Dynamic Multipoint VPN for IPv6 の実装

このマニュアルでは、Dynamic Multipoint VPN for IPv6 機能の実装方法について説明します。この機能を使用すると、ユーザは、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネル、IP Security（IPsec; IP セキュリティ）暗号化、および Next Hop Resolution Protocol（NHRP）を組み合わせることにより、目的に合わせて大小さまざまな規模の IPsec Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を構築できます。Dynamic Multipoint Virtual Private Network（DMVPN）for IPv6 では、パブリック ネットワーク（インターネット）は純粋な IPv4 ネットワークであり、プライベート ネットワーク（イントラネット）は IPv6 に対応しています。

Cisco IOS Release 15.2(1)T では、DMVPN での IPv6 サポートは、Internet Service Provider（ISP; インターネット サービス プロバイダー）方向のパブリック ネットワーク（インターネット）に拡張されました。DMVPN 用の IPv6 トランスポート機能は、IPv6 WAN 側の機能を NHRP トンネルと基礎となる IPsec 暗号化に構築して、IPv6 がインターネットでペイロードを転送できるようにします。

（注） DMVPN 用の IPv6 トランスポート機能はデフォルトでイネーブルにされます。DMVPN 用の IPv6 トランスポート機能を機能させるために、プライベート内部ネットワークを IPv6 にアップグレードする必要はありません。ローカル ネットワークで IPv4 または IPv6 のいずれかのアドレスを使用できます。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「DMVPN for IPv6 の実装の機能情報」（P.25）を参照してください。

プラットフォーム サポートと Cisco 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。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

DMVPN for IPv6 の実装の前提条件

- このマニュアルでは、IPv6 と IPv4 に精通していることを前提としています。IPv6 と IPv4 の設定およびコマンド リファレンス情報については、「その他の関連資料」に記載されている資料を参照してください。
- 「Implementing IPv6 Addressing and Basic Connectivity」の説明に従って、基本的な IPv6 アドレッシングと基本的な接続を実行します。
- IPv6 用の DMVPN が機能するには、Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）、Enhanced Interior Gateway Routing Protocol（EIGRP）、On-Demand Routing（ODR; オンデマンド ルーティング）、Open Shortest Path First（OSPF）、および Routing Information Protocol（RIP; ルーティング情報プロトコル）のいずれかのプロトコルがイネーブルになっている必要があります。
- すべての IPv6 NHRP インターフェイスに、1 つの IPv6 ユニキャスト アドレスを設定します。このアドレスは、グローバルに到達可能なアドレスか、または一意のローカル アドレスにすることができます。
- すべての IPv6 NHRP インターフェイスに、DMVPN クラウド内のすべての DMVPN ホスト（つまり、ハブおよびスポーク）で一意である 1 つの IPv6 リンクローカル アドレスを設定します。
- Multipoint GRE（mGRE; マルチポイント GRE）および IPsec トンネルを確立するためには、**crypto isakmp policy** コマンドを使用して、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）ポリシーを定義しておく必要があります。

DMVPN for IPv6 の実装の制約事項

- IPv6 は、保護されたネットワークだけで設定できます。
- すべての IPv6 NHRP インターフェイスに、1 つの IPv6 ユニキャスト アドレスを設定します。このアドレスは、グローバルに到達可能なアドレスか、または一意のローカル アドレスにすることができます。
- すべての IPv6 NHRP インターフェイスに、DMVPN クラウド内のすべての DMVPN ノード（つまり、ハブおよびスポーク）で一意である 1 つの IPv6 リンクローカル アドレスを設定します。
- IPv6 VRF は、EIGRP や OSPF などの IPv6 ルーティング プロトコルでは完全にサポートされていません。したがって、DMVPN for IPv6 では IPv6 VRF はサポートされません。
- トンネルの QoS DHCP-Tunnels 単位のサポート、および 2547oDMVPN：DMVPN 機能内のトラフィック セグメンテーション機能は、IPv6 ではサポートされません。
- Internet Key Exchange Version 1（IKEv1; インターネット キー エクスチェンジ バージョン 1）および Network Address Translation 66（NAT66; ネットワーク アドレス変換 66）はサポートされていません。

DMVPN for IPv6 の実装に関する情報

DMVPN for IPv6 の概要

DMVPN 機能は、NHRP ルーティング、Multipoint Generic Routing Encapsulation（mGRE; マルチポイント総称ルーティング カプセル化）トンネル、IPsec 暗号化を組み合わせて、ユーザが暗号プロファイル（スタティック クリプト マップ定義するための要件を上書きします）とトンネル エンドポイントのダイナミック ディスカバリを使用して容易に設定できるようにします。

この機能は、シスコが開発した次の拡張標準テクノロジーがベースになっています。

- NHRP：クライアント/サーバ プロトコルの 1 つ。ハブがサーバの役割を果たし、スポークがクライアントとして機能します。ハブには、各スポークのパブリック インターフェイス アドレスが格納された NHRP データベースが保持されます。各スポークでは、起動時にそれぞれの実際のアドレスが登録され、ダイレクト トンネルを確立する場合には、NHRP サーバに対し、宛先スポークの実際のアドレスに関する照会が行われます。
- mGRE トンネル インターフェイス：1 つの GRE インターフェイスで複数の IPsec トンネルをサポートできるため、設定のデータ量が少なくなり、設定操作も簡単になります。
- IPsec 暗号化 : IPsec トンネル インターフェイスは、ネイティブ カプセル化によってサイト間 IPv6 トラフィックの保護を容易にします。

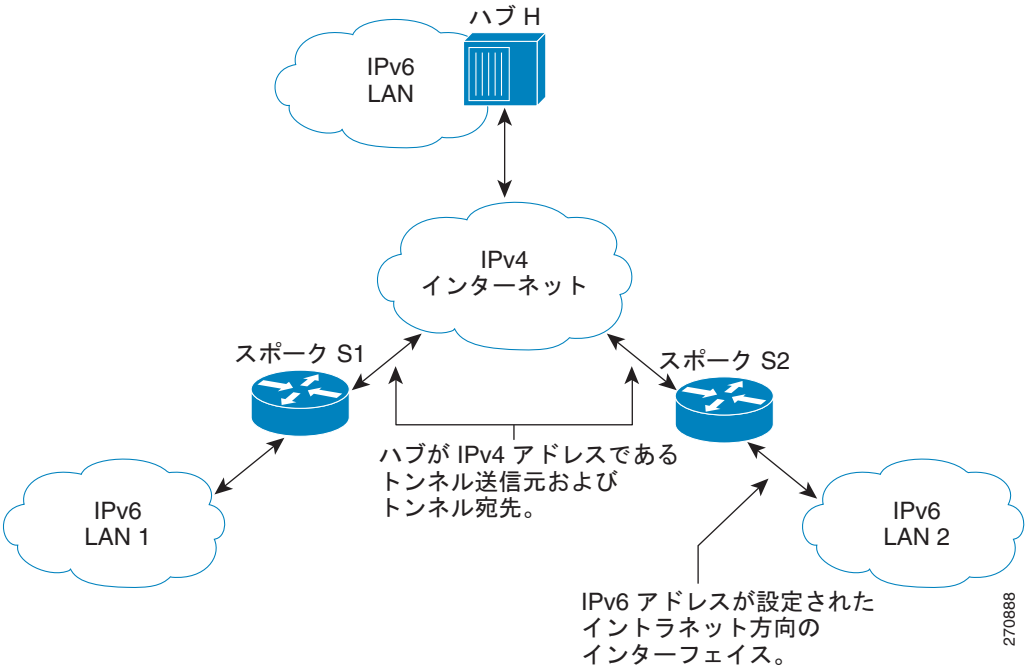
DMVPN for IPv6 では、パブリック ネットワーク（インターネット）は純粋な IPv4 ネットワークであり、プライベート ネットワーク（イントラネット）は IPv6 に対応しています。イントラネットには、DMVPN テクノロジーを使用して相互に接続された IPv4 クラウドまたは IPv6 クラウドを混在させて、基礎となるキャリアを従来の IPv4 ネットワークにすることができます。

NHRP ルーティング

NHRP プロトコルは、特定のイントラネット アドレス（IPv4 または IPv6）をインターネット アドレス（IPv4 NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス）アドレス）に解決します。

図 1 で、DMVPN ネットワークを介して接続されているイントラネットは IPv6 クラウド、インターネットは純粋な IPv4 クラウドです。スポーク S1 および S2 は、スタティックに設定されたトンネルを使用してインターネット経由でハブ H に接続されています。トンネルはイントラネット上の別のノードであるため、トンネル自体のアドレスは IPv6 ドメインです。ただし、トンネル（mGRE エンドポイント）の送信元アドレスと宛先アドレスは、常にインターネット ドメイン内の IPv4 にあります。mGRE トンネルは、IPv6 ネットワークを認識します。これは、GRE パッセンジャ プロトコルが IPv6 パケットであり、GRE トランスポート（またはキャリア）プロトコルが IPv4 パケットであるからです。

図 1　NHRP をトリガーする IPv6 トポロジ



LAN L1 内の IPv6 ホストが LAN L2 内の IPv6 ホスト宛てのパケットを送信すると、パケットはまず LAN L1 内のゲートウェイ（スポーク S1）にルーティングされます。スポーク S1 は、デュアル スタック ルータです。これは、IPv4 と IPv6 の両方がこのスポーク上で設定されていることを意味します。S1 の IPv6 ルーティング テーブルは、スポーク S2 上のトンネルの IPv6 アドレスであるネクスト ホップを指します。これは、NBMA アドレスにマッピングする必要がある VPN アドレスであり、NHRP をトリガーします。

IPv6 NHRP リダイレクトおよびショートカット機能

IPv6 NHRP リダイレクトがイネーブルになっている場合、NHRP は出力機能パス内のすべてのデータ パケットを調べます。データ パケットが同じ論理ネットワーク上で出入りする場合、NHRP は、NHRP トラフィック指示メッセージをデータ パケットの送信元に送信します。NHRP では、論理ネットワークは、複数の物理インターフェイスを 1 つの論理ネットワークにグループ化する NHRP ネットワーク ID によって識別されます。

IPv6 NHRP ショートカットがイネーブルになっている場合、NHRP は出力機能パス内のすべてのデータ パケットを代行受信します。データ パケットの宛先への NHRP キャッシュ エントリがあるかどうかをチェックし、ある場合は、現在の出力隣接を NHRP キャッシュ内の隣接に置き換えます。そのため、データ パケットは、NHRP によって提供された新しい隣接を使用してスイッチングされます。

IPv6 ルーティング

NHRP は、IPv6 パッセンジャ プロトコルを伝送する mGRE トンネルでは自動的に呼び出されます。パケットをルーティングしてスイッチング パスに送信すると、NHRP は特定のネクスト ホップを検索して、必要に応じて NHRP 解決クエリーを開始します。解決に成功した場合、NHRP はトンネル エンドポイント データベースにデータを入力します。これにより、シスコ エクスプレス フォワーディングの隣接関係テーブルにデータが入力されます。シスコ エクスプレス フォワーディングがイネーブルになっている場合、後続のパケットについては、シスコ エクスプレス フォワーディング スイッチングが行われます。

IPv6 アドレッシングと制約事項

IPv6 では、特定の IPv6 インターフェイス上で複数のユニキャスト アドレスを使用できます。また、エニーキャスト、マルチキャスト、リンクローカル アドレス、ユニキャスト アドレスなどの特殊なアドレス タイプも使用できます。

DMVPN for IPv6 には、アドレッシングについて次の制約事項があります。

- すべての IPv6 NHRP インターフェイスに、1 つの IPv6 ユニキャスト アドレスを設定します。このアドレスは、グローバルに到達可能なアドレスか、または一意のローカル アドレスにすることができます。
- すべての IPv6 NHRP インターフェイスに、DMVPN クラウド内のすべての DMVPN ホスト（つまり、ハブおよびスポーク）で一意である 1 つの IPv6 リンクローカル アドレスを設定します。
  - ルータ上に同じトンネル送信元を使用する他のトンネルがない場合は、トンネル送信元アドレスを IPv6 アドレスに組み込むことができます。
  - ルータに DMVPN IPv6 トンネルが 1 つだけある場合は、IPv6 リンクローカル アドレスを手動で設定する必要はありません。代わりに、**ipv6 enable** コマンドを使用してリンクローカル アドレスを自動生成します。
  - ルータに複数の DMVPN IPv6 トンネルがある場合は、**ipv6 address fe80::2001 link-local** コマンドを使用してリンクローカル アドレスを手動で設定する必要があります。

IPv6 を介した mGRE サポート

DMVPN の複数のサイトが IPv6 によって相互接続されています。単一の論理 mGRE トンネル インターフェイスが、ある VPN サイトを別の VPN サイトに相互接続します。IPv6 サブネットは、トンネル インターフェイスをさまざまな VPN サイトの他のトンネル インターフェイスに接続します。VPN サイトを接続しているすべてのトンネル インターフェイスが、論理 IPv6 サブネットでホストとして機能します。この構造は、トンネル オーバーレイ ネットワークと呼ばれます。

DMVPN for IPv6 の設定方法

ハブ ルータおよびスポーク ルータに対して mGRE/IPsec トンネルリングをイネーブルにするには、グローバル IPsec ポリシー テンプレートを使用して IPsec プロファイルを設定すること、および IPsec 暗号化に使用する mGRE トンネルを設定することが必要です。ここでは、次の各手順について説明します。

- 「DMVPN for IPv6 の IPsec プロファイルの設定」（P.6）（必須）
- 「DMVPN を介した IPv6 用のハブの設定」（P.8）（必須）
- 「ハブでの NHRP リダイレクトおよびショートカット機能の設定」（P.10）（必須）
- 「DMVPN を介した IPv6 用のスポークの設定」（P.11）（必須）
- 「DMVPN for IPv6 設定の確認」（P.14）（任意）
- 「DMVPN for IPv6 の設定と動作の監視および維持」（P.19）（任意）

DMVPN for IPv6 の IPsec プロファイルの設定

IPsec プロファイルには、クリプト マップの設定に使用するほとんどのコマンドが使用されます。ただし、それらすべてのコマンドが、各 IPsec プロファイルで有効であるわけではありません。IPsec プロファイルの下で発行できるのは、IPsec ポリシーに使用されているコマンドだけです。したがって、IPsec ピア アドレスや、パケットを暗号化するかどうかを照合するための Access Control List（ACL; アクセス コントロール リスト）は指定できません。

IPv6 用の DMVPN で IPsec プロパティを設定するには、次の作業を実行します。

前提条件

IPsec プロファイルを設定する前に、次の作業を実行する必要があります。

- **crypto ipsec transform-set** コマンドを使用して、トランスフォーム セットを定義する。
- Internet Security Association Key Management Protocol（ISAKMP）プロファイルがデフォルトの ISAKMP 設定を使用して設定されていることを確認します。デフォルトの ISAKMP 設定の詳細については、「*Implementing IPsec in IPv6 Security*」の章および『*Cisco IOS IPv6 Command Reference*』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto identity** *name*
4. **exit**
5. **crypto ipsec profile** *name*
6. **set transform-set** *transform-set-name*
7. **set identity**
8. **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}
9. **set pfs** [**group1** | **group2**]
10. **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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じて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	**crypto identity** *name* **例：** `Router(config)# crypto identity router1`	ルータの証明書内にある Distinguished Name（DN; 識別名）リストを使用してルータのアイデンティティを設定します。
ステップ 4	**exit** **例：** `Router(config-crypto-identity)# exit`	クリプト ID 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 モードを開始します。
ステップ 5	**crypto ipsec profile** *name* **例：** `Router(config)# crypto ipsec profile example1`	「スポークとハブの間」および「スポークとスポークの間」での IPsec 暗号化に使用する IPsec パラメータを定義します。 このコマンドによって、ルータはクリプト マップ コンフィギュレーション モードになります。
ステップ 6	**set transform-set** *transform-set-name* **例：** `Router(config-crypto-map)# set transform-set example-set`	IPsec プロファイルで使用できるトランスフォーム セットを指定します。
ステップ 7	**set identity** **例：** `Router(config-crypto-map)# set identity router1`	（オプション）IPsec プロファイルに対するアイデンティティの制限事項を指定します。
ステップ 8	**set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*} **例：** `Router(config-crypto-map)# set security-association lifetime seconds 1800`	（オプション）IPsec プロファイルに使用するグローバル ライフタイムの値を上書きします。
ステップ 9	**set pfs** [**group1** | **group2**] **例：** `Router(config-crypto-map)# set pfs group2`	（オプション）IPsec において、この IPsec プロファイルに対する新しいセキュリティ アソシエーションが要求される際に、Perfect Forward Secrecy（PFS; 完全転送秘密）が必須となるよう指定します。
ステップ 10	**end** **例：** `Router(config-crypto-map)# end`	クリプト マップ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DMVPN を介した IPv6 用のハブの設定

mGRE と IPsec の統合（つまり、前の手順で設定した IPsec プロファイルとトンネルを関連付ける）のために DMVPN を介した IPv6 用のハブ ルータを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
5. **ipv6 address** *ipv6-address*/*prefix-length* **link-local**
6. **ipv6 mtu** *bytes*
7. **ipv6 nhrp authentication** *string*
8. **ipv6 nhrp map multicast dynamic**
9. **ipv6 nhrp network-id** *network-id*
10. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
11. **tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre ip** | **gre** [**ipv6**] | **gre multipoint** [**ipv6**] | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
12. **tunnel protection ipsec profile** *name* [**shared**]
13. **bandwidth** {*kbps* | **inherit** [*kbps*] | **receive** [*kbps*]}
14. **ipv6 nhrp holdtime** *seconds*
15. **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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じて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	**interface tunnel** *number* **例：** `Router(config)# interface tunnel 5`	トンネル インターフェイスを設定し、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。 • number 引数には、作成または設定するトンネル インターフェイスの数を指定します。作成可能なトンネル インターフェイスの数に制限はありません。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} **例：** `Router(config-if)# ipv6 address 2001:DB8:1:1::72/64`	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 5	**ipv6 address** *ipv6-address*/*prefix-length* **link-local** **例：** `Router(config-if)# ipv6 address fe80::2001 link-local`	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。 • （DMVPN ネットワーク内のすべての DMVPN ノードで）一意の IPv6 リンクローカル アドレスを設定する必要があります。
ステップ 6	**ipv6 mtu** *bytes* **例：** `Router(config-if)# ipv6 mtu 1400`	各インターフェイスにおいて送信される IPv6 パケットの Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズを設定します。
ステップ 7	**ipv6 nhrp authentication** *string* **例：** `Router(config-if)# ipv6 nhrp authentication examplexx`	NHRP を使用するインターフェイス用の認証文字列を設定します。 **（注）** 同一の DMVPN ネットワーク内に存在するハブおよびスポークに対しては、すべて同じ NHRP 認証文字列を設定する必要があります。
ステップ 8	**ipv6 nhrp map multicast dynamic** **例：** `Router(config-if)# ipv6 nhrp map multicast dynamic`	NHRP において、ルータが自動的にマルチキャスト NHRP マッピングへ追加されるようにします。
ステップ 9	**ipv6 nhrp network-id** *network-id* **例：** `Router(config-if)# ipv6 nhrp network-id 99`	インターフェイスに対して NHRP をイネーブルにします。
ステップ 10	**tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} **例：** `Router(config-if)# tunnel source ethernet 0`	トンネル インターフェイスの送信元アドレスを設定します。
ステップ 11	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** [**ipv6**] | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**} **例：** `Router(config-if)# tunnel mode gre multipoint`	トンネル インターフェイスのカプセル化モードを mGRE に設定します。

	コマンドまたはアクション	目的
ステップ 12	**tunnel protection ipsec profile** *name* [**shared**] **例：** `Router(config-if)# tunnel protection ipsec profile example_profile`	トンネル インターフェイスを IPsec プロファイルに関連付けます。 • name 引数には、IPsec プロファイルの名前を指定します。この名前は、**crypto ipsec profile name** コマンドで指定した名前と同じであることが必要です。
ステップ 13	**bandwidth** {*kbps* | **inherit** [*kbps*] | **receive** [*kbps*]} **例：** `Router(config-if)# bandwidth 1200`	上位レベル プロトコルのインターフェイスに対する現在の帯域幅を設定します。 • *bandwidth-size* 引数は、帯域幅をキロビット/秒単位で指定します。デフォルト値は 9 です。帯域幅の推奨値は 1000 以上です。
ステップ 14	**ipv6 nhrp holdtime** *seconds* **例：** `Router(config-if)# ipv6 nhrp holdtime 3600`	信頼できる NHRP 応答により NHRP NBMA アドレスが有効としてアドバタイズされる秒数を変更します。
ステップ 15	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ハブでの NHRP リダイレクトおよびショートカット機能の設定

ハブで NHRP リダイレクトおよびショートカット機能を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
5. **ipv6 nhrp redirect** [**timeout** *seconds*]
6. **ipv6 nhrp shortcut**
7. **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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じて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	**interface tunnel number** **例：** `Router(config)# interface tunnel 5`	トンネル インターフェイスを設定し、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。 • number 引数には、作成または設定するトンネル インターフェイスの数を指定します。作成可能なトンネル インターフェイスの数に制限はありません。
ステップ 4	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} **例：** `Router(config-if)# ipv6 address 2001:DB8:1:1::72/64`	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 5	**ipv6 nhrp redirect** [**timeout** *seconds*] **例：** `Router(config-if)# ipv6 nhrp redirect`	NHRP リダイレクトをイネーブルにします。 **（注）** ハブで **ipv6 nhrp redirect** コマンドを設定する必要があります。
ステップ 6	**ipv6 nhrp shortcut** **例：** `Router(config-if)# ipv6 nhrp shortcut`	NHRP ショートカット スイッチングをイネーブルにします。 **（注）** スポークで **ipv6 nhrp shortcut** コマンドを設定する必要があります。
ステップ 7	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DMVPN を介した IPv6 用のスポークの設定

DMVPN を介した IPv6 用のスポークを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
5. **ipv6 address** *ipv6-address*/*prefix-length* **link-local**
6. **ipv6 mtu** *bytes*
7. **ipv6 nhrp authentication** *string*
8. **ipv6 nhrp map** *ipv6-address nbma-address*
9. **ipv6 nhrp map multicast** {*ipv4-nbma-address* | *ipv6-nbma-address*}
10. **ipv6 nhrp nhs** *ipv6-nhs-address*
11. **ipv6 nhrp network-id** *network-id*
12. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}

13. **tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** [**ipv6**] | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}

    または

    tunnel destination {*host-name* | *ip-address* | *ipv6-address*}

14. **tunnel protection ipsec profile** *name* [**shared**]
15. **bandwidth** {*kbps* | **inherit** [*kbps*] | **receive** [*kbps*]}
16. **ipv6 nhrp holdtime** *seconds*
17. **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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じて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	**interface tunnel** *number* **例：** `Router(config)# interface tunnel 5`	トンネル インターフェイスを設定し、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。 • *number* 引数には、作成または設定するトンネル インターフェイスの数を指定します。作成可能なトンネル インターフェイスの数に制限はありません。
ステップ 4	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} **例：** `Router(config-if) ipv6 address 2001:DB8:1:1::72/64`	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 5	**ipv6 address** *ipv6-address*/*prefix-length* **link-local** **例：** `Router(config-if)# ipv6 address fe80::2001 link-local`	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。 • （DMVPN ネットワーク内のすべての DMVPN ノードで）一意の IPv6 リンクローカル アドレスを設定する必要があります。
ステップ 6	**ipv6 mtu** *bytes* **例：** `Router(config-if)# ipv6 mtu 1400`	インターフェイス上で送信する IPv6 パケットの MTU サイズを設定します。
ステップ 7	**ipv6 nhrp authentication** *string* **例：** `Router(config-if)# ipv6 nhrp authentication examplexx`	NHRP を使用するインターフェイス用の認証文字列を設定します。 **（注）** 同一の DMVPN ネットワーク内に存在するハブおよびスポークに対しては、すべて同じ NHRP 認証文字列を設定する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**ipv6 nhrp map** *ipv6-address nbma-address* **例：** `Router(config-if)# ipv6 nhrp map 2001:DB8:3333:4::5 10.1.1.1`	NBMA ネットワークに接続された IPv6 宛先の IPv6 アドレスと NBMA アドレスのマッピングをスタティックに設定します。 **（注）** IPv4 NBMA アドレスだけがサポートされ、ATM またはイーサネット アドレスはサポートされません。
ステップ 9	**ipv6 nhrp map multicast** *ipv4-nbma-address* **例：** `Router(config-if)# ipv6 nhrp map multicast 10.11.11.99`	宛先 IPv6 アドレスを IPv4 NBMA アドレスにマッピングします。
ステップ 10	**ipv6 nhrp nhs** *ipv6-nhs-address* **例：** `Router(config-if)# ipv6 nhrp nhs 2001:0DB8:3333:4::5 2001:0DB8::/64`	1 つ以上の IPv6 NHRP サーバのアドレスを指定します。
ステップ 11	**ipv6 nhrp network-id** *network-id* **例：** `Router(config-if)# ipv6 nhrp network-id 99`	インターフェイスに対して NHRP をイネーブルにします。
ステップ 12	**tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} **例：** `Router(config-if)# tunnel source ethernet 0`	トンネル インターフェイスの送信元アドレスを設定します。

ステップ 13	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** [**ipv6**] | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
	
	または
	
	tunnel destination {*host-name* | *ip-address* | *ipv6-address*}
	
	例：
	`Router(config-if)# tunnel mode gre multipoint`
	
	または
	
	`Router(config-if)# tunnel destination 10.1.1.1`
		トンネル インターフェイスのカプセル化モードを mGRE に設定します。
		• **tunnel mode** コマンドを使用するのは、データ トラフィックにダイナミック スポークツースポーク トラフィックを使用できる場合です。
		または
		トンネル インターフェイスの宛先を指定します。
		• **tunnel destination** コマンドを使用するのは、データ トラフィックにハブアンドスポーク トンネルを使用できる場合です。

ステップ 14	**tunnel protection ipsec profile** *name* [**shared**] **例：** `Router(config-if)# tunnel protection ipsec profile example1`	トンネル インターフェイスを IPsec プロファイルに関連付けます。 • *name* 引数には、IPsec プロファイルの名前を指定します。この名前は、**crypto ipsec profile name** コマンドで指定した名前と同じであることが必要です。

	コマンドまたはアクション	目的
ステップ 15	**bandwidth** {**interzone** | **total** | **session**} {**default** | **zone** *zone-name*} *bandwidth-size* **例：** `Router(config-if)# bandwidth total 1200`	上位レベル プロトコルのインターフェイスに対する現在の帯域幅を設定します。 • *bandwidth-size* 引数は、帯域幅をキロビット/秒単位で指定します。デフォルト値は 9 です。帯域幅の推奨値は 1000 以上です。 • スポークの帯域幅設定は、DMVPN ハブの帯域幅設定と同じである必要はありません。通常は、すべてのスポークに対して、同一または類似の帯域幅を使用する方が便利です。
ステップ 16	**ipv6 nhrp holdtime** *seconds* **例：** `Router(config-if)# ipv6 nhrp holdtime 3600`	信頼できる NHRP 応答により NHRP NBMA アドレスが有効としてアドバタイズされる秒数を変更します。
ステップ 17	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DMVPN for IPv6 設定の確認

DMVPN for IPv6 設定を確認するための情報を表示するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **show dmvpn** [**ipv4** [**vrf** *vrf-name*] | **ipv6** [**vrf** *vrf-name*]] [**debug-condition** | [**interface tunnel** *number* | **peer** {**nbma** *ip-address* | **network** *network-mask* | **tunnel** *ip-address*}] [**static**] [**detail**]]
3. **show ipv6 nhrp** [**dynamic** [*ipv6-address*] | **incomplete** | **static**] [*address* | *interface*] [**brief** | **detail**] [**purge**]
4. **show ipv6 nhrp multicast** [*ipv4-address* | *interface* | *ipv6-address*]
5. **show ip nhrp multicast** [*nbma-address* | *interface*]
6. **show ipv6 nhrp summary**
7. **show ipv6 nhrp traffic** [*interface* **tunnel** *number*]
8. **show ip nhrp shortcut**
9. **show ip route**
10. **show ipv6 route**
11. **show nhrp debug-condition**

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**show dmvpn** [**ipv4** [**vrf** *vrf-name*] | **ipv6** [**vrf** *vrf-name*]] [**debug-condition** | [**interface tunnel** *number* | **peer** {**nbma** *ip-address* | **network** *network-mask* | **tunnel** *ip-address*}] [**static**] [**detail**]] **例：** `Router# show dmvpn 2001:0db8:1:1::72/64`	DMVPN 固有のセッション情報を表示します。
ステップ 3	**show ipv6 nhrp** [**dynamic** [*ipv6-address*] | **incomplete** | **static**] [*address* | *interface*] [**brief** | **detail**] [**purge**] **例：** `Router# show ipv6 nhrp`	NHRP マッピング情報を表示します。
ステップ 4	**show ipv6 nhrp multicast** [*ipv4-address* | *interface* | *ipv6-address*] **例：** `Router# show ipv6 nhrp multicast`	NHRP マルチキャスト マッピング情報を表示します。
ステップ 5	**show ip nhrp multicast** [*nbma-address* | *interface*] **例：** `Router# show ip nhrp multicast`	NHRP マルチキャスト マッピング情報を表示します。
ステップ 6	**show ipv6 nhrp summary** **例：** `Router# show ipv6 nhrp summary`	NHRP マッピング サマリー情報を表示します。
ステップ 7	**show ipv6 nhrp traffic** [*interface* **tunnel** *number*] **例：** `Router# show ipv6 nhrp traffic`	NHRP トラフィック統計情報を表示します。
ステップ 8	**show ip nhrp shortcut** **例：** `Router# show ip nhrp shortcut`	NHRP ショートカット情報を表示します。
ステップ 9	**show ip route** **例：** `Router# show ip route`	IPv4 ルーティング テーブルの現在の状態を表示します。

	コマンドまたはアクション	目的
ステップ 10	**show ipv6 route** **例：** `Router# show ipv6 route`	IPv6 ルーティング テーブルの現在の内容を表示します。
ステップ 11	**show nhrp debug-condition** **例：** `Router# show nhrp debug-condition`	NHRP 条件付きデバッグ情報を表示します。

例

show dmvpn コマンドの出力例

次に、ハブで **ipv6** および **detail** キーワードを指定した **show dmvpn** コマンドの出力例を示します。

```
Router# show dmvpn ipv6 detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel1 is up/up, Addr. is 10.0.0.3, VRF ""
   Tunnel Src./Dest. addr: 192.169.2.9/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "test_profile"
Type:Hub, Total NBMA Peers (v4/v6): 2
    1.Peer NBMA Address: 192.169.2.10
        Tunnel IPv6 Address: 2001::4
        IPv6 Target Network: 2001::4/128
        # Ent: 2, Status: UP, UpDn Time: 00:01:51, Cache Attrib: D
Type:Hub, Total NBMA Peers (v4/v6): 2
    2.Peer NBMA Address: 192.169.2.10
        Tunnel IPv6 Address: 2001::4
        IPv6 Target Network: FE80::2/128
        # Ent: 0, Status: UP, UpDn Time: 00:01:51, Cache Attrib: D
Type:Hub, Total NBMA Peers (v4/v6): 2
    3.Peer NBMA Address: 192.169.2.11
        Tunnel IPv6 Address: 2001::5
        IPv6 Target Network: 2001::5/128
        # Ent: 2, Status: UP, UpDn Time: 00:26:38, Cache Attrib: D
Type:Hub, Total NBMA Peers (v4/v6): 2
    4.Peer NBMA Address: 192.169.2.11
        Tunnel IPv6 Address: 2001::5
        IPv6 Target Network: FE80::3/128
        # Ent: 0, Status: UP, UpDn Time: 00:26:38, Cache Attrib: D
Pending DMVPN Sessions:

Interface: Tunnel1
  IKE SA: local 192.169.2.9/500 remote 192.169.2.10/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 192.169.2.10
  IPSEC FLOW: permit 47 host 192.169.2.9 host 192.169.2.10
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x BB0ED02, transform : esp-3des esp-sha-hmac
    Socket State: Open
```

```
Interface: Tunnel1
  IKE SA: local 192.169.2.9/500 remote 192.169.2.11/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 192.169.2.11
  IPSEC FLOW: permit 47 host 192.169.2.9 host 192.169.2.11
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0xB79B277B, transform : esp-3des esp-sha-hmac
    Socket State: Open
```

次に、スポークで **ipv6** および **detail** キーワードを指定した **show dmvpn** コマンドの出力例を示します。

```
Router# show dmvpn ipv6 detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel1 is up/up, Addr. is 10.0.0.1, VRF ""
   Tunnel Src./Dest. addr: 192.169.2.10/MGRE, Tunnel VRF ""
   Protocol/Transport: "multi-GRE/IP", Protect "test_profile"

IPv6 NHS: 2001::6 RE
Type:Spoke, Total NBMA Peers (v4/v6): 1
    1.Peer NBMA Address: 192.169.2.9
        Tunnel IPv6 Address: 2001::6
        IPv6 Target Network: 2001::/112
        # Ent: 2, Status: NHRP, UpDn Time: never, Cache Attrib: S

IPv6 NHS: 2001::6 RE
Type:Unknown, Total NBMA Peers (v4/v6): 1
    2.Peer NBMA Address: 192.169.2.9
        Tunnel IPv6 Address: FE80::1
        IPv6 Target Network: FE80::1/128
        # Ent: 0, Status: UP, UpDn Time: 00:00:24, Cache Attrib: D

Pending DMVPN Sessions:

Interface: Tunnel1
  IKE SA: local 192.169.2.10/500 remote 192.169.2.9/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 192.169.2.9
  IPSEC FLOW: permit 47 host 192.169.2.10 host 192.169.2.9
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x6F75C431, transform : esp-3des esp-sha-hmac
    Socket State: Open
```

show ipv6 nhrp コマンドの出力例

次に、ハブとスポークでの **show ipv6 nhrp** コマンドの出力例を示します。

ハブ

```
Router# show ipv6 nhrp

2001::4/128 via 2001::4
   Tunnel1 created 00:02:40, expire 00:00:47
   Type: dynamic, Flags: unique registered used
   NBMA address: 192.169.2.10
2001::5/128 via 2001::5
   Tunnel1 created 00:02:37, expire 00:00:47
```

```
   Type: dynamic, Flags: unique registered used
   NBMA address: 192.169.2.11
FE80::2/128 via 2001::4
   Tunnel1 created 00:02:40, expire 00:00:47
   Type: dynamic, Flags: unique registered used
   NBMA address: 192.169.2.10
FE80::3/128 via 2001::5
   Tunnel1 created 00:02:37, expire 00:00:47
   Type: dynamic, Flags: unique registered used
   NBMA address: 192.169.2.11
```

スポーク

```
Router# show ipv6 nhrp

2001::8/128
   Tunnel1 created 00:00:13, expire 00:02:51
   Type: incomplete, Flags: negative
   Cache hits: 2
2001::/112 via 2001::6
   Tunnel1 created 00:01:16, never expire
   Type: static, Flags: used
   NBMA address: 192.169.2.9
FE80::1/128 via FE80::1
   Tunnel1 created 00:01:15, expire 00:00:43
   Type: dynamic, Flags:
   NBMA address: 192.169.2.9
```

show ipv6 nhrp multicast コマンドの出力例

次に、ハブとスポークでの **show ipv6 nhrp multicast** コマンドの出力例を示します。

ハブ

```
Router# show ipv6 nhrp multicast

  I/F     NBMA address
Tunnel1    192.169.2.10    Flags: dynamic
Tunnel1    192.169.2.11    Flags: dynamic
```

スポーク

```
Router# show ipv6 nhrp multicast

  I/F     NBMA address
Tunnel1    192.169.2.9     Flags: static
```

show ipv6 nhrp traffic コマンドの出力例

次に、**show ipv6 nhrp traffic** コマンドの出力例を示します。

```
Router# show ipv6 nhrp traffic
Tunnel0: Max-send limit:100Pkts/10Sec, Usage:0%
Sent: Total 8
1 Resolution Request 1 Resolution Reply 6 Registration Request
0 Registration Reply 0 Purge Request 0 Purge Reply
0 Error Indication 0 Traffic Indication
Rcvd: Total 5
1 Resolution Request 1 Resolution Reply 0 Registration Request
2 Registration Reply 0 Purge Request 0 Purge Reply
0 Error Indication 1 Traffic Indication
```

DMVPN for IPv6 の設定と動作の監視および維持

DMVPN for IPv6 の設定と動作を監視および維持するための情報を表示するには、必要に応じて次の任意の作業を実行します。

手順の概要

1. **enable**
2. **clear dmvpn session** [**interface tunnel** *number* | **peer** {*ipv4-address* | *fqdn-string* | *ipv6-address*} | **vrf** *vrf-name*] [**static**]
3. **clear ipv6 nhrp** [*ipv6-address* | **counters**]
4. **debug dmvpn** {**all** | **error** | **detail** | **packet**} {**all** | *debug-type*}
5. **debug nhrp** [**cache** | **extension** | **packet** | **rate**]
6. **debug nhrp condition** [**interface tunnel** *number* | **peer** {**nbma** {*ipv4-address* | *fqdn-string* | *ipv6-address*} | **tunnel** {*ip-address* | *ipv6-address*}} | **vrf** *vrf-name*]
7. **debug nhrp error**

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。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear dmvpn session** [**interface tunnel** *number*	**peer** {*ipv4-address*	*fqdn-string*	*ipv6-address*}	**vrf** *vrf-name*] [**static**] **例：** `Router# clear dmvpn session`	DMVPN セッションをクリアします。
ステップ 3	**clear ipv6 nhrp** [*ipv6-address*	**counters**] **例：** `Router# clear ipv6 nhrp`	NHRP キャッシュからすべてのダイナミック エントリを削除します。
ステップ 4	**debug dmvpn** {**all**	**error**	**detail**	**packet**} {**all**	*debug-type*} **例：** `Router# debug dmvpn`	デバッグの DMVPN セッション情報を表示します。
ステップ 5	**debug nhrp** [**cache**	**extension**	**packet**	**rate**] **例：** `Router# debug nhrp ipv6`	NHRP デバッグをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**debug nhrp condition** [**interface tunnel** *number* | **peer** {**nbma** {*ipv4-address* | *fqdn-string* | *ipv6-address*} | **tunnel** {*ip-address* | *ipv6-address*}} | **vrf** *vrf-name*] **例：** `Router# debug nhrp condition`	NHRP 条件付きデバッグをイネーブルにします。
ステップ 7	**debug nhrp error** **例：** `Router# debug nhrp ipv6 error`	NHRP エラー レベル デバッグ情報を表示します。

例

debug nhrp コマンドの出力例

次に、**ipv6** キーワードを指定して **debug nhrp** コマンドを発行した場合の出力例を示します。

```
Router# debug nhrp ipv6

Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST
           - 2001:DB8:3c4d:0015:0000:0000:1a2f:3d2c/32
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded.
Aug  9 13:13:41.486: NHRP: Tunnel NBMA addr 11.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486: src: 2001:DB8:3c4d:0015:0000:0000:1a2f:3d2c/32,
             dst: 2001:DB8:3c4d:0015:0000:0000:1a2f:3d2c/32
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 125
```

DMVPN for IPv6 の実装の設定例

例：IPsec プロファイルの設定

```
Router(config)# crypto identity router1
Router(config)# crypto ipsec profile example1
Router(config-crypto-map)# set transform-set example-set
Router(config-crypto-map)# set identity router1
Router(config-crypto-map)# set security-association lifetime seconds 1800
Router(config-crypto-map)# set pfs group2
```

例：DMVPN 用のハブの設定

```
Router# configure terminal
Router(config)# interface tunnel 5
Router(config-if)# ipv6 address 2001:DB8:1:1::72/64
Router(config-if)# ipv6 address fe80::2001 link-local
Router(config-if)# ipv6 mtu 1400
Router(config-if)# ipv6 nhrp authentication examplexx
Router(config-if)# ipv6 nhrp map multicast dynamic
Router(config-if)# ipv6 nhrp network-id 99
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel mode gre multipoint
Router(config-if)# tunnel protection ipsec profile example_profile
Router(config-if)# bandwidth 1200
Router(config-if)# ipv6 nhrp holdtime 3600
```

例：ハブでの NHRP リダイレクトおよびショートカット機能の設定

```
Router(config)# interface tunnel 5
Router(config-if)# ipv6 address 2001:DB8:1:1::72/64
Router(config-if)# ipv6 nhrp redirect
Router(config-if)# ipv6 nhrp shortcut
```

例：DMVPN 用のスポークの設定

```
Router# show running-config

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spoke-11
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
clock timezone IST 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
ip cef
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
archive
 log config
  hidekeys
```

```
!
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco123 address 10.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set cisco-ts esp-3des esp-md5-hmac
 mode transport
!
crypto ipsec profile cisco-ipsec
 set transform-set cisco-ts
!
interface Tunnel0
 bandwidth 100000
 no ip address
 no ip redirects
 delay 50000
 ipv6 address 2001:DB8::11/64
 ipv6 address FE80::0B:0B:0B:0B link-local
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
 no ipv6 next-hop-self eigrp 1
 ipv6 nhrp map 2001:DB8::99/128 10.11.11.99
 ipv6 nhrp map multicast 10.11.11.99
 ipv6 nhrp network-id 99
 ipv6 nhrp nhs 2001:DB8::99
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile cisco-ipsec
!
interface Ethernet0/0
 ip address 10.11.11.11 255.255.255.0
 ipv6 enable
 ipv6 nd ra mtu suppress
!
interface Ethernet0/1
 no ip address
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 ip address 172.16.11.11 255.255.255.0
 ipv6 address 2001:DB8:dddd::1/64
 ipv6 enable
 ipv6 nd ra mtu suppress
 ipv6 eigrp 1
!
interface Ethernet1/1
 no ip address
 shutdown
 ipv6 enable
 ipv6 nd ra mtu suppress
!
interface Ethernet1/2
 no ip address
 shutdown
!
```

```
interface Ethernet1/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
ip http server
no ip http secure-server
!
ipv6 router eigrp 1
 no shutdown
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
exception data-corruption buffer truncate
```

その他の関連資料

関連資料

関連項目	参照先
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」の章
IPv6 IPsec	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPsec in IPv6 Security」の章
IPv6 基本接続	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」の章
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』
IPv4 用の DMVPN 実装	『*Cisco IOS Security Configuration Guide*』の「Dynamic Multipoint VPN (DMVPN)」の章
IPv4 用の DMVPN コマンド	『*Cisco IOS Security Command Reference*』
IPv4 用の NHRP	『*Cisco IOS IP Addressing Services Configuration Guide*』の「Configuring NHRP」の章
IPv4 用の NHRP コマンド	『*Cisco IOS IP Addressing Services Command Reference*』の「NHRP Commands」の項

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
Cisco NHRP Extension MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、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 2332	『*NBMA Next Hop Resolution Protocol (NHRP)*』
RFC 2677	『*Managed Objects for the NBMA Next Hop Resolution Protocol (NHRP)*』

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。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

DMVPN for IPv6 の実装の機能情報

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。

プラットフォームのサポートおよびソフトウェア 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 を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 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。

表 1　DMVPN for IPv6 の実装の機能情報

機能名	リリース	機能情報
DMVPN for IPv6	12.4(20)T	Dynamic Multipoint VPN 機能を使用すると、総称ルーティング カプセル化トンネル、IPsec 暗号化、および NHRP を組み合せることにより、目的に合せて大小さまざまな規模の IPsec バーチャル プライベート ネットワークを構築できます。DMVPN for IPv6 では、パブリック ネットワーク（インターネット）は純粋な IPv4 ネットワークであり、プライベート ネットワーク（イントラネット）は IPv6 に対応しています。
IPV6 を介した mGRE	15.2(1)T	この機能については、次の項に説明があります。 • 「IPv6 を介した mGRE サポート」（P.5）
DMVPN 用の IPv6 トランスポート	15.2(1)T	DMVPN 用の IPv6 トランスポート機能は、IPv6 WAN 側の機能を NHRP トンネルと基礎となる IPsec 暗号化に構築して、IPv6 がインターネットでペイロードを転送できるようにします。 DMVPN 用の IPv6 トランスポート機能はデフォルトでイネーブルにされます。