns）は、特定のドメインに対する権威ネーム サーバを示します。
		• サービス（srv）レコードは、サービスの場所を指定します。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかを実行します。
	• **ipdomainname***name*
	• **ipdomainlist***name*
	
	例：
	`Device(config)# ip domain name cisco.com`
	
	例：
	`Device(config)# ip domain list cisco1.com`
		（任意）非修飾ホスト名を完成させるために Cisco IOS XE ソフトウェアで使用されるデフォルトのドメイン名を定義します。
		または
		（任意）非修飾ホスト名を完成させるためのデフォルト ドメイン名のリストを定義します。
		• ドメイン名要求を完成させるために Cisco IOS XE ソフトウェアで使用され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では、名前が検索される前に、指定したデフォルト ドメイン名が付加されます。
		
		（注） ドメイン リストがない場合、**ipdomainname** 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。**ipdomainlist** コマンドは **ipdomainname** コマンドに似ています。ただし、**ipdomainlist** コマンドでは、システムが一致を検出するまで順番にそれぞれ試行が行われるドメインのリストを定義できます。

ステップ 5	**ipname-server***server-address1* [*server-address2...server-address6*] 例： `Device(config)# ip name-server 172.16.1.111 172.16.1.2`	名前情報を提供する 1 つ以上のホストを指定します。 • DNS に名前情報を提供するネーム サーバとして機能できる 1 つ以上（6 つまで）のホストを指定します。
ステップ 6	**ipdomainlookup** 例： `Device(config)# ip domain lookup`	（任意）DNS ベースのアドレス変換をイネーブルにします。 • DNS はデフォルトでイネーブルになっています。DNS がディセーブルの場合、このコマンドを使用します。

次の作業

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 XE 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。キャッシュに格納されたホスト名および DNS 設定を表示するには、**showhosts** 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 機能のない複数サーバ設定の場合、多くのプログラムは、キャッシュの存続可能時間（TTL）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にだけ、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、ネットワーク アクセス サーバ（NAS）は DNS クエリーを送信します。DNS サーバは、設定された IP アドレスのリストを使用して 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、すべてのホストの IP アドレスを返してホスト名のキャッシュをローテーションします。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 クエリーの量を減らします。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipdomaintimeout***seconds*
4. **ipdomainretry***number*
5. **ipdomainround-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**ipdomaintimeout***seconds* 例： `Device(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。

	コマンドまたはアクション	目的
		• **ipdomaintimeout** コマンドが設定されていない場合、Cisco IOS XE 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	**ipdomainretry***number* 例： `Device(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。 • **ipdomainretry** コマンドが設定されていない場合、Cisco IOS XE 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	**ipdomainround-robin** 例： `Device(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。

ISO CLNS アドレスに対する DNS クエリーの無効化

ISO CLNS アドレスに対する DNS クエリーを無効にするには、このタスクを実行します。

デバイスで IP と ISO Connectionless Network Service（ISO CLNS）の両方が有効になっているときに、ISO CLNS ネットワーク サービスアクセスポイント（NSAP）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に問い合わせることができます。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. イネーブル化
2. **configureterminal**
3. **noipdomainlookupnsap**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**noipdomainlookupnsap** 例： `Device(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。

手順の概要

1. イネーブル化
2. **ping***host*
3. **showhosts**
4. **debugip domain**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**ping***host* 例： `Device# ping cisco-rtp`	基本的な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	**showhosts** 例： `Device# show hosts`	デフォルトのドメイン名、名前ルックアップサービスの方式、ネームサーバホストのリスト、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。

	コマンドまたはアクション	目的
		• DNS を使用して名前が解決されたら、**showhosts** コマンドを使用して、キャッシュに格納されたホスト名と DNS 設定を表示します。
ステップ 4	**debugip domain** 例： `Device# debug ip domain`	DNS のデバッグを有効にし、DNS デバッグ情報を表示します。 • DNS サーバ応答のデバッグなど、他の DNS デバッグ オプションを表示するには、疑問符（?）のオンライン ヘルプ機能を使用してください。

DNS ビューの定義

DNS ビューを定義するには、次の作業を実行します。DNS ビュー定義を使用することにより、着信 DNS クエリー、または内部生成された DNS クエリーのいずれにも応答できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipdnsview** [**vrf***vrf-name*] {**default** | *view-name*}
4. [**no**] **dnstrust***name*
5. [**no**] **domainlookup**
6. 次のいずれかを実行します。
   - **domainname***domain-name*
   - **domainlist***domain-name*
7. 次のいずれかを実行します。
   - **domainname-server**[**vrf** *vrf-name*]*name-server-ip-address*
   - **domainname-serverinterface***interface*
8. **domainmulticast***domain-name*
9. [**no**] **dnsforwarding**
10. **dnsforwarder** [**vrf***vrf-name*] *forwarder-ip-address*
11. **dnsforwardingsource-interface***interface*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**イネーブル化** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**ipdnsview** [**vrf***vrf-name*] {**default** | *view-name*} 例： `Device(config)# ip dns view vrf vpn101 user3`	DNS ビューを定義し、DNS ビュー コンフィギュレーション モードを開始します。
ステップ 4	[**no**] **dnstrust***name* 例： `Device(cfg-dns-view)# dns trust name`	（任意）ビューで信頼できるキーのストレージを有効または無効にし、DNS ビュー コンフィギュレーション モードを開始します。dns trust キーによって DNS セキュリティ機能が有効になります。
ステップ 5	[**no**] **domainlookup** 例： `Device(cfg-dns-view)# domain lookup`	（任意）DNS ビューを使用して処理された内部生成の DNS クエリーについて DNS ベースのホスト名/アドレス変換をイネーブルまたはディセーブルにします。 （注） ドメイン ルックアップ機能はデフォルトによりイネーブルになります。

ステップ 6	次のいずれかを実行します。
	• **domainname***domain-name*
	• **domainlist***domain-name*
	
	例：
	`Device(cfg-dns-view)# domain name example.com`
	
	例：
	`Device(cfg-dns-view)# domain list example1.com`
		（任意）DNS クエリーの対応時に修飾されていないホスト名を補完するために、この DNS ビューが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）DNS クエリーの対応時に修飾されていないホスト名を補完するために、この DNS ビューが使用するドメイン名のリストを定義します。
		• デバイスは、選択した DNS ビューで指定されたパラメータを使用して、クエリーへの応答を試みます。Cisco IOS ソフトウェアはまず、ビューに関連付けられたホスト名キャッシュを調べます。この情報によってクエリーへの対応が可能な場合、デバイスはクエリーに応答します。これ以外の場合は、

	コマンドまたはアクション	目的

		ホスト名キャッシュを使用したクエリーへの応答ができなくなるため、デバイスは、設定されたドメイン ネーム サーバを使用してクエリーを転送します。
		• デバイスがこのビューを使用して修飾されていないホスト名に対する DNS クエリーを処理している場合、ビューのドメイン ルックアップがイネーブルになっていると、Cisco IOS ソフトウェアは、ドメイン名（ドメイン名リストにあるドメイン名、またはデフォルトのドメイン名）を付加して、次のアクティビティのいずれかを実行します。
		  • ネーム サーバ キャッシュにあるホスト名のルックアップ
		  • 別のネーム サーバへのクエリーの転送（選択したビューで DNS フォワーダとして指定されたホスト、または制限付きブロードキャスト アドレスへの転送）
		• 単一のデフォルト ドメイン名、またはドメイン名の順序付きリスト、あるいはその両方を指定できます。ただし、デフォルト ドメイン名はドメイン リストが空の場合に限り使用します。

ステップ 7	次のいずれかを実行します。
	• **domainname-server**[**vrf** *vrf-name*]*name-server-ip-address*
	• **domainname-serverinterface***interface*
	例：
	`Device(cfg-dns-view)# domain name-server 192.168.2.124`
	例：
	`Device(cfg-dns-view)# domain name-server interface FastEthernet0/1`
		（任意）内部生成された DNS クエリーをこの DNS ビューが解決するときに使用するネーム サーバのリストを定義します。ネーム サーバの IP アドレスには IPv4 アドレスまたは IPv6 アドレスを使用でき、その IP アドレスをバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスに関連付けることができます。
		または
		（任意）内部生成された DNS クエリーをこの DNS ビューが解決する際に使用する DNS ネーム サーバのリストに対し、追加する DNS サーバの IP アドレスを取得（インターフェイスにおける DHCP または PPP のやり取りを介して）するときのインターフェイスを定義します。
		• これらのコマンドが両方設定されている場合、インターフェイス上に DHCP または PPP のやり取りが生じると、別の IP アドレスがリストに追加されます。

	コマンドまたはアクション	目的
ステップ 8	**domainmulticast***domain-name* 例： `Device(cfg-dns-view)# domain multicast www.example8.com`	（任意）DNS ビューによるマルチキャスト ルックアップの際に使用する IP アドレスを指定します。
ステップ 9	[**no**] **dnsforwarding** 例： `Device(cfg-dns-view)# dns forwarding`	（任意）DNS ビューを使用して処理された着信 DNS クエリーの転送をイネーブルまたはディセーブルにします。 （注） クエリーの転送機能はデフォルトによりイネーブルになります。
ステップ 10	**dnsforwarder** [**vrf***vrf-name*] *forwarder-ip-address* 例： `Device(cfg-dns-view)# dns forwarder 192.168.3.240`	この DNS ビューが着信 DNS クエリーを転送するときに使用するネーム サーバのリストを定義します。 • 転送 IP アドレスは、IPv4 または IPv6 アドレスを使用できます。 • 転送するネーム サーバが定義されていない場合は、設定されているドメイン ネーム サーバのリストが使用されます。 • ネーム サーバがいずれも設定されていない場合は、制限付きブロードキャスト アドレスにクエリーが転送されます。
ステップ 11	**dnsforwardingsource-interface***interface* 例： `Device(cfg-dns-view)# dns forwarding source-interface FastEthernet0/0`	この DNS ビューでクエリーを転送するときのインターフェイスを定義します。
ステップ 12	**end** 例： `Device(cfg-dns-view)# end`	特権 EXEC モードに戻ります。

DNS ビューの確認

DNS 設定を確認するには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **showipdnsview** [**vrf***vrf-name*] [**default** | *view-name*]
3. **showipdnsserver** [**vrf***vrf-name*] [**default** | *view-name*]
4. **clearipdnsservers**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showipdnsview** [**vrf***vrf-name*] [**default** | *view-name*] 例： `Device# show ip dns view vrf vpn101 user3`	特定の DNS ビュー、ビュー グループ（名前が共通するビュー、または同じ VRF に関連付けられたビュー）、または設定されたすべての DNS ビューに関する情報を表示します。
ステップ 3	**showipdnsserver** [**vrf***vrf-name*] [**default** | *view-name*] 例： `Device# show ip dns server vrf vpn101 user3`	ネーム サーバ キャッシュからの情報を表示します。
ステップ 4	**clearipdnsservers**	ネーム サーバ キャッシュからサーバをクリーン アップします。

DNS ビュー リストの定義

DNS ビューの順序付きリストについて、個々のビュー リスト メンバーごとにオプションの使用制限を追加して定義する場合は、次の作業を実行します。デバイスは、DNS ビュー リストを使用して、DNS クエリーの処理に使用する DNS ビューを選択します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipdnsview-list***view-list-name*
4. **ipdnsname-list** [*number*] [*permit/deny*] [*name*]
5. **view** [**vrf***vrf-name*] {**default** | *view-name*} *order-number*
6. **restrictname-group***name-list-number*
7. **restrictsourceaccess-group***acl-number*
8. **exit**
9. **end**
10. **showipdnsview-list***view-list-name*
11. **showipdnsname-list***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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**ipdnsview-list***view-list-name* 例： `Device(config)# ip dns view-list userlist5`	DNS ビュー リストを定義し、DNS ビュー リスト コンフィギュレーション モードを開始します。
ステップ 4	**ipdnsname-list** [*number*] [*permit/deny*] [*name*] 例： `Device(config)# ip dns name-list 10`	DNS 名リストを定義し、DNS 名リスト 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 5	**view** [**vrf***vrf-name*] {**default** | *view-name*} *order-number* 例： `Device(cfg-dns-view-list)# view vrf vpn101 user5 10`	DNS ビュー リスト メンバーを定義し、DNS ビュー リスト メンバー コンフィギュレーション モードを開始します。
ステップ 6	**restrictname-group***name-list-number* 例： `Device(cfg-dns-view-list-member)# restrict name-group 500`	（任意）この DNS ビュー リスト メンバーが、クエリー ホスト名が、指定の DNS 名リスト中の permit 句に一致する場合、またいずれの deny 句に一致しない場合に限って DNS クエリーへの応答に使用できることを指定します。 • DNS 名リストのエントリを定義するには、**ipdnsname-list** コマンドを使用します。
ステップ 7	**restrictsourceaccess-group***acl-number* 例： `Device(cfg-dns-view-list-member)# restrict access-group 99`	（任意）この DNS ビュー リスト メンバーは、DNS クエリーの送信元 IP アドレスが、指定の標準 ACL に一致する場合に限って DNS クエリーの処理に使用できることを指定します。 • 標準 ACL のエントリを定義するには、**access-list** コマンドを使用します。
ステップ 8	**exit** 例： `Device(cfg-dns-view-list-member)# exit`	DNS ビュー リスト メンバー コンフィギュレーション モードを終了します。 • リストに別のビュー リスト メンバーを追加する場合は、ステップ 4 に戻ってください。
ステップ 9	**end** 例： `Device(cfg-dns-view-list)# end`	特権 EXEC モードに戻ります。
ステップ 10	**showipdnsview-list***view-list-name* 例： `Device# show ip dns view-list userlist5`	特定の DNS ビュー リスト、または設定されたすべての DNS ビュー リストに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 11	**showipdnsname-list***number* 例： `Device# show ip dns name-list 5`	特定の DNS 名リスト、または設定されたすべての DNS 名リストに関する情報を表示します。

DNS ビュー リストの変更

ビュー リスト中の各メンバーの順序を効率的に管理するために、個々のビュー リスト メンバー定義には、リスト中の該当するメンバーの位置が指定されています。つまり、ビュー リスト中の各メンバーの順序が、それぞれリストに追加された順番ではなく、個々の位置の値を表す明示的な指定によって定義されるということです。これにより、すべてのビューリストメンバーを削除しなくても、次のいずれの作業も実行できるようになります。さらにビューリストメンバーシップも必要な順序に従って再定義できるようになります。

すでに使用中の DNS ビュー リストへのメンバーの追加

すでに使用されている DNS ビュー リストに別のメンバーを追加するには、次の任意の作業を実行します。

たとえば、userlist5 という DNS ビュー リストがすでに定義され、デフォルトのビュー リスト、またはインターフェイス固有のビュー リストとして使用されているものとします。ビュー リストは、次のメンバーで構成されていることを前提とします。

- DNS ビュー user1、位置番号 10
- DNS ビュー user2、位置番号 20
- DNS ビュー user3、位置番号 30

リストの 2 つ目のメンバーとして DNS ビュー user4 を追加する場合、リストにこのビューを追加し、位置番号として 11 ～ 19 の値を割り当てます。一度、3 つの既存メンバーを削除して、新たに 4 つの全メンバーを必要な順序でリストに追加し直す必要はありません。

手順の概要

1. イネーブル化
2. **showipdnsview-list***view-list-name*
3. **configureterminal**
4. **ipdnsview-list***view-list-name*
5. **view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number*
6. **end**
7. **showipdnsview-list***view-list-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showipdnsview-list***view-list-name* 例： `Device# show ip dns view-list userlist5`	特定の DNS ビュー リスト、または設定されたすべての DNS ビュー リストに関する情報を表示します。
ステップ 3	**configureterminal** 例： `Device# 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 4	**ipdnsview-list***view-list-name* 例： `Device(config)# ip dns view-list userlist5`	DNS ビュー リストを定義し、DNS ビュー リスト コンフィギュレーション モードを開始します。
ステップ 5	**view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number* 例： `Device(cfg-dns-view-list)# view user4 15`	DNS ビュー リスト メンバーを定義し、DNS ビュー リスト メンバー 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 6	**end** 例： `Device(cfg-dns-view-list-member)# end`	特権 EXEC モードに戻ります。
ステップ 7	**showipdnsview-list***view-list-name* 例： `Device# show ip dns view-list userlist5`	特定の DNS ビュー リスト、または設定されたすべての DNS ビュー リストに関する情報を表示します。

すでに使用中の DNS ビュー リスト メンバーの順序変更

すでに使用されている DNS ビュー リストのメンバーについて順序を変更するには、次の任意の作業を実行します。

たとえば、userlist5 という DNS ビュー リストがすでに定義され、デフォルトのビュー リスト、またはインターフェイス固有のビュー リストとして使用されているものとします。ビュー リストは、次のメンバーで構成されていることを前提とします。

- DNS ビュー user1、位置番号 10
- DNS ビュー user2、位置番号 20
- DNS ビュー user3、位置番号 30

DNS ビュー user1 をリストの最後に移動する場合は、まずこのビューをリストから削除します。次に、再びこのビューをリストに追加し、位置番号として 30 より大きい値を割り当てます。一度、3 つの既存メンバーを削除して、新たに全メンバーを必要な順序でリストに追加し直す必要はありません。

手順の概要

1. イネーブル化
2. **showipdnsview-list***view-list-name*
3. **configureterminal**
4. **ipdnsview-list***view-list-name*
5. **noview** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number*
6. **view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number*
7. **end**
8. **showipdnsview-list***view-list-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showipdnsview-list***view-list-name* 例： `Device# show ip dns view-list userlist5`	特定の DNS ビュー リスト、または設定されたすべてのDNS ビュー リストに関する情報を表示します。
ステップ 3	**configureterminal** 例： `Device# 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 4	**ipdnsview-list***view-list-name* 例： `Device(config)# ip dns view-list userlist5`	DNS ビュー リストを定義し、DNS ビュー リスト コンフィギュレーション モードを開始します。
ステップ 5	**noview** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number* 例： `Device(cfg-dns-view-list)# no view user1 10`	リストから DNS ビュー リスト メンバーを削除します。
ステップ 6	**view** [**vrf** *vrf-name*] {**default** | *view-name*} *order-number* 例： `Device(cfg-dns-view-list)# view user1 40`	DNS ビュー リスト メンバーを定義し、DNS ビュー リスト メンバー コンフィギュレーション モードを開始します。
ステップ 7	**end** 例： `Device(cfg-dns-view-list-member)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**showipdnsview-list***view-list-name* 例： `Device# show ip dns view-list userlist5`	特定の DNS ビュー リスト、または設定されたすべての DNS ビュー リストに関する情報を表示します。

デバイスの DNS サーバに対するデフォルト DNS ビュー リストの指定

デバイスの DNS サーバに対し、デフォルトの DNS ビュー リストを指定するには、次のタスクを実行します。デバイスは、デフォルトの DNS ビュー リストを使用して、インターフェイス固有の DNS ビュー リストが定義されていないインターフェイスに到着する着信 DNS クエリーの処理に使用する DNS ビューを選択します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipdnsserverview-group***name-list-number*
4. **exit**
5. **showrunning-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**ipdnsserverview-group***name-list-number* 例： `Device(config)# ip dns server view-group 500`	デバイスの DNS サーバに対するデフォルトの DNS ビュー リストを設定します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**showrunning-config** 例： `Device# show running-config`	DNS ビュー リストをどのように適用するかに関する情報を表示します。デフォルトの DNS ビュー リストが設定されている場合は、**ip dns server view-group** コマンドの引数として、デフォルトの DNS ビュー情報にこのリストが表示されます。

デバイス インターフェイスに対する DNS ビュー リストの指定

特定のデバイス インターフェイスに対して DNS ビュー リストを指定するには、次の任意のタスクを実行します。デバイスはこのビュー リストを使用して、そのインターフェイスに到着する DNS クエリーの処理に使用する DNS ビューを選択します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***interface*
4. **ipdnsview-group***view-list-name*
5. **end**
6. **showrunning-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**interface***interface* 例： `Device(config)# interface ATM2/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。これにより、特定のインターフェイスを設定できます。
ステップ 4	**ipdnsview-group***view-list-name* 例： `Device(config-if)# ip dns view-group userlist5`	デバイスで、このインターフェイスに対する DNS ビュー リストを設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showrunning-config** 例： `Device# show running-config`	DNS ビュー リストをどのように適用するかに関する情報を表示します。個々のインターフェイスに対する情報には、**ip dns view-group** コマンドの引数として、インターフェイスに対応付けられたすべての DNS ビュー リストが表示されます。

DNS クエリー転送時の送信元インターフェイスの指定

DNS クエリーを転送する送信元インターフェイスを指定するには、次の任意の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipdnsview** [**vrf** *vrf-name*] {**default** | *view-name*}
4. **domainresolversource-interface***interface-typenumber*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**ipdnsview** [**vrf** *vrf-name*] {**default** | *view-name*} 例： `Device(config)# ip dns view vrf vpn32 user3`	指定した VRF インスタンスに関連付けられた指定の名前の DNS ビューを作成し、DNS ビュー コンフィギュレーション モードを開始します。
ステップ 4	**domainresolversource-interface***interface-typenumber* 例： `Device(cfg-dns-view)# domain resolver source-interface fastethernet 0/0`	DNS リゾルバ機能に対する DNS クエリーの送信元 IP アドレスを設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	（任意）特権 EXEC モードに戻ります。

DNS の設定例

例：代替ドメイン名を使用したドメイン リストの作成

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 csi.com
ip domain list telecomprog.edu
ip domain list merit.edu
```

例：IP アドレスへのホスト名のマッピング

次に、ホスト名からアドレスへのマッピング 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 host name-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 device uses to complete
! Set the name for unqualified host names
ip domain name cisco.com
```

例：DNS のカスタマイズ

次に、ip dns サーバの例を示します。

```
show ip dns server

   IP            VRF      TTL(s)   RTT(ms)  RTO(ms)  EDNS  DNSSEC  RECURSION
-------------------------------------------------------------------------------
2::1             red      628      1451     1451      Yes     Yes     Yes
172.168.10.1              875      1787     1787      Yes     Yes     Yes
2.2.2.1          red      606      1447     1447      Yes     Yes     Yes
1::1                      207      300      300       Yes     Yes     Yes
1.1.1.1                   179      242      242       Yes     Yes     Yes
```

例：異なるビュー使用制限によるスプリット DNS ビュー リストの設定

次に、2 つの DNS ビュー リスト、userlist1 および userlist2 を定義する例を示します。いずれのビュー リストも次の 3 つの共通する DNS ビューで構成されるものとします。

- DNS ビュー user1、usergroup10 VRF に関連付ける
- DNS ビュー user2、usergroup20 VRF に関連付ける
- DNS ビュー user3、usergroup30 VRF に関連付ける

いずれのビュー リストにも、同じ順序で指定された同じ DNS ビューが含まれます。

```
ip dns view-list userlist15
 view vrf usergroup100 user1 10
  restrict name-group 121
  exit
view vrf usergroup200 user2 20
  restrict name-group 122
  exit
view vrf usergroup300 user3 30
  restrict name-group 123
  exit
!
exit
ip dns view-list userlist16
 view vrf usergroup100 user1 10
  restrict name-group 121
```

```
  restrict source access-group 71
  exit
 view vrf usergroup200 user2 20
  restrict name-group 122
  restrict source access-group 72
  exit
 view vrf usergroup300 user3 30
  restrict name-group 123
  restrict source access-group 73
  exit
exit
```

ただし、この 2 つの DNS ビュー リストで、それぞれのビュー リスト メンバーに適用する使用制限が異なります。DNS ビュー リスト userlist15 では、そのメンバーに対してクエリー ホスト名の制限だけが適用されます。一方、ビュー リスト userlist16 では、クエリーのホスト名と送信元 IP アドレスに基づいて各メンバーが制限されます。

- userlist15 のメンバーは、クエリーが発信された VRF だけを基準として制限されるため、userlist15 は、内部クライアントから送られた DNS 要求を処理するときの DNS ビューを選択する場合に、標準的なビュー リストとして利用できます。
- userlist16 のメンバーは、クエリーの VRF とホスト名だけでなく、クエリーの送信元 IP アドレスにも制限されるため、userlist16 は、外部クライアントから送られた DNS 要求を処理するときの DNS ビューの選択時に、標準的なビュー リストとして利用できます。

DNS の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
『Master Command List』	『Cisco IOS Master Command List』
IP アドレッシング サービス コマンド リファレンス	『Cisco IOS IP Addressing Services Command Reference』

標準および RFC

標準/RFC	Title
RFC 1348	『DNS NSAP Resource Records』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DNS の設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1*：***DNS*** の設定の機能情報

機能名	リリース	機能の設定情報
DNS の設定	Cisco IOS XE Release 2.1	ドメイン ネーム システム（DNS）は、DNS サーバから DNS プロトコルを使用してホスト名を IP アドレスにマッピングできる分散データベースです。一意の各 IP アドレスにホスト名を関連付けることができます。Cisco IOS XE ソフトウェアは、ホスト名からアドレスへのマッピングのキャッシュを維持します。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。
	Cisco IOS XE リリース 3.13S	Cisco IOS XE リリース 3.13S では、Cisco ASR 1000 シリーズのルータのサポートが追加されました。 次のコマンドが導入または変更されました。**debug ip domain**、**debug ip domain replies**。
	Cisco IOS XE リリース 3.16S	Cisco IOS XE リリース 3.13S では、Cisco ASR 1000 シリーズのルータのサポートが追加されました。 次のコマンドが導入または変更されました。**ddns trust**、**clear ip dns servers**。

第 3 章

VRF-Aware DNS

VRF-Aware DNS 機能によって、ドメイン ネーム システム（DNS）がグローバル IP アドレス空間内の名前付き DNS サーバデータ セットではなく VRF テーブルを使用してネーム サーバにクエリーを転送できるように、バーチャルプライベート ネットワーク（VPN）VPN ルーティング/転送（VRF）インスタンス テーブルの設定が可能になります。この機能を使用することによって、適切なマルチプロトコル ラベル スイッチング（MPLS）VPN 内で DNS 要求を解決できるようになります。

- 機能情報の確認，37 ページ
- VRF-Aware DNS に関する情報，38 ページ
- VRF-Aware DNS の設定方法，39 ページ
- VRF-Aware DNS の設定例，44 ページ
- その他の参考資料，45 ページ
- VRF-Aware DNS の機能情報，46 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool および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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VRF-Aware DNS に関する情報

Domain Name System; ドメイン ネーム システム

ドメイン ネーム システム（DNS）は、TCP/IP で使用されるドメイン名指定手順を定義する標準です。ドメインは、構造を識別するドメイン名を使用して、ネットワークをグループとサブグループに階層的に分離するものです。名前付きグループは、名前付きオブジェクト（通常 IP ホストなどのデバイス）で構成され、サブグループがドメインです。DNS には次の 3 つの基本機能があります。

- ネーム スペース：この機能は、単一ルートからドメインに編成される階層的なスペースです。各ドメインには、デバイス名やより詳細な情報を含めることができます。特別な構文によって有効な名前が定義され、ドメイン名が識別されます。
- 名前登録：この機能は、名前を DNS データベースに入力するために使用されます。ポリシーは、競合やその他の問題を解決するために示されるものです。
- 名前解決：この機能は、分散クライアントおよびサーバ名解決標準です。ネーム サーバは、サーバ上で動作するソフトウェア アプリケーションで、DNS ネーム スペースにあるエンティティの名前とアドレスを記述するリソース レコード（RR）が含まれます。ネーム リゾルバは、クライアントとサーバ間のインターフェイスです。ネーム リゾルバは、サーバから名前に関する情報を要求します。キャッシュは、学習された名前およびアドレスを格納するためにネーム リゾルバによって使用できます。

DNS サーバは、専用デバイスまたはデバイスで動作するソフトウェア プロセスのいずれでも可能です。サーバは、ドメインに関するデータを格納して管理し、名前の競合を解決するための要求に応答します。大規模な DNS 実装では、多くのデバイスにまたがる分散データベースにすることもできます。サーバは専用キャッシュにすることができます。

VRF マッピングおよび VRF-Aware DNS

ドメイン名を追跡するために、IP がネーム サーバの概念を定義します。そのジョブは、IP アドレスに追加される名前のキャッシュ（またはデータベース）を保持するためのものです。キャッシュされた情報は、要求 DNS が再び同じ情報を照会する必要をなくし、DNS をうまく機能させるために重要です。データを保存していないためにサーバが同一アドレスについて毎回照会する必要がある場合、照会されたサーバはフラッディングされ、クラッシュしてしまいます。

リモート ユーザを VRF ドメインにマッピングすることによって、複数のエンタープライズ顧客向けのゲートウェイを保護できます。マッピングとは、リモート ユーザに対する VRF ドメインの IP アドレスの取得を意味します。VRF ドメイン マッピングを使用することで、VRF ドメイン固有 AAA サーバによってリモート ユーザを認証できるため、VRF ドメイン内のリモートアクセス トラフィックをコーポレート ネットワーク上のサーバに転送できるようになります。

複数の VRF ドメインのトラフィックをサポートするために、競合を解決するために使用される DNS およびサーバは VRF を認識する必要があります。VRF 認識とは、DNS サブシステムが最初に VRF 名キャッシュを、次に VRF ドメインを照会し、特定の VRF 名キャッシュに返された RR を格納することです。ユーザは、VRF ごとに個別の DNS ネーム サーバを設定できます。

VRF-Aware DNS が VRF テーブルを使用してクエリーをネーム サーバに転送します。同じ IP アドレスが別の VRF ドメインにある別の DNS サーバに関連付けられるため、各 VRF に対するネーム キャッシュの個別リストが保持されます。テーブルが指定されている場合、DNS はまず特定の VRF ネーム キャッシュを検索し、その後で VRF ネーム サーバにクエリーを送信します。VRF 固有ネーム キャッシュから取得されたすべての IP アドレスは、VRF テーブルを使用してルーティングされます。

VRF-Aware DNS の設定方法

VRF-Aware DNS を有効にするための VRF テーブルの定義とネーム サーバへの割り当て

この作業を実行して、VRF テーブルを定義し、ネーム サーバを割り当てます。

ipname-servervrf コマンド オプションを使用して VRF 固有ネーム サーバが設定されるか、**iphostvrf** コマンド オプションを使用して永続名エントリが設定されるたびに、VRF 固有ネーム キャッシュが存在しない場合これがダイナミックに作成されます。VRF 内のすべてのネーム サーバおよび永続エントリがディセーブルになるたびに、VRF ネーム キャッシュが削除されます。

複数のネーム サーバを同じ VRF 名で構成することは可能です。システムは、これらのサーバに対して、応答があるまで最後に応答を送信したサーバから順番にクエリーを送信します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipvrf***vrf-name*
4. **rd***route-distinguisher*
5. **exit**
6. **ipname-server**[**vrf***vrf-name*] *server-address1* [*server-address2...server-address6*]
7. **ipdomainlookup** [**vrf***vrf-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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Router> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**ipvrf***vrf-name* 例： `Router(config)# ip vrf vpn1`	VRF テーブルを定義し、VRF コンフィギュレーション モードを開始します。 • *vrf-name* 引数に指定できる文字数は、最大 32 文字です。
ステップ 4	**rd***route-distinguisher* 例： `Router(config-vrf)# rd 100:21`	VRF のルーティング テーブルと転送テーブルを作成します。
ステップ 5	**exit** 例： `Router(config-vrf)# exit`	VRF コンフィギュレーション モードを終了します。
ステップ 6	**ipname-server**[**vrf***vrf-name*] *server-address1* [*server-address2...server-address6*] 例： `Router(config)# ip name-server vrf vpn1 172.16.1.111 172.16.1.2`	1 つ以上のネーム サーバのアドレスを VRF テーブルに割り当てて、名前およびアドレス解決に使用します。 • **vrf** キーワードはオプションですが、ネーム サーバが VRF とともに使用されている場合は指定する必要があります。*vrf-name* 引数は、名前を VRF に割り当てます。
ステップ 7	**ipdomainlookup** [**vrf***vrf-name*] 例： `Router(config)# ip domain lookup vrf`	（任意）DNS ベースのアドレス変換をイネーブルにします。 • DNS はデフォルトでイネーブルになっています。DNS がディセーブルになっている場合だけこのコマンドを使用する必要があります。

IP アドレスへの VRF 固有ホスト名のマッピング

この作業を実行して、VRF 固有ホスト名を IP アドレスにマッピングします。

手順の概要

1. イネーブル化
2. **configureterminal**
3. 次のいずれかを実行します。
   - **ipdomainname** [**vrf***vrf-name*] *name*
   - **ipdomainlist** [**vrf***vrf-name*] *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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	次のいずれかを実行します。
	• **ipdomainname** [**vrf***vrf-name*] *name*
	• **ipdomainlist** [**vrf***vrf-name*] *name*
	
	例：
	`Device(config)# ip domain name vrf vpn1 cisco.com`
	
	例：
	`Device(config)# ip domain list vrf vpn1 cisco.com`
		未修飾ホスト名を完成させるために ソフトウェアが使用するデフォルト ドメイン名を定義します。
		または
		修飾されていないホスト名を完全なものにするためにデフォルト ドメイン名のリストを定義します。
		• ソフトウェアがドメイン名要求を実行するために使用するデフォルト 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では、名前が検索される前に、指定したデフォルト ドメイン名が付加されます。
		• **vrf** キーワードと *vrf-name* 引数でデフォルトの VRF ドメイン名を指定します。
		• **ipdomainlist** コマンドを複数回入力して、DNS クエリーを実行する際に付加するためのドメイン名を複数指定することができ

	コマンドまたはアクション	目的
		ます。システムは、一致が見つかるまでそれぞれを順番に付加していきます。

VRF 固有ネーム キャッシュでのスタティック エントリの設定

この作業を実行して、VRF 固有ネーム キャッシュにスタティック エントリを設定します。

ipname-servervrf コマンド オプションを使用して VRF のネーム サーバが設定されるか、**iphostvrf** コマンド オプションを使用して永続名エントリが設定されるたびに、VRF 固有ネーム キャッシュが存在しない場合これがダイナミックに作成されます。VRF 内のすべてのネーム サーバおよび永続エントリがディセーブルになるたびに、VRF ネーム キャッシュが削除されます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **iphostvrf** [*vrf-name*] *name*[*tcp-port*] *address1*[*address2 ...address8*] [*mx ns srv*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**iphostvrf** [*vrf-name*] *name*[*tcp-port*] *address1*[*address2 ...address8*] [*mx ns srv*]
	
	例：
	
	`Device(config)# ip host vrf vpn3 company1.com 172.16.2.1`
	`Device(config)# ip host test mx 1 mx_record`
	`Device(config)# ip host test ns`
		ホスト キャッシュ内にホスト名/アドレスのスタティック マッピングを定義します。
		
		• ホストの IP アドレスには IPv4 アドレスまたは IPv6 アドレスを使用でき、その IP アドレスをバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスに関連付けることができます。

	コマンドまたはアクション	目的
	`ns_record` `Device(config)# ip host test srv 0 0 0 srv_record`	• **vrf** キーワードおよび *vrf-name* 引数が指定されている場合、VRF 固有ネーム キャッシュ内だけに永続エントリが作成されます。 • メール エクスチェンジャ（mx）は、特定のドメイン名宛の電子メールの処理を担うメール サーバを特定します。 • ネーム サーバ（ns）は、特定のドメインに対する権威ネーム サーバを示します。 • サービス（srv）レコードは、サービスの場所を指定します。

VRF テーブル内のネーム キャッシュ エントリの確認

この作業を実行して、VRF テーブル内のネーム キャッシュ エントリを確認します。

手順の概要

1. イネーブル化
2. **showhosts** [**vrf** *vrf-name*] {**all**| *hostname*} [**summary**]
3. **clearhost**[**vrf** *vrf-name*] {**all**| *hostname*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showhosts** [**vrf** *vrf-name*] {**all**| *hostname*} [**summary**] 例： `Device# show hosts vrf vpn2`	• デフォルトのドメイン名、名前ルックアップ サービスのスタイル、ネーム サーバ ホストのリスト、ホスト名およびアドレスのキャッシュ済みリスト、特定のバーチャルプライベート ネットワーク（VPN）固有のホスト名およびアドレスのキャッシュ済みリストを表示します。 • **vrf** キーワードと *vrf-name* 引数は、VRF 名が設定された場合にのみエントリを表示します。

	コマンドまたはアクション	目的
		• VRF を指定せずに **show hosts** コマンドを入力すると、グローバル ネーム キャッシュ内のエントリだけが表示されます。
ステップ 3	**clearhost**[**vrf** *vrf-name*] {**all**| *hostname*} 例： `Device# clear host vrf vpn2`	（任意）ホスト名対アドレス グローバル アドレス キャッシュまたは VRF 名キャッシュからエントリが削除されます。

VRF-Aware DNS の設定例

例：VRF 固有ネーム サーバの設定

次に、IP アドレスが 172.16.1.111 および 172.16.1.2 の、vpn1 という名前の VPN をネーム サーバとして指定する例を示します。

```
ip name-server vrf vpn1 172.16.1.111 172.16.1.2
```

例：VRF 固有ドメイン名リストの設定

次に、vpn1 および vpn2 内のリストに複数のドメイン名を追加する例を示します。ドメイン名は、指定された VRF の名前クエリーだけに使用されます。

```
ip domain list vrf vpn1 company.com
ip domain list vrf vpn2 school.edu
```

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** コマンドに似ています。ただし、**ip domain list** コマンドでは、一致が見つかるまで順番にそれぞれ試行が行われるドメインのリストを定義できます。

VRF 固有ドメイン名設定の例

次に、vpn1 という名前の VPN に対して cisco.com をデフォルト ドメイン名として定義する例を示します。ドメイン名は、指定された VRF の名前クエリーだけに使用されます。

```
ip domain name vrf vpn1 cisco.com
```

ドメイン名を含まない IP ホスト名（つまりドットのない名前）にはドットと cisco.com が追加され、その後で検索されます。

VRF 固有 IP ホストの設定の例

次に、vpn2 および vpn3 のホスト キャッシュで、2 つのスタティック ホスト名からアドレスへのマッピングを定義する例を示します。

```
ip host vrf vpn2 host2 10.168.7.18
ip host vrf vpn3 host3 10.12.0.2
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
VRF 対応の DNS 設定作業：VRF 対応 DNS のイネーブル、VRF 固有のホスト名から IP アドレスへのマッピング、VRF 固有のホスト名キャッシュ中のスタティック エントリの設定、VRF テーブル中のホスト名キャッシュ エントリの確認	「VRF-Aware DNS」モジュール
DNS の設定作業	「DNS の設定」モジュール
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*』

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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	Title
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html

VRF-Aware DNS の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2*：***DNS*** の機能情報

機能名	リリース	機能の設定情報
VRF-Aware DNS	Cisco IOS XE Release 2.1	VRF-Aware DNS 機能によって、ドメイン ネーム システム（DNS）がグローバル IP アドレス空間内の名前付き DNS サーバデータ セットではなく VRF テーブルを使用してネーム サーバにクエリーを転送できるように、バーチャル プライベート ネットワーク（VPN）VPN ルーティング/転送（VRF）インスタンス テーブルの設定が可能になります。この機能を使用することによって、適切なマルチプロトコル ラベル スイッチング（MPLS）VPN 内で DNS 要求を解決できるようになります。

第 4 章

Service Discovery Gateway

Service Discovery Gateway 機能はマルチキャスト ドメイン ネーム システム（mDNS）を有効にして、レイヤ 3（L3）の境界を越えて動作します。mDNS ゲートウェイは、サービスをフィルタリングして、キャッシングし、1 つのサブネットから別のサブネットへ拡張することによって、L3 の境界を越えたサービス検出のための転送を実現できます。この機能が実装されるまで、リンクローカル範囲内のマルチキャスト アドレスが使用されていたため、mDNS の範囲はサブネット内に限定されていました。この機能により、個人所有デバイスの持ち込み（BYOD）が強化されます。

注意 サービス拡張は適切に行う必要があります。通常は特定のサービスのみを拡張すべきです。サービス名はネットワーク内で一意にし、重複した名前による競合を避ける必要があります。

お使いのプラットフォーム リリース バージョンに使用可能な機能を確認するには、「Service Discovery Gateway の機能情報」の項を参照してください。

- Service Discovery Gateway に関する情報，49 ページ
- Service Discovery Gateway の設定方法，56 ページ
- Service Discovery Gateway の確認とトラブルシューティング，65 ページ
- Service Discovery Gateway の設定例，67 ページ
- Service Discovery Gateway に関する追加情報，69 ページ
- Service Discovery Gateway の機能情報，71 ページ

Service Discovery Gateway に関する情報

サービス アナウンスの再配布とサービス拡張

アナウンスの再配布とはアナウンスやクエリー応答を実際に転送することであり、サービス拡張とはサブネット間でのプロキシサービス機能のことです。サービスアナウンスの実際の複製は、

新たにアナウンスされたサービスの表示や、サービスまたはデバイスがオフになった場合のサービスの取り消しの表示を高速化するのに役立ちます。

（注） プリンタや Apple TV などのサービスの拡張は、サービス アナウンスを実際に複製しなくても十分に機能します。Service Discovery Gateway が、アナウンス、クエリー、およびその応答をキャッシュに格納します。別のデバイスがサービスを問い合わせた場合は、Service Discovery Gateway がそのキャッシュから回答を提供することができます。

redistribution mdns-sd コマンドは、インターフェイス単位でのみ、実際に必要な場合に限って有効にできます。サービス アナウンスの再配布が有効になっているインターフェイスに対応するネットワーク トポロジにループがないことを確認する必要があります。ループによってブロードキャスト ストームが発生する可能性があります。

サービス アナウンス情報の再配布はグローバルに実行することはできません。サービス情報の再配布はインターフェイス レベルでのみ有効にできます。

サブネット間でのサービス拡張：概要

サブネット境界を越えてサービスを拡張するには、マルチキャスト ドメイン ネーム システム（mDNS）ゲートウェイを有効にする必要があります。デバイスまたはインターフェイスに対して mDNS ゲートウェイを有効にできます。有効にする前に、デバイスに対するサービスのルーティングをインターフェイスで有効にする必要があります。mDNS ゲートウェイをデバイスまたはインターフェイスで有効にした後は、サブネット境界を越えてサービスを拡張できます。

サブネット間でサービスを拡張するには、次の手順を実行する必要があります。

1. サブネット間にサービスを拡張するためのフィルタ オプションの設定：サブネット間でプリンタ サービスなどのサービスにアクセスできるようにします。プリンタ x がインターフェイス 1 で使用できる場合、インターフェイス 2 のユーザは、ローカル システムにプリンタを設定しなくてもプリンタ x を使用できます。
2. サブネット間でのサービス拡張：ステップ 1 で作成したフィルタをインターフェイス 1 と 2 に適用する必要があります。それを行った後でのみ、他のインターフェイスのユーザがプリンタ サービスにアクセスできるようになります。

他のインターフェイスのクライアントがプリンタ サービスにアクセスできるこのシナリオでは、次のフィルタを適用する必要があります。

- プリンタ サービスを使用できるインターフェイス上（IN フィルタ）：他のサブネットのユーザがアクセスできるように、mDNS キャッシュでプリンタ サービスを受信できるようにします。
- プリンタ サービスを使用できるインターフェイス上（OUT フィルタ）：他のインターフェイスのクライアントがサービス（プリンタ x など）にアクセスするため、デバイスから着信するクエリーを許可する必要があります（デバイスの観点からの OUT フィルタ）。

- クライアントが存在する各インターフェイス上（IN フィルタ）：プリンタ サービスにアクセスする他のインターフェイス（サブネット）上のクライアントに対して、ユーザから mDNS キャッシュへのクエリーを許可する必要があります。

メモ　IN フィルタを適用すると、デバイスの mDNS キャッシュでプリンタ サービスを受信することを許可することになり、他のインターフェイスがそのプリンタ サービスにアクセスできるようになります。OUT フィルタを適用すると、キャッシュからクエリーが送信されることを許可することになり、他のインターフェイスのクライアントからのクエリーがプリンタインターフェイスに到達できるようになります。クライアント側の他のインターフェイス上では、IN フィルタを適用してクエリーの受信を許可します。

（注）

- グローバル レベルおよびインターフェイス レベルでクエリーを適用できます。インターフェイス レベルで適用されたフィルタは、グローバル レベルで適用されたフィルタよりも優先されます。
- 「サービス検出情報」という語は、サブネットをまたいで拡張するサービス（プリンタ サービスなど）、クエリー（1 つのインターフェイスから別のインターフェイスへのプリンタ サービスなどを要求するクエリー）、アナウンス（プリンタ サービスが削除されたなど）、およびサービス インスタンス（プリンタ x、Apple TV 3 などの特定のサービス）のことです。

サブネット間にサービスを拡張するためのフィルタオプションの設定

プリンタ サービスなどのサービスがデバイスやインターフェイスで送受信できるようにフィルタ オプションを設定することができます。また、インターフェイス、特定のサービス インスタンス、および場所から学習したクエリー、アナウンス、サービスを許可または拒否することもできます。**service-list mdns-sd** コマンドを使用して、サービス リストを作成し、フィルタ オプションを設定します。

サービス リストを作成し、そのリスト内でフィルタ オプションを使用する必要があります。サービス リストの作成時に、次のいずれかのオプションを使用します。

- **permit** オプションは、サブネットをまたいだ特定のサービス、アナウンス、およびサービス インスタンスを許可します。
- **deny** オプションは、サービス、アナウンス、およびサービス インスタンスがサブネット間で転送されることを制限します。
- **query** オプションは、サービスを参照するために指定します。たとえば、プリンタ サービスを定期的に参照する場合は、**query** オプションを使用してサービス リストを作成し、プリンタ サービスをクエリーに追加します。クエリーの期間を設定すると、キャッシュ メモリ内でサービス エントリが更新されます。

permit または **deny** オプションを使用する場合は、シーケンス番号を指定する必要があります。フィルタリングは、昇順で順番に実行されます。同じサービス リストを複数のシーケンス番号に関連付けることができます。シーケンス内で、match ステートメント（コマンド）を使用して、フィルタリングが必要なものを指定する必要があります。通常は、match ステートメントを使用して、クエリー（たとえば、プリンタ サービスや FAX サービスを検出するためのクライアントからのクエリー）、アナウンス（新規サービスの追加など）、特定のサービス インスタンス、プリンタ サービスなどのサービスのタイプ（その結果、サービスがキャッシュに格納されて使用可能になる）、特定のインターフェイス（プリンタや VLAN に関連付けられた Apple TV）で利用できるサービス、および場所をフィルタリングします。

（注） サービス リスト自体にはどのようなサービスも含まれていません。サービスを許可または禁止するには、フィルタ オプションの設定時に match ステートメントでサービス タイプを指定する必要があります（たとえば、「_ipp._tcp」は TCP 上で実行している IPP 印刷サービスのサービス タイプです）。

サンプル シナリオ：クライアントセグメントにデバイスがあるとします。目標は、デバイス上で次を許可することです。

- クライアントからデバイスへのすべてのクエリー。
- 別のサブネット上のクライアントへのプリンタ サービス。

次に、この目標の達成方法の例を示します。

```
!
service-list mdns-sd mixed permit 10
  match message-type query
!
service-list mdns-sd mixed permit 20
  match message-type announcement
  match service-type _ipps._tcp.local
!
```

上記の例では、「mixed」と呼ばれるサービス リストが作成され、クエリーのフィルタリング用とプリンタ サービスおよびアナウンスメントのフィルタリング用に **permit** オプションが 2 回使用されています。フィルタリングは、次に示す順序で実行されます。

- シーケンス 10：match ステートメントを使用してクエリーをフィルタリングする。
- シーケンス 20：match ステートメントを使用してアナウンスとプリンタ サービスをフィルタリングする。

シーケンス番号 10 の match ステートメントでデバイス上でのクエリーに対するフィルタを設定します。ただし、このステートメントでは、デバイスがクエリーを受信する許可を指定していません。クライアントからのクエリーを許可するには、インターフェイスの IN 方向にフィルタを適用する必要があります。この例は、「サブネット間でのサービス拡張」の項に示されています。

同様に、シーケンス番号 20 の match ステートメントでデバイス上でのアナウンスとプリンタ サービスに対するフィルタを設定します。ただし、このステートメントでは、デバイスでアナウンス

やプリンタ サービスを受信する許可を指定していません。デバイスでのアナウンスやプリンタ サービスの受信を許可するには、必要なインターフェイスのIN方向にフィルターを適用する必要があります。この例は、「サブネット間でのサービス拡張」の項に示されています。

permit オプションも **deny** オプションも使用しない場合、デフォルトにより、他のサブネットへのサービスの転送は許可されません。

定期的なサービスの参照：**query** タイプのサービス リストを使用してサービスを参照することができます。このようなクエリーをアクティブ クエリーと呼びます。アクティブなクエリーは、すべてのインターフェイス上でクエリー内に指定されたサービスの要求を定期的に送信します。サービスには特定の存続可能時間（TTL）があるため、アクティブ クエリーはキャッシュ メモリ内のサービスを最新に維持するのに役立ちます。

次に、「active-query」という名前で、タイプが **query** のサービス リストを作成する例を示します。プリンタ サービスなどのサービスはクエリー内で指定されており、これらのサービスを拡張します。通常、これらのサービスは、IN フィルタの「permitted」サービスとして設定されているサービスと一致します。

```
!
service-list mdns-sd active-query query
  service-type _universal._sub._ipp._tcp
  service-type _ipp._tcp.local
  service-type _ipps._tcp.local
  service-type _raop._tcp.local
!
```

アクティブ クエリーと、match ステートメントに関連付けられたクエリーの目的は異なります。アクティブ クエリーを有効にすると、サービスは定期的に参照されます。インターフェイス上で（アクティブ クエリーではない）クエリーを許可または禁止するには、match ステートメントにクエリーを使用します。

（注）

- サービス リストの作成はグローバルにのみ使用でき、インターフェイス レベルでは使用できません。
- **service-instance mdns-sd** コマンドを使用すると、特定のサービス タイプの新しいサービス インスタンスを作成できます。
- サービスの起動時に、サービス エンドポイント（プリンタ、ファックスなど）サービスが未承認のアナウンスを送信します。その後、ネットワーク変更イベント（インターフェイスの表示や消去）が発生するたびに、非請求アナウンスメントを送信します。デバイスは常にクエリーに応答します。

メモ

フィルタリングではフィルタ オプションのみを設定し、特定のサービスをフィルタリングする必要があることを指定します。インターフェイスで実際に許可または禁止するサービス、クエリー、またはアナウンスに対して、そのインターフェイス上にフィルタを適用する必要があります。フィルタや他の使用可能なサービス検出設定オプションの適用方法については、「サブネット間でのサービス拡張」の項を参照してください。

サブネット間でのサービス拡張

サブネット間にサービスを拡張する前に、デバイスに対してフィルタ オプションを設定しておく必要があります。特定のサービスに対してフィルタ オプションを設定し、他のサービス検出情報を許可する、禁止する、または定期的に問い合わせるように設定しておくと、1つのインターフェイスに複数のフィルタを適用することができます。

フィルタを適用する前に、次の点に注意してください。

- デバイスのマルチキャスト ドメイン ネーム システム（mDNS）を有効にしてフィルタ オプションを適用する必要があります。mDNS は **service-routing mdns-sd** コマンドを使用して有効にできます。
- デバイスでのサービスの受信を許可したり、インターフェイスでのサービスの学習を禁止したりできるため、フィルタは必要な方向に適用する必要があります。**IN** オプションと **OUT** オプションはインターフェイス上で必要なアクションを実行します。
- 通常は、インターフェイスにサービス ポリシーが適用されます。グローバル サービス ポリシーはオプションであり、すべての L3 インターフェイスに影響します。

サンプル シナリオ：クライアント セグメントにデバイスがあり、目標はデバイス インターフェイス間で次を許可することです。

- クライアントからデバイスへのすべてのクエリー。
- プリンタ サービス。

フィルタ オプションに関するメモ：「mixed」というサービス リストを作成し、そのサービス リストにフィルタ オプションを追加することで、上記のシナリオに対してフィルタ オプションが設定されています（詳細については「サブネット間にサービスを拡張するためのフィルタ オプションの設定」を参照してください）。次に、フィルタを適用する例を示します。

```
!
interface Ethernet0/0
 description *** (wireless) Clients here plus some printers
 ip address 172.16.33.7 255.255.255.0
 service-routing mdns-sd
  service-policy mixed IN
!
interface Ethernet0/3
 description *** (wireless) Clients here plus some printers
 ip address 172.16.57.1 255.255.255.0
 service-routing mdns-sd
  service-policy mixed IN
!
```

上記の例では、インターフェイスでサービス ルーティングが有効になり、サービス ポリシー「mixed」のフィルタ オプションが **IN** 方向に適用されます。つまり、インターフェイスのイーサネット 0/0 とイーサネット 0/3 からデバイスへのすべてのクエリーとプリンタ サービスが許可されます。

特定のサービスを参照するためのサンプル シナリオ：タイプが **query** のサービス リスト（アクティブ クエリーと呼ぶ）が作成されています。このサービス リストには定期的に参照するサービ

スが含まれています（アクティブ クエリーの作成の詳細については、「サブネット間にサービスを拡張するためのフィルタ オプションの設定」を参照してください）。クエリー内のサービスの参照を有効にするには、デバイスに対してアクティブ クエリーを適用する必要があります。

```
!
service-routing mdns-sd
 service-policy-query active-query 900
!
```

上記の例では、時間は900秒に設定されます。900秒の間隔の後に、デバイスのすべてのインターフェイスでアクティブ クエリー内のサービスが問い合わせられます。

（注）

- 特定のインターフェイスに対して、サービスの参照を有効にすることができます。サービスの参照をグローバルに有効にすると、特定のインターフェイスのサービスの参照を無効にすることができます。
- mDNS プロセスにより、デバイスまたはインターフェイスを特定してサービスが参照されます。つまり、サービスの参照には IN オプションも OUT オプションも関係ありません。

mDNS をデバイスまたはインターフェイスで有効にした後は、次のオプションを使用できます。

目的	使用するコマンド （注） 完全なシンタックスは、対応するタスクで示します。	グローバル設定とインターフェイス設定のオプション
サービス リストでは、フィルタを適用してサービスを許可または禁止します。	**service-policy**	グローバルおよびインターフェイス レベル。
キャッシュのシステム メモリの一部を設定します。	**cache-memory-max**	グローバル レベル。
指定したサービスを定期的に問い合わせるように、アクティブ クエリーとクエリの期間を設定します。	**service-policy-query**	
mDNS アナウンスとクエリー情報をルーティングするために、ドメインの特定のデバイスかインターフェイスを指定します。	**designated-gateway**	グローバルおよびインターフェイス レベル。

デバイスに近接するサービスにアクセスします。 （注） サービス ポリシーのプロキシミティ フィルタリング機能は、ワイヤレス デバイスとそのインターフェイスでのみ使用できます。	**service-policy-proximity**	グローバルおよびインターフェイス レベル。
デバイスのサービス タイプ列挙期間を設定します。	**service-type-enumeration period**	グローバル レベル。
デバイスの発信 mDNS パケットの代替送信元インターフェイスを指定します。	**source-interface**	グローバル レベル。
デバイスの着信 mDNS パケットの最大レート制限を設定します。	**rate-limit**	グローバル レベル。
新たにアナウンスしたサービスや、サービスまたはデバイスがオフになったときのサービスの取り消しを迅速に表示します。	**redistribute**	インターフェイス レベル。

Service Discovery Gateway の設定方法

サービス検出に対するフィルタ オプションの設定

はじめる前に

フィルタ オプションを設定するときに、クエリーまたはアナウンスを許可したことを確認します。**permit** オプションを使用せずに **deny** オプションのみを使用した場合は、フィルタを適用できません。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **service-list mdns-sd** *service-list-name* {**deny***sequence-number* | **permit** *sequence-number* | **query**}
4. **match message-type** {**announcement** | **any** | **query**}
5. **match service-instance** {*instance-name* | **any** | **query**}
6. **match service-type** *mDNS-service-type-string*
7. **match location civic** *civic-location-name*
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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	**service-list mdns-sd** *service-list-name* {**deny***sequence-number* | **permit** *sequence-number* | **query**}
	
	例：
	
	`Device(config)# service-list mdns-sd sl1 permit 3`
	
	Or
	
	`Device(config)# service-list mdns-sd sl4 query`
		mDNS サービス検出サービス リスト モードを開始します。
		
		• サービス リストを作成し、シーケンス番号に適用された **permit** オプションまたは **deny** オプションに従って、サービス リストにフィルタを適用します。
		
		または
		
		• サービス リストを作成し、**query** オプションが使用されている場合にはサービス リスト名に対するクエリーを関連付けます。
		
		メモ　フィルタ オプションを設定するときは、サービス リストに対してクエリーまたはアナウンスが許可されていることを確認します。**permit** オプションを使用せずに **deny** オプションのみを使用した場合は、フィルタを適用できません。

	コマンドまたはアクション	目的
ステップ 4	**match message-type** {**announcement** | **any** | **query**} 例： `Device(config-mdns-sd-sl)# match message-type announcement`	サービス アナウンスまたはクエリーに基づいて、サービス リストにパラメータを設定します。 （注） **query** オプションを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** オプションまたは **deny** オプションにのみ使用できます。
ステップ 5	**match service-instance** {*instance-name* | **any** | **query**} 例： `Device(config-mdns-sd-sl)# match service-instance printer-3`	サービス インスタンスまたはクエリーに基づいて、サービス リストにパラメータを設定します。
ステップ 6	**match service-type** *mDNS-service-type-string* 例： `Device(config-mdns-sd-sl)# match service-type _ipp._tcp.local`	サービス タイプに基づいて、サービス リストにパラメータを設定します。
ステップ 7	**match location civic** *civic-location-name* 例： `Device(config-mdns-sd-sl)# match location civic location3`	都市ロケーションに基づいて、サービス リストにパラメータを設定します。
ステップ 8	**exit** 例： `Device(config-mdns-sd-sl)# exit`	mDNS サービス検出サービス リスト モードを終了し、グローバル コンフィギュレーション モードに戻ります。

次の作業

インターフェイスで実際に許可または禁止するサービス、クエリー、またはアナウンスに対して、そのインターフェイス上にフィルタを適用します。

サービス検出フィルタの適用とサービス検出パラメータの設定

デバイスに対してマルチキャスト ドメイン ネーム システム（mDNS）ゲートウェイを有効にした後に **service-policy** コマンドと **service-policy-query** コマンドを使用すると、フィルタ（インバウン

ド フィルタリングまたはアウトバウンド フィルタリング）とアクティブ クエリーをそれぞれ適用できます。

（注） ステップ 5 ~ 11 は mDNS サービス検出設定のオプションです。これらのステップはオプションであり、特定の順序での使用を意味するものではありません。

はじめる前に

フィルタを適用する前に、デバイスに対してフィルタ オプションを設定する必要があります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **service-routing mdns-sd**
4. **service-policy** *service-policy-name* {**IN** | **OUT**}
5. **cache-memory-max** *cache-config-percentage*
6. **service-policy-query** *service-list-name query-period*
7. **designated-gateway enable** [**ttl** *duration*]
8. **service-policy-proximity** *service-list-name* [**limit** *number-of-services*]
9. **service-type-enumeration period** *period-value*
10. **source-interface** *type number*
11. **rate-limit in***maximum-rate-limit*
12. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**service-routing mdns-sd** 例： `Device(config)# service-routing mdns-sd`	デバイスに対して mDNS ゲートウェイ機能を有効にし、マルチキャスト DNS コンフィギュレーション（config-mdns）モードを開始します。
ステップ 4	**service-policy** *service-policy-name* {**IN** | **OUT**} 例： `Device(config-mdns)# service-policy sl1 IN`	サービス リストでは、着信サービス検出情報（インバウンド フィルタリング）または発信サービス検出情報（アウトバウンド フィルタリング）にフィルタを適用します。 （注） グローバル サービス ポリシーはオプションであり、すべてのL3インターフェイスに影響します。通常は、インターフェイスにサービス ポリシーが適用されます。
ステップ 5	**cache-memory-max** *cache-config-percentage* 例： `Device(config-mdns)# cache-memory-max 20`	キャッシュのシステムメモリの一部を設定します（パーセント単位）。 （注） デフォルトでは、システム メモリの 10％がキャッシュ用として確保されます。このコマンドを使用して、デフォルト値を上書きできます。
ステップ 6	**service-policy-query** *service-list-name query-period* 例： `Device(config-mdns)# service-policy-query sl4 100`	アクティブ クエリーを作成し、サービス リストのクエリー期間を設定します。
ステップ 7	**designated-gateway enable** [**ttl** *duration*] 例： `Device(config-mdns)# designated-gateway enable`	デバイスを指定して、ドメインの mDNS アナウンスとクエリー情報をルーティングします。
ステップ 8	**service-policy-proximity** *service-list-name* [**limit** *number-of-services*] 例： `Device(config-mdns)# service-policy-proximity sl1 limit 10`	デバイスのサービス ポリシーのプロキシミティ フィルタリングを設定します。 • サービス ポリシーのプロキシミティ フィルタリングはワイヤレスクライアントでのみ使用できます。これは、Radio Resource Management（RRM）に基づいています。有線クライアントとサービスはこの制限の影響を受けません。 • 返すことができるサービスの最大数のデフォルト値は 50 です。

	コマンドまたはアクション	目的
ステップ 9	**service-type-enumeration period** *period-value* 例： `Device(config-mdns)# service-type-enumeration period 45`	デバイスのサービス タイプ列挙期間を設定します。
ステップ 10	**source-interface** *type number* 例：	デバイスの発信 mDNS パケットの代替送信元インターフェイスを指定します。
ステップ 11	**rate-limit in***maximum-rate-limit* 例： `Device(config-mdns)# rate-limit in 80`	デバイスの着信 mDNS パケットの最大レート制限を設定します。
ステップ 12	**exit** 例： `Device(config-mdns)# exit`	マルチキャスト DNS コンフィギュレーション モードを終了してグローバルコンフィギュレーションモードに戻ります。

インターフェイスに対するサービス検出フィルタの適用

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface** *type number*
4. **service-routing mdns-sd**
5. **service-policy** *service-policy-name* {**IN** | **OUT**}
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**interface** *type number* 例：	インターフェイス マルチキャスト NDS コンフィギュレーション モードを開始し、インターフェイス設定を有効にします。
ステップ 4	**service-routing mdns-sd** 例： `Device(config-if)# service-routing mdns-sd`	インターフェイスに対して mDNS ゲートウェイ機能を有効にし、マルチキャスト DNS コンフィギュレーション（config-mdns）モードを開始します。
ステップ 5	**service-policy** *service-policy-name* {**IN** | **OUT**} 例： `Device(config-if-mdns-sd)# service-policy sl1 IN`	サービス リストでは、着信サービス検出情報（インバウンド フィルタリング）または発信サービス検出情報（アウトバウンド フィルタリング）にフィルタを適用します。 メモ　フィルタ オプションを設定するときは、サービス リストに対してクエリーまたはアナウンスが許可されていることを確認します。フィルタ オプションを設定中にサービス、クエリー、またはアナウンスを許可しなかった場合は、フィルタを適用すると次の警告が表示されます。 **Warning**: Please enable explicit service-list rule with the permit action to allow queries and responses.
ステップ 6	**exit** 例： `Device(config-if-mdns-sd)# exit`	インターフェイス マルチキャスト DNS コンフィギュレーション モードを終了し、インターフェイス コンフィギュレーション モードに戻ります。

サービス インスタンスの作成

手順の概要

1. イネーブル化
2. **configureterminal**
3. **service-instance mdns-sd service** *instance-name* **regtype** *service-type* **domain** *name*
4. {**ipv4addr** | **ipv6addr**}*IP-address*
5. **port***number*
6. **target-hostname***host-name*
7. **txt***text-record-name*
8. **priority***value*
9. **weight***value*
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**service-instance mdns-sd service** *instance-name* **regtype** *service-type* **domain** *name* 例： `Device(config)# service-instance mdns-sd service printer-3 regtype _ipp._tcp.local domain tcp4`	特定のサービスタイプのサービスインスタンスを作成して、マルチキャスト ドメイン ネーム システム（mDNS）のサービス検出サービス インスタンス（config-mdns-sd-si）モードを開始します。 （注） このモードでは、サービス インスタンスにさまざまなパラメータを設定できます。以降のステップで、サービスインスタンスパラメータの設定方法を示します。
ステップ 4	{**ipv4addr** | **ipv6addr**}*IP-address* 例： `Device(config-mdns-sd-si)# ipv4addr 209.165.200.230 255.255.255.0`	サービスを使用できるポートの IPv4 アドレスまたは IPv6 アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 5	**port***number* 例： `Device(config-mdns-sd-si)# port 9100`	サービスを使用できるポートを指定します。
ステップ 6	**target-hostname***host-name* 例： `Device(config-mdns-sd-si)# target-hostname fqdn-of-printer.example.com.`	ターゲット ホストの完全修飾ドメイン名（FQDN）を指定します。
ステップ 7	**txt***text-record-name* 例： `Device(config-mdns-sd-si)# txt _ipp._tcp.local=printer3`	サービスインスタンスに関連付けられているテキスト レコードを指定します。 （注） TXT レコードは、ドメイン外の送信元にテキスト情報を提供するタイプの DNS レコードです。「service-type=service-name」形式のテキスト レコードを指定します。複数のレコードを指定するには、区切り文字としてセミコロン（;）を使用します。
ステップ 8	**priority***value* 例： `Device(config-mdns-sd-si)# priority 3`	（任意）サービス インスタンスのプライオリティ値を指定します。デフォルトのプライオリティ値はゼロです。
ステップ 9	**weight***value* 例： `Device(config-mdns-sd-si)# weight 20`	（任意）サービス インスタンスの重み値を指定します。デフォルトの重み値はゼロです。
ステップ 10	**exit** 例： `Device(config-mdns-sd-si)# exit`	マルチキャスト ドメイン ネーム システム（mDNS）のサービス検出サービス インスタンス（config-mdns-sd-si）モードを終了し、グローバル コンフィギュレーション モードに戻ります。

Service Discovery Gateway の確認とトラブルシューティング

（注） 次に示す show コマンドと debug コマンドは、どのような順序でも使用できます。

手順の概要

1. **show mdns requests** [**detail** | [**type***record-type*] [**name** *record-name*]]
2. **show mdns cache** [**interface** *type number* [**detail**] | [**name** *record-name*] [**type** *record-type*] [**detail**]]
3. **show mdns statistics** {**all** | **interface** *type number* | **service-list***list-name* | [**cache** | **service-policy**] {**all** | **interface** *type number*} | **services orderby providers**}
4. **show mdns service-types** [**all** | **interface***type number*]
5. **debug mdns** {**all** | **error** | **event** | **packet** | **verbose**}

手順の詳細

ステップ 1 **show mdns requests** [**detail** | [**type***record-type*] [**name** *record-name*]]

例：

```
Device# show mdns requests detail

MDNS Outstanding Requests
=====================================================
Request name  :   _ipp._tcp.local
Request type  :   PTR
Request class :   IN
```

このコマンドは、未処理のマルチキャストドメインネームシステム（mDNS）要求のレコード名やレコード タイプ情報などの情報を表示します。

ステップ 2 **show mdns cache** [**interface** *type number* [**detail**] | [**name** *record-name*] [**type** *record-type*] [**detail**]]

例：

（注） 特定のインターフェイス、レコード、またはタイプに対して **detail** キーワードを使用できます。このキーワードは **show mdns cache** コマンドと切り離して使用することはできません。

```
Device# show mdns cache

mDNS CACHE
==========================================================================================
[<NAME>]                                          [<TYPE>][<CLASS>] [<TTL>/Remaining] [Accessed]
 [If-index] [<RR Record Data>]


_services._dns-sd._udp.local                          PTR     IN      4500/4496              0
       3       _ipp._tcp.local

_ipp._tcp.local                                       PTR     IN      4500/4496              1
       3       printer1._ipp._tcp.local
```

```
printer1._ipp._tcp.local                                SRV     IN      120/116         1       3
       0       0       5678    much-WS.local

printer1._ipp._tcp.local                                TXT     IN      4500/4496               1
       3       (1)''

music-WS.local                                      A       IN      120/116         1       3
    192.168.183.1
```

このコマンドは mDNS のキャッシュ情報を表示します。

ステップ 3 **show mdns statistics** {**all** | **interface** *type number* | **service-list***list-name* | [**cache** | **service-policy**] {**all** | **interface** *type number*} | **services orderby providers**}

例：

```
Device# show mdns statistics all

mDNS Statistics
 mDNS packets sent       : 0
 mDNS packets received   : 31
 mDNS packets dropped    : 8
 mDNS cache memory in use: 64264(bytes)
```

このコマンドは、mDNS の統計情報を表示します。

ステップ 4 **show mdns service-types** [**all** | **interface***type number*]

例：

```
Device# show mdns service-types

mDNS SERVICES
================================
[<NAME>]          [<TTL>/Remaining] [If-name]
_ipp._tcp.local     4500/4496
```

このコマンドは、mDNS の統計情報を表示します。

ステップ 5 **debug mdns** {**all** | **error** | **event** | **packet** | **verbose**}

例：

```
Device# debug mdns all
```

このコマンドは、すべての mDNS デバッグ フローを有効にします。

Service Discovery Gateway の設定例

例：サービス検出に対するフィルタ オプションの設定

次に、サービスリスト sl1 を作成する例を示します。permit オプションがシーケンス番号 3 で適用され、メッセージタイプがアナウンスのすべてのサービスがフィルタリングされて、デバイスに関連付けられたさまざまなサブネット間での転送に使用できるようになります。

```
Device> enable
Device# configure terminal
Device(config)# service-list mdns-sd sl1 permit 3
Device(config-mdns-sd-sl)# match message-type announcement
Device(config-mdns-sd-sl)# exit
```

例：サービス検出フィルタの適用とサービス検出パラメータの設定

```
Device> enable
Device# configure terminal
Device(config)# service-routing mdns-sd
Device(config-mdns)# service-policy serv-pol1 IN
Device(config-mdns)# cache-memory-max 20
Device(config-mdns)# service-policy-query sl-query1 100
Device(config-mdns)# designated-gateway enable
Device(config-mdns)# rate-limit in 80
Device(config-mdns)# exit
```

例：インターフェイスに対するサービス検出フィルタの適用

例：複数のサービス検出フィルタ オプションの設定

次に、mixed、permit-most、permit-all、および deny-all というサービス リストを使用してフィルタを作成する例を示します。その後に、フィルタは、必要に応じてさまざまなインターフェイスで適用されます。

```
!
service-list mdns-sd mixed permit 10
 match message-type query
!
service-list mdns-sd mixed permit 20
 match message-type announcement
 match service-type _ipps._tcp.local
!
service-list mdns-sd mixed permit 30
 match message-type announcement
 match service-type _ipp._tcp.local
 match service-type _universal._sub._ipp._tcp
!
service-list mdns-sd mixed permit 40
 match message-type announcement
```

```
!
service-list mdns-sd mixed deny 50
!
service-list mdns-sd permit-most deny 10
 match service-type _sleep-proxy._udp.local
!
service-list mdns-sd permit-most permit 20
!
service-list mdns-sd permit-all permit 10
!
service-list mdns-sd deny-all permit 10
 match message-type query
!
service-list mdns-sd deny-all deny 20
!
service-list mdns-sd active-query query
 service-type _universal._sub._ipp._tcp.local
 service-type _ipp._tcp.local
 service-type _ipps._tcp.local
 service-type _raop._tcp.local
!
service-routing mdns-sd
 service-policy-query active-query 900
!
!
interface Ethernet0/0
 description *** (wireless) Clients here plus some printers or aTVs
 ip address 172.16.33.7 255.255.255.0
 service-routing mdns-sd
  service-policy mixed IN
  service-policy permit-all OUT
!
interface Ethernet0/1
 description *** AppleTVs, Print Servers here
 ip address 172.16.57.1 255.255.255.0
 service-routing mdns-sd
  service-policy permit-most IN
  service-policy permit-all OUT
!
interface Ethernet0/2
 description *** Clients only, we don't want to learn anything here
 ip address 172.16.58.1 255.255.255.0
 service-routing mdns-sd
  service-policy deny-all IN
  service-policy permit-all OUT
!
interface Ethernet0/3
 no ip address
 shutdown
!
```

上記の例では、次のサービス リストが作成されます。

- permit-all：名前が示すように、このサービスリストは、すべてのリソース レコードを許可します。そのため、使用するには注意が必要です。通常、OUT 方向に適用され、クエリーの内容やクエリーのタイプに関係なく、キャッシュはすべての要求に応答できます。
- permit-most：スリープ プロキシ サービス以外の受信が許可されます。これは、スリープ プロキシ サービスを拡張すると、Service Discovery Gateway でスリープ プロキシに登録するデバイスに問題が生じるためです。スプリット ホライズンにより、実際の（スリープ中の）デバイスは、ポインタ（PTR）レコードがスリープ プロキシを指しているときに再度起動してもそのサービスを再登録できません。
- deny-all：キャッシュは何も学習しなくなります。この場合も、クライアントのみがライブであるセグメント上での着信です。その結果、クライアントはキャッシュからのサービスを問

い合わせることができますが（この場合は、permit 10 match クエリー）、それらのクライアントからは何も学習する必要はありません。

- mixed：これはクライアントセグメントで使用するために作成します。クライアント（iPad、PC など）の他に、予備のプリンタや TV も接続されます。ここでは、クライアントが提供するサービスではなく、このような特定のサービスについて学習します。適用されるフィルタは IN です。その結果、次のアクションを適用できます。
  - すべてのクエリーに IN を許可する。
  - 特定のサービスの受信（プリンタ サービス [IPP] など）を許可する。
  - 他のすべてを拒否する。

さらに、キャッシュ内でサービス PTR を最新に保つために、アクティブ クエリーを設定します。アクティブ クエリーで、拡張するサービスを問い合わせます。通常、これは、IN フィルタで「permitted」サービスとして設定したサービスに一致します。値は 900 秒に設定します。PTR は通常 4500 秒の TTL があるため、最新に保つにはこの期間で十分です。

例：サービス インスタンスの作成

```
Device> enable
Device# configure terminal
Device(config)# service-instance mdns-sd service printer-3 regtype _ipp._tcp.local domain
tcp4
Device(config-mdns-sd-si)# ipv4addr 209.165.200.230 255.255.255.0
Device(config-mdns-sd-si)# port 9100
Device(config-mdns-sd-si)# target-hostname fqdn-of-printer.example.com.
Device(config-mdns-sd-si)# txt _ipp._tcp.local=printer3
Device(config-mdns-sd-si)# priority 3
Device(config-mdns-sd-si)# weight 20
Device(config-mdns-sd-si)# exit
```

（注） サービス インスタンスを作成すると、サービス インスタンスのパラメータを設定していない場合でもテキスト レコードが作成されます。

Service Discovery Gateway に関する追加情報

関連資料

関連項目	マニュアル タイトル
『Master Command List』	『Cisco IOS Master Command List』
IP アドレッシング サービス コマンド リファレンス	『Cisco IOS IP Addressing Services Command Reference』

関連項目	マニュアル タイトル
DNS の設定	『IP アドレッシング：DNS コンフィギュレーション ガイド』
DNS の概念情報	『IP Addressing: DNS Configuration Guide』の「Information About DNS」の項

標準および RFC

標準/RFC	Title
RFC 6762	『Multicast DNS』
RFC 6763	『DNS-Based Service Discovery』
マルチキャスト DNS インターネット ドラフト	『Multicast DNS Internet draft』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Service Discovery Gateway の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ 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 にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 3：***Service Discovery Gateway*** **の機能情報**

機能名	リリース	機能情報
Service Discovery Gateway	Cisco IOS XE Release 3.11S	Service Discovery Gateway 機能はマルチキャスト ドメイン ネーム システム（mDNS）を有効にして、境界を越えて（さまざまなサブネットで）動作します。 次のコマンドが導入または変更されました。 **cache-memory-max**、**clear mdns cache**、**clear mdns statistics**、**debug mdns**、**match message-type**、**match service-instance**、**match service-type**、**redistribute mdns-sd**、**service-list mdns-sd**、**service-policy**、**service-policy-query**、**service-routing mdns-sd**、**show mdns cache**、**show mdns requests**、**show mdns statistics**

機能名	リリース	機能情報
Service Discovery Gateway：フェーズ 2	Cisco IOS XE リリース 3.13S	Service Discovery Gateway 機能は、追加のフィルタと設定オプションによって強化されました。 Cisco IOS XE リリース 3.13S では、Cisco ASR 1000 シリーズのルータのサポートが追加されました。 次のコマンドが導入または変更されました。**clear mdns cache**、**clear mdns service-types**、**clear mdns statistics**、**designated-gateway**、**match location**、**rate-limit**、**service-instance mdns-sd**、**service-policy-proximity**、**service-routing mdns-sd**、**service-type-enumeration**、**show mdns cache**、**show mdns statistics**、**source-interface**
Service Discovery Gateway：フェーズ 3	Cisco IOS XE リリース 3.15S	Service Discovery Gateway 機能は、次の機能により強化されました。 • **レート制限メカニズムを使用した着信 mDNS トラフィックの輻輳解除**：レート制限値の範囲を 1 ～ 100 p/s にリセットしました。 • **mDNS キャッシュの効率性向上とメッセージ ループの回避を目的としたサービス取り消しアナウンスのサブネット間への再配布**：**redistribute mdns-sd** コマンドに **withdraw-only** オプションを追加しました。 • **特定のインターフェイスで学習される使用可能なサービスに対するフィルタ基準**：**matchlearnt-interface** コマンドをフィルタ サービスに追加しました。 • **特定のインターフェイスでのサービスの定期的な参照の有効化および無効化**：**service-policy-query (interface)** コマンドを追加しました。既存のグローバルに設定されたアクティブ クエリーについては、インターフェイスでのサービスの参照を無効にし、他のインターフェイスの設定を保持する **disable** オプションを追加しました。 次のコマンドが導入または変更されました。**match learnt-interface**、**rate-limit**、**redistribute mdns-sd**、**service-policy-query (interface)**